# COMPUTATIONAL METHODS FOR VIDEO BLOCKCHAIN IN INTELLIGENT SURVEILLANCE

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY

IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

2024

By

Kasun Moolikagedara

School of Engineering, Computer and Mathematical Sciences

# Abstract

This PhD thesis explores how blockchain can enhance intelligent surveillance by improving security and data integrity. It addresses issues such as video tampering, privacy breaches, and security threats in smart cities. The study details how recorded videos are broken into frames and stored within a private blockchain to ensure the immutability of records, boosting trust and security through cryptographic methods. A new concept called Video Blockchain has been introduced to organize surveillance data better. The research demonstrates that video integrity is preserved using the blockchain's tamper-proof features and SHA-256 cryptographic hash functions, while the Merkle tree structure tracks any changes in video frames. This thesis highlights how blockchain has evolved from a cryptocurrency tool into a solution for securing video data in smart cities. It emphasizes blockchain's impact on data safety, particularly in intelligent transportation and surveillance. The private blockchain model used here stores video frames within the blockchain, ensuring secure data transmission across widely dispersed surveillance cameras. More importantly, blockchain ensures the authenticity of surveillance recordings, with potential future applications in artificial intelligence and machine learning. The contributions of this PhD thesis include:

- Evaluating Cryptographic Function Performance for Blockchain Implementations.
- Implementing Video Blockchain Computation Method for Intelligent Surveillance.
- Established a decentralized surveillance system with Video Blockchain.
- Addressing Privacy Preservation Issues in Blockchain Implementations
- Implementing IoT Video Network Privacy-Secure Mechanisms with Video Blockchain.
- Detecting AI-Generated Video Misinformation Using Video Blockchain.

Overall, this research is truly significant regarding improved security for surveillance systems, data integrity, and reliability in intelligent surveillance video footage.

**Keywords:** Video Blockchain, Intelligent Surveillance, AI-Generated Video, Authentication, Cryptography.

# Table of Contents

# List of Tables

# List of Figures

# Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: Date: 20 June 2024

# List of Publications During PhD Study

Moolikagedara, K., Nguyen, M., Yan, W., Li, X. (2024) Advancing video data privacy preservation in IoT networks through Video Blockchain. *Information*.

Moolikagedara, K., Nguyen, M., Yan, W. (2023) Video Blockchain: A decentralised approach for secure and sustainable networks with distributed video footages from vehicle-mounted cameras in smart cities. *Electronics*.

Moolikagedara, K., Nguyen, M., Yan, W. (2023) Enhancing privacy protection in intelligent surveillance: Video Blockchain solutions. *BLOCKCHAIN'23*.

Moolikagedara, K., Nguyen, M., Yan, W. (2022) Visual blockchain for intelligent surveillance in a smart city. *Blockchain Technologies for Sustainable Development in Smart Citie*s, Book Chapter, IGI Global.

# Acknowledgment

I express my sincere appreciation to my supervisor Wei Qi Yan. Dr Yan's expertise, meticulous guidance, and unwavering support have been pivotal in the successful completion of this study. His contributions have not only enriched my professional knowledge but have also profoundly shaped my learning experience. His dedication and insightful instructions have been a source of inspiration and motivation, and I am immensely thankful for his guidance throughout this journey.

My sincere thanks also go to my supervisors Minh Nguyen and Xuejun Li, their invaluable advice and support have significantly contributed to my research and academic development. I am profoundly grateful to the school administrators of AUT for their guidance and backing support, which have been vital in navigating my academic endeavours.

The journey of completing this thesis has been an enriching and enlightening experience, made possible by the collective support and guidance of these remarkable individuals. I am forever indebted to them for their contributions to my academic journey.

Kasun Moolikagedara
Auckland, New Zealand
June 2024

# Chapter 1 - Introduction

*The evolution of modern society has impacted every dimension of human life, motivating people to acknowledge the essential role that advanced technologies play in creating a convenient day-to-day lifestyle. However, considering both the negative and positive aspects is crucial when dealing with these complex modern technologies. When it comes to addressing problems in modern technological applications, blockchain-based implementations play a major role due to their resistance to many types of attacks. Because of this, blockchain-based solutions are in high demand in research fields and provide sustainable solutions for sophisticated implementations.*

## 1.1 Background and Motivation

In the domain of technologically advanced smart cities, infrastructures are paramount importance of security is inevitably intertwined with the handling of sensitive data and its secure storage. Since its inception in 2009, blockchain has been increasingly utilised across various large-scale industries, encompassing global trade, insurance, finance, distributed energy, and healthcare sectors (Nakamoto, 2009). This innovative technology has profoundly revolutionised the way data integrity is maintained in intelligent transportation systems, governance, identity management, and food supply chains, as elucidated by (Singhal et al., 2018).

Blockchain's emergence as a state-of-the-art technology is further exemplified by the advent of Bitcoin (Duong et al., 2018; Taylor et al., 2020) a leading cryptocurrency that is inherently secure and challenges the establishment of counterfeit transactions. Operational since 2009, Bitcoin's influence extends beyond mere financial transactions, permeating into other technologically advanced domains, notably intelligent surveillance (Taylor et al., 2020). A key feature of blockchain is its design that eliminates the need for third-party intermediaries in transactions, thereby facilitating direct and transparent processes. This characteristic not only simplifies transactions but also addresses critical issues of data integrity, particularly in validating medical records and monitoring utility systems within smart city frameworks.

In the contemporary context of urban development, the notion of smart cities has seen increasing recognition as a response to the increasing complexities of urbanisation and the potential offered by connected intelligent technologies. This concept, as outlined by (Pramod & Sankaran, 2019) , is being adopted by various cities globally. A fundamental objective underpinning the 'smart city' initiative is the enhancement of public safety and security, with a specific focus on diminishing crime and accident rates, thereby safeguarding the well-being of citizens (Khan et al., 2020a). Concurrently, the field of surveillance systems has evolved into a significant research focus within modern society, reflecting the growing need to integrate advanced technologies for maintaining urban security and safety.

In addressing the emergent challenges of urban security, video surveillance has been identified as a pivotal technology (Gipp, Kosti, & Breitinger, 2016). The primary mission in deploying these surveillance systems is the selection of an appropriate cryptographic algorithm. This selection is crucial for creating a secure blockchain infrastructure that ensures data communication remains unaltered and resistant to various forms of cyber-attacks (Tian et al., 2021). Advanced video surveillance systems play a significant role in mitigating crimes, detecting anomalous activities, and upholding privacy standards. The integrity and reliability of recorded video footage thus become central to a multitude of applications, particularly in scenarios where evidentiary material is required. However, this raises pressing concerns regarding data security, as skilled hackers and malicious entities possess the capability to manipulate video repositories and camera feeds, potentially skewing evidence and rendering the surveillance ineffective in legal contexts (Khan et al., 2020).Therefore, ensuring the fidelity of data stored within intelligent surveillance systems is not only a technical challenge but also a requisite for maintaining public trust and safety.

In the evolving domain of data security, the contribution of blockchain has gained significant prominence, particularly for its effectiveness in securing stored data. This growing recognition can be attributed to its decentralised architecture, which is instrumental in ensuring data authenticity and upholding its integrity (Fattahi et al., 2020). Central to this robust security infrastructure is the strategic use of hashing. As a foundational mechanism, hashing reliably builds and strengthens trust within each block of the chain. It guarantees that each block is securely interconnected with its predecessor, forming a chain that is resistant to tampering. This characteristic of blockchain not only reinforces the security of data but also enhances the system's resilience, instilling a sense of reliability and confidence against potential security infringements.

An integral component of blockchain's security framework is the cryptographic hash function, an algorithm designed to transform arbitrary data into a fixed-size string. Essential to ensuring the efficacy of these functions are the security conditions of one-witness uniqueness and collision resistance, confirming that no two distinct data items produce matching hash values. To uphold a minimum-security standard of 80 bits, the output length of hash functions is typically set at a minimum of 160 bits. Within the blockchain domain, SHA256 stands out as a prominent algorithm, belonging to the family of Secure Hash Algorithms (SHA). This hash function plays a pivotal role in various blockchain operations, including proof-of-work (PoW), block generation within the

Merkle-tree concept, address generation, signature authentication, pseudorandom number creation, and fundamental features of bridge mechanisms like the Fiat-Shamir approach (FSM), among others.

In the evolving landscape of digital technology, blockchain emerges as a paradigm shift extending beyond its original application in cryptocurrency. Current research trends in intelligent surveillance have begun to harness blockchain's decentralised nature in several innovative ways. In smart city environments, vehicle accidents are increasingly being captured through dashboard cameras, a method advocated (Gipp, Kosti, and Breitinger, 2016). This approach marks a significant step in utilising blockchain for real-time incident documentation.

Blockchain integration with IoT devices facilitates the secure collection and storage of critical data, such as air and water quality monitoring and food delivery tracking. This fundamental operation, proposed by Mobility as a Service (MaaS) (Anwer, Saad & Ashfaque, 2020), underscores blockchain's versatility in various data management applications. To authenticate recorded videos, blockchain employs unique features like time-stamping to ensure the distribution of unaltered data to a shared repository. This method enhances accessibility and reliability compared to traditional closed-circuit television (CCTV) systems (Anwer, Saad, & Ashfaque, 2020).

Blockchain-based systems guarantee the integrity of recorded information, maintaining its originality and preventing unauthorised alterations. This technology offers a robust alternative to centralised systems, efficiently handling computation requirements and securing data transfers between nodes. It overcomes geographical barriers inherent in traditional ledger technologies (Nguyen et al., 2020).

In the realm of surveillance systems, securing and linking the operations of geographically dispersed cameras presents substantial challenges (Kalbo et al., 2020). Traditional mechanisms addressing these challenges often result in complex and cost-intensive solutions. Blockchain technology, with its decentralised nature, provides a unified solution to these security concerns, eliminating the need for centralised control and facilitating the expansion of secure connections within the network.

This thesis aims to harness the decentralised, cryptographic, and unalterable characteristics of blockchain to bolster the security and integrity of the intelligent surveillance systems. The endeavour involves developing new computational methods for visual blockchain, integrating selected cryptographic algorithms, and creating a visual blockchain system. This two-fold task focuses on ensuring the reliability and security of the surveillance system, while maintaining the performance and efficacy of blockchain technology for deployment. Our contribution to this field lies in creating a visual blockchain that seamlessly integrates with cryptographic algorithms, forging a path in the realm of intelligent surveillance.

## 1.2 Problem Definition

In the contemporary technological landscape, blockchain stands as a formidable innovation, revolutionising secure operations in distributed networks across domains including decentralised applications, finance, logistics, and operations, transcending geographical boundaries. The core objective of visual blockchain within this context is to harness computational methods for delivering precise and intelligent surveillance data in smart city environments. A critical challenge encountered in intelligent surveillance, particularly with location-based visualisations derived from multiple city cameras, is the inadequacy the inadequacy of tamper resistance in the gathered data. This project proposes a solution through the integration of blockchain technology into surveillance systems to secure video frames. It involves judiciously selecting cryptographic algorithms to construct a sustainable and effective visual blockchain model. This approach aims to enhance the reliability of current systems by infusing them with blockchain's inherent decentralised nature. A key contribution of this research is the development of an enhanced blockchain security framework, achieved by employing optimal cryptographic algorithms tailored to specific requirements. Furthermore, the project endeavours to bridge existing gaps in intelligent surveillance by building a web-based blockchain prototype. This prototype is envisioned to seamlessly integrate visual blockchain components, thereby establishing a more secure, efficient, and comprehensive surveillance system in the realm of smart cities.

## 1.3 Research Questions

In this section, we articulate the core inquests that guide our investigative journey. Based on the literature review in Chapter 2, and the hypotheses derived from these research questions, we establish the bedrock upon which our research is built acting as a compass that directs our methodological choices and analytical focus. They are crafted to address the multifaceted aspects of implementing secure computational methods in intelligent surveillance within smart city ecosystems. Through these questions, we aim to dissect the intricacies of cryptographic algorithms, explore the implementation of secure video frame capture, and devise robust security measures to protect surveillance data. The clear articulation of these questions ensures a targeted and methodical approach to our research endeavours.

**Key Question: How to implement featuring data securing computation method for intelligent surveillance in a smart city?**

**RQ 1: What are the issues related exiting related to blockchain implementation for Intelligent Surveillance.**

a) How does issue propagation in these implementations?

b) What is the best way to select efficient and effective cryptographic algorithms?

c) Are they compatible to enhancing the data transfer between intelligent surveillance nodes?

This question effectively addresses the challenges and opportunities in applying blockchain to visual data in smart city surveillance. It's important to explore issues in existing implementations (RQ 1a), the selection of effective cryptographic algorithms (RQ 1b), and their compatibility with intelligent surveillance networks (RQ 1c).

**RQ 2: How to implement Video Blockchain computation method?**

a) How to implement a computation method for intelligent surveillance?

b) How to capture video frames secure mechanism to achieve the integrity of data?

The focus on implementing a computation method (RQ 2a) and developing a secure mechanism for capturing video frames (RQ 2b) is crucial. This will contribute to the integrity and security of the data within the surveillance system.

**RQ 3: How to achieve the required security measurement for implementation by resulting in considerable data protection to surveillance data with efficient and effective way?**

a) How to achieve the required security measurement for implementation?

b) Are resulting in considerable data protection to surveillance data with efficient and effective way?

Investigating how to establish effective security measures (RQ 3a) and ensuring considerable data protection in a practical way (RQ 3b) is fundamental. This aligns with the need for robust security in intelligent surveillance systems.

The first research question examines the challenges and possibilities of applying blockchain to visual data in smart city surveillance. It involves experimenting with various cryptographic algorithms to identify the most suitable ones for visual blockchain. The second question seeks to integrate the selected blockchain method practically to meet cryptographic requirements, ensuring data immutability, integrity, and availability. The third question's focus will evolve during the project, intending to establish a security measurement for data protection. Addressing these questions sequentially will culminate in a comprehensive solution to the overarching question, enhancing the security framework of visual blockchain in intelligent surveillance systems.

### 1.3.1 Hypotheses

Based on research questions, identified gaps, the proposed research directions are six hypotheses that align with research objectives:

**Hypothesis 1 (Efficient Cryptographic Algorithms):**

- Statement: Integrating advanced cryptographic algorithms into intelligent surveillance systems significantly improves the efficiency and effectiveness of data transfer between surveillance nodes in a smart city.

- Rationale: This hypothesis addresses the gap in current cryptographic paradigms and aims to test whether the selection of more sophisticated cryptographic algorithms can enhance the overall data transfer process in intelligent surveillance systems.

This hypothesis aptly addresses the need for advanced cryptographic algorithms in intelligent surveillance systems. It's focused on enhancing data transfer efficiency between surveillance nodes, which is a critical aspect of smart city surveillance

**Hypothesis 2 (Enhanced Cryptographic Functions):**

- Statement: Enhanced cryptographic functions, specifically designed for intelligent surveillance systems, will significantly mitigate vulnerabilities in current cryptographic paradigms.
- Rationale: Targeting the development of enhanced cryptographic functions, this hypothesis aims to address the identified gap in current cryptographic methods used in surveillance systems.

Targeting the development of enhanced cryptographic functions is essential to mitigate vulnerabilities in current systems. This hypothesis is important for advancing the security capabilities of intelligent surveillance systems.

**Hypothesis 3 (Data Integrity in Video Frame Capturing):**

- Statement: Implementing a computation method that focuses on capturing video frames securely will substantially increase the integrity and reliability of the data acquired by intelligent surveillance systems.
- Rationale: This hypothesis relates to the challenge of ensuring sequential integrity and confidentiality in data handling, particularly in the context of video frame capturing and storage.

Focusing on the integrity and reliability of data in video frame capturing is crucial. This hypothesis is directly related to ensuring the quality and trustworthiness of surveillance data.

**Hypothesis 4 (Effective Data Protection):**

- Statement: A well-designed, security-focused computational method will result in considerably improved protection of surveillance data, achieving a high level of security without compromising efficiency.
- Rationale: This hypothesis tests the balance between effective data protection and operational efficiency in intelligent surveillance systems.

Testing the balance between data protection and operational efficiency is vital. This hypothesis is key to ensuring that security measures do not impede the functionality of surveillance systems.

**Hypothesis 5 (Video Blockchain for Data Privacy protection):**

- Statement: The integration of blockchain technology in intelligent surveillance systems will lead to a notable enhancement in data privacy protection.
- Rationale: This hypothesis aims to test the potential of blockchain technology in improving data privacy protection, addressing the gap in existing blockchain applications within the domain of intelligent surveillance.

Investigating blockchain's contribution to strengthening data privacy in surveillance systems is a forward-thinking approach. This hypothesis is significant for exploring innovative applications of blockchain technology in this domain.

**Hypothesis 6 (Interdisciplinary Cryptographic Solutions):**

- Statement: Interdisciplinary approaches in cryptographic solutions, combining insights from computer science, data security, and urban planning, will result in more robust and versatile security mechanisms for intelligent surveillance in smart cities.
- Rationale: This hypothesis explores the effectiveness of interdisciplinary cryptographic solutions, aiming to bridge the current gap in the limited integration of blockchain and other cryptographic methods across various domains.

Proposing an interdisciplinary approach to cryptographic solutions is a comprehensive strategy. This hypothesis recognises the importance of integrating knowledge from multiple fields to develop robust security mechanisms.

These hypotheses collectively aim to address the key research questions and gaps identified our research, focusing on enhancing data security, integrity, and efficiency in intelligent surveillance systems within smart cities.

## 1.4 Research Methodology

We undertake a critical exploration of the computational methods used in Video Blockchain, focusing particularly on their application within smart city surveillance systems. This exploration is underpinned by an extensive review of the available research, which has unveiled a plethora of challenges inherent in current surveillance frameworks. These challenges span across various dimensions, including data integrity, privacy concerns, and the pressing need for robust cryptographic methodologies in the surveillance of smart cities. The elucidation of these challenges has precipitated the adoption of an innovative approach that not only bolsters security measures but also enhances the functional efficacy of surveillance systems.

As we advance into this research, we bridge the theoretical foundations laid out in the preceding literature review with the practical implementation of Video Blockchain solutions designed to address the identified gaps. The core of this chapter lies in distilling the challenges observed in current intelligent surveillance implementations and outlining the proposed methodologies to tackle them. This process is instrumental in formulating our research questions and hypotheses, which are deeply rooted in the findings presented in the previous chapter.

Our methodological framework is guided by the principles of Design Science Research Methodology (DSRM) specifically tailored to meet the unique demands of this study. DSRM comprehensive nature, which adeptly amalgamates theoretical constructs with practical innovation, makes it a fitting choice for our interdisciplinary research. The organisation of this chapter delineates our methodological journey, detailing how each step of the DSRM is seamlessly integrated into our research process. This approach underscores our commitment to a methodological rigor that is both academically sound and pragmatically relevant, aiming to contribute meaningful and actionable insights to the field of Video Blockchain in intelligent surveillance.

The DSRM framework enables a systematic navigation through the complexities involved in developing and implementing a robust Video Blockchain system. It commences with the stage of

problem identification, where we dissect the intricacies and challenges prevalent in the current landscape of Video Blockchain and intelligent surveillance. This stage is not limited to the mere identification of problems but extends to the formulation of clear, actionable objectives that are intimately connected to the gaps and needs unearthed during our extensive literature review.

One of the key strengths of our methodology is its inherent iterative nature – a process characterised by continual refinement and improvement. This iterative cycle is particularly critical for our study, as it involves the meticulous selection and alignment of the most suitable cryptographic algorithms. Our aim transcends the mere identification of theoretically sound algorithms; we endeavour to ensure their practical applicability and congruence with the specific requirements of Video Blockchain within the context of surveillance systems.

Furthermore, the DSRM framework emphasises the significance of an empirical approach. This approach is essential for our study, as it necessitates that our hypotheses and theoretical concepts are not only rigorously tested but are also contextualised within real-world scenarios. It is this empirical grounding that ensures our proposed Video Blockchain system transcends the realm of conceptual models to emerge as a viable, functional, and efficient solution, applicable to real-world intelligent surveillance scenarios.

## 1.5 Objectives of This Research

Firstly, in our research, we aim to gather more information about the research problem and to identify the research questions. Based on these research questions, we employ sophisticated methods to address them.

During the process of implementing new methods, the Video Blockchain computational method was launched to address problems related to intelligent video surveillance in smart cities. Moreover, this method was tested using interdisciplinary approaches to evaluate its capabilities.

Throughout this research project, we utilized the Research Methodology for Design Science, supported by Formal Methods. These methods were chosen to ensure our research process meets all necessary requirements to deliver an effective solution. Finally, this PhD thesis contributes by introducing the Video Blockchain method and two interdisciplinary methods to address the challenges associated with Video Blockchain implementation.

## 1.6 Structure of This Thesis

This thesis provides a detailed analysis of blockchain technology in relation to intelligent surveillance, structured into distinct chapters that systematically build upon each other.

In Chapter 1, we set the foundation with an introduction, problem definition, methodology, and the research contributions, including publications. It also outlines the overall structure of the thesis. Chapter 2 presents a detailed analysis of the literature, providing an overview of Video Blockchain in intelligent surveillance and its security and privacy implications. This chapter includes a thorough methodology of the literature review, an in-depth analysis of blockchain technology, and a comparative discussion on cryptographic schemes, culminating in identifying research gaps and future directions.

Chapter 3 presents the research methodology, outlining various methods employed in the study, such as PRISMA for reviewing current research and enhancing cryptographic functions. This chapter also discusses the integration and security aspects of Video Blockchain.

In Chapter 4, we detail the findings and experimental outcomes, focusing on the effectiveness of cryptographic functions and the validation of the Video Blockchain computational method. It also evaluates the compatibility of Video Blockchain with interdisciplinary implementations.

Chapter 5 engages in a discussion, drawing conclusions from the hypotheses, addressing limitations and challenges, and providing suggestions for future research. To conclude, Chapter 6 finalises the thesis, summarising the main conclusions and contributions to the research field, followed by a comprehensive list of references. This structure not only facilitates a coherent flow of information but also ensures a thorough examination of the subject matter from theoretical, practical, and future perspectives.

# Chapter 2 - Literature review

*The literature examined highlights the development and implementation of these computational method. It examines existing challenges in the sphere of intelligent surveillance technology for smart cities and how the visual blockchain technology Research and Development and of computational methodology can provide reliable solutions. The review also encompasses an in-depth analysis of various cryptographic algorithms, assessing their suitability for different tasks within the Video Blockchain framework. By doing so, the research aims to strengthen the security of the blockchain, thus guaranteeing the integrity and reliability of the surveillance data.*

*Overall, this chapter lays the foundation for understanding the present state of research in the field, pinpointing gaps, and setting the stage for further exploration and development of enhanced surveillance methods in smart city environments.*

## 2.1 Introduction

In this chapter, we conduct a systematic literature review aimed at meticulously dissecting and analysing existing research in the realm of Video Blockchain and its application in intelligent surveillance. This introductory section sets the stage for a comprehensive examination of the current state of knowledge, bridging the gap between blockchain technology and intelligent video surveillance. It critically assesses the evolution of blockchain from its financial origins to its transformative role in enhancing video data integrity and security. The review delves into various computational methodologies, exploring how they have been adapted and integrated into surveillance systems to address contemporary security challenges. This section not only contextualises the study within the broader field but also highlights the innovative potential of blockchain technology in reshaping intelligent surveillance paradigms.

This chapter is organised as follows, Section 2.1.1 provides an overview of Video Blockchain, detailing its significance in the implementation of security and privacy measures. Section 2.1.2 further expands on these concepts. The methodology of the literature review is then discussed in Section 2.2, with a specific focus on the Literature Search Process in Section 2.2.1. Section 2.3 explores into the foundational aspects of blockchain technology. Subsequently, Section 2.4 offers an in-depth exploration of the state-of-the-art concepts and technologies in Video Blockchain. Section 2.5 presents a comprehensive analysis, including a comparative study and discussion on cryptographic functions and their role in addressing various challenges.

The identified research gaps and potential future directions are outlined in Section 2.6. Section 2.7 highlights the contributions of this thesis. Finally, Section 2.8 concludes the chapter by summarising the key findings of the literature review in Chapter 2.

### 2.1.1 Overview of Video Blockchain in Intelligent Surveillance

Within the landscape of smart cities, the integration of blockchain technology with video surveillance termed 'Video Blockchain' represents a groundbreaking advancement (Moolikagedara et al., 2023). This innovative approach combines the meticulous capture of video frames from surveillance systems with the application of sophisticated cryptographic algorithms. The core objective of this integration is to substantially improve the security and integrity of video data

within intelligent surveillance networks. By leveraging a Video Blockchain framework, this technology ensures that surveillance footage is not only stored securely but also retrieved in a manner that is resilient to tampering and unauthorised access.

The application of Video Blockchain in intelligent surveillance is transformative. It enhances the ability to maintain an immutable record of video data, thus providing a reliable and verifiable chain of evidence that is critical in various applications, including law enforcement and urban management. The use of blockchain technology in this context is not merely an addition to existing systems. It is a fundamental reimagining of how video data can be secured, processed, and utilised in smart city environments.

**Comparison with Existing Industry-Level Blockchain Solutions**

**Traditional Blockchain Solutions**: Most blockchain implementations, such as those used in cryptocurrency (Bitcoin, Ethereum), are focused on financial transactions. These systems emphasize decentralization, transparency, and immutability. However, their resource demands are significant, especially in terms of storage and processing power. The consensus mechanisms, like Proof of Work (PoW), require substantial computational resources, which may not be feasible for industries using resource-constrained devices like surveillance cameras or edge computing systems.

**Permissioned Blockchains**: Solutions such as Hyperledger Fabric and Quorum are designed for more controlled environments, where participants are known and permissioned. While these solutions are more resource-efficient than public blockchains, they are often over-engineered for video data applications. The complexity of managing permissions and maintaining consensus among multiple stakeholders in real-time video processing applications can introduce unnecessary overhead.

**Distributed Ledger Technology (DLT) Alternatives**: DLT-based solutions like IOTA (cryptocurrency) and Hedera Hashgraph (Alternative to Blockchains) are also gaining popularity due to their focus on lightweight, scalable systems suitable for IoT applications. These technologies aim to provide low-latency and high-throughput environments but often lack the specialized cryptographic features needed for ensuring video data integrity and authentication.

## 2.1.2 Requirement to Security and Privacy in Video Blockchain

The objectives of integrating blockchain technology into video surveillance systems are twofold and deeply rooted in the principles of security and privacy. Firstly, the implementation of advanced cryptographic functions is central to this endeavour. These functions serve as the backbone of security, ensuring that each video frame, once entered into the blockchain, remains unaltered and traceable, thereby providing a tamper-proof ledger of surveillance data.

In judicial proceedings, surveillance footage plays a crucial role. Blockchain technology can authenticate the metadata, preserving the integrity of unaltered videos and safeguarding individual privacy. This method, as presented by Aditya Dhiran et al., (2020), leverages blockchain's capabilities to detect video fraudulence effectively. By decentralising the process, it enhances data transparency, security, and privacy. Blockchain technology ensures the integrity and authenticity of video content by employing cryptographic algorithms to generate unique hashes for each video.

Furthermore, the incorporation of cryptographic data structures is aimed at establishing a comprehensive security mechanism within the blockchain's transparent ledger. This approach is crucial for protecting user identity and data security in blockchain applications. The use of ring signature technology, as proposed by (X. Li, Mei, et al., 2020) further strengthens the system against risks of malicious attacks, data tampering, and privacy violations. In an era increasingly prone to data breaches, this level of security is indispensable.

Furthermore, the research work (Fitwi et al., 2019) has the significance of their method of security video surveillance systems that implement by connecting blockchain technology and Internet of Things (IoT). This method forms the bedrock for ensuring the blockchain base privacy protection for data transferring in the surveillance system. Traditional video surveillance systems often fall short in terms of secure data transfer capabilities. In other hand, the proposed Video Blockchain approach is meticulously designed to overcome these deficiencies. It ensures not only the correct sorting and storage of videos but also enhances the overall reliability and effectiveness of surveillance operations, particularly in scenarios involving crime and public safety.

In brief, the fusion of blockchain technology with intelligent video surveillance systems heralds a paradigm shift in the treatment of security and privacy within the framework of smart city

initiatives. This novel approach potentials to uphold in a new era of surveillance operations characterised by enhanced security, data integrity, and trust.

## 2.2 Methodology of Literature Review

In this section, we outline the systematic approach employed in the compilation and analysis of pertinent literature central to computational methods in Video Blockchain for intelligent surveillance. The preferred reporting items for systematic reviews and meta-analyses (PRISMA) was developed (Moher et al., 2009), the goal was to create this comparative set of guidelines to improve the reporting of systematic reviews and meta-analyses. This method leads to a clear and transparent account of what was conducted and what was found. The recent works (Chlomoudis et al., 2022), employed the PRISMA method for systematic literature review.

This method PRISMA is anchored in a structured review process, encompassing a wide array of academic databases and journals to ensure a comprehensive understanding of the subject. By following this PRISMA guiding principles, (Mousa et al., 2015) use to conducted a survey regarding Trust management and reputation systems, it entails a rigorous selection criterion, focusing on peer-reviewed articles, seminal papers, and recent advancements in the field. The studies able to decompose the data and research problems with critical gaps to address withing the scope of current research objective the methodology employs systematic evaluation and synthesis techniques (Nisrine, n.d.). This approach enables the identification and analysis of key themes and trends within the literature. The meticulous nature of PRISMA ensures that each selected study is evaluated for its relevance, methodological rigor, and contribution to the field. This process facilitates a thorough understanding of the research landscape, highlighting areas where further investigation is needed. The ultimate goal is to provide a robust, evidence-based foundation that informs and guides the current research, aligning with its objectives and filling identified gaps in the knowledge base. This section also details the criteria for inclusion and exclusion of literature, ensuring the relevance and quality of sources. The approach adopted facilitates an unbiased, thorough exploration of existing research, providing a solid foundation for the study's theoretical framework and subsequent analysis.

The literature search process in this thesis adopts a methodical approach to aggregate and analyse relevant studies, reports, and scholarly articles, forming the foundational research for this

thesis. This section details a carefully strategized approach to source literature pertinent to the integration of blockchain technology within intelligent surveillance systems, particularly in the context of smart cities. To conduct a systematic literature review, the following refined questions were considered:

- **Necessity of Video Blockchain in Intelligent Surveillance:** Why is the implementation of Video Blockchain essential for enhancing intelligent surveillance systems in smart cities?
- **Challenges in Current Intelligent Surveillance:** What are the prevalent issues and challenges associated with current implementations of intelligent surveillance systems?
- **Blockchain Solutions for Surveillance**: How can Video Blockchain technology provide solutions to overcome these challenges in surveillance systems?
- **Research on Video Blockchain Solutions**: Do the reviewed papers present practical Video Blockchain solutions or merely propose theoretical concepts?

The PRISMA method is used for these questions aim to dissect the role of blockchain in intelligent surveillance, scrutinising both the existing challenges in surveillance systems and the potential solutions offered by Video Blockchain technology. By focusing on these aspects, the literature review endeavours to provide a comprehensive understanding of the current state of blockchain technology in intelligent surveillance and its future trajectory. This approach ensures a thorough exploration of the subject, contributing to the depth and breadth of the research.

#### 2.2.1.1 *Search Strategy and Sources*

The process utilised the PRISMA systematic review method to explore various academic databases and search engines. This approach was in relation to the refined questions mentioned in section **Error! Reference source not found.** on page 22, each chosen for its specific strengths in covering technological and cryptographic research.

This literature review process involved 878 papers, including web references. The primary databases included Springer, IEEE Xplore, ACM and Elsevier known for its extensive collection of technical and engineering literature, ScienceDirect, offering a wide range of scientific and technological research articles, and Google Scholar, which provides a broad and inclusive search of scholarly literature across various disciplines. The keywords such as "**intelligent surveillance**,"

"**Video Blockchain**," "**cryptographic algorithms**," and "**smart city data security"** were strategically selected to encapsulate the core themes of the research. These keywords were combined with advanced search strings, such as "**blockchain in intelligent surveillance systems**" and "**security algorithms in smart city frameworks**," to refine and focus the search results.

Furthermore, as per the systematic reviews (Moher et al., 2009), the search strategy was not limited to direct queries. It was augmented by a methodical review of references cited in key papers. This snowballing technique allowed for the discovery of inspiring works and important research studies that may not have appeared in direct database searches. For instance, pivotal papers on blockchain applications in smart cities or groundbreaking research on cryptographic algorithms in surveillance systems were likely to cite earlier foundational studies or contemporary research that might have been otherwise overlooked.

Additionally, attention was paid to the dates of publication to ensure the relevance and timeliness of the information. Given the rapidly evolving nature of blockchain technology and cryptographic methods, emphasis was placed on sourcing the most recent publications, while also recognising the value of inspiring works in providing a foundational understanding of the field.

To complement the academic sources, white papers, technical reports, and industry publications were also reviewed. These sources often provide insights into practical applications and real-world implementations of blockchain and cryptographic techniques in intelligent surveillance, which are crucial to understanding the full scope of current research and development in the field.

The literature search process was iterative, with initial findings leading to adjustments in search strategies and keywords. This flexible approach ensured a thorough and comprehensive coverage of the literature, providing a solid foundation for the research presented in the thesis. The combination of database searches, citation tracking, and the inclusion of both academic and grey literature ensured a holistic view of the current state of research in blockchain technology and its applications in intelligent surveillance within smart cities.

#### 2.2.1.2 *Inclusion and Exclusion Criteria*

Specifically, under 'Inclusion and Exclusion Criteria', a systematic and meticulous approach was employed to ensure the relevance and quality of the selected literature. This process was critical

in constructing a comprehensive and focused review that directly supports the research questions at hand. Inclusion Criteria:

- **Direct Application of Blockchain in Intelligent Surveillance**: Our studies were included if they explored the use of blockchain technology specifically in the realm of intelligent surveillance systems. This included research on blockchain's role in enhancing security, privacy, and data integrity within surveillance networks.
- **Cryptographic Methods in Data Integrity**: Given the importance of data security in intelligent surveillance, papers discussing the use of cryptographic algorithms to ensure data integrity were also included. This encompassed studies on various cryptographic techniques, from traditional methods to advanced cryptographic protocols like SHA-256, Schnorr signatures, and Pedersen commitments.
- **Advancements in Surveillance Technologies within Smart City Frameworks**: Literature focusing on the latest advancements in surveillance technologies, particularly within smart city environments, was included. This criterion was particularly important for understanding how blockchain technology integrates with other smart city technologies to improve surveillance systems.
- **Empirical Studies and Case Analyses**: To gain insights into practical implementations, empirical studies and case analyses detailing real-world applications of blockchain in surveillance were prioritised. These included analyses of pilot projects, implementations in various cities, and evaluations of the technology's efficacy in different scenarios.

Exclusion Criteria:

- **Studies Outside the Scope of Video Blockchain Technology**: Research papers that did not directly focus on the use of blockchain in video surveillance or smart city applications were excluded. This included general blockchain studies without a specific focus on surveillance or smart city contexts.
- **Irrelevant Cryptographic Research:** While cryptographic methods are central to the thesis, studies that discussed cryptographic techniques unrelated to blockchain or surveillance systems were excluded. This helped maintain the focus on how cryptography specifically enhances blockchain applications in surveillance.

- **Outdated or Redundant Studies:** Due to the rapidly evolving nature of blockchain technology, older studies, unless seminal, were excluded to ensure the review's relevance. Redundant studies that did not provide additional insights beyond what was already covered in the selected literature were also excluded.
- **Non-Academic and Non-Peer-Reviewed Sources:** To maintain the academic rigor of the thesis, non-academic sources and articles that were not peer-reviewed were largely excluded, except in cases where they offered significant practical insights into the application of blockchain in surveillance.

This inclusion and exclusion criteria ensured a focused, relevant, and high-quality literature base for the research. It allowed for a thorough exploration of how blockchain technology and cryptographic methods are being developed and implemented in the context of intelligent surveillance, particularly within the context of smart cities.

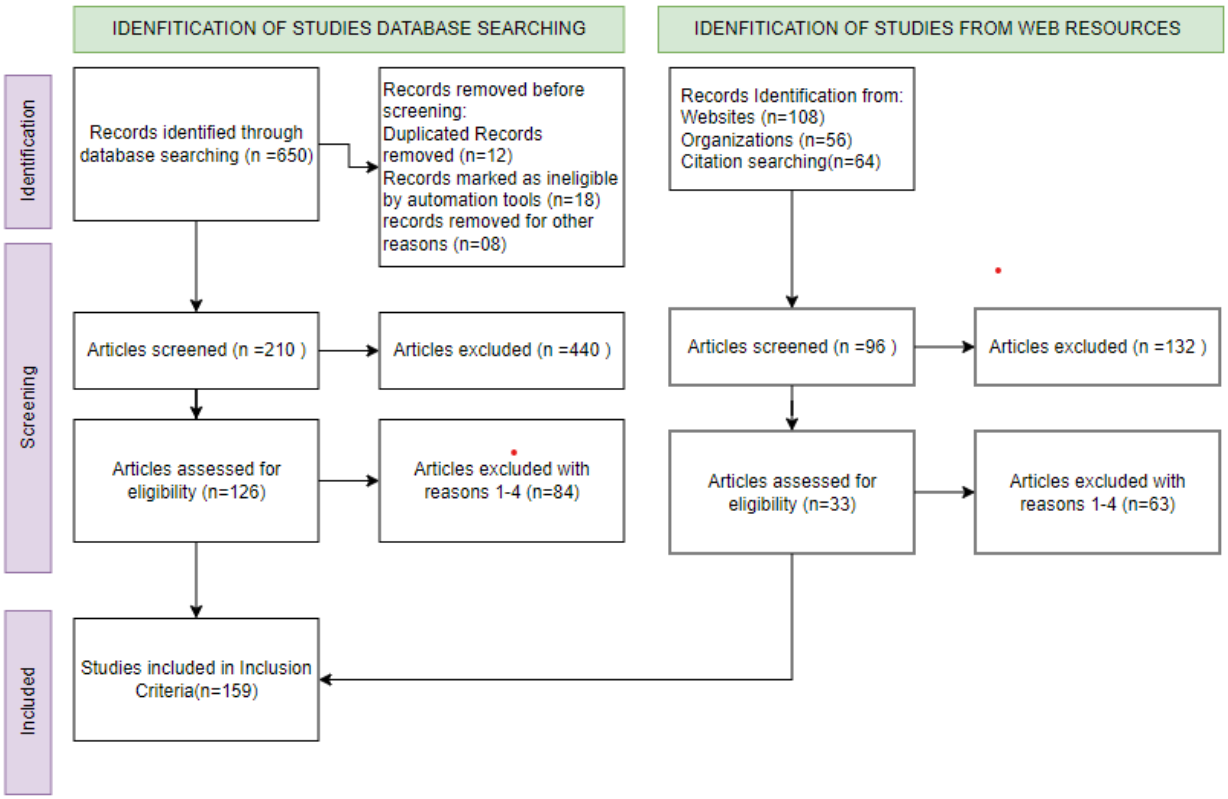


Figure 2.1: PRISMA Literature Identification Chart

In this thesis, a total of 650 papers identification forms the studies database searching were initially involved in the PRISMA literature review process. At the very first stage of this process, 38 records were excluded. In the subsequent screening stage, we adhered to the criteria outlined in Section 2.2.1.2 on page 22, 'Inclusion and Exclusion Criteria.' As a result, 440 records previously chosen were further eliminated. This step included a parallel process of identifying studies from databases and registers, following the same criteria as mentioned above. Of the 228 records involved in this phase, 132 were removed in accordance with Section 2.2.1.2 on page 22.

After completing the PRISMA process, 159 records were ultimately selected for inclusion, based on the criteria specified in Section 2.2.1.2. These records will be utilised for future research work. Figure 2.2 on page 28 presents a detailed breakdown of the sources and percentages of the records selected.

#### 2.2.1.3 *Study Selection and Data Extraction*

In the process of finalising the study inclusion, the recorded selection as mentioned in Figure 2.1 on page 33 was rigorously and structurally approached to ensure the selection of the most relevant and impactful studies. This section is vital for establishing the credibility and depth for our research, particularly in the context of blockchain technology and its applications.

Study Selection Process:

- **Initial Screening:** The first phase of the review process involved an initial screening of titles and abstracts. This step was crucial in quickly identifying studies that were potentially relevant to the research areas of blockchain in intelligent surveillance, cryptographic methods in data integrity, and advancements in surveillance technologies within smart city frameworks. During this phase, studies that clearly did not meet the inclusion criteria or directly addressed the research questions were excluded.
- **Full-Text Review:** The next step was a comprehensive full-text review of the selected studies. This phase involved a detailed examination of each study's content to confirm its relevance and contribution to the research objectives. Studies that met the inclusion criteria and offered significant insights into blockchain applications in intelligent surveillance,

effective cryptographic methods for data security, or innovative surveillance technologies in smart cities were retained.

Data Extraction Process:

- **Key Findings**: Data extraction was systematically conducted, with a focus on extracting key findings from each study. This included insights into the application of blockchain technology in surveillance systems, the effectiveness of different cryptographic methods in ensuring data security, and innovations in smart city surveillance technologies.
- **Methodologies**: The methodologies employed in each study were carefully examined and documented. This included the type of research (Empirical, Theoretical, Case Study), the specific cryptographic algorithms or blockchain technologies used, and the evaluation methods employed to assess their effectiveness.
- **Results and Relevance to Research Hypotheses**: The results of each study were analysed in the context of how they informed the research hypotheses and objectives. This involved assessing the outcomes of different blockchain implementations in surveillance systems, the security and integrity assured by various cryptographic methods, and the practical implications of these technologies in smart city contexts.
- **Comparative Analysis**: As part of the data extraction process, a comparative analysis of the studies was undertaken. This allowed for the identification of common themes, discrepancies, and emerging trends in the research area. It also helped in highlighting gaps in the existing literature and potential areas for future research.

The dual-phase review and meticulous data extraction processes ensured that the studies selected for the thesis were not only relevant but also provided substantial evidence and insights to support the research objectives. This approach laid a solid foundation for a comprehensive understanding of the current state of blockchain technology in intelligent surveillance and its role in enhancing security and efficiency within smart city frameworks.

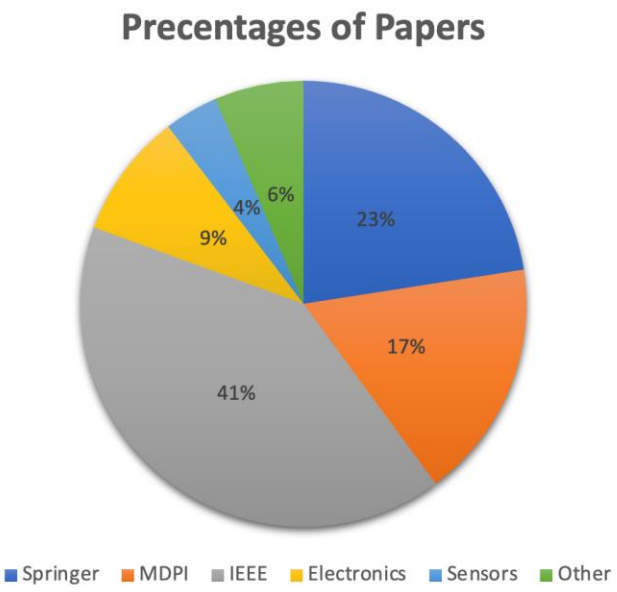


Figure 2.2: The Source and Percentage of Reviewed Papers

Figure 2.2 illustrates the percentages of reviewed papers that will be utilised in our future research work. This research aims to identify and address defined problems by crafting appropriate solutions. To uncover gaps in these studies, we will follow a systematic approach leading to the final outcome. This involves adhering to the methodology outlined in Section 2.2.1.4, 'Synthesis of Findings.'

In this phase, we will categorise the selected studies based on their authors, the technologies or algorithms used, and their functions. This process is essential to gain a clear overview of the gaps identified by other researchers and to understand the current technological advancements in the field.

### 2.2.1.4 *Synthesis of Findings*

The synthesis of findings began with a structured comparative analysis using a narrative synthesis approach. This method was chosen for its suitability in accommodating diverse study designs and data types commonly encountered in blockchain technology research (Saputro et al., 2021; Trung et al., 2021). The process was guided by the framework suggested by (Popay et al., 2006) for narrative synthesis in systematic reviews, allowing for a comprehensive understanding of the interconnections between studies. This process is critical for drawing comprehensive conclusions and identifying gaps in the existing body of knowledge.

- **Comparative Analysis**: The synthesis began with a comparative analysis of the findings from the selected studies. This involved juxtaposing the results, methodologies, and conclusions of different research papers to identify commonalities and variances. For instance, studies focusing on the use of blockchain technology in intelligent surveillance systems were compared to understand the varying approaches and outcomes reported.
- **Thematic Identification:** Through this comparative analysis, prevailing themes and trends within the research were identified. This included themes such as the application of specific blockchain platforms (e.g., Ethereum, Hyperledger) in surveillance, the integration of advanced cryptographic techniques (like SHA-256, Schnorr Signatures, or Pedersen Commitments), and innovative use-cases in smart city frameworks.
- **Convergence of Cryptographic Techniques:** Part of the synthesis involved examining how different cryptographic techniques converged within the blockchain space to enhance intelligent surveillance systems. This included analysing how encryption, hashing algorithms, and digital signatures were being utilised to ensure data integrity and security in blockchain-based surveillance systems.
- **Elucidation of Research Gaps:** The synthesis also focused on highlighting gaps within the current literature. This involved identifying areas where further research is needed, such as the scalability of blockchain solutions in surveillance, the integration of quantum-resistant cryptographic techniques, or the exploration of decentralised identity verification methods in smart cities.
- **Comprehensive Overview:** The synthesis aimed to provide a comprehensive view of the current state of Video Blockchain technology. This included its developmental trajectory, current applications in intelligent surveillance, challenges faced, and potential future directions.

**Integration of Findings:**

- **Cross-Study Insights:** The integration of findings across studies allowed for a deeper understanding of the complex interplay between blockchain technology and intelligent surveillance. It highlighted how different cryptographic methods impacted the efficiency and security of these systems.

- **Technological and Methodological Insights:** The synthesis offered insights into both the technological advancements in blockchain and the methodological approaches used in current research. This included understanding the practical implications of blockchain in real-world surveillance systems and the theoretical underpinnings that guide its application.
- **Current State and Future Directions**: Finally, the synthesis provided a snapshot of the current state of blockchain technology in intelligent surveillance, while also paving the way for future research directions. It identified areas ripe for innovation and exploration, such as the integration of AI with blockchain in surveillance or the development of more user-centric blockchain surveillance systems.

In summary, the synthesis process - Study Selection and Data Extraction on the page subsection was integral in creating a cohesive understanding of the vast and varied research on 27 blockchain in intelligent surveillance. It facilitated a comprehensive understanding of the field, identified prevailing themes and gaps, and provided a clear direction for future research in this dynamic and evolving domain.

Table 2.1: Extracting Synthesis of Findings

| Author(s) | Research title | Date Type | Technology Involved |
|---|---|---|---|
| 01.(Gipp et al., 2016a) | Securing Video Integrity Using Decentralised Trusted Timestamping on the Bitcoin | Video | Blockchain<br>Applications<br>Trusted Timestamping<br>SHA256 |

| | | | |
|---|---|---|---|
| 02.(Michelin et al., 2020) | Leveraging lightweight blockchain to establish data integrity for surveillance cameras | Video | Interplanetary File System (IPFS) Network, Surveillance Cameras Raspberry Pi 3 platform |
| 03.(Deepak et al., 2020) | A data verification system for CCTV surveillance cameras using blockchain technology in smart cities | Video | Hyperledger Fabric Blockchain CCTV |
| 04.(Deepak et al., 2020) | Blockchain-based Management of Video Surveillance Systems: A Survey | Video | Interplanetary File System (IPFS) Network, Hyperledger Fabric Blockchain |
| 05.(Kullig et al., 2020) | Prototype implementation and evaluation of a blockchain component on IoT devices | IoT Data (Internet-of-Things) | Ethereum, Blockchain, LoRaWAN, |
| 06.(Wong et al., 2019) | Prototype of running clinical trials in an untrustworthy environment using blockchain | Patients Data | Blockchain Interactive Voice Response System (IVRS) |
| 07.(George et al., 2019) | Food quality traceability prototype for restaurants using blockchain and food quality data index | Radio Frequency Identification Devices (RFID) data | Blockchain, RFID |
| 08.(Hou et al., 2021) | Design and Prototype Implementation of a | LoRa data | long range (LoRa) Internet-of-Things (IoT) security |

| | | | |
|---|---|---|---|
| | Blockchain-Enabled LoRa System with Edge Computing | | Hyperledger Fabri Blockchain, edge computing |
| 09.(Chen et al., 2020) | BCVehis: A Blockchain-Based Service Prototype of Vehicle History Tracking for Used-Car Trades in China | Vehicle Service Records | smart contract Consensus |
| 10.(Engelhardt, 2017) | Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | Healthcare data | Permissioned blockchain, |
| 11.(L. Liu et al., 2019) | Research on Risk Avoidance and Coordination of Supply Chain Subject Based on Blockchain Technology | Supply Chain Data | Blockchain technology |
| 12.(Kalbo et al., 2020) | The Security of IP-Based Video Surveillance Systems | Video | Video Surveillance, IoT, Network Security |
| 13.(Gallo et al., 2018; Gipp et al., 2016b) | Securing Video Integrity Using Decentralised Trusted Timestamping On The Bitcoin Blockchain | Video | Blockchain Applications, Trusted Timestamping, Video Integrity, Mobile Application |
| 14.(Gallo et al., 2018) | BlockSee: Blockchain for IoT video surveillance in smart cities | Video | Blockchain Distributed Ledger Technology (DLT) |
| 15.(Y. Chen et al., 2017) | An improved P2P File System Scheme based on IPFS and Blockchain | P2P Data | P2P File System, Blockchain, Zigzag Codes |

| | | | |
|---|---|---|---|
| 16.(Hao et al., 2020) | A Novel Visual Analysis Method of Food Safety Risk Traceability Based on Blockchain | Video | Blockchain, Radio Frequency Identification (RFID) |
| 17.(Y. C. Chen et al., 2019) | An Image Authentication Scheme Using Merkle Tree Mechanisms | Image | Image Authentication, Merkle Tree, Hash Function, Interplanetary File System (IPFS |
| 18.(Liu J, Huang C ,2021) | Efficient and Trustworthy Authentication in 5G Networks Based on Blockchain | 5G Network data | 5G, Authentication, Blockchain, |
| 19.(M. Singh & Kim, 2018) | Trust Bit: Reward-based Intelligent Vehicle Commination using Blockchain Paper | Intelligent Vehicles broadcasted data | Blockchain Technology, Intelligent Vehicles, Communication Security |
| 20. (Weir & Yan, 2010) | Resolution Variant Visual Cryptography for Street View of google Maps | Video | Secret Sharing |

In Table 2.1, we extract the essence of the final selected papers that have been used as the foundation for our research buildup. In the next section, we will identify and extract the research gaps and problems from these selected papers for further exploration. In summary, a meticulously crafted approach to identifying, selecting, and synthesising relevant studies in the field of blockchain technology and its application in intelligent surveillance systems within smart cities. The process began with a comprehensive search strategy employing multiple academic databases and search engines, utilising specific keywords and advanced search strings to filter pertinent literature. This was followed by a rigorous two-phase study selection process, involving initial screening of titles and abstracts and a detailed full-text review to ensure the studies' relevance and contribution to the research objectives.

The data extraction phase was methodical, focusing on key findings, methodologies, and results that directly informed the research hypotheses. A comparative analysis was then conducted to integrate these findings, allowing for the identification of prevailing themes, convergence of cryptographic techniques, and elucidation of gaps within the current literature. This approach provided a holistic view of the state of Video Blockchain technology, highlighting its potential in enhancing intelligent surveillance systems.

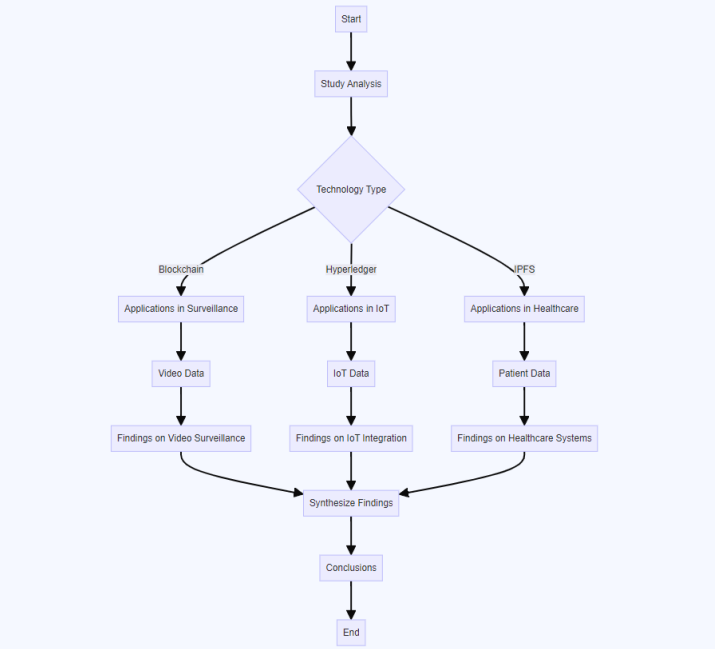


Figure 2.3: Overview of the synthesised findings

Findings, it's given the high-level overview of how different technologies are applied across various data types. The conclusion of this subsection emphasises the depth and breadth of the research conducted. The process ensured a comprehensive understanding of the current advancements, challenges, and future potential of blockchain technology in intelligent surveillance, particularly within the context of smart city frameworks. This thorough literature search process lays a solid foundation for the research, ensuring that the subsequent analysis and findings are well-grounded, relevant, and contribute significantly to the field.

## 2.3 Blockchain: Foundations and Applications

We explore the fundamental aspects of blockchain and its diverse applications (Aste et al., 2017) discovered foreseeable impact on society and industry by using Blockchain, particularly focusing

on its role in intelligent surveillance. Blockchain, a decentralised ledger technology, emerged as a groundbreaking innovation (Yang et al., 2020) in the realm of digital transactions with the advent of cryptocurrencies like Bitcoin. Its foundational principle lies in maintaining a tamper-proof, transparent, and secure record of data transactions across a network of computers. This feature is achieved through a combination of cryptographic principles, consensus algorithms, and data structuring in blocks linked in a chain (Homoliak et al., 2021).

The section further explores the evolution of blockchain beyond its initial financial applications. It has increasingly become an integral component in various fields, including supply chain management, healthcare, and digital identity verification, due to its inherent characteristics of decentralisation, immutability, and transparency (Li et al., 2021). In the realm of intelligent surveillance, blockchain offers a novel approach to address data security and privacy concerns (Li, Jiang, et al., 2020; Yaga et al., 2018). By leveraging blockchain, surveillance systems can ensure the integrity and verifiability of video data, making it resistant to unauthorised tampering and ensuring the authenticity of the surveillance footage (Cybersecurity & States, 2019; Sheth & Dattani, 2019; Zheng et al., 2017).

The application of blockchain in intelligent surveillance is multifaceted (Engelhardt, 2017). It ranges from securing the data transmission across networks to enhancing the trustworthiness of the stored surveillance data. The decentralised nature of blockchain eliminates the single point of failure (Li et al., 2020), enhancing the resilience of surveillance systems against cyber-attacks(Mosakheil, 2018). Furthermore, smart contracts, an extension of blockchain, allow for the automation of processes and protocols within digital surveillance, ensuring compliance with predefined rules and regulations.

In summary, this section presents an extensive review of the existing literature on blockchain, elucidating its fundamental concepts and examining its growing applications across various industries, with a keen focus on intelligent surveillance. The review synthesised the findings from a range of sources, offering a comprehensive understanding of how blockchain is being adapted and implemented in the context of intelligent surveillance, and how it contributes to the advancement of computational methods in this field. The exploration of these aspects is crucial in understanding the potential of blockchains in transforming the landscape of intelligent surveillance systems, paving the way for more secure, efficient, and reliable surveillance practices.

## 2.3.1 Blockchain in Intelligent Surveillance

The integral role of blockchain in enhancing intelligent surveillance systems. This subsection explores how blockchain's intrinsic attributes. In Section 2.3, we discussed the overview of the blockchain, such as decentralised data management, immutable record-keeping, and cryptographic security, are leveraged to address the unique challenges in surveillance contexts, especially in smart city environments. In this section, the focus is on understanding how blockchain can transform conventional surveillance mechanisms into more secure, efficient, and reliable systems. It critically examines the current literature on blockchain applications in surveillance, analysing how the technology's potential is harnessed to ensure data integrity and privacy. This subsection also evaluates different blockchain frameworks and algorithms, such as the Schnorr Signature Scheme, in the context of video data encryption and authentication, emphasising their suitability for real-world surveillance applications. The goal is to establish a clear understanding of the intersection between blockchain and intelligent surveillance, setting the foundation for exploring novel computational methods in subsequent sections of the thesis.

#### 2.3.1.1 *Security and Privacy Aspects*

Modern society undergoes continuous transformation in various aspects, fuelled by sophisticated and intricate technologies that play a pivotal role in community development. These advancements significantly enhance the convenience of day-to-day life. However, a comprehensive evaluation of both the positive and negative aspects of modern technology is imperative before widespread implementation.

Security holds a paramount position in this era of technological advancement. In smart cities, where the real world is intricately intertwined with sensitive information, the need for a highly secure repository becomes indispensable. The emergence of blockchain in 2009 marked a significant shift, operating as a distributed network in large-scale industries such as global trade, insurance, banking, distributed energy, healthcare, smart transportation systems, food supplier management, government, and identity (Nakamoto, 2009; Singhal et al., 2018) Proving its adaptability, blockchain has transcended into various high-tech domains, including intelligent surveillance.

Blockchain, originally designed for Bitcoin (Duong et al., 2018) eradicates the need for a third party in transactions, ensuring increased security and transparency. Its implementation since 2009 has extended to critical areas like intelligent surveillance. Blockchain effectively addresses data integrity concerns related to medical record verification, gas and electricity monitoring systems in smart cities.

The concept of a "smart city" serves as a progressive objective for numerous cities globally, responding to the increasing complexity of urban areas and leveraging associated intelligent technologies (Pramod & Sankaran, 2019) .In the context of surveillance systems, especially in the modern community, it is crucial to investigate and ensure safety and security. Smart cities aspire to enhance safety by reducing crime and accident rates (Khan et al., 2020a).Video surveillance, widely applied to address these issues (Gipp et al., 2016b) necessitates the selection of suitable cryptographic algorithms to establish secure blockchain communication, resist tampering while thwart various types of attacks (Tian et al., 2021).

However, challenges arise in the form of potential manipulations by malicious attackers, knowledgeable hackers, or other unauthorised third parties, who can illegitimately tamper with cameras and video repositories. Such attacks compromise the integrity of stored data captured in intelligent surveillance systems. Blockchain proves invaluable in addressing these challenges by providing tamper resistance for saved data. Its decentralised nature is employed for data verification and ensuring data integrity (Fattahi et al., 2020). Notably, hashing emerges as a reliable technique to establish trust between each block in the chain.

Furthermore, a cryptographic hash function, a crucial element in blockchain, operates as an algorithm systematically mapping arbitrary data to a fixed-size string. This process adheres to stringent security requirements, including one-witness and collision-resistance (Raman & Varshney, 2018a). For robust security, the output length of hash functions in blockchains, exemplified by the widely adopted SHA256, must meet a minimum of 160 bits to ensure at least 80-bit security. The versatile role of hash functions in blockchains spans proof-of-work (PoW) (D. Liu & Camp, 2006; van Flymen et al., 2006), address generation, block generation within the Merkle-tree paradigm (Becker, 2008), comprehension in signatures, pseudorandom number generation, and bridge components like the Fiat-Shamir mechanism (FSM) (Fiat & Shamir, 1987).

The decentralised nature of blockchains extends beyond cryptocurrency applications, aligning with the latest trends in intelligent surveillance and blockchain research. Two noteworthy applications are:

a) **Enhanced Video Integrity in Smart Cities**

In smart cities, the collection of surveillance videos plays a pivotal role in augmenting video integrity. A proposed method, documented by (Gřivna & Drápal, 2019), involves transferring visual data through blockchains. This innovative approach ensures the integrity of accident videos recorded from vehicle dashboards. Utilising built-in accelerometers, digital videos undergo cryptographic hashing and are securely stored on distributed blockchains, providing an immutable record of events.

**b) IoT-Enabled Mobility as a Service (MaaS)**

Blockchain facilitates the connection of IoT devices, enabling monitoring of air and water quality, transport services, global goods delivery and tracking, and food distribution services. This approach, termed Mobility as a Service (MaaS), ensures the collection of accurate and timely data. (Anwer et al., 2020) highlight the broader applications of blockchain in establishing a reliable and transparent network for diverse IoT applications.

These applications leverage the unique features of blockchain, including its distributed and tamper-proof characteristics, to safeguard the integrity of recorded videos. Timestamping features within blockchains play a pivotal role, providing a means to verify and transfer unaltered data to a distributed repository. This methodology extends to data captured from closed-circuit television (CCTV) cameras in smart cities, emphasising the need for secure and unalterable surveillance data.

The blockchain-based approaches not only guarantee the preservation of recorded data without alteration but also aids in averting data integrity breaches from original videos. The distributed ledger of the blockchain, enriched with metadata from CCTV systems, offers law enforcement and clients a secure mechanism for accessing surveillance data.

#### 2.3.1.2 *Computational Methods and Algorithms for Blockchain*

When it talking about the computational method and algorithms, the Saving tamper-proofed video data holds immense advantages, serving as critical evidence for criminal investigations and

establishing a trusted source for public scrutiny. In the realm of intelligent surveillance, numerous research endeavours have been undertaken to refine computational methods, recognising their pivotal role in enhancing various aspects of security and criminal investigations. This emphasis on computation methods has become imperative due to its empowering impact in numerous situations, particularly in criminal investigations where the integrity of evidence is paramount. An exemplary framework, developed by (Michelin et al., 2020), leverages lightweight blockchain. This innovative approach involves storing video metadata as blockchain transactions, thereby supporting the validation of recording data integrity. The lightweight blockchain not only ensures the tamper resistance of the video data but also facilitates efficient validation mechanisms. As a result, these advancements contribute significantly to the overall reliability and credibility of intelligent surveillance systems, positioning them as invaluable tools for law enforcement and public trust.

A groundbreaking approach (Gipp et al., 2016b) utilises smartphones to establish a tamper-proof dashboard camera system specifically tailored for collision detection. By incorporating blockchain decentralisation, the method introduces an additional layer of security, significantly heightening the difficulty of manipulating video files. This ensures that the recorded data holds up as verifiable, tamper-proof evidence, strengthening its admissibility in a legal context, such as a court of law.

An application was developed that automates the generation of relevant video recordings. These recordings, once created, find a permanent and secure home within the public ledger of the blockchain. This strategic integration not only guarantees the integrity and authenticity of the video data but also elevates the overall security posture, providing an innovative and robust solution for preserving, validating, and accessing critical video evidence in a tamper-resistant manner.

In the pursuit of enhancing video integrity and achieving tamper-proof status for video data,(Bansal et al., 2021; Hakak et al., 2020; Khan & Salah, 2018; Khan et al., 2020a) dedicated their efforts to establishing a robust data verification system for CCTV surveillance cameras through the application of blockchain. Their innovative blockchain-based system serves as a steadfast guardian, ensuring the trustworthiness of stored recordings. This technological advancement empowers authorities to validate the authenticity of video content, offering a means to discern whether a video has undergone any alterations. The research works discussed above each possess a unique aspect, where one of the outcomes is the contribution of computational

methods or algorithms to the field of research. These advancements have not only enriched the academic discourse but also provided practical solutions to complex problems. By leveraging these innovative approaches, the research community can explore new horizons and address challenges more efficiently, thereby enhancing the overall impact and value of their work in both theoretical and applied contexts.

The blockchain-based solution plays a crucial role in distinguishing between fake and original videos, adding an additional layer of security to the surveillance ecosystem. By leveraging the inherent characteristics of blockchain, such as decentralisation and immutability, the system provides a reliable mechanism for confirming the legitimacy of surveillance camera footage. This not only safeguards the integrity of video data but also instils confidence in the authenticity of surveillance materials crucial for investigative and legal purposes.

## 2.3.2 Advances in Cryptographic Functions

In Section 2.3.1, we point out the security and privacy aspect int the blockchain. In order to get the overall idea about current computational method and algorithm developments have been discuss in the 2.3.1.2 Sub section. In this subsection realm of Video Blockchain in intelligent surveillance has witnessed significant strides through advancements in cryptographic functions. These functions, pivotal in securing and authenticating video data, have evolved to address the intricate challenges of digital surveillance. Innovative cryptographic methods, such as hash functions and digital signatures, play a critical role in ensuring data integrity and privacy within blockchain frameworks. The integration of these advanced cryptographic methods has empowered Video Blockchain systems to offer robust security against data tampering and unauthorised access, underscoring their indispensability in fortifying intelligent surveillance systems in smart cities.

#### 2.3.2.1 *Role in Blockchain Applications*

The integration of cryptographic functions into blockchain applications has been pivotal in the evolution, particularly in enhancing intelligent surveillance. In the context of smart cities, blockchain is leveraged in a multitude of sectors, including transportation, supply chain management, and government services, primarily for its capacity to enable secure and transparent transactions without intermediaries, thus enhancing trust and efficiency in urban infrastructures (Singhal et al., 2018). Initially, blockchain platforms relied on fundamental cryptographic

functions like digital signatures and hashing functions. However, with the maturation of blockchain, more sophisticated features such as smart contracts, Proof of Work (PoW) (King, 2013), Proof of Stake (PoS) (Fu et al., 2022), and Blockchain as a Service (BaaS) (Grandhi et al., 2023) have been integrated. These developments have not only expanded the scope of blockchain's applications but have also significantly fortified its security framework. This section will explore how these cryptographic advancements are applied in blockchain-based intelligent surveillance systems, focusing on their role in ensuring data integrity, privacy, and the seamless functioning of these systems. After discussing the role of blockchain applications, the next subsection will illustrate the innovations and limitations in blockchain implementations.

#### 2.3.2.2 *Innovations and Limitations*

In Section 2.3.2, we extract the Innovations in cryptographic functions have propelled blockchain forward, particularly in intelligent surveillance applications. Recent advancements have extended beyond basic encryption and hashing algorithms to more complex cryptographic structures, such as zero-knowledge proofs and advanced digital signatures (Singhal et al., 2018). These innovations have broadened the applicability of blockchain, enabling more secure and efficient data handling. However, these advancements are not without limitations. The computational overhead of complex cryptographic algorithms, scalability concerns, and energy consumption issues are significant challenges (Shyu & Chen, 2008). Additionally, the rapid development of quantum computing poses a potential threat to current cryptographic methods, necessitating the exploration of quantum-resistant algorithms (Harris, 2019). This subsection evaluates these innovations and limitations, offering insights into the current state of cryptographic functions in blockchain and their impact on intelligent surveillance systems. It underscores the need for continuous research and development to address these challenges, ensuring that blockchain remains a viable and secure solution for modern surveillance needs.

## 2.4 Deep Dive into Video Blockchain

In this section, we explore the nuanced ways blockchain is being tailored and utilised within the domain of video surveillance. This the section, it focuses on the synthesis of blockchain with video data, examining how blockchain's inherent characteristics of decentralisation, immutability, and transparency can be harnessed to address the unique challenges posed by video surveillance data, such as issues of data integrity, privacy, and secure storage. This subsection further explores how

blockchain can enhance the trustworthiness and verifiability of video data in surveillance systems, making it resistant to unauthorised alterations and validating its authenticity for legal and security purposes. The discussion includes an analysis of current implementations, case studies, and research efforts directed toward developing blockchain-based solutions for managing, processing, and storing video data in intelligent surveillance systems. This deep dive aims to provide a detailed understanding of how Video Blockchain is revolutionising surveillance practices, offering a novel approach to data security and integrity in the era of digital surveillance.

## 2.4.1 State-of-the-Art Concepts and Technologies

The field of Video Blockchain has witnessed a surge in state-of-the-art concepts and technologies, fostering groundbreaking advancements in intelligent surveillance. This subsection studies into the latest innovations, such as the development of sophisticated cryptographic algorithms and consensus mechanisms tailored for video data processing. Recent studies have explored how blockchain can be adapted for high-definition video streams, focusing on enhancing data integrity and privacy while optimising storage and bandwidth requirements (Lee & Park, 2021). Innovations like off-chain storage solutions and advanced data compression techniques have emerged as critical enablers in this domain, addressing the scalability challenges inherent in handling large volumes of video data (Chlomoudis et al., 2022). These technological strides have significantly elevated the capability of blockchain systems to secure and manage surveillance footage, making them more robust against cyber threats and efficient in real-time processing. This subsection provides an in-depth analysis of these contemporary technologies, emphasising their impact on the practical deployment of blockchain in video surveillance systems and their potential to transform the landscape of urban security.

#### 2.4.1.1 *Innovative Algorithms and Consensus Mechanisms*

In our works getting in to the cutting-edge developments in blockchain, particularly focusing on its application in video surveillance within smart city frameworks. This exploration is pivotal in understanding how blockchain is revolutionising the field of intelligent surveillance.

- **Encryption and Hashing Algorithms:** This part of the subsection explores advanced cryptographic algorithms used in Video Blockchain. Studies have highlighted the use of SHA-256 for hashing video data, ensuring its integrity and immutability. Additionally, the

adoption of advanced encryption techniques, like AES (Advanced Encryption Standard), enhances the security of video data transmitted across blockchain networks(Dhumwad et al., 2017).

- **Digital Signature Schemes**: The application of digital signatures, specifically Schnorr Signatures, has been crucial in verifying the authenticity of video data. Research indicates that Schnorr Signatures, known for their efficiency and security, are increasingly being integrated into blockchain solutions for intelligent surveillance, offering a compact and secure way of validating video data transactions(Tian et al., 2021).
- **Smart Contracts for Video Surveillance**: The deployment of smart contracts in blockchain-based surveillance systems is another innovative concept. Studies have shown that smart contracts can automate various aspects of video surveillance, like access control, data sharing policies, and real-time alerts, thus enhancing the system's efficiency and responsiveness(Harris, 2019).

Consensus Mechanisms in Video Blockchain:

- **Proof of Work (PoW) vs. Proof of Stake (PoS**): The subsection compares the two predominant consensus mechanisms - PoW and PoS - in the context of Video Blockchain. PoW, while secure, is often criticised for its high energy consumption, making it less suitable for large-scale surveillance systems. PoS, on the other hand, is emerging as a more energy-efficient alternative, with studies exploring its feasibility in Video Blockchain networks(Fill & Haerer, 2018).
- **Delegated Proof of Stake (DPoS)** and Other Variants: Research into DPoS and other consensus variants, like Proof of Authority (PoA), is also examined. These consensus mechanisms offer faster transaction speeds and better scalability, crucial for handling high-volume video data in smart city surveillance systems(Kim et al., 2023).
- **Challenges and Future Directions**: The subsection also discusses the challenges associated with implementing these consensus mechanisms in Video Blockchain, such as security concerns in PoS and the centralisation issues in DPoS. It investigates ongoing research aimed at addressing these challenges and enhancing the overall efficiency and security of Video Blockchain systems (Islam et al., 2021; Mosakheil, 2018).

In this section, we emphasise on the significance of innovative algorithms and consensus mechanisms in optimising blockchains for intelligent surveillance. It showcases how these advancements not only enhance the security and integrity of video data but also contribute to the scalability and efficiency of blockchain networks in smart city applications. The exploration of these state-of-the-art concepts provides a comprehensive understanding of the current capabilities and future potential of Video Blockchain.

#### 2.4.1.2 *Privacy-Preserving Techniques*

In this section, we extract how innovative blockchain technologies are being employed to enhance privacy and security in video surveillance systems within smart city frameworks. This exploration is critical for understanding the advancements in ensuring data confidentiality and integrity in surveillance data.

**Integration of Privacy-Preserving Techniques:**

- **Enhancing Video Integrity**

  A key study (Y. C. Chen et al., 2019; Gipp et al., 2016b) illustrates the use of the Blocksee system in enhancing the integrity of video data (Gallo et al., 2018), particularly in car accident scenarios. This system employs built-in accelerometers to detect accidents, with the relevant videos being cryptographically hashed and securely recorded on the blockchain. This method leverages blockchain's tamper-proof characteristics, using timestamping to verify and securely transfer unaltered data to a distributed repository.

- **Securing CCTV Data**

  Another significant (Rodríguez-Silva et al., 2012) study investigated the use of blockchain in securing data recorded by CCTV cameras in smart cities. By storing this data on the blockchain, unauthorised alterations or tampering can be effectively prevented. This approach not only supports law enforcement efforts but also provides a reliable mechanism for safeguarding surveillance data.

- **Adherence to CIA Principles**

Research has emphasised the importance of adhering to the principles of confidentiality, integrity, and availability (CIA) (Y. C. Chen et al., 2019; Gřivna & Drápal, 2019) in both video surveillance and blockchain contexts. Methodologies for sorting and correctly ordering videos (P. W. Khan et al., 2020a) play a crucial role in ensuring the secure storage and integrity of video data on the blockchain.

- **Efficient Data Organisation and Storage**

  The Video Blockchain mechanism is adept at organising videos in a specified order (ascending or descending) from the video website and securely storing large volumes of data within the blockchain (Lee & Park, 2020; T. Li et al., 2020; Majdoubi et al., 2020). This organisation is essential for maintaining the integrity and accessibility of surveillance data.

- **Extending Applications Beyond Surveillance**

  Blockchain's applications in ensuring data integrity extend beyond surveillance systems, including medical record keeping and intelligent gas monitoring systems in smart cities (J. Chen et al., 2020; Chukwu & Garg, 2020; Majdoubi et al., 2020). These applications showcase the versatility of blockchain in various smart city domains.

**Recent Developments and Future Directions:**

- **Innovative Algorithms and Consensus Mechanisms**

  Recent studies have showcased the development of novel algorithms and advanced consensus mechanisms that enhancing the privacy and security of Video Blockchain systems. These developments contribute significantly to the state-of-the-art in the field (Gergely & Crainicu, 2020; Hasan et al., 2023) .

- **Opportunities for Computational Methods:**

  The continual advancement of Video Blockchains presents opportunities for developing more robust and sophisticated computational methods in intelligent surveillance. This ongoing evolution is crucial for enhancing the efficiency and security of surveillance systems in smart cities (Ghuli et al., 2017; Mandalapu et al., 2019).

In this section, we emphasise on the significant strides made in integrating privacy-preserving techniques in Video Blockchains. By examining the latest studies and technological advancements, the thesis provides a comprehensive understanding of how blockchain is being utilised to enhance

the privacy, security, and integrity of video surveillance systems in smart cities. This exploration of cutting-edge developments underscores the potential of blockchains in transforming the landscape of intelligent surveillance and its applications in smart city infrastructures.

#### 2.4.1.3 *Off-chain data Storage Mechanisms*

In this section, we deeply dive into the emerging solutions and strategies for handling the vast amounts of data generated by video surveillance systems in smart city frameworks, particularly in the context of blockchains.

#### 2.4.1.4 *Off-Chain Data Storage Mechanisms:*

- **Decentralised Storage Solutions**

  A prominent approach in off-chain data storage involves the use of decentralised storage solutions, such as the Interplanetary File System (IPFS) or distributed ledgers. These solutions address the limitations of on-chain storage, such as scalability and cost, by storing large volumes of video data off the blockchain while maintaining a secure and accessible environment (Ali et al., 2017; Pozo, 2017; Reno et al., 2021).

- **Integration with Blockchain**

  Studies have shown how off-chain storage solutions can be seamlessly integrated with blockchain (Adhikari & Ramkumar, 2023; Panarello et al., 2018). For instance, a hash of the off-chain stored video data can be placed on the blockchain, ensuring data integrity and traceability without overburdening the blockchain network.

- **Security and Privacy Considerations**

  Research into off-chain storage also focuses on enhancing security and privacy. Techniques such as encryption and access control mechanisms are implemented to ensure that only authorised users can access the stored video data (Aldairi & Tawalbeh, 2017; Koo et al., 2018). This is particularly important in surveillance systems where sensitive data is handled.

- **Data Retrieval and Efficiency**

  Efficient data retrieval from off-chain storage is another critical area of research. Studies have explored various indexing and querying mechanisms to ensure quick and efficient

access to the stored video data. This is crucial for real-time surveillance and rapid response scenarios in smart cities (Treiblmaier et al., 2020; Xu et al., 2020) .

- **Smart Contracts for Data Management**
  The use of smart contracts in managing off-chain data storage has been a subject of recent studies. Smart contracts can automate data storage and retrieval processes, enforce data sharing policies, and ensure compliance with legal and regulatory standards (Harris, 2019; Hasan & Salah, 2019).

## 2.4.2 Security Challenges in Blockchain Applications

In this section, we discuss the security challenges associated with the implementation of blockchain applications, building upon the foundation laid in Section 2.3 on page 41, where the functioning of blockchains is examined in detail. We explore the various measures other research studies have taken and identify what more needs to be done to address these challenges effectively. To enhance reliability and provide a clearer understanding, we incorporate case studies and examples. These practical illustrations will help elucidate the complex aspects of blockchain security and its application in real-world scenarios.

In this section, we conduct a comprehensive analysis of the vulnerabilities inherent in blockchain applications. This involves identifying and understanding the potential weak points that could be exploited within blockchains.

- Protocol Flaws: We examine inherent flaws in blockchain protocols that might lead to security breaches, as discussed by Nakamoto (2008) in the foundational Bitcoin whitepaper, and further elaborated by (Eyal & Sirer, 2018) in their study on blockchain protocol vulnerabilities.
- Smart Contract Vulnerabilities: The vulnerabilities within smart contracts are analysed, drawing from (Maffei & Ryan, 2017a) comprehensive review of smart contract programming pitfalls.
- Network Security Issues: We explore risks associated with the decentralised nature of blockchain networks, including the possibility of 51% attacks. This is based on the analysis presented by (Gervais et al., 2016a) on the security and performance of proof-of-work-based blockchain networks.

- Cryptographic Challenges: The potential weaknesses in the cryptographic foundations of blockchain, such as key management and quantum vulnerability, are investigated, referencing the works of (Karame et al., 2015) on the implications of quantum computing for cryptographic algorithms used in blockchain.
- Scalability and Performance Risks: The scalability issues and the increasing size of the blockchain and how they may pose security risks are understood by referencing the studies by Croman et al. (2016) on blockchain scalability solutions.

The realm of blockchain cybersecurity is rife with challenges and vulnerabilities, as evidenced by several key studies. Despite blockchain's cryptographic foundation, it remains susceptible to cyberattacks. (Hasanova et al., 2019) considered into various potential attacks on blockchain, proposing countermeasures to fortify its vulnerabilities. In the specific context of Ethereum, (Rameder et al., 2022) conducted a comprehensive literature review to categorise vulnerabilities in smart contracts, examining detection methods and tools for security analysis. Similarly, (H. Chen et al., 2020) provided a thorough overview of Ethereum's security, encompassing its vulnerabilities, potential attacks, and defensive strategies.

After compared different approaches for detecting vulnerabilities in smart contracts, highlighting the limitations and implications for security testing. (Averin A & Averina O, 2019) reviewed known vulnerabilities and attacks on blockchain platforms, emphasising the need for robust security measures. Addressing the effectiveness of countermeasures, (Ji et al., 2021) evaluated various strategies to combat vulnerabilities in Ethereum smart contracts, using statistical indicators to determine their efficacy. Finally, vulnerabilities (Gervais et al., 2016b; Karame et al., 2015) in Bitcoin's blockchain are analysed by offering insights into how countermeasures can mitigate these security threats. Collectively, these studies underscore the complexity and critical nature of ensuring security in blockchain applications.

In Subsection 2.4.2. **Error! Reference source not found.** ,we conduct a detailed examination of the inherent vulnerabilities in blockchain applications. This analysis, summarised in Table 2.2. Types of Vulnerabilities in Blockchain Applications, involves identifying and understanding various weak arguments in blockchain that could be exploited.

The section begins by addressing protocol flaws, highlighting inherent weaknesses in blockchain protocols that may lead to security breaches. Collectively, these studies, as

consolidated in Table 2.2, underscore the complexity and critical importance of ensuring security in blockchain applications, illustrating the multifaceted nature of the vulnerabilities and the ongoing efforts to fortify against them.

In the next section, we will investigate various cases and examples of incidents that have occurred in blockchain. This examination aims to provide a clear view of the real-world implications and consequences of the vulnerabilities discussed earlier. By analysing these specific incidents, we can better understand how theoretical risks translate into practical challenges. This section will not only highlight key examples of security breaches and failures within blockchain systems but also shed light on how these incidents were managed and resolved. Through this comprehensive analysis, we aim to illustrate the importance of robust security measures and the need for continuous vigilance in the ever-evolving landscape of blockchains. The insights gained from these cases will be invaluable for developers, researchers, and practitioners in the field, offering lessons learned and best practices for enhancing the security and reliability of blockchain applications.

Table 2.2 :Types of vulnerabilities in blockchain applications

| **Vulnerability** | **Description** | **Key References** |
|---|---|---|
| **Protocol Flaws** | Inherent flaws in blockchain protocols that might lead to security breaches. | (Eyal & Sirer, 2018; Nakamoto, 2009) , |
| **Smart Contract Vulnerabilities** | Vulnerabilities within smart contracts, including programming pitfalls. | (Maffei & Ryan, 2017b) |
| **Network Security Issues** | Risks associated with the decentralised nature of blockchain networks, including 51% attacks. | (Gervais et al., 2016b) |
| **Cryptographic Challenges** | Weaknesses in the cryptographic foundations of blockchain, such as key management and quantum vulnerability. | (Karame et al., 2015) |

| | | |
|---|---|---|
| **Scalability and Performance Risks** | Scalability issues and the increasing size of the blockchain posing security risks. | Croman et al. (2016) |
| **General Blockchain Cybersecurity** | Various potential attacks on blockchain with a focus on Ethereum's security vulnerabilities and countermeasures. | (Hasanova et al., 2019), (Rameder et al., 2022), (T. Li et al., 2020) , (Kissoon & Bekaroo, n.d.) , (Averin A & Averina O, 2019) (Ji et al., 2021) (Gervais et al., 2016a) |

## 2.4.3 Case Studies and Examples

This critical analysis outlines the strengths and weaknesses of cryptographic functions currently deployed in intelligent surveillance and related fields, thereby setting the foundational groundwork for proposing novel or enhanced cryptographic methods. Therefore, we have to gathered the knowledge regarding security challenges for blockchain implementation. In next paragraphs we going to extract about the attacks and preventative measures against them.

### 2.4.3.1 *Majority Attacks and Their Implications*

One of the most critical security challenges in blockchains is the vulnerability to majority attacks, often referred to as “51% attacks.” This concern is particularly prominent in blockchain networks that utilise a proof-of-work (PoW) system.(Lin & Liao, 2017) highlight the inherent risks in PoW systems, especially when large mining pools gain control over a substantial portion of the network's computational power. Their investigation sheds light on the potential for significant disruptions, such as transaction manipulation and validation issues.

Furthermore, the seminal works of (Courtois & Bahack, 2014) delve deeper into this problem. They discuss the technicalities of how majority attacks can occur and the potential impact on the blockchain's integrity. These attacks not only pose a threat to the trustworthiness of the blockchain but also can lead to financial instability and loss of confidence among users.

Theoretical implications of majority attacks in blockchain applications include undermining the decentralised nature of blockchains. The possibility of such attacks contradicts the fundamental principle of blockchain as a trust less system where no single entity has overarching control. Practically, a successful majority attack can lead to double-spending problems, where the same digital asset is spent more than once, severely undermining the blockchain's reliability and utility.

To mitigate the risks associated with majority attacks, blockchain developers and researchers are exploring various solutions. One approach is the implementation of more robust consensus algorithms that are less susceptible to such attacks. For instance, the shift from PoW to proof-of-stake (PoS) models in some blockchain applications aims to address these vulnerabilities.

Additionally, future research is focusing on developing more decentralised mining pools and enhancing network monitoring systems to detect unusual activities indicative of potential majority attacks. The objective is to create a more resilient blockchain infrastructure that can withstand the evolving landscape of cyber threats.

#### 2.4.3.2 *Private Key Security and Vulnerabilities in ECDSA*

Private key security remains a paramount concern in blockchain applications, particularly due to vulnerabilities in widely used signature algorithms like the Elliptic Curve Digital Signature Algorithm (ECDSA). The in-depth research (Li et al., 2020) reveals weaknesses in ECDSA that could potentially allow attackers to retrieve a user’s private key. This type of security breach is not just theoretical but has been observed and reported in practical scenarios, as evidenced by Hartwig's findings in 2016 (Hartwig, 2016).

The implications of such a breach are severe. Since private keys are akin to the master key of a user’s blockchain assets and identity, unauthorised access to these keys can lead to irreversible loss and theft of assets. In blockchain systems where transactions are immutable, the recovery of lost assets due to compromised private keys is often impossible, highlighting the critical nature of this security issue.

To address these vulnerabilities, blockchain developers and security experts are continuously exploring more secure signature schemes and key management practices. Advanced cryptographic methods, such as Quantum-resistant algorithms, are being researched as potential solutions to enhance private key security. Moreover, there is a growing emphasis on educating users about secure key management practices, including the use of hardware wallets and multi-signature protocols, which can significantly reduce the risk of key compromise.

Our future research is increasingly directed towards developing more robust and secure cryptographic protocols that can withstand sophisticated cyber-attacks. This includes not only enhancing the security of signature algorithms like ECDSA but also exploring alternative methods for user authentication and authorisation in blockchain networks.

#### 2.4.3.3 *Double Spending in Proof-of-Work Blockchains*

Double spending represents a significant security challenge in blockchain applications, particularly within networks based on the proof-of-work (PoW) consensus mechanism. In their pivotal study, (Akbar et al., 2021) shed light on the tangible risk of double spending in such blockchains. They illustrate how an attacker could feasibly execute multiple transactions using the same digital currency before the official confirmation and recording in the blockchain ledger.

The research work (Moroz et al., 2020) delves into the specifics of how double spending can be executed in PoW blockchains. It examines the window of vulnerability that exists between transaction initiation and final confirmation on the ledger. During this period, an attacker can potentially manipulate the system to acknowledge multiple transactions involving the same digital assets, thereby causing significant disruptions and financial irregularities within the network.

The implications of successful double spending attacks are far-reaching, undermining the fundamental premise of blockchains as a secure and trustworthy digital ledger. Such attacks can lead to loss of user confidence, financial damages to parties involved in the transactions, and broader implications for the stability and reliability of the blockchain system.

In response to these vulnerabilities, blockchain developers (Gervais et al., 2016b) are actively exploring strategies to mitigate the risk of double spending. This includes the implementation of enhanced network monitoring tools, faster transaction confirmation processes, and more robust consensus algorithms. Additionally, there is an ongoing effort to educate users and stakeholders

about the risks and signs of potential double spending attacks, enhancing the overall resilience of blockchain networks against such threats.

The continued research in this area is focused on further strengthening the security of blockchain networks against double spending. This includes exploring alternative consensus mechanisms that may be less susceptible to such attacks, as well as developing more advanced cryptographic techniques and protocols to ensure the integrity of transactions on the blockchain.

#### 2.4.3.4 *Transaction Privacy Leakage in Blockchain Systems*

The commonly held belief that blockchain inherently ensures transaction privacy has been critically examined and contested in recent years. A seminal study by (Shin et al., 2021) significantly contributed to this reassessment. Their research unveiled that privacy in blockchain transactions might not be as impregnable as generally presumed. This revelation has profound implications for users who rely on blockchain for confidential transactions, believing their financial activities are shielded from external scrutiny.

Shin et al., investigation into blockchain privacy highlighted how certain blockchain designs and user behaviours could lead to inadvertent leaks of transactional information. This could occur through patterns in transaction sizes, frequencies, or even the metadata associated with transactions. These leaks pose serious concerns, especially for users who depend on the anonymity features of blockchain technologies for sensitive financial activities.

Regarding privacy preservation in permissionless (Peng et al., 2021) blockchains take the part in these insights into privacy vulnerabilities have catalysed significant advancements in cryptographic methodologies within the blockchain domain. Recognising these privacy issues is crucial in steering the development of blockchains, particularly in applications demanding high levels of confidentiality, such as intelligent surveillance systems. Enhancing transaction privacy is not only about patching existing gaps but also about innovating novel computational methods that can fortify blockchain systems against emerging security threats.

The endeavour to bolster transaction privacy in blockchain is multidimensional. It involves refining existing cryptographic techniques, exploring new forms of digital identity verification, and implementing more sophisticated privacy-preserving protocols. These advancements are

pivotal for the evolution of blockchains, ensuring it remains a reliable tool in an increasingly security-conscious digital landscape.

Specifically, in the realm of intelligent surveillance, the integration of enhanced cryptographic methods with blockchain holds significant promise. By addressing the identified privacy gaps, there is potential to develop more resilient, secure, and dependable systems. Such systems could revolutionise how data is managed and protected in sensitive applications, paving the way for broader adoption of blockchains in various sectors where privacy is paramount.

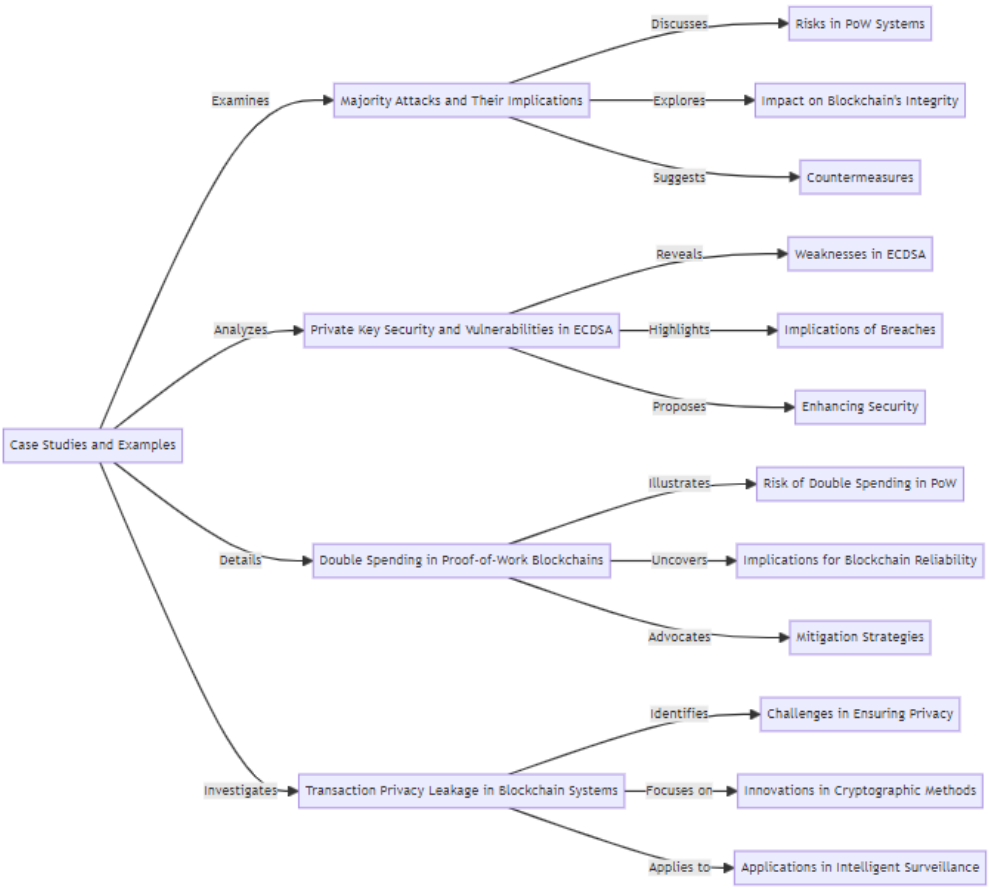


Figure 2.4: Flowchart for the Case Studies and Examples

In Figure 2.4, we provide a clear visual representation of how our examination process of case studies and examples progresses through the main subject areas. Figure 2.4 methodically illustrates the step-by-step analysis undertaken in each case study, beginning with the identification of key issues and vulnerabilities within blockchains. It maps out how each case is dissected to understand

the underlying causes, impacts, and potential solutions. Figure 2.4 also highlights how these individual cases contribute to our broader understanding of blockchain security, showing the interconnections between different types of vulnerabilities and the comprehensive strategies developed to address them. By tracing the path from initial problem identification to the development of countermeasures, Figure 2.4 encapsulates the essence of our analytical approach, providing a holistic view of the methodology applied in dissecting and understanding the complex landscape of blockchain security challenges.

## 2.5 Comparative Analysis and Discussion: Cryptographic Schemes

In Section 2.4, we have extracted state-of-the-art concepts, technologies, and security challenges pertaining to blockchain. This has resulted in a clear understanding of the involvement of cryptographic functions and the identification of some of the best cryptographic schemes most suitable for blockchain implementation. This section will further discuss the practical applications of these cryptographic schemes in various blockchain scenarios. It will also explore how these schemes enhance security and integrity in blockchain networks and the potential trade-offs in terms of performance and scalability. Additionally, the section will review into emerging trends and future directions in blockchain security, providing a comprehensive overview of the field.

### 2.5.1 Overview of Cryptographic Applications in Smart Cities

#### 2.5.1.1 *Blockchain-Based Cryptographic Functions in Smart Cities*

In synthesising the literature on cryptographic functions within the realm of Smart Cities, it is evident that while current technologies offer a foundation of security, they are also fraught with significant vulnerabilities that adversaries can exploit. The salient issues identified include the risks of majority attacks on proof-of-work systems, the fragility of private key security, the persistent threat of double-spending, and the often-misunderstood limitations of transaction privacy. These challenges have not only theoretical implications but also practical repercussions, as seen in the development of applications like the BlockSee method by (Gallo et al., 2018) which seeks to fortify data integrity and availability within blockchain-based surveillance systems.

The implementation (Asif et al., 2022) has revealed how blockchains can mitigate the risks inherent in the existing traditional centralised methodologies used in smart cities. By adopting blockchain, these urban centres can address conventional security issues through its robust cryptographic functions. This shift towards a decentralised approach promises enhanced security and transparency, potentially transforming how smart cities operate and manage data (Bhushan et al., 2020). The integration of blockchains in this context is not just a theoretical exploration but a practical solution to the pressing challenges of urban digital infrastructure.

#### 2.5.1.2 *Integration of Blockchain in Urban Infrastructure*

The incorporation of blockchains within the context of smart cities marks a revolutionary shift in urban infrastructure management and data security. Initially conceptualised by (Nakamoto, 2009), blockchain has rapidly evolved from its initial application in digital currencies to a broader spectrum of industries, including global trade, banking, healthcare, and intelligent surveillance. The inherent qualities of decentralisation, immutability, and transparency make it particularly suitable for applications in smart city ecosystems (Alketbi et al., 2020; Chen et al., 2021; Novotny et al., 2018).

To address some of these issues, the BlockSee method was developed to enhance data hashing and availability. It presents a blockchain-based video surveillance system that secures camera settings and surveillance videos' validation and immutability. Nevertheless, (Gipp et al., 2016b) highlighted that BlockSee does not comprehensively tackle the confidentiality of data transfer between network nodes and requires further refinement to ensure the proper sequencing and integrity of recorded videos.

In smart cities, blockchain finds its application in diverse areas, from smart transportation systems to food supply chain management and government services (Bhushan et al., 2020) . One of the key aspects of blockchain in these applications is its ability to facilitate secure and transparent transactions without the need for intermediaries. This characteristic not only streamlines operations but also significantly enhances trust and efficiency in urban infrastructural processes.

### 2.5.1.3 *Cryptographic Foundations and Evolutions in Blockchain*

Blockchain, fundamentally, is anchored in a robust cryptographic architecture. In its infancy, blockchain platforms primarily leveraged basic cryptographic functions such as digital signatures and hashing functions. These methods were instrumental in creating a secure and unalterable record of transactions. Digital signatures ensured the authenticity of the transaction parties, while hashing provided a secure and efficient way to encode transaction data.

As blockchain evolved, it began to incorporate more sophisticated cryptographic tools. Smart contracts, Proof of Work (PoW), Proof of Stake (PoS), and Blockchain as a Service (BaaS) (Singhal et al., 2018) are some significant advancements that have emerged over time. Smart contracts, in particular, have revolutionised the way agreements are executed in a digital environment, automating the execution process and reducing reliance on intermediaries. PoW and PoS, on the other hand, are consensus mechanisms that not only secure the network but also democratise the process of transaction validation and block creation.

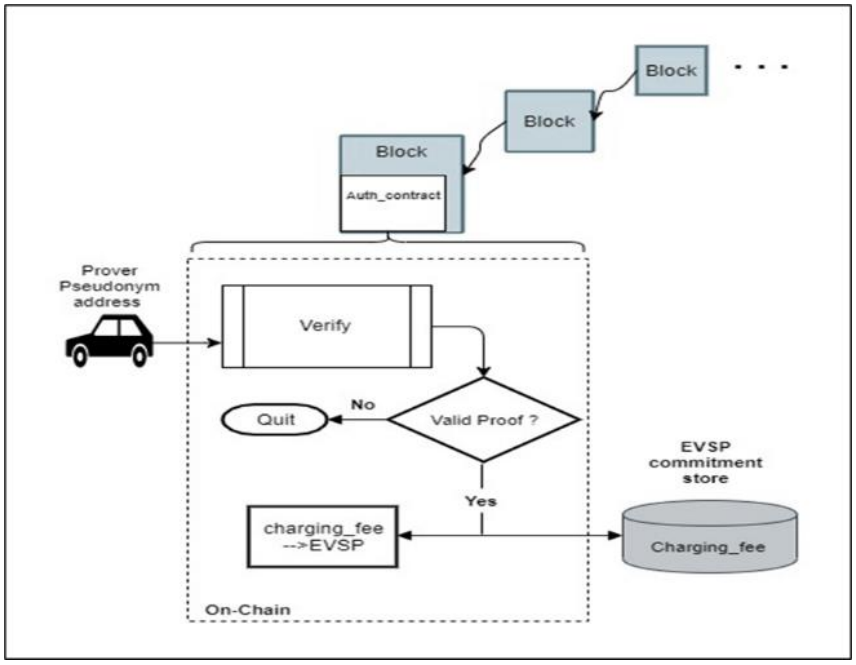


Figure 2.5:Authentication Scheme

Figure 2.6 in the literature highlights an innovative application of (Gabay et al., 2020) blockchain in the context of interconnected electric vehicles. It aims to establish a privacy-

protecting authentication framework by employing blockchain and Zero Knowledge Proofs cryptographic algorithms. This technique introduces a dual-strategy approach: initially, it develops a token-based system, and subsequently it employs the Pedersen Commitment scheme for anonymous authentication. The integration of zero-knowledge proofs with blockchain smart contracts marks a significant stride in enhancing privacy and security in this domain. The Pederson scheme, in terms of efficiency and cost, surpasses the token-based method, demonstrating the evolving nature of blockchain cryptography in practical applications.

Another cornerstone of blockchain's security mechanism is the concept of decentralised consensus. This feature is critical in preventing fraudulent activities such as double-spending and in protecting against cyber threats like Distributed Denial-of-Service (DDoS) attacks (Anwer et al., 2020). The decentralised nature of blockchain means that no single entity has control over the entire network, making it inherently resistant to various forms of cyber-attacks. The cryptographic rigor of blockchain thus plays a pivotal role in safeguarding data integrity and establishing trust in the data shared across the network.

As blockchain continues to grow and find new applications, the cryptographic foundation upon which it is built also evolves. This evolution is driven by the need to address emerging security challenges and to adapt to the changing landscape of digital interactions and transactions (D. Singh & Rajput, n.d.). For instance, the advent of quantum computing poses a potential threat to current cryptographic standards (Fernandez-Carames & Fraga-Lamas, 2020). As such, blockchain researchers and developers are actively exploring post-quantum cryptographic algorithms to ensure future-proof security.

Moreover, the expanding scope of blockchain applications from finance to healthcare, supply chain management, and beyond, demands a versatile and robust cryptographic framework (Shaikh & Mohammad, 2020). In healthcare, for instance, ensuring data privacy while maintaining the integrity and accessibility of patient records is paramount. Blockchain, with its cryptographic underpinnings, offers a promising solution to these challenges.

Thus, the cryptographic foundations and evolutions in blockchain are not just technical achievements but also enablers of a new era of digital trust and security. As the technology matures, its cryptographic backbone will continue to be a central focus, evolving to meet the

demands of a digital world that increasingly relies on blockchain for secure, transparent, and efficient transactions.

#### 2.5.1.4 *Blockchain's Role in Enhancing Smart City Data Security*

In the innovative landscape of smart cities, securing critical infrastructure and safeguarding data privacy stand as paramount challenges. Blockchain with its cryptographic underpinnings plays a crucial role in addressing these concerns. By establishing a decentralised ledger that is resistant to tampering, blockchain ensures the integrity and security of vital urban data. This is particularly critical in areas such as traffic management, public safety, healthcare, and utility services, where the reliability and security of data are indispensable (Söderström et al., 2014).

The discussion begins with an examination of decentralised trusted timestamping mechanisms implemented (Gipp et al., 2016a) on the Bitcoin blockchain as show in Figure 2.7. These mechanisms ingeniously transform smartphones, equipped with video-capturing capabilities, into cost-efficient, tamper-proof dashboard cameras. This transformation is achieved by securely embedding the hash of the video file into the blockchain's decentralised and immutable public ledger, thereby ensuring the authenticity and unalter ability of the recorded data (Loss et al., 2019).

An analysis of the SHA-256 hashing function, known for its widespread use and cryptographic robustness, reveals certain vulnerabilities. Despite its prevalent application, the commonality of SHA-256 has led to an increased risk of security breaches, underscoring the need for a more diverse cryptographic approach. Furthermore, current applications do not fully address sequential integrity ensuring the chronological order of recorded videos nor do they adequately protect confidentiality, highlighting significant areas for improvement and further research.

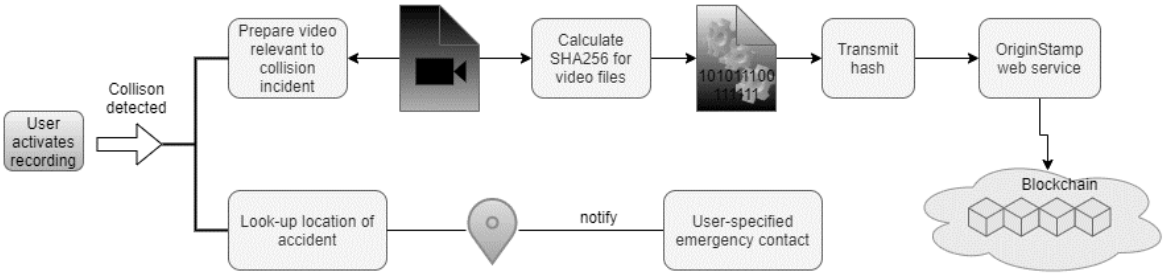


Figure 2.6: The system for timestamping dashcam videos

Blockchain’s cryptographic functions also extend to the domain of intelligent surveillance. Securely recording and storing surveillance video footage on a blockchain platform not only assures its integrity but also protects against unauthorised access and tampering (Fitwi & Chen, n.d.). This application is particularly vital in scenarios where surveillance data is utilised for legal or security purposes, as it guarantees the authenticity and reliability of the recorded footage.

In addition to these applications, blockchain also contributes to the secure management of smart city utilities. For instance, in the energy sector, blockchain can facilitate secure and transparent transactions in smart grids, enabling efficient energy distribution and billing(Khrais, 2020). Similarly, in the healthcare sector, blockchain can be used to securely store and manage patient data, ensuring privacy and enabling efficient data sharing among authorised parties.

The integration of blockchain in smart cities also fosters a more participatory and transparent governance model. Citizens can interact with various city services in a secure manner, contributing to and accessing data without compromising their privacy. This approach not only enhances the security of data transactions but also builds trust between city authorities and residents.

Moreover, the potential of blockchains in smart cities extends to the field of urban planning and development. By securely storing and sharing data related to land use, building permits, and public works, blockchain can streamline administrative processes and reduce the risk of fraud and corruption. This transparent and efficient handling of data can significantly improve the decision-making process in urban development projects.

In assumption, blockchain's role in enhancing smart city data security is multifaceted and indispensable. From transforming smartphones into secure recording devices to safeguarding critical infrastructure and sensitive data, blockchain’s cryptographic functions are at the forefront of building smarter, safer, and more efficient urban environments. As smart cities continue to evolve, the integration of blockchains will be key to ensuring the security and integrity of the data that underpins these complex and dynamic ecosystems.

#### 2.5.1.5 *Advancements and Limitations of Existing Cryptographic Techniques*

The application of BlockSee in the surveillance sector (Gallo et al., 2018), marks a significant step forward in enhancing data security. However, despite this progress, there remains an essential need

for further advancements, particularly in the areas of safeguarding the confidentiality of data transfer and strengthening the integrity of chronologically recorded data. The evolution from traditional token-based methods to the Pedersen Commitment scheme, demonstrates the dynamic development and refinement of cryptographic techniques, aimed at balancing efficiency with cost-effectiveness.

The exploring decentralised trusted timestamping and the potential vulnerabilities of the SHA-256 hashing function, highlights the critical need for a diversification of cryptographic strategies. Ensuring the integrity of unbroken recording sequences and enhancing data confidentiality are primary objectives for future research in this field. Existing literature provides a foundational critique of current cryptographic limitations while outlining potential directions for future breakthroughs. This dissertation aims not only to address these gaps but also to introduce new computational methods to strengthen the application of Video Blockchain in intelligent surveillance systems, pushing the industry towards more secure and reliable architectures.

As blockchain continues to evolve, its integration into smart city infrastructures is expected to become more complex and widespread. However, this advancement is accompanied by emerging challenges, including the need for scalable, energy-efficient blockchain solutions, seamless integration across various blockchain ecosystems, and the development of comprehensive regulatory frameworks to govern public use.

One of the critical challenges facing blockchains in smart cities is scalability (W. Li et al., 2021). As the number of transactions and the amount of data managed by these systems grows, the need for blockchain networks that can handle this increased load becomes paramount. Innovations in blockchain scalability, such as sharding and off-chain solutions, are critical areas of research that aim to address these concerns.

Another significant challenge is energy efficiency. Traditional blockchain models, particularly those based on Proof of Work (PoW) consensus mechanisms, are known for their high energy consumption. This is a significant concern for smart cities, where sustainability is a key objective. Therefore, the development of more energy-efficient consensus mechanisms, like Proof of Stake (PoS), is an essential area of focus(Khatoon et al., 2019).

Additionally, the integration of blockchains across diverse urban systems presents a complex challenge. Smart cities comprise various subsystems (X. Li, Jiang, et al., 2020; Prewett et al., 2020), each with its unique requirements and standards. Developing blockchain solutions that can seamlessly integrate with these disparate systems is crucial for the holistic implementation of this technology in urban environments.

Finally, the regulatory aspect of blockchains in public cannot be overlooked. As blockchain becomes more prevalent in urban infrastructure, the need for comprehensive laws and regulations to oversee its use and ensure data privacy and security becomes increasingly important.

In summary, the integration of blockchain-driven cryptographic functions into the ecosystem of smart cities represents a significant leap in urban technological innovation. By enhancing data security, improving operational efficiency, and building trust among city stakeholders, blockchain establishes itself as a fundamental component in the evolution of smart, resilient, and efficient urban landscapes. As this technology continues to mature, its role in shaping the smart cities of the future is expected to become even more prominent and impactful.

## 2.5.2 Comparative Analysis of Approaches

This analysis critically assesses and compares various cryptographic schemes employed in smart city infrastructures, particularly in the context of intelligent surveillance systems. The comparative study examines the diverse applications of blockchain-based cryptographic functions as outlined in the literature, evaluating their strengths and limitations within urban settings.

One primary area explored is the application of blockchains in enhancing data security and privacy in smart city ecosystems (Mosakheil, 2018). For instance, the BlockSee method represents a notable advancement in securing camera settings and ensuring the validation and immutability of surveillance videos. However, as Gipp et al. (2016) point out, this method falls short in addressing the confidentiality of data transfers between network nodes and in ensuring the proper sequencing and integrity of recorded videos. This gap underscores the need for continued refinement in blockchain-based surveillance solutions.

Furthermore, Section 2.4 analysis researches into the cryptographic foundations of blockchains, noting its evolution from initial focuses like digital signatures and hashing functions to more advanced features like smart contracts and Proof of Work (PoW). These developments have

broadened blockchain's applicability and strengthened its security framework, evidenced in applications ranging from transportation systems to government services in smart cities. However, challenges persist in ensuring data transfer confidentiality and chronological data integrity. The limitations of the SHA-256 hashing function and the necessity for more diverse cryptographic strategies highlight these challenges.

The comparative analysis also examines the effectiveness of different cryptographic techniques in various smart city applications. For instance, while the SHA-256 hashing function (Dhumwad et al., 2017) offers robust security for general transactions, its application in intelligent surveillance systems may require additional layers of encryption and privacy protection to address specific security concerns. Similarly, while smart contracts have revolutionised automated execution in digital agreements, their application in urban governance requires a careful consideration of legal, ethical, and privacy implications.

Moreover, the analysis acknowledges the dynamic nature of blockchains and its cryptographic underpinnings. As smart cities evolve, so too must the cryptographic methods employed within these ecosystems. This necessitates a continuous innovation cycle, where new cryptographic methods are developed and existing ones are refined to meet the ever-changing demands of urban environments.

The study also highlights the importance of scalability and energy efficiency in cryptographic solutions for smart cities. Given the vast amount of data generated and processed in urban settings, blockchain solutions must be scalable to handle high transaction volumes while maintaining energy efficiency, particularly in the context of environmental sustainability goals.

Hence, this comparative analysis provides a critical evaluation of the current state of cryptographic schemes in smart cities. It identifies areas for improvement and future research directions, emphasising the need for ongoing innovation in cryptographic methods. This is essential to address the evolving challenges in intelligent surveillance and the broader smart city landscape. The study underscores the necessity of tailoring cryptographic solutions to the unique requirements of different smart city applications, ensuring that they not only provide robust security but also align with the overarching goals of urban innovation and sustainability.

## 2.5.3 Extracting Cryptographic Functions: Advances and Limitations

In Sections 2.4, we deep dive about the Video Blockchain function and in Section 2.5.1, point out the blockchain function and its relevancy in the surveillance camera implementation in smart cities. After having clear idea about the direction need to take to identified the research gaps and problem in the current state. The detailed examination of various cryptographic functions integral to blockchains, particularly focusing on their roles in smart cities and intelligent surveillance systems. This analysis investigates into the intricacies of several key cryptographic schemes, assessing their strengths and addressing their limitations within the dynamic landscape of blockchain applications. This comprehensive review aims to present a clear understanding of how these cryptographic functions shape the security and efficiency of blockchain systems, while also identifying avenues for future research and development in enhancing these technologies for blockchain applications.

### 2.5.3.1 Shamir's Secret Sharing Scheme

A detailed examination of Shamir's Secret Sharing Scheme (SSSS) is vital, especially in the context of blockchain and its applications. Shamir's Secret Sharing, introduced by Adi Shamir in 1979, is a form of secure key distribution and has become a cornerstone in cryptographic protocols (Back, 1997).

Shamir's Secret Sharing Scheme (SSSS) stands out in cryptographic methods for its unique (t, n) threshold structure, where a secret S is divided into n parts or shares, and at least t shares are needed to reconstruct the original secret. This framework ensures that having fewer than t shares is inadequate for compromising the secret, thereby bolstering security against partial disclosure.

In the realm of blockchain, the application of SSSS has been pivotal in augmenting security, particularly for the management and safeguarding of private keys crucial for accessing blockchain assets like cryptocurrencies. Sharma et al. (2022) emphasised the use of a multiscript-sharing scheme based on SSSS for enhancing privacy, security, integrity, and scalability in blockchain networks, particularly smart contract-enabled consortium blockchain networks (Sharma et al., 2022). Additionally, Raman and Varshney (2018) integrated distributed storage with SSSS to

manage transaction data in blockchain systems, highlighting the balance between storage cost and data loss probability (Raman & Varshney, 2018b).

SSSS is also instrumental in facilitating secure multi-party computations within blockchain networks. For example, Mi et al. (2022) used Shamir's SSS for non-interactive transaction verification in public blockchains, addressing the conflict between extensive consensus and individual privacy (Mi et al., 2022). In addition, the scheme's application in scenarios where t equals n ensures that every share is vital, and all shares are needed to retrieve the secret, as showcased by Popovska-Mitrovikj et al. (2020) in their novel approach to reducing storage costs in blockchain systems (Popovska-Mitrovikj et al., 2020).

Recent advancements include the integration of SSSS in data privacy and secure storage, as noted by Fan and Chen (2022) in their editable blockchain scheme based on Shamir's chameleon hash key sharing, addressing immutable but erroneous data in blockchain (Fan & Chen, 2022.).

However, a significant vulnerability lies in the potential for malicious participants to provide incorrect shares, compromising the security and integrity of the scheme. This issue is exacerbated in traditional implementations of SSSS that rely on centralised key generation, conflicting with blockchain's decentralisation principle.

In summary, Shamir's Secret Sharing Scheme is a cornerstone in the security infrastructure of modern blockchain systems, offering versatile solutions for key management, secure multi-party computations, and enhanced data privacy. Its alignment with blockchain's decentralised, secure, and trustworthy ethos makes it a focal point in ongoing blockchain research and development.

#### 2.5.3.2 Limitations of Blakley's Scheme

Examining on the limitations and research gaps of Blakley's Secret Sharing Scheme (BSSS) is crucial, particularly in comparison to Shamir's Secret Sharing Scheme (SSSS) within blockchains. While BSSS, like SSSS, is a (t, n) threshold scheme for secret sharing, its practical application, especially in blockchain scenarios, has been limited. Chen et al. (2022) explored a blockchain data sharing query scheme based on threshold secret sharing using BSSS, highlighting its potential yet also underscoring its complexity and potential security vulnerabilities in practical scenarios (L. Chen et al., 2022).

BSSS's inherent security concerns, stemming from its geometric approach to constructing secrets using n-dimensional planes, have been found more susceptible to cryptographic attacks compared to SSSS. This vulnerability arises from its linear algebraic method, which, as Xia et al. (2018) suggest, can be more easily compromised, particularly with lower thresholds (Xia et al., 2018).

Additionally, the practical applications of BSSS in modern cryptographic systems, like blockchain networks, are limited, partly due to the geometric computations' complexity. Shamsoshoara (2019) noted that while theoretically sound, the real-world application of BSSS in systems as complex as blockchain networks is not straightforward, mainly due to the intricacies involved in its geometric calculations (Shamsoshoara, 2019).

Furthermore, Ghosh et al. (2021) and Yu and Weizhang (2020) also explored multi-secret sharing schemes based on Blakley's method, indicating potential applications but also underlining inherent limitations. The development and documentation of BSSS are incomplete compared to SSSS. This gap has resulted in a lesser understanding of BSSS's potential applications and optimisations in the rapidly evolving blockchain field. The blockchain environment, requiring robust security against sophisticated cyber threats, highlights the limitations of BSSS in terms of security, practical implementation, and well-documented methodologies (Ghosh et al., 2021; P. Yu & Weizhang, 2020).

In short, while BSSS has contributed foundational knowledge in threshold-based secret sharing, its practical limitations, particularly in blockchains, have restricted its application. This research thus focuses on exploring and utilising SSSS, offering a more secure, well-documented, and practically viable solution for blockchain applications.

#### 2.5.3.3 Fiat Shamir Scheme (Secret-Sharing)

In Literature Review chapter, it is crucial to examine the Fiat Shamir Scheme, a significant cryptographic protocol, particularly in terms of its applications and limitations in blockchains and secure communications. The Fiat Shamir Scheme, developed by Amos Fiat and Adi Shamir in 1986, is a cryptographic method that revolutionised the way authentication and digital signatures are handled in a cryptographic context.

The Fiat Shamir Scheme is renowned for transforming the interactive zero-knowledge proof into a non-interactive one, using a hash function as a replacement for the verifier in the protocol. In practice, this protocol involves two parties - the Prover and the Verifier. The Prover begins by generating a hash $x$ of a secret (like a password) and then computes $y = g^x \bmod p$, where $p$ is a prime number. This value $y$ is shared with the Verifier to establish a secure communication channel. The scheme aims to enhance security by complicating the authentication process for unauthorised entities, thereby bolstering defences against attacks.

However, the application of Fiat Shamir Scheme, particularly in the rapidly evolving field of blockchains, reveals certain limitations and research gaps:

**Computational Efficiency**

One of the limitations in the Fiat Shamir Scheme is its computational intensity, especially when applied in blockchain environments that demand high efficiency and speed. The calculation of modular exponentiations can be resource-intensive, which may not align well with the lightweight and fast-processing requirements of certain blockchain applications (Kiltz et al., 2018).

**Quantum Computing Threats**

With the advent of quantum computing, the Fiat Shamir Scheme, like many cryptographic protocols based on number theory, faces potential vulnerabilities. Quantum computers have the capability to solve mathematical problems, which are currently deemed infeasible for classical computers, thus posing a threat to the security assumptions of the Fiat Shamir Scheme (Liu & Zhandry, 2019).

**Implementation Challenges**

The implementation of the Fiat Shamir Scheme in real-world applications, particularly in blockchain, has its challenges. Ensuring that the scheme is integrated securely and effectively into blockchain protocols without introducing vulnerabilities requires meticulous design and testing (Fan & Chen, 2022).

**Scalability**

As blockchain networks grow and the number of transactions increases, the scalability of the Fiat Shamir Scheme becomes a concern. Ensuring that the scheme remains efficient and secure at scale is an area that needs further exploration(C. Xu et al., 2022).

**Adaptation to Blockchain-Specific Needs**

While the Fiat Shamir Scheme has found applications in creating challenging puzzles for potential attackers, its adaptation to specific blockchain-related needs, such as smart contract execution or consensus mechanisms, is an area that requires more in-depth research(Sharma et al., 2022).

This research project explores the application of the Fiat Shamir Scheme in creating challenging puzzles for potential attackers attempting to intercept communications or crack shared passwords. While the scheme aligns old cryptographic functions with contemporary needs, its practical implementation, especially in the context of blockchains, necessitates further investigation and adaptation to overcome its existing limitations and fully leverage its potential in enhancing security against sophisticated cyber-attacks.

**2.5.3.4 Pedersen Commitments**

In the blockchain implementation Pedersen Commitments can be identified as an imperative technique, also addressing the limitations and research gaps of Pedersen Commitments is crucial, especially in their application within blockchains. Pedersen Commitments, introduced by Torben Pryds Pedersen in 1991, are cryptographic protocols that enable the commitment to a specific value while keeping it hidden, with the ability to reveal it later. They have become an integral part of cryptographic solutions in various blockchain applications due to their properties of hiding and binding.

Pedersen Commitments are cryptographic tools that allow for secure message transmission without revealing the message content until a predetermined condition is met. This method is vital in scenarios requiring confidentiality and time-sensitive disclosure of information. In a typical use case, a sender commits to a message 'M' and a random secret 'R', creating a commitment 'C (M, R)'. This commitment, along with the original message and secret, is later disclosed to the receiver for verification. Pedersen Commitments are particularly significant in blockchain-based

applications, like voting systems, where they help maintain the confidentiality of transaction inputs and outputs while ensuring the integrity of the overall process.

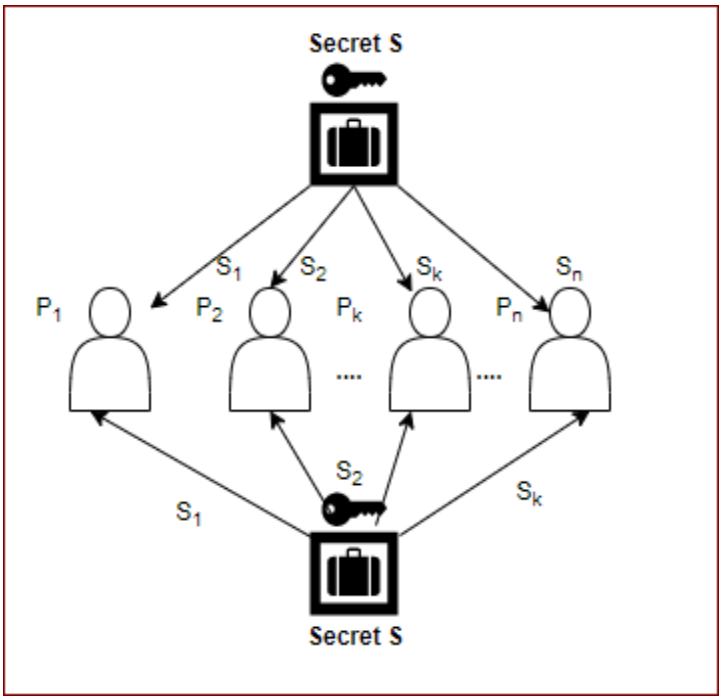


Figure 2.7:Explanation of Shamir's Secret Sharing scheme

Despite their utility, Pedersen Commitments come with certain limitations and gaps that need to be addressed, particularly in the context of blockchains:

**Computational Efficiency**

Pedersen Commitments can be computationally intensive, especially in blockchain applications that require processing large volumes of transactions. The efficiency of creating and verifying commitments is a critical factor in blockchain environments where speed and scalability are essential (Rezaeibagha & Mu, 2019).

**Integration Challenges**

Integrating Pedersen Commitments into existing blockchain architectures and protocols can be complex. Ensuring that the commitment scheme aligns with the consensus mechanisms and smart contract functionalities of blockchain platforms requires careful design and optimisation (H. Wang & Liao, 2021).

**Scalability Issues**

As with many cryptographic tools, scalability remains a challenge for Pedersen Commitments in blockchain applications. The increasing volume of transactions in blockchain networks demands efficient commitment schemes that can scale without compromising security (Duan et al., 2021).

**Security Concerns**

While Pedersen Commitments offer a high level of security, they are not immune to all types of cryptographic attacks. The research work into strengthening these commitments against advanced threats, such as quantum computing attacks, is ongoing (Bagad & Vijayakumaran, 2020).

**Practical Implementation**

The practical implementation of Pedersen Commitments in real-world blockchain applications needs further exploration. Identifying and addressing the practical challenges, such as user interface design, interaction with other blockchain components, and real-time processing, are crucial for their widespread adoption (Yu, 2020).

In summary, while Pedersen Commitments play a vital role in ensuring the confidentiality and integrity of data in blockchain applications, addressing their computational efficiency, scalability, and security challenges is crucial. Further research and development in this area are needed to fully leverage the potential of Pedersen Commitments in blockchains, especially in applications requiring secure and confidential communication.

**2.5.3.5 Schnorr Signatures in Cryptography**

In Literature Review, a comprehensive exploration of Schnorr Signatures in cryptography is crucial, particularly considering their application in blockchains. Schnorr signatures, developed by Claus Schnorr, are known for their efficiency and security within the realm of digital signatures. They are based on the difficulty of solving discrete logarithm problems, a cornerstone of public-key cryptography.

Schnorr signatures represent a significant advancement in cryptographic digital signatures, known for their simplicity and reliance on the difficulty of solving discrete logarithm problems. This signature method stands out due to its minimal computational requirement to generate a message-based signature. In the domain of public-key cryptography, digital signatures play a

crucial role in ensuring secure communication between parties. They offer unique security features akin to a handwritten signature, such as timestamp verification, content validation at the time of signing, and third-party confirmation to resolve disputes.

Digital signatures employ direct and arbitrated methods. Direct digital signatures involve only the communicating parties, using public-key algorithms. The process entails encrypting the message or its hash with the sender's private key, ensuring confidentiality. However, the security of these methods heavily depends on the sender's private key. The loss or theft of this key and subsequent forgery of signatures pose significant risks. Global practices like digital certificates, certificate authorities, and timely key revocation are standard solutions to these challenges.

The Schnorr technique focuses on reducing message-dependent computational efforts. Most of the signature creation work is independent of the message and can be executed during idle processor times. The method hinges on a prime modulus $p$, where $p - 1$ has a suitable prime factor '$q$', as expressed in the formula: $p - 1 = 1 \bmod q$.

Despite these strengths, Schnorr signatures have certain limitations and research gaps, particularly in blockchain applications:

**Quantum Computing Threats**

The threats posed by quantum computing to blockchain networks and suggest solutions for quantum resistance in blockchain systems were discussed (Allende et al., 2021). This includes the design and development of a layer-two solution to secure the exchange of information between blockchain nodes using post-quantum key (Allende et al., 2021)

**Standardisation and Adoption**

Schnorr signatures, until recently, faced challenges in standardisation and widespread adoption, particularly in blockchains. The lack of uniformity in implementation could lead to compatibility issues in diverse blockchain ecosystems. Gao et al. (2018) propose a secure cryptocurrency scheme based on post-quantum blockchain, addressing the challenges in standardisation and the adoption of quantum-resistant cryptographic algorithms, which is relevant to the implementation of Schnorr signatures in blockchains (Gao et al., 2018).

**Scalability Concerns**

In blockchain networks, where transaction throughput and scalability are critical, the efficiency of Schnorr signatures in processing large numbers of transactions simultaneously is a subject of ongoing research. Khalifa, Bahaa-Eldin, and Sobh (2019) suggest general defences for quantum-resilient blockchains and analyse post-quantum signature schemes, relevant to the scalability of Schnorr signatures in blockchain networks(Khalifa et al., 2019).

**Security Proofs and Analysis**

While Schnorr signatures are known for their security, comprehensive security proofs in the context of blockchain's varied and evolving threats are necessary. Ensuring that Schnorr signatures can withstand new forms of cryptographic attacks is a crucial area of ongoing research. The lockable signatures (Thyagarajan and Malavolta 2021) were introduced for blockchains, compatible with various digital signature schemes including Schnorr, focusing on security in payment channel networks. This research contributes to the security analysis of Schnorr signatures in blockchain application (Krishnan Thyagarajan & Malavolta, 2021).

In summary, Schnorr signatures offer a promising cryptographic tool for digital signatures in blockchains, known for their efficiency and security features. However, addressing their quantum resistance, standardisation challenges, scalability, and comprehensive security analysis is essential to fully leverage their potential in enhancing the security and integrity of blockchain networks.

**2.5.3.6 *Merkle Tree***

A comprehensive discussion of the Merkle Tree, particularly in the context of blockchains, is essential. Merkle Trees, a fundamental component in blockchain systems, are data structures that enable efficient and secure verification of large data sets. They are particularly crucial in blockchain because they provide a means to encapsulate the integrity of a sequence of transactions or data records.

At the heart of a Merkle Tree is the concept of hashing, where each non-leaf node is a hash of its child nodes. This structure, initially proposed by Ralph Merkle in 1987, ensures that any change in a single transaction will result in a different hash at the root of the tree, thus securing the integrity of the entire blockchain. The Merkle Tree's hierarchical nature allows for quick and efficient

verification of the contents of large data blocks, a critical requirement in blockchain systems where the ledger is distributed across multiple nodes.

Previous research work has extensively leveraged Merkle Trees for various blockchain applications. For instance, Deepak et al. (2020) highlighted the use of Merkle Trees in ensuring data integrity in blockchain-based video surveillance systems. This approach is particularly relevant in smart city applications where large volumes of data from surveillance cameras need to be securely managed and verified. Similarly, Khan, Byun, and Park (2020) proposed a data verification system for CCTV surveillance cameras using blockchains, where Merkle Trees played a pivotal role in ensuring the immutability and integrity of the surveillance data (Deepak et al., 2020; P. W. Khan et al., 2020b).

Moreover, the use of Merkle Trees is not limited to data integrity alone. They are also integral in enhancing the privacy and security aspects of blockchain applications. By enabling efficient cryptographic verification, Merkle Trees contribute to the overall robustness of the blockchain against various security threats, including tampering and unauthorised data alterations. Shcherbina and Mesyura (2021) explore the integration of blockchains with each other, focusing on the role of Merkle Trees in constructing and verifying transaction blocks. They address both the technical and economic aspects of Proof of Work in blockchain system(Shcherbina & Mesyura, 2021).

Table 2.3 : Merkle Trees recent research on their applications

| **Reference** | **Focus of Study** | **Key Insights** |
|---|---|---|
| (H. Liu et al., 2021) | Role in Blockchain | Provides systematic insights into Merkle Trees, emphasising their importance in blockchain for efficient and secure verification of large data structures. |
| (Shcherbina & Mesyura, 2021) | Integration with Blockchains | Explores blockchain integration focusing on Merkle Trees in constructing and verifying transaction blocks, including Proof of Work aspects. |
| (Mizrahi et al., 2021) | Optimising Merkle Proof Size | Proposes algorithms to optimise Merkle Trees for better blockchain network performance, reducing communication costs for Merkle proofs. |

| | | |
|---|---|---|
| (Castellon et al., 2021) | Energy Efficiency | Applies an energy-reducing technique to Merkle Tree calculations in blockchain, aiming to preserve security with less system availability compromise. |
| (Gracy & Jeyavadhanam, n.d.) | Sustainable Energy Consumption | Presents MTTBA for enhanced transaction speed and reduced node duplication in Merkle Trees, showing improvements in throughput and security. |
| (J. Wang et al., 2020) | Data Storage in Cyber-Physical Systems | Suggests using blockchains for secure data storage in cyber-physical systems, with improvements to the traditional Merkle hash tree. |

In summary, **Table *2.3*** shows the Merkle Tree's significance in blockchain research lies in its ability to provide a secure, efficient, and reliable mechanism for data verification and integrity assurance. This technology has been instrumental in advancing blockchain applications in diverse fields, including intelligent surveillance and smart city infrastructures, where maintaining the integrity and security of vast data sets is of utmost importance.

#### 2.5.3.7 *SHA 256*

Investigating the technical nuances and applications of SHA-256 in blockchain is crucial. SHA-256, standing for Secure Hash Algorithm 256-bit, is a key cryptographic function in many blockchain systems, especially in cryptocurrencies like Bitcoin. Developed by the NSA, SHA-256 is integral to the security and integrity of blockchain networks.

SHA-256 works by converting input data into a fixed 256-bit hash, a unique sequence of characters. Its collision resistance, whereby it's nearly impossible to find two distinct inputs producing the same hash is vital for ensuring the distinctiveness and permanence of each blockchain block.

In blockchain, SHA-256's primary uses include mining and transaction validation. In Bitcoin's proof-of-work mechanism, miners find a value that, when hashed with SHA-256, meets certain criteria. This mining process is central to adding new blocks and preserving the network's decentralisation and security.

Recent research work has delved into SHA-256's applications and impacts within blockchain. Harvilla and Du (2019) analysed SHA-256 in Proof-of-Work consensus mechanisms, showing its vulnerability to attacks like the 51% attack and proposing a hybrid PoW and PoS consensus to address these risks. Furthermore, Bensalem, Blaquière, and Savaria (2021) studied FPGA implementations of SHA-256 using OpenCL, offering insights into optimising throughput for high-performance blockchain systems (Bensalem et al., 2021).

SHA-256 also transcends technical applications, playing a pivotal role in ensuring trust and security in digital transactions. Its implementation in blockchain platforms has been instrumental in maintaining transaction integrity and non-reputability. Gad et al. (2020) presented an architecture for SHA-256 on FPGA, focusing on low power consumption and area, suitable for various blockchain applications (Gad et al., 2020).

In summary, SHA-256 is multifaceted in its contribution to blockchain, covering security, data integrity, and mining efficiency. Its role in assuring blockchain record immutability and enabling secure digital transactions cements it as a fundamental element of blockchains. Ongoing research in optimising and applying SHA-256 in diverse blockchain frameworks remains a crucial area of focus, with significant implications for secure digital transactions and decentralised networks.

#### 2.5.3.8 *Block Matrix*

The discussion of Block Matrix in the context of blockchains warrants a detailed exploration. Block Matrix, though not a standard term in blockchain literature, can be interpreted as a method of organising and processing data in block-like structures, which is particularly relevant for applications involving complex data processing and storage, such as those found in blockchain systems.

The concept of a Block Matrix generally refers to a matrix divided into smaller matrices or blocks, allowing for more efficient computation and storage. In blockchain, this concept can be analogously applied to the way data is segmented and stored in blocks. Each block in a blockchain can be seen as a part of a larger matrix (the blockchain), where the blocks contain transactions or data elements and are linked through cryptographic methods(Kumar & Kaur, 2022).

Previous research work has discovered into the applications of matrix-like structures in blockchain and related technologies. For example, in the context of cryptographic functions and

data integrity, the organisation of data into block structures facilitates efficient hashing and verification processes. (Zhu et al., 2023) explored the utilisation of block matrix operations, including matrix multiplication and inversion, for tasks like data compression and restoration, which can be vital for blockchain's efficient data handling.

Additionally, the concept of a Block Matrix aligns with the structure of Merkle Trees, a fundamental component in blockchain. A Merkle Tree organises transaction data into a tree-like structure, where each leaf node is a hash of individual transactions, and each non-leaf node is a hash of its children. This hierarchical organisation bears similarities to a Block Matrix in terms of efficient data retrieval and verification.

In the broader scope of blockchains, the Block Matrix concept can be extended to the way blockchain networks manage and process large volumes of data. The segmentation of data into blocks, coupled with the chain-like structure linking these blocks, echoes the principles of a Block Matrix, emphasising efficiency and robustness in data handling.

In summary, while the term "Block Matrix" is not commonly used in direct reference to blockchains, the principles it represents are inherently aligned with blockchain's data structuring and processing methodologies. The efficient segmentation and linking of data, essential for blockchain's integrity and functionality, reflect the core ideas of a Block Matrix, making it a relevant concept in the analysis of blockchain systems and their applications in various fields.

#### 2.5.3.9 *IPFS*

The InterPlanetary File System (IPFS) represents a pivotal innovation in the realm of distributed file systems, uniquely designed to address the limitations of traditional client-server protocols like HTTP. As a peer-to-peer (P2P) network, IPFS enables decentralised storage and sharing of data, promoting greater efficiency and robustness. Its core technology is based on a content-addressable storage model, where files are identified by their content rather than their location. This feature not only enhances data retrieval speed but also significantly reduces redundancy, as each unique piece of content is stored only once across the network. In the context of blockchain, IPFS has gained notable traction, particularly in addressing scalability and data storage challenges. For instance, in blockchain applications like smart contracts and decentralised applications (dApps),

IPFS can be utilised for off-chain storage of large data sets, thereby alleviating the burden on the blockchain itself and improving overall system performance.

In terms of previous research relevant to blockchain and IPFS, there are notable studies that demonstrate the integration of IPFS with blockchain technologies to enhance data integrity and security. For example, in the realm of intelligent surveillance within smart cities, research has focused on employing blockchain and IPFS for secure, tamper-resistant storage of surveillance data. This integration ensures that surveillance footage is immutable and verifiable, leveraging the decentralised nature of both blockchain and IPFS. Another significant application is found in the domain of digital asset management and distribution, where blockchain provides an immutable record of ownership and transactions, while IPFS offers an efficient means to store and access the digital assets themselves. This synergy is evident in platforms that aim to provide decentralised digital content delivery, enhancing both security and accessibility.

#### 2.5.3.10 *Web3*

In Literature Review, the exploration of Web3, or the third generation of internet services, holds significant relevance, especially in the context of blockchains. Web3 represents a paradigm shift in the internet's evolution, emphasising decentralisation, blockchain technologies, and token-based economics.

Web3 is characterised by its use of blockchain as a foundational technology, enabling decentralised applications (dApps) that operate on a peer-to-peer network rather than relying on central servers. This shift addresses key issues associated with the traditional web, such as data ownership, privacy, and security. In the Web3 ecosystem, users have control over their data, and transactions are transparent and immutable, thanks to blockchain's inherent properties.

The integration of blockchain in Web3 is not just limited to cryptocurrency transactions. It extends to various sectors including finance (DeFi or Decentralised Finance), content distribution, supply chain management, and more. For instance, Ethereum, one of the key players in the Web3 space, provides a platform for developing dApps with its own cryptocurrency (Ether) and smart contract functionality. Smart contracts automate contractual agreements and transactions, removing the need for intermediaries, which is a core aspect of Web3's decentralised nature.

Recent research work in the field has focused on how Web3 technologies can revolutionise different sectors. One area of interest is decentralised file storage systems, such as the InterPlanetary File System (IPFS), which leverage blockchain to create a more efficient and secure way of storing and sharing data on the internet. IPFS allows files to be stored across a distributed network of nodes, ensuring high availability and resistance to censorship attributes that are crucial in the Web3 framework.

Moreover, Web3 technologies are being explored for their potential in creating more democratic and transparent systems for content creation and distribution. Blockchain-based social media platforms, for example, aim to give power back to the users, both in terms of content control and revenue generation. These platforms use blockchain to ensure transparency in how content is moderated and monetised, a stark contrast to the central control seen in traditional social media platforms.

In summary, Web3 represents the convergence of blockchains with the broader internet ecosystem, aiming to create a more decentralised, user-centric web. Its emphasis on decentralisation, transparency, and user empowerment aligns with the foundational principles of blockchain, making it a critical area of exploration in your research. As this field continues to evolve, it promises significant transformations in how we interact with and perceive the internet.

Table 2.4: Summary of the Comparative Analysis

| **Cryptographic Function** | **Description and Application in Blockchain** | **Challenges and Limitations** |
|---|---|---|
| **Shamir's Secret Sharing Scheme (SSSS)** | Used for secure key distribution, enhances security in managing private keys in blockchain systems, and facilitates secure multi-party computations. | Vulnerable to malicious participants, reliance on centralised key generation can be a point of failure in decentralised blockchain systems. |
| **Blakley's Secret Sharing Scheme** | A (t, n) threshold scheme, less applied due to inherent security vulnerabilities and complex geometric computations. | Susceptible to cryptographic attacks, lacks practical use cases and comprehensive documentation for blockchain applications. |

| | | |
|---|---|---|
| **Fiat Shamir Scheme** | Transforms interactive zero-knowledge proofs into non-interactive ones, enhances security in authentication processes. | Computational intensity, potential vulnerability to quantum computing, implementation challenges, scalability issues, and need for adaptation to blockchain-specific needs. |
| **Pedersen Commitments** | Allows for secure message transmission without revealing content until a predetermined condition is met, used in voting systems and transaction privacy. | Computational efficiency, integration complexity, scalability issues, security concerns against advanced threats, and challenges in practical implementation. |
| **Schnorr Signatures** | Known for efficiency in public-key cryptography, used for digital signatures based on discrete logarithm problems. | Vulnerable to quantum computing attacks, challenges in standardisation and adoption, scalability concerns, need for comprehensive security proofs and analysis. |
| **Merkle Tree** | Used for efficient and secure verification of large datasets in blockchain, fundamental in ensuring data integrity. | Requires optimisation for efficient data handling and verification in large-scale blockchain applications. |
| **SHA-256** | Secure Hash Algorithm used predominantly in mining and transaction verification, particularly in cryptocurrencies like Bitcoin. | Optimisation needed for unique hardware and software architecture of blockchain networks, ensuring resistance to quantum computing threats. |
| **Block Matrix** | Conceptual method for data organisation and processing, analogous to data segmentation in blockchain. | Efficient handling and verification of large data volumes in blockchain, aligns with principles of Merkle Trees for data integrity. |

| | | |
|---|---|---|
| **InterPlanetary File System (IPFS)** | Peer-to-peer network for decentralised data storage, addresses scalability and data storage challenges in blockchain. | Integration with blockchain technologies for enhanced data integrity and security, efficient and secure storage of large data sets. |
| **Web3** | Third generation of internet services emphasising decentralisation and blockchain technologies. | Focuses on decentralised applications, data ownership, privacy, and security, extending blockchain use beyond cryptocurrencies. |

This section has provided a comprehensive review of the existing cryptographic functions used in blockchains, as we summarised in Table *2.4*: Summary of the Comparative Analysis, particularly cryptographic schemes in the context of smart cities and intelligent surveillance. It has highlighted the challenges and limitation of current cryptographic schemes, such as the vulnerabilities of blockchain's decentralised consensus mechanism, and the limitations of cryptographic tools like Shamir's Secret Sharing, Fiat Shamir Scheme, and Pedersen Commitments in enhancing security and privacy.

However, it also identified significant vulnerabilities, including risks in proof-of-work systems, private key security concerns, the threat of double spending, and the limitations in transaction privacy. The BlockSee method, while a step forward in securing video surveillance data, still requires advancements to fully address these issues.

The literature review also underscored the importance of integrating blockchains more holistically into multidisciplinary domains, suggesting a vast area for future research and development. The proposed research direction aims to bridge these gaps by developing enhanced cryptographic functions and exploring innovative, interdisciplinary cryptographic solutions.

## 2.6 Identifying Research Gaps and Future Directions

This section aims to synthesise the insights gained from our extensive literature review, focusing on identifying the prevailing research gaps and potential future directions in the intersection of blockchain technologies and intelligent surveillance. The review, encompassing Sections 2.1 and

Section 2.2, introduced the methodology and preliminary concepts. Following this, Section 2.3 surveyed into the integration of blockchains with intelligent surveillance, underscoring the advancements in cryptographic functions and their role in bridging current research gaps.

A particular focus of our review in Section 2.4 was on Video Blockchains. This section critically analysed how blockchain is revolutionising video data management and security in surveillance systems. The subsequent Section 2.5, presented a comparative analysis of various cryptographic schemes, offering a detailed overview of the current state of cryptographic functions used in blockchain technologies.

## 2.6.1 Challenges and Limitations in Video Blockchain Research

In the field of Video Blockchain, especially within the ambit of smart cities, a plethora of challenges surfaces, particularly in safeguarding data security and privacy. The advent of blockchains, gaining prominence since its association with Bitcoin in 2009 (Gallo et al., 2018; George et al., 2019) , has profoundly influenced diverse realms, including the sphere of intelligent surveillance in smart cities (Gabay et al., 2020). This innovation provides a decentralised and secure framework, negating the necessity for intermediaries and augmenting transparency. Nonetheless, the application of blockchain to video data in smart cities presents multifaceted complexities.

A pivotal element in blockchain security is the hashing algorithm, as we discussed in the subsection 2.5.3.7 commonly the SHA-256 from the Secure Hash Algorithms (SHA) family. This algorithm plays a crucial role in transforming plain text into irreversible hash data, which is vital for safeguarding the integrity of transactional data in blockchain networks (Khan et al., 2020b). The transformation of data into a unique numeric string is fundamental in securing the stored data. However, the challenge emerges in tailoring these cryptographic techniques to meet the specific requirements of video surveillance in smart cities. The substantial volume of data produced by video surveillance systems calls for cryptographic solutions that are both efficient and scalable.

As we extract the details of Secret Sharing in Section 2.5.3.3 to tackle challenges for Secret Sharing, we advocate an integrated strategy that merges a *(k, n*) Secret Sharing mechanism with a Software-Defined Networking (SDN) framework. This methodology ensures data security via the Secret Sharing scheme and capitalises on the benefits of SDN in network management. This

approach is particularly advantageous in managing the dynamic conditions of smart city networks, thereby effectively diminishing the likelihood of cyber-attacks (Gergely & Crainicu, 2020) . The amalgamation of these technologies aims to counteract the challenges inherent in the real-time, secure transmission, and storage of video data in smart cities.

Moreover, the incorporation of the Merkle tree structure in blockchain is a crucial consideration. This structure is instrumental in organising and representing transaction data, more so in Video Blockchain where each transaction might symbolise a segment of video data. The process of iterative hash value computation in the Merkle tree, culminating in the Merkle root, necessitates optimisation for video data to assure efficiency and scalability.

The Schnorr signature scheme, recognised for its efficacy and security in public-key cryptography, introduces another layer of complexity in Video Blockchain (Maxwell et al., 2019) . The scheme's minimal computational demand is beneficial for smart city applications, where resources are often constrained. The challenge, however, lies in integrating such cryptographic schemes into a blockchain framework specifically designed for video data, ensuring that the system remains secure while efficiently managing large-scale video data.

In supposition, the challenges in Video Blockchain research for smart cities centre on customising and enhancing blockchain and cryptographic technologies to suit the specific needs of video data. This encompasses efficient data encryption, scalable data storage, and real-time data transmission, all while upholding the utmost levels of security and privacy. Our proposed solution, which blends secret-sharing mechanisms with SDN and harnesses efficient cryptographic methods like the Schnorr signature, is aimed at effectively addressing these challenges, thereby facilitating more secure and proficient smart city infrastructures.

## 2.6.2 Identifying Gaps in Current Literature

In the realm of intelligent surveillance, especially within smart city contexts, the integration of advanced computational methods with blockchains has emerged as a pivotal area of research. The current literature, while extensive, often treats these two domains in isolation, thereby overlooking the potential synergies that could arise from their combined application. This gap highlights a crucial need for comprehensive research that examines how blockchain can augment computational efficiency and reliability in surveillance systems. It is imperative to explore holistic

approaches that integrate blockchain with computational methods, thereby creating robust, efficient surveillance systems suited for the dynamic requirements of smart cities.

Another significant gap lies in the application and exploration of cryptographic algorithms that are tailored for the unique demands of high-volume, high-velocity video data typical of surveillance systems. Standard cryptographic methods, while effective in general applications, may not be optimally suited for the complexities inherent in processing and securing video surveillance data. This oversight in the literature suggests a need for the development of scalable blockchain solutions that are specifically designed to handle the intricacies of video data. Research in this area should focus on identifying and utilising cryptographic algorithms that can efficiently process large volumes of video data while ensuring its security and integrity within a blockchain framework.

The evolving landscape of security threats, particularly in smart city environments, also presents a gap in current research. There is an urgent need for studies that specifically address how blockchains can counteract these advanced threats to ensure the security and integrity of surveillance data. This involves not only leveraging blockchain's inherent security features but also innovating new approaches that can effectively mitigate emerging threats in intelligent surveillance systems.

Moreover, the practical implications of implementing blockchain in real-world surveillance scenarios are often underrepresented in academic literature. Challenges related to scalability, data privacy, and regulatory compliance are critical aspects that need empirical research and case studies. Such studies are essential to understand the real-world challenges and opportunities of integrating blockchain into intelligent surveillance systems, thereby facilitating the successful application of this technology in practice.

The ethical and legal implications of Video Blockchain in surveillance also represent a significant research gap. Issues concerning data ownership, consent, and the potential misuse of surveillance data are becoming increasingly important as surveillance systems proliferate in smart cities. Yet, these issues remain largely unaddressed in the current body of research. It is vital to explore these ethical and legal dimensions to ensure that the deployment of Video Blockchain in surveillance systems is responsible and respects privacy and data rights.

The absence of standardised best practices and guidelines for implementing Video Blockchain in intelligent surveillance is another notable gap. As this field continues to evolve rapidly, the development of standardised frameworks is crucial. Such guidelines would not only guide practitioners and policymakers but also ensure the consistency and reliability of implementations across various contexts.

The existing body of literature, while providing valuable insights into the theoretical underpinnings of cryptographic techniques and blockchain architectures in video surveillance, demonstrates a need for more empirical research and real-world implementations. Few studies offer concrete insights into the practical challenges and solutions encountered in integrating Video Blockchain into existing surveillance infrastructures. This gap underscores the importance of bridging theoretical research with practical applications, providing tangible solutions and strategies for effective implementation in intelligent surveillance systems.

In terms of scalability and performance, the literature reveals a limited focus on the challenges arising from managing large volumes of video data in blockchain systems. Addressing how blockchains can efficiently process high-throughput video data, particularly in real-time processing scenarios, is imperative for the advancement of intelligent surveillance systems.

Additionally, as highlighted in the review of Schnorr signatures and Merkle Trees, there is a need for in-depth research focused on optimising these cryptographic tools for intelligent surveillance. Schnorr signatures, known for their efficiency and robustness, require further exploration to address challenges related to quantum resistance and scalability. Similarly, the advancement of Merkle Trees, fundamental for data integrity and efficient verification, is crucial for enhancing the performance and security of surveillance systems.

Lastly, considering emerging technologies and the potential impact on the development of blockchain applications in intelligent surveillance is essential. The future trajectory of this field and the technological innovations that might shape it necessitate a holistic view that contemplates both current capabilities and future possibilities. By identifying these research gaps and future directions, this study contributes to the ongoing discourse in the field, it encourages further investigation into the synergies between blockchains and intelligent surveillance.

In summary, while the existing body of literature on computational methods in Video Blockchain for intelligent surveillance is extensive, it reveals critical gaps that need addressing. Empirical research, exploration of scalability and performance issues, ethical and legal considerations, and the development of standardised practices are vital for advancing this field. This study aims to bridge these gaps, enhancing the practical applicability and effectiveness of computational methods in intelligent surveillance within smart cities.

## 2.6.3 Proposed Directions for Future Research

In navigating the dynamic landscape of computational methods for Video Blockchain in intelligent surveillance, there exists a promising avenue for future research and innovation. This interdisciplinary field, blending blockchains with computer vision applications such as face detection, behaviour analysis, and traffic rule violation detection, presents significant potential in crime prevention, anomaly detection, and privacy policy enforcement. Prior research in blockchain and computer vision has substantially contributed to developing robust methodologies countering manipulation of video repositories and surveillance cameras by malicious entities. Blockchain's inherent tamper-resistance and immutability are central to protecting data integrity within surveillance systems.

The employment of blockchain is crucial in fortifying defences against tampering and attacks. Its core features of tamper-resistance and immutability are instrumental in safeguarding stored data and ensuring data integrity. Cryptographic hash functions, pivotal in converting sensitive data into randomised strings, are key in maintaining confidentiality and linking blocks within the blockchain. Blockchain-based systems like BlockSee exemplify how validation and immutability can be applied to surveillance videos, thereby bolstering their security and reliability.

The research work in intelligent surveillance and blockchain is expanding into diverse applications. These include the use of dashboard cameras for accident documentation in smart cities, IoT devices for environmental monitoring, and blockchain in tracking food delivery processes. Blockchain's attributes of decentralisation, data filtering, and privacy preservation play a critical role in these contexts, ensuring data authenticity. Time-lapse features, crucial in transferring unaltered data to shared repositories, maintain the chronological accuracy of surveillance data.

Blockchain's versatility extends beyond surveillance, impacting large-scale industries like global trade, healthcare, banking, distributed energy, and more. Its adaptation in domains such as smart transportation, food supplier management, and government services highlights its wide-ranging applicability. Blockchain's role in data integrity is evident in applications like medical record verification and intelligent gas monitoring systems.

To develop robust computational methods for Video Blockchain in intelligent surveillance, the strategic selection of cryptographic functions is paramount. This approach is effective in fortifying resistance against digital surveillance system attacks. Innovative design, integrating distinct cryptographic algorithms and implementing novel techniques, is key in mitigating attacks and building upon existing blockchain platforms.

However, blockchain in securing surveillance ensuring data integrity is ongoing. Continual evolution of new methods and integration of diverse cryptographic algorithms are necessary to enhance resistance against attacks on existing blockchain platforms. The careful selection of cryptographic functions and innovative implementation of techniques are crucial in augmenting the privacy and security of blockchain-based systems in intelligent surveillance.

Specifically, the application of Schnorr signatures within the blockchain framework needs further exploration to address challenges in quantum resistance, scalability, and standardisation. An in-depth security analysis is vital to adapt to the rapidly evolving threat landscape in blockchains. Additionally, the role of Merkle Trees, foundational for data integrity and verification, must be further explored for optimised performance in intelligent surveillance systems.

Finally, considering emerging technologies and their potential impact on the development of blockchain applications in intelligent surveillance is essential. Providing a holistic view of the field and its future trajectory, including technological innovations that might shape it, is crucial. Identifying these research gaps and future directions contributes to the ongoing discourse in the field and encourages further investigation into the synergies between blockchains and intelligent surveillance, thereby shaping a more secure and efficient future for smart city infrastructure.

## 2.6.4 Overview of Identified Gaps

In the exploration of cryptographic functions within the ambit of blockchains and intelligent surveillance, a meticulous examination unveils significant gaps in the existing corpus of knowledge. These gaps, identified through a comprehensive analysis of the current literature, are instrumental in shaping the future trajectory of research in this field.

- Vulnerabilities in Current Cryptographic Paradigms: The blockchain, despite its revolutionary impact on security across various domains, is not devoid of vulnerabilities. Pivotal research work (Chang and Chun 2017, Li et al. 2020, Hartwig 2016, Karame et al. 2015, Möser et al. 2017) has shed light on critical weaknesses that permeate through proof-of-work systems. These include the fragility of private key security, the risks of double spending, and the potential for transaction privacy leakage. Such vulnerabilities underscore an urgent need to enhance the cryptographic resilience of blockchain to counteract these threats effectively.
- Inadequate Addressal of Sequential Integrity and Confidentiality: Current implementations of blockchain, as exemplified by the BlockSee method, reveal a significant inadequacy in ensuring sequential integrity and confidentiality of data, particularly within the realm of intelligent surveillance systems. This gap underscores the necessity for more robust cryptographic methods that can guarantee both the security and the chronological accuracy of data within such systems.
- Limited Integration of Blockchain in Multidisciplinary Domains: Despite blockchain's widespread adoption across diverse sectors, its integration with interdisciplinary fields such as artificial intelligence, machine learning, and intelligent surveillance is still in a nascent stage. This observation points to a fertile ground for research aimed at developing multidisciplinary cryptographic solutions, harnessing the synergies between blockchains and these complementary disciplines.

To bridge these identified gaps, the proposed research direction focuses on three core areas:

- Development of Enhanced Cryptographic Functions: This aspect of the research explores into the investigation and development of advanced cryptographic functions, meticulously tailored to address the vulnerabilities identified in blockchains. The research aims to place

a strong emphasis on augmenting security against majority attacks, fortifying private key security, preventing double spending, and safeguarding transaction privacy.

- Enhancement of Data Integrity in Blockchain Applications: Another pivotal research objective is to pave the way for innovative methods that ensure not only the sequential integrity but also the confidentiality of data within blockchain-based systems. This is especially critical in applications like intelligent surveillance, where the accuracy and security of data are of paramount importance.

- Exploration of Interdisciplinary Cryptographic Solutions: The research embarks on an ambitious journey to explore the seamless integration of blockchains with other disciplines, particularly artificial intelligence and machine learning. The ultimate aim is to pioneer innovative, efficient, and secure cryptographic solutions that are specifically designed to cater to the unique challenges and demands of intelligent surveillance systems.

In summary, the identified gaps present a compelling case for a focused research approach that addresses the vulnerabilities in current cryptographic paradigms, improves data integrity and confidentiality in blockchain applications, and explores interdisciplinary cryptographic solutions. Such a research path holds immense potential in advancing the field of computational methods for Video Blockchain in intelligent surveillance, ultimately contributing to the development of more secure, reliable, and efficient smart city infrastructures.

## 2.7 Contributions of This Thesis

In this subsection, we extract the significant contributions of our research, delineating the outcomes and advancements it brings to the field. This thesis provides a clear and defined understanding of how our work contributes to the current landscape of research in computational methods for Video Blockchain in intelligent surveillance. Building upon the comprehensive comparative analysis presented in Section 2.5 on page 52, and the identification of research gaps in Section 2.6 on page 78, we have gained a nuanced understanding of the existing research gaps. These insights have guided us in identifying potential avenues for contribution to this evolving field of study. This section meticulously outlines the novel approaches and enhancements that this research introduces, demonstrating the distinctive and innovative nature of our work. These

contributions not only bridge identified gaps but also pave the way for future explorations and advancements in intelligent surveillance and blockchains.

## 2.7.1 Novel Approaches and Enhancements

This thesis presents groundbreaking advancements in the field of Video Blockchain, particularly focusing on enhancing cryptographic functions, addressing storage and computational challenges, and extending the multidisciplinary applications of blockchain.

#### 2.7.1.1 *Enhancing Cryptographic Functions in Video Blockchain*

This research marks a significant milestone in the domain of Video Blockchain by introducing innovative enhancements to cryptographic functions. Recognising the paramount importance of robust cryptographic measures for securing and maintaining the integrity of video data in intelligent surveillance systems, the study pioneers novel algorithms and methodologies. These advancements are pivotal in strengthening the resilience of Video Blockchain against cyber threats and in enhancing the reliability and efficiency of data encryption and decryption processes. This leap in cryptographic functions sets new standards for data security within the realm of blockchains, particularly in the context of smart city infrastructures.

#### 2.7.1.2 *Addressing Storage and Computational Challenges*

This thesis tackles the inherent storage and computational challenges in Video Blockchain systems, this thesis unveils innovative solutions that significantly improve data storage efficiency and computational resource management. By integrating off-chain storage mechanisms and employing advanced data compression techniques, the research effectively addresses issues related to scalability and high resource consumption. Additionally, the thesis introduces refined computational methods that accelerate the speed and efficiency of blockchain operations. This enhancement in computational processes substantially uplifts the performance of intelligent surveillance systems in smart cities, making them more effective and efficient.

#### 2.7.1.3 *Advancing Multidisciplinary Applications of Blockchain*

The research transcends traditional boundaries by extending the applications of blockchains into various multidisciplinary domains. The study discovers into the impactful utilisation of blockchain in diverse fields, including healthcare, urban planning, and environmental monitoring. These explorations not only highlight the adaptability and versatility of blockchains but also emphasise its potential to revolutionise a plethora of sectors. By enhancing data integrity, security, and transparency, the applications of blockchain demonstrated in this thesis provide a blueprint for its integration into multiple aspects of smart city frameworks, showcasing its capacity to bring transformative changes across various industries.

In summary, this subsection "2.7.1 Novel Approaches and Enhancements" underscores the significant contributions of this thesis to the field of Video Blockchain. The research encapsulates groundbreaking enhancements in cryptographic functions, innovative solutions to storage and computational challenges, and the pioneering exploration of blockchain's multidisciplinary applications, all of which are integral to advancing intelligent surveillance systems within the smart city paradigm.

## 2.8 Chapter Summary

This thesis culminates by encapsulating the significant strides made in enhancing cryptographic functions within Video Blockchain, addressing storage and computational challenges, and advancing multidisciplinary applications of blockchains. The research underscores the pivotal role of blockchain in revolutionising data security and integrity in smart city infrastructures. Through innovative cryptographic enhancements, it fortifies the security measures necessary for the robust operation of intelligent surveillance systems. Tackling storage and computational inefficiencies, the study introduces efficient data management and computational methodologies, marking a significant advancement in blockchain scalability and performance. Furthermore, the exploration into the diverse applications of blockchain across various sectors highlights its transformative potential beyond its traditional use cases. This conclusion reaffirms the thesis's contribution to the field, setting a foundation for future research and practical applications in blockchains, particularly within the context of smart cities and their evolving technological landscapes.

This thesis makes substantial contributions to the field of computational methods for Video Blockchain in intelligent surveillance, focusing on key aspects of security, privacy, and storage challenges. These contributions represent a significant advancement in the current state-of-the-art and aim to address critical gaps in existing solutions.

One major contribution lies in the meticulous selection and implementation of cryptographic functions for the Video Blockchain. By identifying the most effective cryptographic algorithms, the research aims to bolster the security shield of blockchain, ensuring a resilient and tamper-resistant environment for intelligent surveillance data in smart cities. The careful choice of cryptographic functions is purposeful, tailored to meet specific tasks within the visual blockchain framework.

Privacy preservation over the blockchain is another essential focus of this thesis. Recognising the sensitivity of surveillance data, especially in smart cities, innovative solutions are proposed to safeguard privacy concerns. Techniques such as zero-knowledge proofs and homomorphic encryption are incorporated within the blockchain structure to enable secure transactions and data computations while preserving the confidentiality of sensitive information.

This thesis also tackles the challenges associated with blockchain storage, particularly in handling video data. The research provides effective solutions to address storage complexities within the blockchain, ensuring the seamless integration and retrieval of video frames as data output from surveillance systems across smart cities.

The advancements in computational methods for visual blockchain represent a key pillar of this thesis. The introduction of a novel web-based image prototype leverages the decentralised nature of blockchain to enhance the computation method of visual blockchain. This prototype not only minimises existing gaps in intelligent surveillance but also sets the stage for more reliable and sustainable solutions.

In strategically aligning with the goal of filling existing gaps in intelligent surveillance, the contributions of this thesis are poised to make a significant impact. By addressing issues related to security, privacy, and storage, the research offers a comprehensive approach that bridges the lacunae in current solutions. The emphasis on selecting the most appropriate cryptographic

algorithms and creating a web-based image prototype adds unique dimensions to the field, providing practical and innovative solutions to prevalent challenges.

In summary, the contributions of this thesis significantly elevate the field of computational methods for Video Blockchain in intelligent surveillance. They offer a nuanced and holistic approach to enhance the security, privacy, and efficiency of visual blockchain systems deployed in smart cities, thereby contributing to the advancement of knowledge in this crucial domain.

# Chapter 3 - Methodology

*In Chapter 3, we are presented and extracted the significance of the Video Blockchain computation method for surveillance systems, focusing on addressing the issues related to surveillance systems in smart cities. This focus stemmed from a careful gathering and analysis of literature pertinent to the current research area. The research findings revealed a myriad of challenges, including data integrity, privacy concerns, and the need for robust cryptographic methods within the realm of smart city surveillance. These challenges highlighted the necessity for an innovative approach that not only enhances security but also ensures the practical functionality of surveillance systems.*

## 3.1 Introduction

In Chapter 3, we enter a critical phase of our research, bridges the theoretical underpinnings outlined in Chapter 2 with the practical implementation of blockchain in video surveillance. This chapter aim to address the gaps identified in the literature by extracting challenges in current intelligent surveillance systems and proposing novel methods. Our research questions and hypotheses, rooted in the findings of Chapter 2, guide this endeavour.

The chapter provides an overview of our study's design, including the research framework and methodology adopted to steer the research work. We have chosen methodical approach of Formal Methods for our study titled 'Computational Methods for Video Blockchain in Intelligent Surveillance. This selection is both intentional and strategic, as Formal Methods comprehensive nature effectively integrates theoretical concepts with practical innovation. This approach is particularly suited to our interdisciplinary research, combining academic rigor with practical applicability.

The organisation of this chapter delineates our methodological journey. It details how each step of the Design Science Research Methodology (DSRM) is intricately integrated into our research process. This structure underscores our commitment to a methodology that is academically rigorous and pragmatically relevant, aiming to contribute meaningful and actionable insights to the field of Video Blockchain in intelligent surveillance.

## 3.2 Research Methodology

Our methodology synergistically combines Formal Methods and Design Science Research Methodology (DSRM), providing a comprehensive and structured approach to developing and implementing an innovative Video Blockchain system for intelligent surveillance.

Formal Methods form the backbone of our approach, initiating with a meticulous problem identification process. This involves a detailed analysis of the current landscape of Video Blockchain and intelligent surveillance, pinpointing specific challenges and intricacies. Guided by an extensive literature review. This phase ensures that our research objectives are deeply rooted in the identified gaps and needs of the field. The precision and rigor of Formal Methods are crucial

in the selection and alignment of suitable cryptographic algorithms, ensuring their theoretical soundness and practical applicability to the unique requirements of Video Blockchain in surveillance systems.

Incorporating DSRM into our methodology enriches the research process with its iterative and empirical nature. DSRM guides the structured development of artifacts – from the initial conceptualisation to the final implementation and evaluation. Each phase of the DSRM process is informed and enhanced by the precision of Formal Methods, ensuring that our artifacts, whether they are new computational models, algorithms, or frameworks, are not only innovative but also reliable and secure.

The iterative cycle of DSRM facilitates continuous refinement and enhancement of our solutions, aligning perfectly with the dynamic and evolving nature of Video Blockchains. This iterative process includes the design and development of artifacts, their demonstration in realistic scenarios, thorough evaluation against set objectives, and subsequent refinements based on feedback and findings.

Moreover, DSRM's emphasis on empirical approaches complements Formal Methods by ensuring that our theoretical concepts and hypotheses undergo rigorous testing and validation in real-world scenarios. This empirical orientation is essential to transcend theoretical modelling, aiming to offer a viable, efficient, and functional Video Blockchain system that addresses the practical challenges of intelligent surveillance applications.

By intertwining Formal Methods with DSRM, our methodology stands not only on the foundation of mathematical rigor and precision but also gains practical relevance and applicability. This dual approach ensures that our research outcomes effectively bridge the gap between theoretical innovation and real-world utility in intelligent surveillance systems.

### 3.2.1 Methods for Testing Hypotheses

| | |
|---|---|
| **Method 1 (M1)** | Review the current research by using PRISMA method work for blockchain with cryptographic schemes and intelligent surveillance. |
| Utilising the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method for reviewing current research on blockchain and cryptographic schemes is a rigorous approach. This method helps in systematically identifying, evaluating, and summarising the existing literature, which is essential for Hypothesis 1,2, and 3. | |
| **Method 2 (M2)** | Explore targeted development to enhance the cryptographic function to address the identified problems. |
| Exploring targeted development to enhance cryptographic functions directly addresses Hypothesis 2. This method involves practical development and experimentation, which is key for enhancing cryptographic functions in Blockchain solutions. | |
| **Method 3 (M3)** | Develop the 'Video Blockchain' computation method by using Design Science Research Methodology (DSRM) with support of Formal Methods. |
| Applying Design Science Research Methodology (DSRM) supported by Formal Methods for developing a Video Blockchain computation method is highly appropriate for Hypothesis 3. DSRM provides a structured framework, while Formal Methods ensure rigor in the development process. | |
| **Method 4 (M4)** | Explore effective data storage solutions for Method 3 development of Video Blockchain. |
| Investigating effective data storage solutions for the developed Video Blockchain system aligns with Hypothesis 4. This method is crucial for ensuring that the security measures do not compromise the efficiency and functionality of the surveillance system. | |
| **Method 5 (M5)** | Explore Video Blockchain a solution possible way to address the privacy protection in the blockchain implementations. |
| Exploring Video Blockchain solutions for privacy protection in blockchain implementations is well-suited for Hypothesis 5. This method is essential for investigating how blockchains can be leveraged to enhance data privacy in intelligent surveillance systems. | |

| **Method 6 (M6)** | Explore the interaction of Video Blockchain with the interdisciplinary approaches. |
|---|---|
| Exploring the interaction of Video Blockchain with interdisciplinary approaches aligns with Hypothesis 6. This method acknowledges the importance of integrating diverse perspectives and expertise to develop robust and versatile security solutions. | |

Each of these methods is tailored to investigate specific aspects of our research, from literature review and development of cryptographic functions to practical implementation and interdisciplinary collaboration. This comprehensive approach ensures that thoroughly address each hypothesis, contributing valuable insights and advancements to the field of intelligent surveillance in smart cities.

Overall, our methods for testing the hypotheses are well-conceived and should provide a strong foundation for achieving your research objectives. They are instrumental in exploring the multifaceted challenges of implementing secure computational methods in intelligent surveillance systems within smart cities.

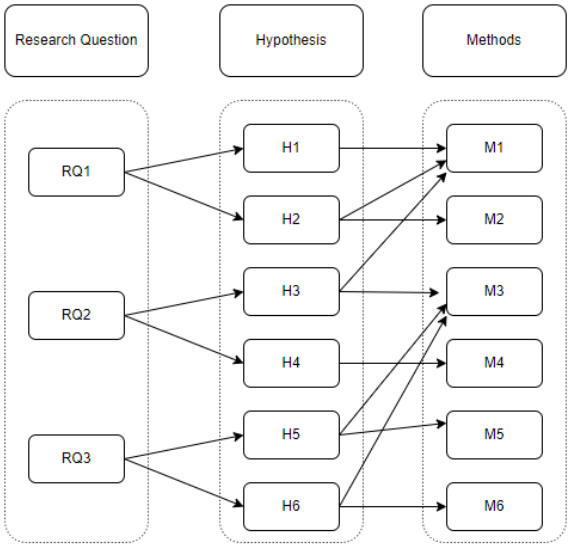


Figure 3.1: Mapping Relationship between research questions

### 3.2.2 Relationship Between Research Questions

In Section 3.2, we extract what methods are used to address the research questions based on the identified research gaps in Chapter 2. In order to get a clear overview of the relationship, between research questions, hypothesis and research methods. We explain how each of the methods aligns with specific research questions and hypotheses. This alignment is critical for ensuring that the methodology is appropriately tailored to address the core objectives of the study. The figure illustrates a matrix or a flowchart, where each method is linked to the corresponding research question and hypothesis it is designed to test or explore.

The research involves quantitative methods by using experiments to testing the implementing methods to address the identified research problems, the figure shows how these methods are used to test hypotheses for answer research questions related to measurable variables relationships. In the case of quantitative methods like content analysis, the figure depicts how these approaches are employed to explore more in-depth, subjective experiences and themes identified in the literature review.

Furthermore, Figure 3.1 visual representation serves as a guide to ensure that each aspect of the research question and hypothesis is comprehensively addressed through the selected methods. It also provides a clear roadmap for readers, illustrating the logical flow from research gaps identified in Chapter 2 to the methods chosen for investigation. This helps in establishing the rigor and validity of the research methodology and in demonstrating how the study contributes to filling the identified gaps in existing knowledge.

## 3.3 Method I: Review the Current Research by Using PRISMA

This method aligns with literature review process in Chapter 2. Here, we access the relevant literature using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method. As extracted in Section 2.2, we have gathered the literature accordingly to the PRSIMA method and analysed the collected data. This systematic approach ensured a structured and comprehensive literature review, aligning with PRISMA guidelines which emphasise transparency and replicability in research. The PRISMA Flow Diagram depicted in Figure 2.1 serves as a visual summary of the database and record screening process, illustrating the rigorous

methodological steps undertaken to consolidate relevant literature, from identification to final inclusion.

## 3.3.1 Selection of Cryptographic Algorithms

In the process of selecting cryptographic algorithms for Methods, we have meticulously adhered to the principles outlined in the Design Science Research Methodology's (DSRM) design and development stage. This strategic alignment ensures that our choice of cryptographic algorithms is not only theoretically sound but also practically applicable in enhancing intelligent surveillance systems in smart cities.

#### 3.3.1.1 *Criteria for Selection*

- Efficiency and Effectiveness (Hypothesis 1)

Our primary criterion revolves around the algorithms' ability to improve data transfer efficiency and effectiveness between surveillance nodes in a smart city. This focus stems from our hypothesis that advanced cryptographic algorithms can significantly enhance the operational capability of intelligent surveillance systems. The rationale is to overcome the current limitations of cryptographic paradigms and to investigate if sophisticated algorithms can optimise data transfer processes in surveillance systems.

- Enhanced Cryptographic Functions (Hypothesis 2)

The potential of cryptographic functions to address vulnerabilities in existing cryptographic paradigms forms another vital criterion. We hypothesise that enhanced cryptographic functions, specifically tailored for intelligent surveillance systems, will provide substantial defence against current security threats. The development of these functions is a direct response to identified gaps in existing cryptographic methods, aiming to bolster the integrity and security of surveillance systems.

- Data Integrity in Video Frame Capturing (Hypothesis 3)

While ensuring data integrity in video frame capturing is critical. The selected cryptographic algorithms should be capable of maintaining the integrity of video data, ensuring its authenticity and reliability.

#### 3.3.1.2 *Application of Cryptographic Algorithms*

Our journey began with a comprehensive analysis of existing literature and cryptographic functions, aiming to understand the current state and identify potential gaps. We employed a blockchain prototype to evaluate various cryptographic functions, emphasising attributes such as lightweight architecture, robust security, and low energy consumption. The integration of these functions into our visual blockchain model was driven by the need for a secure and efficient data transfer mechanism, particularly crucial in smart city surveillance contexts.

- **Final Selection and Comparative Analysis**

As a result of comparative analysis of cryptographic algorithms in the section 2.5.2, its outcome the cryptographic functions like SHA256 and Merkle tree for hashing, Schnorr Signature, and Elliptic Curve Digital Signature Algorithm (ECDSA) for signatures, alongside functions for smart contracts and consensus mechanisms, enabled us to identify the most effective combinations. This analysis ensured alignment with our research objectives and the unique requirements of Video Blockchain in intelligent surveillance.

The outcome of this comprehensive selection process is a robust cryptographic framework that addresses both the technical demands of our research and the practical challenges in advanced surveillance implementation. By meticulously selecting and implementing these cryptographic algorithms, we aim to make a significant contribution to the evolution of intelligent surveillance systems, ensuring they are secure, efficient, and adaptable to the dynamic landscape of smart cities.

## 3.4 Method II: Enhance the Cryptographic function

The implementation phase of cryptographic methods in our study on 'Computational Methods for Video Blockchain in Intelligent Surveillance' is a crucial element within the DSRM framework. This phase extends beyond merely selecting cryptographic algorithms; it encompasses the practical application of these algorithms to construct a robust Video Blockchain system, which serves as a key artifact in our DSRM-driven research.

We have resonant on a meticulous process of implementing cryptographic functions that are integral to the establishment of a secure and efficient Video Blockchain system. Our focus has centred on deploying algorithms like SHA-256 and SHA-3, renowned for their effectiveness in

blockchain environments. These functions were specifically chosen for their proven security capabilities against various threats and their operational efficiency, crucial for performance optimisation within the unique architecture of blockchain systems.

A significant aspect of our implementation strategy is ensuring the compatibility of these cryptographic functions with prevalent blockchain platforms such as Ethereum. We have selected algorithms like Schnorr signature or SHA-256 that harmonise with these platforms, facilitating seamless integration into existing blockchain infrastructures. These steps are imperative for enabling our Video Blockchain system to function effectively across diverse blockchain ecosystems.

In line with DSRM's emphasis on empirical testing, we conducted performance evaluations using a Python script for benchmarking. This script was pivotal in assessing the average execution time of the SHA-256 hashing process on test data strings. By repeatedly executing this hashing process, we gathered precise performance metrics. Such thorough evaluation methods are consistent with DSRM's principles, focusing on the empirical assessment and continual refinement of our Video Blockchain system artifact.

The practical application of these cryptographic methods emphasises our commitment to developing a feasible and robust Video Blockchain system. Research by Jiang et al. (2022) utilised a performance evaluation method for cryptographic functions to optimise blockchain transactions and reduce latency. Conversely, Lee and Park (2021) employed the Merkle Tree method to enhance the efficient transmission of video data for cloud-based surveillance systems. This research also serves as an example of how others aim to measure and improve the performance of cryptographic functions used in blockchain, ensuring optimal performance to achieve the desired outcomes. This system is expected to significantly enhance the integrity and confidentiality of video data in intelligent surveillance networks within smart cities. Through the systematic application and evaluation of these cryptographic algorithms, we aim to create an artifact that aligns with both the theoretical and practical aspects of our research. Algorithms designed to evaluate the performance of blockchain functions, is finalised in Chapter 2's literature review process. This process has led to the identification of the most suitable cryptographic functions to address the issues identified in Chapter 2, (X. Jiang et al., 2022; Lee & Park, 2021).

This algorithm calculates the average time required to perform cryptographic function over a specified number of iterations. It is used to evaluate the efficiency of the cryptographic function within our blockchain framework.

**Algorithm 3.1:** Performance Evaluation of Cryptographic function

**Input**: Data to be hashed/ Signature (**data_to_hash**), Number of iterations (**num_iterations**)

**Output**: Average time for XX hashing (**average_time_XX**)

Initialise: a timer to record the starting time (**start_time**).

Initialise: a variable to store the cumulative time (**cumulative_time**) as 0.

For each iteration in **num_iterations**:

Start the timer.

Perform XX hashing on the input data (**data_to_hash**).

Stop the timer and record the ending time (**end_time**).

Calculate the elapsed time for this iteration (**elapsed_time = end_time - start_time**).

Add **elapsed_time** to **cumulative_time**.

Calculate the average time for XX hashing (**average_time_XX = cumulative_time / num_iterations**).

Return the **average_time_XX**.

In Algorithm 3.1, *if* **data_to_hash** is "sample data" and **num_iterations** is 1000, the algorithm will perform XX hashing 1000 times on "sample data", and then calculate and return the average hashing time.

After we design the performance evaluation algorithm using Pseudocode, in next we have created the functioning algorithm to get the most appropriate result. Therefore, in Algorithm 3.2 have implement to get more accurate and result for our Method 2 (M2). Its objective to evaluate the computational efficiency of various cryptographic functions, including SHA256, Merkle Trees, Schnorr Signatures, and ECDSA.

**Algorithm 3.2:** Advanced Performance Evaluation of Cryptographic Functions

Inputs:

***D***: Data to be processed.

***n***: Number of iterations for each cryptographic function.

***CF*:** Cryptographic function to be evaluated, selected from (SHA256, Merkle Tree, Schnorr Signature, ECDSA).

**Output:**

$T_{CF}$**:** Average time for the selected cryptographic function *CF*.

**Procedure**:

Initialisation:

Let $T_{\text{cumulative}} = 0$.

Define Timer () to record the current time.

**Function Evaluation Loop**:

For $i = 1$ to n

Start the timer: $T_{start}$= Timer ().

Perform the selected cryptographic function CF(D).

Stop the timer: $T_{end}$=Timer ().

Compute elapsed time: $\Delta = T_{end} - T_{start}$.

Update cumulative time: $T_{\text{cumulative}} \mathrel{+}= \Delta t_i$

**Average Time Calculation:**

Compute the average time: $T_{CF} = nT_{\text{cumulative}}$

**Return Result:**

Return $T_{CF}$

Function Definitions:

- CF(D) for SHA256: Perform SHA256 hashing on D.
- CF(D) for Merkle Tree: Construct a Merkle Tree using D and calculate the root hash.
- CF(D) for Schnorr Signature: Generate and verify a Schnorr Signature on D.
- CF(D) for ECDSA: Generate and verify an ECDSA signature on D.

The algorithm conducts a performance analysis by computing the average time taken $T_{CF}$ for a selected cryptographic function *CF* over n iterations. The function $CF(D)$ varies based on the cryptographic operation being evaluated.

In summary, the implementation of cryptographic methods in our research is a pivotal step within the DSRM process. It effectively bridges theoretical concepts and practical application, ensuring the Video Blockchain system we develop is not only theoretically sound but also practically efficacious in enhancing the security and efficiency of intelligent surveillance systems in smart cities.

## 3.5 Method III: Research Design and Framework

In aligning our mixed methods approach with the Design Science Research Methodology (DSRM), we adopt a framework that proficiently accommodates the intricate balance of qualitative and quantitative methods. This alignment is crucial, considering DSRM's emphasis on the creation and evaluation of technological artifacts, in our case, specifically the development of a Video Blockchain system. The mixed methods approach integrates seamlessly within the DSRM framework, providing a robust structure for exploring the multifaceted aspects of Video Blockchain in intelligent surveillance systems. It facilitates the development of this innovative artifact by ensuring its comprehensive examination from both a quantitative efficiency standpoint, through empirical performance measurements, and a qualitative user experience perspective, through stakeholder feedback and usability studies. This methodological synergy is pivotal in addressing the complexities of our research, as it allows for an all-encompassing understanding and assessment of the blockchain system as an innovative solution in smart city surveillance, capturing both its technical efficacy and its practical applicability.

### 3.5.1 DSRM Stages and Framework Alignment

In the initial stage of the Design Science Research Methodology (DSRM), as outlined in Section 3.2, we embarked on problem identification. Here, we meticulously delineated the method to pinpoint the core issues, specifically focusing on the critical challenges in intelligent surveillance

systems, such as data integrity and security. This process culminated in the clear objective of creating a secure and efficient Video Blockchain system.

Following this, the second stage of DSRM involved defining our objectives, influenced by our ambition to elevate the reliability and functionality of surveillance systems within smart city frameworks. In addressing this stage, detailed in Section 3.7, we employed Method 2. This approach guided us in selecting the most suitable cryptographic functions for the system's implementation.

During the design and development phase, encapsulated in Method 2, our attention turned to constructing the Video Blockchain system. This phase was marked by integrating advanced cryptographic algorithms to bolster data security and enhance transfer efficiency. It entailed rigorous planning and execution, ensuring each system component was in line with our defined objectives and effectively addressed the challenges in intelligent surveillance.

The final phase, demonstration and evaluation, is pivotal. We intend to conduct exhaustive testing and assessment of our Video Blockchain system. The demonstration phase will involve deploying the system within simulated smart city environments. Concurrently, the evaluation phase will concentrate on gauging the system's performance against our established objectives. This includes evaluating data transfer efficiency, security, and user adaptability, thereby offering a holistic assessment of the system's efficacy in real-world settings. This stage is critical in affirming the practical utility of our research, solidifying our contributions to the field of intelligent surveillance as both innovative and practical.

## 3.5.2 Data Collection Methods

In our quest to thoroughly comprehend the integration of Video Blockchains in smart city surveillance, our research adopts a dual methodology for data collection, aligning with the principles of the Design Science Research Methodology (DSRM). This approach necessitates leveraging both primary and secondary data sources to facilitate a comprehensive and multi-dimensional analysis.

**Primary Data Source**

At the core of our primary data collection lies an extensively documented video dataset. Captured by using the advanced Samsung Galaxy S23 Ultra, known for its superior rear camera capabilities (200.0 MP + 10.0 MP + 12.0 MP + 10.0 MP), we recorded a 30-minute video in Auckland city. From this, a 5-minute segment was chosen, yielding about 7000 video frames. This extensive collection of frames forms a vital primary dataset, crucial for the analysis and validation of our Video Blockchain system. The choice of this data is rooted in its applicability to real-world urban surveillance, offering a practical framework for testing the efficiency of our cryptographic algorithms and blockchain integration.

**Secondary Data Sources**

To augment our primary dataset, we have compiled an extensive array of secondary data, including academic conference papers and journal articles WildDeepfake (Zi et al., 2020), (L. Jiang et al., 2020), Celeb-DF (Y. Li et al., 2019) and FaceForensics++ (Rössler et al., 2019)datasets. These scholarly resources were carefully chosen to enhance our literature review, aiding in the identification of research gaps and influencing the trajectory of our study. This secondary data is integral to the DSRM process, laying the theoretical groundwork and providing contemporary perspectives essential for the development and refinement of our Video Blockchain system.

**DSRM Utilisation**

Within the DSRM framework, these data sources are instrumental during the demonstration and evaluation stages. The primary data, encompassing video frames, will be utilised to showcase the system's functionality and to evaluate its performance under real-world conditions. This includes thorough testing of data transfer efficiency, integrity, and the overall efficacy of the cryptographic methods applied. Conversely, the secondary data will contribute to the evaluation phase by offering a theoretical benchmark for comparing the practical outcomes of the system. Adopting this holistic approach ensures that our research is not only academically rigorous but also practically relevant and applicable in the context of intelligent surveillance in smart cities.

## 3.5.3 Development of Video Blockchain Integration

Blockchain, renowned for its immutable and decentralised nature, offers significant enhancements in the security and reliability of surveillance data within intelligent systems. In our approach, each video frame captured by surveillance cameras is encrypted and assimilated into the blockchain as a distinct block. This integration ensures the non-alterability of data without network consensus, thereby augmenting the trustworthiness and integrity of the surveillance data.

**Integration Strategy**

The incorporation of blockchain into surveillance systems follows a comprehensive strategy. This begins with the acquisition of video data, which is then encrypted and securely stored within the blockchain. We utilise advanced cryptographic algorithms to ensure the data's security and privacy. The blockchain architecture is custom-designed to meet the specific demands of surveillance systems, considering factors such as the volume of data, the need for real-time processing, and swift data retrieval capabilities. As mentioned in the section 3.5.2, both primary and secondary video data are harnessed to fulfil the objectives of our study. For primary data, videos from mobile phone cameras were collected, and images extracted from these videos were subjected to experimental analysis, as part of our investigations into Video Blockchain. During image encryption, raw image data were transformed into a byte sequence, rendering the original image data inaccessible post-encryption.

The primary aim of this research project is to develop a blockchain-based chain of video blocks from surveillance cameras, distributed and connected to preserve the correct sequence of frames in the video without tampering and minimal third-party involvement in smart city contexts. To achieve secure data communication in surveillance. In the development of Method 4 mentioned in the Section 3.2, the method results the most appropriate amalgamation of cryptographic functions, which are the SHA-256 hash function with the Merkle Tree. The hash function ensures collision resistance, while the Merkle Tree scheme significantly bolsters the communication's security.

In Algorithm 3.3, we operate under the assumption that a blockchain web service is available. Our goal is to process incoming requests (Ri) from authenticated nodes (Ni). Having identified the most appropriate cryptographic functions, our computational method for data integration in the

Video Blockchain is tailored to test the three hypotheses associated with Method 3. This involves ensuring that the order of the recorded image frames remains unaltered under any condition. As the initial step in designing the algorithm for our method, we first utilise a Pseudocode approach to gain a clear overview of Algorithm 3.3. Subsequently, we employ mathematical functions to implement our Algorithm 3.4. resenting our algorithms in both pseudocode and mathematical form enhances their comprehensibility, making it easier for readers to grasp.

**Algorithm 3.3** Blockchain-Based Image Encryption Process

```
Require: Blockchain Web Service
Ensure: Genesis Block
 while T has not expired do
    if node Ni is authenticated == True then
       if request Ri is matched == True then
          if Ri is identified as a processed request == False then
             process the response to Ci
             Hash (video_frame_metadata)
              Sign (video_frame_metadata)
              Update chain
             else
             Response to Ni that Ri is not a valid request
             end if
             else
           Deny the request
         end if
       Validate and add block into chain
    end if
  end while
```

Algorithm 3.3 involves the process of encryption through a series of methodical steps. First, nodes (Ni) are authenticated, and valid incoming requests (Ri) are processed. Next, the most

suitable cryptographic functions for data integration are identified and applied. To ensure the chronological integrity of image frames in the Video Blockchain, specific measures are taken. The process begins with pseudocode for an initial, understandable overview, followed by the implementation of the algorithm using precise mathematical functions for clarity. Finally, data is encrypted according to the outlined steps, ensuring secure integration into the blockchain.

This structured approach in Method 3 not only aligns with the objectives set forth but also ensures that the research is accessible and technically sound, adhering to the principles of effective blockchain implementation in intelligent surveillance systems.

**Algorithm 3.4:** Blockchain-Based Image Encryption Process

**Objective**: To encrypt and store video frame metadata in a blockchain

**Inputs**:

- *T*: Time duration for the encryption process.
- *N*: Set of nodes$\{N1, N2, \ldots, Nn\}$.
- *R*: Set of requests$\{R1, R2, \ldots, Rm\}$ corresponding to each node.
- *C*: Set of video frame metadata for encryption.

**Output**:

- A blockchain with encrypted video frame metadata.

**Procedure**:

1. **Initialisation**:
    - Start a timer for duration $T$.
    - Initialise a blockchain with a genesis block.
2. **Encryption Loop**:
    - While the timer has not expired:
        - For each node $Ni\ in\ N$:
            - Check if $Ni$ is authenticated:
                - If True:
                    - For each request $Ri\ in\ R$:
                        - Check if $Ri$ matches and is not already processed:
                            - If True:

- Process the response to corresponding video frame metadata $Ci$.
- Perform Hash on $Ci$: $Hi = Hash\ (Ci)$.
- Perform Sign on $Ci$: $Si = Sign\ (Ci)$.
- Update the blockchain with the new block containing *Hi* and *Si*.

- Else:
  - Respond to *Ni* that *Ri* is not a valid request.

- Else:
  - Deny the request from *Ni*.

3. **Validation and Block Addition**:
   - Validate and add the new block to the blockchain.

**End Procedure**.

---

The algorithm operates within a specified time frame *T* and iterates over a set of nodes *N*. For each authenticated node, it processes valid requests by encrypting the corresponding video frame metadata, hashing, and signing it. The encrypted data is then added to the blockchain. The algorithm ensures that each request is unique and has not been processed before.

The algorithm outlines a process for image encryption using blockchain and assumes the availability of a blockchain web service. Authenticated nodes can submit requests for image encryption, which are then validated and processed according to specific conditions. Valid requests undergo the encryption process, which includes generating a response for the requesting node, hashing the video frame metadata, and signing it for integrity. The algorithm updates the blockchain by adding a new block containing the encrypted image or relevant information. Invalid requests are responded to accordingly, either by notifying the node of the issue or denying the request outright. The algorithm ensures the integrity and security of the blockchain by validating and adding processed blocks. It continues processing requests until a specified time has not expired.

### 3.5.4 Video Blockchain for Data Integrity

This section shows how to enhance its features using SHA 256 and Merkel Tree. This method for enhancing data integrity through blockchain involves creating a digital fingerprint for each video frame captured by the surveillance system. This fingerprint is then added to the blockchain, creating a chronological and unalterable record of all surveillance footage. The use of Merkle trees further enhances the efficiency of this process, allowing for the aggregation of multiple hashes into a single block, thereby ensuring the integrity of large volumes of data.

In the context of intelligent surveillance, blockchain serves not just as a technology for data storage, but as a mechanism for validating the authenticity and reliability of the surveillance data. By using blockchain, the surveillance system can detect and prevent unauthorised manipulation of video data, ensuring that the footage remains an accurate and trustworthy source of information.

In line with the Design Science Research Methodology (DSRM), the application of blockchains and its role in enhancing data integrity are evaluated rigorously. This involves assessing the system's ability to withstand security threats and data breaches, along with evaluating the efficiency of the data retrieval process. The evaluation stage plays a crucial role in determining the feasibility and effectiveness of blockchain integration in real-world surveillance scenarios.

Moreover, in this process we create the two separate algorithms for SHA256 and Merkle tree and combine together to test Hypothesis 3, 5 and 6. Based on the outcomes of Methods 1 and 2, we have developed Method 3. This method is focused on designing and implementing the computational methodology for the Video Blockchain system. Moreover, in this process, we have devised two separate algorithms for SHA256 and the Merkle tree, which are then combined to rigorously test Hypotheses 3, 5, and 6. The SHA256 algorithm focuses on ensuring data integrity and security through cryptographic hashing, while the Merkle tree algorithm is utilised for efficiently verifying the consistency and completeness of the data blocks within the blockchain. By integrating these two algorithms, we aim to leverage the strengths of both cryptographic techniques, thereby enhancing the overall robustness and reliability of our Video Blockchain system.

This integration is particularly crucial for validating Hypothesis 3, which posits that the use of SHA256 in conjunction with a Merkle tree will significantly improve the integrity of video data

within the blockchain. Hypothesis 5 explores the privacy of data retrieval and verification processes in the blockchain network, which is inherently bolstered by the Merkle tree structure. Lastly, Hypothesis 6 examines interdisciplinary cryptographic solutions of our blockchain solution in handling large volumes of video data, a challenge aptly addressed by the combined use of SHA256 for data security and Merkle trees for efficient data management.

In implementing this combined approach, we meticulously ensure that each video frame is hashed using SHA256, and these hashes are then organised into a Merkle tree. This method not only secures individual data blocks but also facilitates a quick verification process, allowing for faster validation of data integrity across the entire blockchain. The success of this combined algorithm will be a testament to the efficacy of using advanced cryptographic techniques in enhancing the functionality and security of blockchain-based surveillance systems in smart cities.

**Algorithm 3.5**: Hashed Features Authentication Procedures (SHA256)

```
Function: hash_feature(features_set)
    string_features = empty_string
    for each feature_vector in features_set do
        feature_string = Convert_to_string(feature_vector)
        string_features = string_features || feature_string
    end for
    bytes_features = Convert_to_bytes(string_features)
    feature_hash = SHA256_Hash(bytes_features)
    feature_id = features_set.name
    return {feature_id: feature_hash}
Procedure: record_hashed_feature(features_set)
    feature_tx = hash_feature(features_set)
    certificate = CertificateAuthority.generate_certificate(feature_tx)
    tx_result = transaction_commit(feature_tx, certificate)
    return tx_result
Procedure: verify_hashed_feature(features_set)
    feature_tx = hash_feature(features_set)
    query_feature_tx = transaction_query(feature_tx)
```

```
    if query_feature_tx == feature_tx then
        verify_hash = True
    else
        verify_hash = False
    end if
  return verify_hash
```

In Algorithm 3.5, we implement a mathematical and cryptographic approach to ensure the integrity and authentication of feature data within a blockchain system. The algorithm initiates with a function called **hash_feature**, which is central to transforming and securing the feature set data. In this function, we begin by amalgamating individual feature vectors from the given **features_set** into a unified string. This is achieved through a mathematical conversion function **Convert_to_string**, which meticulously translates each vector into a string format. These strings are then concatenated to form a comprehensive representation of the features. Following this, the concatenated string undergoes a byte-level transformation via **Convert_to_bytes**, effectively preparing the data for cryptographic processing.

The crux of this process involves the application of the SHA256 hash function, symbolised as **SHA256_Hash (bytes features)**. This step is pivotal as it leverages the mathematical prowess of SHA256 to generate a unique and irreversible hash value, thus ensuring the data's integrity and resistance to collisions. The outcome is a securely hashed representation of the feature data, tagged with its corresponding feature set name.

Subsequently, the **record_hashed_feature** procedure takes centre stage. Here, the hashed features are first obtained using the previously mentioned **hash_feature** function. To authenticate the transaction within the blockchain, a digital certificate is generated via **CertificateAuthority.generate_certificate(feature_tx)**, a function likely involving cryptographic algorithms for digital signing. This certificate serves as a hallmark of authenticity for the transaction. The hashed data, now certified, is committed to the blockchain through the **transaction_commit** function, ensuring its permanence and traceability within the decentralised ledger.

In the final procedure, **verify_hashed_feature**, the algorithm re-engages the hashing process to verify the authenticity and integrity of the feature data. It rehashes the features and queries the blockchain for a matching transaction record. A mathematical comparison is then conducted to ascertain if the queried record aligns with the newly computed hash. If congruence is found, the data's integrity is affirmed; if not, it indicates potential alteration or inauthenticity.

Through its intricate design, Algorithm 3.5 effectively marries mathematical transformations with cryptographic principles, ensuring that feature data within the blockchain is handled securely and authentically. This approach not only aligns with the fundamental tenets of data security but also harmonises with the blockchain's inherent qualities of decentralisation and tamper-evidence, thus bolstering the robustness and reliability of the blockchain system in managing feature data.

After working through Algorithm 3.5, the next step involves exploring into the utilisation of the Merkle tree for algorithm design. The Merkle tree, a fundamental component in blockchains, offers an efficient and secure way to summarise and verify large sets of data. In the context of our algorithm, the Merkle tree is employed to enhance the integrity and efficiency of data handling.

The implementation begins by creating a Merkle tree from the hashed data produced in Algorithm 3.5. Each piece of hashed data, representing a unique feature or a set of features, is treated as a leaf node in the Merkle tree. The algorithm then pairs these nodes and hashes their combined values, creating parent nodes. This process is iteratively repeated, combining and hashing parent nodes to form higher-level nodes in the tree, until a single root hash, the Merkle root, is derived. This Merkle root is a compact representation of all the underlying data and serves as a powerful tool for data verification.

Incorporating the Merkle tree into our algorithm design significantly streamlines the verification process. Instead of validating each data point individually, which could be time-consuming and resource-intensive, the Merkle root provides a means to verify the entire dataset's integrity quickly and efficiently. When a specific data point needs to be validated, the algorithm can simply reconstruct the path from the targeted leaf node to the Merkle root, checking hashes along the path. If the reconstructed path's Merkle root matches the original one, the data's integrity is confirmed.

This approach not only saves computational resources but also adds an extra layer of security. The structure of the Merkle tree makes it infeasible to alter any part of the data without affecting

the entire tree, ensuring the data's tamper-resistance. Thus, the Merkle tree's integration into our algorithm is a strategic choice, aligning with the overarching goals of enhancing data security and operational efficiency in blockchain-based systems. As we progress, the focus will be on optimising the Merkle tree construction and its integration with other components of our blockchain solution, ensuring a seamless and robust implementation.

**Algorithm 3.6:** Authentication Procedures Using Merkle Tree

**Function:** hash_feature

**Input:** `features_set`: A set of feature vectors.

**Output:** A dictionary with feature_id as the key and feature_hash as the value.

```
function hash_feature(features_set)
    string_features = ""
    for each feature_vector in features_set do
        feature_string = Convert_to_string(feature_vector)
        string_features = string_features || feature_string
    end for
    bytes_features = Convert_to_bytes(string_features)
    feature_hash = SHA256_Hash(bytes_features)
    feature_id = features_set.name
    return {feature_id: feature_hash}
end function
```

**Function:** create_merkle_tree

**Input:** `hashed_features`: A list of hashed features.

**Output:** The root hash of the Merkle tree.

```
function create_merkle_tree(hashed_features)
    leaf_nodes = []
    for each hashed_feature in hashed_features do
        leaf_nodes.append(SHA256_Hash(hashed_feature))
    end for
    while length of leaf_nodes > 1 do
        parent_nodes = []
        for i = 0 to length of leaf_nodes - 2 step 2 do
            parent_hash = SHA256_Hash(leaf_nodes[i] || leaf_nodes[i+1])
            parent_nodes.append(parent_hash)
        end for
```

```
        leaf_nodes = parent_nodes
    end while
    return leaf_nodes[0]
end function
```

**Procedure:** record_hashed_feature

**Input:** `features_set`: A set of feature vectors.

**Output:** Transaction result of committing the Merkle root and certificate.

```
procedure record_hashed_feature(features_set)
    feature_hashes = []
    for each feature in features_set do
        feature_hashes.append(hash_feature(feature))
    end for
    merkle_root = create_merkle_tree(feature_hashes)
    certificate = CertificateAuthority.generate_certificate(merkle_root)
    tx_result = transaction_commit(merkle_root, certificate)
    return tx_result
end procedure
```

Procedure**:** **`verify_hashed_feature`**

**Input:**

- **`features_set`: A set of feature vectors.**
- **`merkle_root`: The root hash of the Merkle tree to be verified.**

**Output: A boolean value indicating whether the verification was successful (True) or not (False).**

```
procedure verify_hashed_feature(features_set, merkle_root)
    feature_hashes = []
    for each feature in features_set do
        feature_hashes.append(hash_feature(feature))
    end for
    new_merkle_root = create_merkle_tree(feature_hashes)
    if new_merkle_root == merkle_root then
        verify_hash = True
    else
        verify_hash = False
    end if
    return verify_hash
```

```
end procedure
```

Algorithm 3.6 presents a sophisticated method for authenticating and securely storing feature data within a blockchain system, utilising SHA256 for hashing and a Merkle tree for efficient data verification. The process begins with the **hash_feature** function, which takes a set of feature vectors as input. For each vector in this set, the algorithm converts it into a string format and concatenates these strings to form a single, comprehensive string. This string is then transformed into a byte array, preparing it for cryptographic processing.

SHA256 hash function is applied to this byte array, generating a unique hash value for each feature, ensuring the data's integrity and preventing collisions. The function returns a dictionary mapping the feature set's name to its hash.

The **create_merkle_tree** function comes into play, specifically designed to structure these hashed features into a Merkle tree. It starts by converting each hashed feature into a leaf node. Then, it iteratively combines pairs of these nodes and computes their parent nodes' hashes. This process continues up the tree, halving the number of nodes in each iteration, until it culminates in a single hash, known as the Merkle root. This root hash represents the entire set of features and is critical for verifying the integrity of the data in the blockchain.

The **record_hashed_feature** function procedure is responsible for recording the features in the blockchain. It first hashes the features using the **hash_feature** function and then constructs a Merkle tree from these hashes. A certificate is generated for the Merkle root, acting as a digital signature to authenticate the transaction. This certificate, along with the Merkle root, is then committed to the blockchain, ensuring the transaction's permanence and traceability.

Finally, the **verify_hashed_feature** procedure is employed to validate the authenticity and integrity of the features. It rehashes the feature set and reconstructs the Merkle tree to obtain a new Merkle root. This root is then compared with the original one stored in the blockchain. If they match, it confirms the data's integrity; if not, it indicates a potential alteration or inauthenticity.

In summary, Algorithm 3.6 effectively combines SHA256 hashing with Merkle tree construction to enhance the security and efficiency of feature authentication in blockchain systems. This approach ensures that the data is not only secure but also quick and efficient to verify, making it highly suitable for blockchain applications where data integrity and rapid verification are crucial.

**Algorithm 3.7:** Authentication Procedures with SHA256 and Merkle Tree

**Inputs:**

- A set $F=\{f_1,f_2,...,f_n\}$ be the set of feature vectors.

**Process:**

- Convert each $f_i$ into a string $s_i$ and then to bytes $b_i$.
- Convert each string $s_i$ into bytes $b_i$.
- Apply SHA256 hash: $h_i = SHA256(b_i)$.
- The final hash is $\boldsymbol{H = \oplus\ i = \frac{n}{i=1} h_i}$ (where $\oplus\oplus$ denotes concatenation and hashing of all feature hashes).

**Output:**

- $\textbf{Final Has H} = \textbf{SHA256}(\boldsymbol{h_1 \oplus h_2 \oplus ... \oplus h_n})$

1. **Hashed Features Authentication (SHA256):**
   - Let $F=\{f_1,f_2,...,f_n\}$ be the set of feature vectors.
   - Convert each $f_i$ into a string $s_i$ and then to bytes $b_i$.
   - Apply SHA256 hash: $h_i = SHA256(b_i)$.
   - The final hash is $\boldsymbol{H = \oplus\ i = \frac{n}{i=1} h_i}$ (where $\oplus\oplus$ denotes concatenation and hashing of all feature hashes).
2. **Blockchain-Based Image Encryption:**
   - Let $N_i$ be a node in the blockchain network.
   - A request $R_i$ from $N_i$ is processed if $R_i$ is valid and new.
   - For each valid $Ri$, metadata is hashed and signed: $H(R_i)=Hash\ (Sign(Metadata(R_i)))$.
   - The blockchain is updated by adding a new block $B_i$ containing $H(R_i)$.
3. **Authentication Using Merkle Tree:**
   - Given a set of hashed features $\{h_1,h_2,...,h_m\}$, construct a Merkle tree.
   - The Merkle root $M$ is computed by repeatedly hashing pairs of nodes until one root node remains: $M=MerkleRoot(\{h_1,h_2,...,h_m\})$.

**Combining these interpretations into a single framework:**

- Let $F$ represent the set of features and $R$ the set of requests in a blockchain network.

- For each feature $f_i$ in $F$, we compute $h_i = SHA256(f_i)$, and for each request $R_i$, we compute $H(R_i)$.
- Construct a Merkle tree using the hashes $\{h_1, h_{2,\ldots,} h_n\}$, obtaining the Merkle root $M$.
- For the blockchain process, each $H(R_i)$ is added as a block $B_i$ to the blockchain.
- The combined process involves the interaction of these individual steps: hashing features, constructing a Merkle tree, processing blockchain requests, and updating the blockchain with hashed data and Merkle roots.

---

By integrating Algorithm 3.4, Algorithm 3.5, and Algorithm 3.6, we've created a comprehensive Algorithm of 3.7 that amalgamates blockchain-based authentication, encryption, and data integrity processes. The core of this framework lies in the application of SHA256 hashing to feature sets (Algorithm 3.5) and the innovative use of Merkle trees for efficient and secure data verification (Algorithm 3.6). In essence, each feature in a given dataset is transformed into a unique hash using SHA256, ensuring data integrity and providing a basis for secure authentication. These hashes then form the leaf nodes of a Merkle tree, a data structure renowned for its efficiency in summarising and verifying large datasets. This Merkle tree construction is crucial for the framework, as it enables quick and secure verification of large data sets with minimal information exchange.

In tandem, we've incorporated the blockchain-based image encryption process (Algorithm 3.4), where each valid transaction or data request within the network is hashed, signed, and then added as a new block to the blockchain. This integration ensures that each piece of data is not only securely stored but also immutably recorded in a decentralised ledger. The combination of these algorithms results in a robust system that leverages the cryptographic strength of SHA256, the efficiency of Merkle trees, and the reliability of blockchains. This unified system is ideal for applications requiring high levels of data security, integrity, and traceability, such as in secure communications, digital identity management, and distributed data storage solutions.

## 3.6 Method IV: Video Blockchain Data Storing in Secure ways

In Method IV create on the process presented in Method III, it directly connects to Method IV. As extract and design in Method III Video Blockchain method. In Method IV use to make the data

storing method for Video Blockchain in secure ways. By addressing this method test Hypothesis 4. We are use of the cryptographic function name call block matrix to make the robust.

In the realm of intelligent surveillance, the integrity and confidentiality of video data are paramount. Our approach to achieving these in the context of Video Blockchain aligns with Hypothesis 4, focusing on the implementation of strategic methods to maintain data integrity. This subsection also links these strategies with the evaluation stage of the Design Science Research Methodology (DSRM).

The foundational aspect of our strategy is the integration of cryptographic functions with computational methods tailored for Video Blockchain. This approach not only bridges the technological gap between video frame capture and blockchains but also ensures the authenticity and reliability of the data captured.

A pivotal element in our system is the use of Merkle tree hashing functions. Each video frame, regarded as a transaction within the blockchain, is incorporated into a block that generates its Merkle tree. The root hash of these trees, once stored in the blockchain, provides a robust mechanism for verifying the integrity of each video frame. This technique allows for precise identification of any alterations in the video sequence, thereby maintaining the integrity of the surveillance data.

In our system, each video frame's hash is uploaded to a web interface designed to test the functionality of the blockchain application. This step is crucial in ensuring that each frame's hash can generate and update the entire blockchain chain, thereby maintaining data integrity across the system.

Our strategies for maintaining data integrity are closely tied to the DSRM's evaluation stage. The evaluation of our Video Blockchain system involves rigorous testing of the cryptographic methods and computational approaches employed. The Merkle tree hashing function, in particular, is a critical component of our evaluation process, as it enables us to assess the effectiveness of our strategies in real-time scenarios. The evaluation stage also includes analysing the system's capability to resist various types of attacks, thereby ensuring the confidentiality and integrity of the surveillance data. By meticulously testing and validating these aspects, our research contributes

significantly to the field of intelligent surveillance, offering robust and secure solutions for video data management within smart city environments.

Table 3.1:Video Blockchain Data Sorting with Block Matrix

| Steps | Description |
|---|---|
| **Frame Division into Blocks** | Divide frame F into n blocks, denoted as B1, B2, …, Bn. |
| **Block Compression** | Each block Bi is compressed to Bi′ using a JPEG compression algorithm. |
| **SHA256 Hashing** | Calculate the SHA256 hash for each compressed block: Hi = SHA256(Bi′) for i=1 to n. |
| **Merkle Tree Construction** | Construct a Merkle tree from the hashes H1, H2, …, Hn. Let Mi be the Merkle tree for frame F, with Merkle root Ri. |
| **Storing Block Matrix and Merkle Roots** | The matrix M = [B1′, B2′, …, Bn′] along with Ri is stored. |
| **Accessing a Specific Frame** | To access frame F, load M and Ri. Verify F by recomputing Mi and checking if Ri matches the recomputed root. |
| **Accessing a Specific Block within a Frame** | To access block Bi, retrieve Bi′ from M. Decompress Bi′ to get Bi. Verify Bi by checking if Hi = SHA256(Bi′) matches the corresponding hash in Mi. |

In Table 3.1, our methodology for ensuring data integrity in Video Blockchain encompasses a combination of advanced cryptographic techniques and computational methods. This approach not only addresses the technical requirements of intelligent surveillance systems but also aligns with the broader objectives and evaluation criteria set forth by the DSRM framework.

**Algorithm 3.8**: Block Matrix

**Input:** A video file consisting of frames.

**1**) Divide each frame into fixed-size blocks (16x16 pixels).

2) Store the blocks of each frame in a matrix, where each row represents a block, and each column represents a frame.

3) Apply compression algorithms (JPEG) to each block to reduce the amount of data.

4) Store the compressed block matrix as a binary file.

5) To access a specific frame, load the compressed block matrix and retrieve the corresponding column of blocks.

6) To access a specific block within a frame, retrieve the corresponding row of the block matrix and decompress the block.

---

In Algorithm 3.8, show how block matrix function takes in an array of data and a block size, and constructs a matrix where each row represents a block of data. The matrix is filled in by iterating over the data array, slicing it into blocks of the given size, and placing each block in the appropriate row of the matrix. If the length of the data array is not a multiple of the block size, the last row of the matrix will contain padding to fill out the remaining space. In the design of the Method 4 solution, it has connected with method 3 design. Below algorithm show how it connects with SHA256 and Merkle tree to make secure data storing of Video Blockchain,

---

**Algorithm 3.9**: Video Blockchain Data Sorting with Block Matrix

---

**Input**: A video file consisting of frames.

1. **Frame Division into Blocks:**
    - Let $F$ be a frame in the video.
    - Divide $F$ into $n$ blocks, denoted as $B1, B2, \ldots, Bn$.
2. **Block Compression:**
    - Each block $B_i$ is compressed to $'B_i'$ using a JPEG compression algorithm.
3. **SHA256 Hashing:**
    - Calculate the SHA256 hash for each compressed block:
        - $Hi = SHA256(B_i')$ for $i=1$ to $n$.
4. **Merkle Tree Construction:**
    - Construct a Merkle tree from the hashes $H1, H2, \ldots, Hn$.
    - Let $Mi$ be the Merkle tree for frame $F$, with Merkle root $Ri$.
5. **Frame Division into Blocks:**
    - Let $F$ be a frame in the video.

---

- Divide $F$ into $n$ blocks, denoted as $B1, B2, \ldots, Bn$.

6. **Block Compression:**
    - Each block $B_i$ is compressed to $'B_i'$ using a JPEG compression algorithm.
7. **SHA256 Hashing:**
    - Calculate the SHA256 hash for each compressed block:
        - $Hi = SHA256(B_i')$ for $i = 1$ to $n$.
8. **Merkle Tree Construction:**
    - Construct a Merkle tree from the hashes $H1, H2, \ldots, Hn$.
    - Let $Mi$ be the Merkle tree for frame $F$, with Merkle root $Ri$.
9. **Storing Block Matrix and Merkle Roots:**
    - The matrix $M = [B_1', B_2', \ldots, B_n']$ along with $R_i$ is stored.
10. **Accessing a Specific Frame:**
    - To access frame $F$, load $M$ and $R_i$.
    - Verify $F$ by recomputing $M_i$ and checking if $R_i$ matches the recomputed root.
11. **Accessing a Specific Block within a Frame:**
    - To access block $B_i$, retrieve $'B_i'$ from $M$.
    - Decompress $'B_i'$ to get $B_i$.
    - Verify $B_i$ by checking if $H_i = SHA256(B_i')$ matches the corresponding hash in $M_i$.

---

In Algorithm 3.9 the compression, hashing, and Merkle tree construction are conceptualised as functions applied to the blocks of the video frames. The integrity of each block and frame is ensured through the cryptographic strength of SHA256 and the efficient structure of the Merkle tree, making the algorithm suitable for secure video data processing and storage.

In the enhanced Block Matrix algorithm to store data in the Video Blockchain, which integrates SHA256 hashing and Merkle Tree construction, each frame of a video (denoted as $F$) is subdivided into a set of smaller, fixed-size blocks, labelled as $B_1, B_2 \ldots, Bn$. These blocks are then individually compressed using a JPEG algorithm, resulting in a set of compressed blocks $'B_1', B_2' \ldots, Bn'$. To ensure the integrity and security of these compressed blocks, each one is processed through the

SHA256 hashing function, generating a unique hash $H_i$ for every block $'B_i'$. These hashes serve as the leaf nodes of a Merkle tree a data structure that allows efficient and secure verification of large datasets. The construction of the Merkle tree culminates in a single hash at the top, known as the Merkle root $R_i$, which acts as a comprehensive integrity check for the entire frame $F$.

Algorithm 3.9 stores this data in a matrix format, with each matrix corresponding to a frame and containing its compressed blocks along with the frame's Merkle root. This method not only conserves space through compression but also attaches a reliable verification mechanism through the Merkle root. When accessing a specific frame from the video, the algorithm retrieves the corresponding matrix and the Merkle root, reconstructing the Merkle tree to verify the frame's integrity. If the recomputed Merkle root matches the stored one, the integrity of the frame is confirmed. Similarly, to access and verify a specific block within a frame, the block is decompressed and its SHA256 hash recalculated. This hash is then compared to the corresponding hash in the Merkle tree to ensure the block has not been tampered with.

In essence, this algorithm effectively combines the efficiency of JPEG compression, the cryptographic strength of SHA256 hashing, and the structural advantages of Merkle trees. This integration not only secures the data against tampering but also ensures efficient and reliable verification of both individual blocks and entire frames within a blockchain-based system.

## 3.7 Method V: Privacy Prevising with Video Blockchain

The proposed method for enhancing intelligent surveillance data integrity in smart cities involves using a Merkle tree, hashing function, and peer-to-peer data storage. The verification process detects changes in image frame order and identifies the specific image modifications. A Merkle tree is generated for each block, and its root is stored in the blockchain to ensure integrity. The experimental design utilises selected cryptographic algorithms, generating output from video frames to validate the blockchain implementation. An interface is designed to test functionality and address video frame-related issues.

The solution emphasises on lightweight functions for inter-block communication to enhance security and prevent attacks like man-in-the-middle interception. Selected cryptographic features create a robust mechanism for blockchain-based computing. The initial computational method incorporates connection hashing and block matrix functions for Video Blockchain, bridging gaps

between frames and improving security. However, adversaries may still estimate the amount of legal data, even with blocked public information equity for verification rate, hash value, and sibling path size.

This research establishes a connection between surveillance video footage and blockchains, storing the data in a decentralised repository. The main contribution is enhancing the security of observational data through the use of cryptographic algorithms for hashing and signature, distinguishing it from other works. These algorithms ensure accurate connection of video frames and enable detection and location of any frame changes. The verification procedure, using Merkle trees and hashing functions, further strengthens the security measures.

Furthermore, privacy-preserving problem exists in blockchain implementation (Casino & Patsakis, 2020; Fitwi & Chen, n.d.). We propose a blockchain-based solution for ensuring and improving the integrity of surveillance data in smart cities, aiming for increased loyalty, reliable results, and controlled disclosures. Combining computational approaches and Video Blockchain regulates data security, reducing unauthorised access. This enables close monitoring of law enforcement, insurance firms, and traffic management systems, facilitating necessary modifications for improved security and compliance in smart city video surveillance.

To verify frame integrity, a Merkle tree is constructed from the block matrix hash values. The Merkle tree's root hash is stored in the blockchain, allowing detection of any modifications by comparing block and Merkle tree hashes. This tamper-resistant approach enhances system security.

In addition, block matrix operations (Zhu et al., 2023), such as matrix multiplication and matrix inverse, can be employed for video processing tasks, such as compression, filtering, and restoration. These operations can be performed on the block matrices stored in the blockchain, which allows for highly efficient and secure video processing.

Overall, storing video frames in a blockchain-based system using block matrices provides a secure and efficient method for video storage. The use of hash values, Merkle trees, and block matrix operations enhances the tamper-resistance, integrity, and reliability of the system.

In this implementation, the Merkle Tree function takes in an array of data and recursively constructs a Merkle tree. In the base case, when there is only one data item left. The function

returns the data item itself. Otherwise, it recursively constructs the left and right subtrees, hashes them together using SHA-256 algorithm, and returns the resulting hash. The resultant hash is the root of Merkle tree.

---

**Algorithm 3.10:** Privacy Prevising with Video Blockchain implementation

---

**Input:**

- None (the generation process typically relies on the cryptographic parameters of the system).

**Process:**

- Generate a private key $sk \in G$(where G is a group used in the cryptographic system).
- Compute the public key $vk = g^{sk}$ (where g is a generator of the group G)

1. **Key Generation (G′):**
   - Private Key: $sk \in G$
   - Public Key: $vk = gsk$
2. **Signing (S′):**
   - Input Message: $m$
   - Random Value:$b \in \mathrm{Z} \mid G \mid$
   - Intermediate Value:$u = gb$
   - Hash Calculation: $a=H(u, m)$
   - Signature:$(a \cdot sk + b) \mathrm{mod} q$
   - Signature Output: $(a, s)$
3. **Verification (V′):**
   - Input: $m$ and $(a, s)$
   - Intermediate Value: $u' = gs \cdot vk - a$
   - Hash Recalculation: $a' = H(u', m)$
   - Validation: If $a'=a$, then the signature is valid; otherwise, it's invalid.

---

Algorithm 3.10 described is a digital signature scheme, which ensures the privacy and integrity of a message. It consists of three main phases: Key generation, signing, and verification. In the

key generation phase $G'$, a pair of cryptographic keys is generated: a private key $sk$, known only to the signer, and a public key $vk$, derived from the private key using a generator $g$ of a cryptographic group $G$, which can be shared openly. During the signing phase $S'$, the signer creates a digital signature for a message mmm by selecting a random value $b$ from the group, computing an intermediate value $u$ as $g$ raised to the power of $b$, and calculating a hash $a$ of the intermediate value and the message. The signature ($a$, $s$) is then created, where $s$ is derived from the private key, the hash $a$, and the random value $b$, proving that the message was signed by someone possessing the private key. In the verification phase $V'$, the recipient checks the validity of the signature by using the signature ($a$, $s$) and the public key $vk$ to compute an intermediate value $u'$, recalculating a hash $a'$ using $u'$ and the message mmm. The signature is valid if the recalculated hash $a'$ matches the hash $a$ from the signature, confirming that the message was signed by the owner of the private key and has not been altered.

This digital signature scheme ensures that a message m is authentic and has not been tampered with. The private key $sk$ is used to sign the message, while the public key $vk$ is used to verify the signature. The use of cryptographic hashes and group operations provides security, making it computationally infeasible to forge signatures without the private key.

### 3.7.1 Security Metrics and Standards

In the domain of computational methods for Video Blockchain in intelligent surveillance, the evaluation of security is pivotal. The metrics and standards adopted for this assessment are intricately aligned with DSRM, specifically within the evaluation stage of the developed system. These metrics, which encompass a broad range of security aspects like data encryption strength, hashing algorithm efficiency, and system resilience to cyber-attacks, are essential for ensuring the robustness of the Video Blockchain system.

Given the critical nature of intelligent surveillance data, especially in smart city contexts, the security standards adhere to stringent industry benchmarks. These include compliance with international cybersecurity protocols and encryption standards (Li et al., 2020), ensuring that the Video Blockchain system meets the highest levels of data protection. This approach not only safeguards the integrity of the surveillance data but also enhances the trustworthiness of the system among stakeholders.

In the key generation phase *G′,* given a cryptographic group *G* with a generator *g*, *a* private key $sk$ is randomly generated from the group *G*. This private key is kept secret and used for signing messages. The corresponding public key *vk* is computed as $vk = g^{sk}$ and is made publicly available for signature verification. In the signing phase *S′*, for a message *m* to be signed, a random value *b* is generated from the integers modulo the order of the group *G*. An intermediate value u is computed as $g^b$. The hash function *H* is applied to *u* and the message *m*, resulting in $a = H(u, m)$.The signature component s is calculated as $s = a.ak + b\ mob\ q$, where *q* is the modulus of the group *G*. The resulting signature *(a, s)* is output for use in the verification process. In the verification phase *(V′),* given a message *m* and *a* signature *(a, s)*, the public key *vk* is retrieved. An intermediate value u′ is computed as $g^s.vk^{-a}$. The hash function *H* is applied to $u'$ and the message *m*, resulting in a′ $= H(u', m)$.The signature is deemed valid if $a'$ is equal to *a*; otherwise, it is considered invalid.

This signature scheme is important for ensuring the integrity and authenticity of messages transmitted over the blockchain, particularly in the context of transmitting sensitive surveillance data. The use of a hash function with collision resistance ensures that it is computationally infeasible to find two different messages that produce the same hash, thereby reinforcing the security of the signature scheme. The algorithm is designed to be secure against various cryptographic attacks, making it suitable for applications that require high levels of data security and integrity.

## 3.7.2 Data Protection

The techniques employed in the thesis for data protection within the Video Blockchain system are a testament to the meticulous design and development phase of the DSRM. These techniques are not just about encrypting data but also about ensuring its integrity from the moment of capture through to its storage and eventual analysis. They involve the utilisation of advanced cryptographic algorithms, specifically tailored for video data, and the integration of blockchains to create a secure and immutable ledger of surveillance footage.

The combination of these techniques addresses the potential vulnerabilities in traditional surveillance systems, which often include risks of data tampering or unauthorised access. By embedding these advanced data protection methodologies into the design of the Video Blockchain system, the research directly contributes to the enhancement of security measures in intelligent

surveillance. This integration not only ensures the confidentiality and integrity of the data but also aligns with the broader objectives of DSRM to create artifacts that are both innovative and pragmatically secure.

## 3.8 Method VI: Interdisciplinary Approaches with Video Blockchain

In these approaches we are testing our implementation feasibility to address the different type of empowerment to address the unit solution. It ensures the system robustness with the different actors like IoT, AI and ML functions. In here we try to test the feature connection with IoT and AI generated video detection misinformation detection functions.

### 3.8.1 Video Privacy in IoT Networks with Video Blockchain

The pivotal element in our system is the implementation of the Merkle Tree function. This function takes an array of data and recursively constructs a Merkle tree algorithm 3.6. In the base case, where only one data item remains, the function simply returns the data item itself. However, in all other cases, it constructs both the left and right subtrees, hashes them together using the SHA-256 algorithm, and returns the resulting hash, which ultimately becomes the root of the Merkle tree.

**Algorithm 3.11**: Compresence data in to the data blocks in the chain

**Input**: A list of data blocks.

1) Break down the data blocks into consistent fixed-size chunks, typically ranging from 1 to 2KB.
2) Utilise a cryptographic hash function to calculate the hash for each data chunk
3) Form pairs of neighbouring data chunk hashes and compute the hash for each pair.
4) Iterate through step 3 until only one hash remains, representing the Merkle root hash.
5) Save the Merkle root hash as the distinctive identifier for the data blocks.

In Algorithm 3.11, the process of constructing a Merkle Tree involves breaking down data blocks into consistent fixed-size chunks, denoted as $D_i = [C_{i1,}C_{i2}, \ldots . C_{in}$ For each chunk $C_{ij,}$ a cryptographic hash $H(C_{i1)}$ is computed, resulting in a list of hashes $H_i =$

$[H(C_{i1})\, H(C_{i2})$ ,….,H($C_{in}$). Next, pairs of neighbouring data chunk hashes are concatenated and hashed together to form new hashes $P_{ij} = H(H_i[j]\#H_i[j+1])$ This pairing and hashing process is repeated iteratively, reducing the number of hashes in each iteration, until only one hash remains. The final single hash, derived from all previous pairs, is known as the Merkle root hash Merkle RootHash $=$ $P_{final}$ .This root hash uniquely represents the entire set of data blocks, ensuring data integrity and consistency.

**Algorithm 3.12**: Block Matrix Process to secure the IoT video data

**Input:** A video file consisting of frames.

Divide each frame into uniform blocks of 16×16 pixels

Let $F_i$ be the i-th frame of the video

$$\boldsymbol{F_i = \left\{B_{i,j,k}: 1 \le i \le \frac{M}{16}, 1 \le k \le \frac{N}{16}\right\}} \quad (3.1)$$

where $B_{i,j,k}$ is the $j,k-th$ 16x16 block in frame $F_i$, and M×N is the frame resolution.

Arrange the blocks from each frame into a matrix format, with rows indicating blocks and columns denoting frames.

Let $B_{j,k}$ be the matrix of blocks for all frames.

$$\boldsymbol{B_{j,k} = \{B_{i,j,k}: 1 \le i \le n\}} \quad (3.2)$$

where $n$ is the number of frames.

Apply compression techniques (e.g., JPEG) to each block for data size reduction. $Let\ C(B_{i,j,k}\ be\ the\ compression\ function\ applied\ to\ block\ B_{i,j,k}.)$

$$\boldsymbol{C_{i,j,k} = C(B_{i,j,k})} \quad (3.3)$$

where $C_{i,j,k}$ is the compressed version of block $B_{i,j,k}$ )

Store the resulting compressed block matrix in a binary format.

Let $M_c$ be the compressed block matrix.

$$\boldsymbol{M_C = \left\{C_{i,j,k}: 1 \le i \le n, 1 \le j \le \frac{M}{16}, 1 \le k \le \frac{N}{16}\right\}} \quad (3.4)$$

Store $M_C$ in binary format.

To retrieve a specific frame, load the compressed matrix and select the appropriate column of blocks.
Let $Fi'$ be the retrieved frame.

$$\boldsymbol{F_i = \left\{C_{i,j,k}: 1 \le i \le \frac{M}{16}, 1 \le k \le \frac{N}{16}\right\}} \quad (3.4)$$

To access a particular block within a frame, locate and decompress the corresponding row from the matrix.

Let $D(C_{i,j,k})$ be the decompression function applied to block $C_{i,j,k}$.

$$\boldsymbol{B_{i,j,k} = D(C_{i,j,k})} \quad (3.6)$$

where $B_{i,j,k}$ is the decompressed version of block $C_{i,j,k}$

---

The process of transforming a video file into a block matrix involves several steps that ensure efficient data storage and retrieval. Initially, each frame of the video is divided into 16x16 pixel blocks. These blocks are then arranged into a matrix, where each row represents a block, and each column represents a frame. Next, compression techniques, such as JPEG, are applied to reduce the size of each block. The resulting compressed block matrix is stored in a binary format. To retrieve a specific frame, the corresponding column of blocks from the compressed matrix is selected. Similarly, to access a particular block within a frame, the relevant row is located and decompressed from the matrix. This method facilitates efficient storage, compression, and retrieval of video data.

## 3.8.2 AI-Generated Video Misinformation Detection with Video Blockchain

AI has more powerful with-it new implementation now days, as a result of it impact to the video files manipulating has become more vulnerable area to be address by using effective solutions. In the area of blockchain has solution with its resistance to vital attacks. In this scenario we are using

our Video Blockchain method with cryptographic functions. As we define *V* as the input video composed of frames *Fa* where a range from 1 to *b*, with b being the total number of frames in the video. Each frame *Fa* is divided into blocks of size *p*×*p* times *p*×*p* pixels. In this thesis, we choose an 16 × 16 block. This division results in q blocks per frame. The function to represent a block of the *a-th* frame at position $\boldsymbol{c}$ is:

$$\boldsymbol{B\_ac = Block(F\_a, c) for\ a \in [1, b]\ and\ c \in [1, q]} \tag{3.7}$$

We store these blocks in a matrix *N*, we extracted details on how the blockchain data structure operates in conjunction with the Merkle tree. In the future, we will further examine the video frame securing method of the Block Matrix algorithm and explore how it works with the Merkle tree to achieve our desired outcomes.

**Algorithm 3.13:** Block Matrix for partition each frame into fixed-size

**Input**: A video file consisting of frames

1) Partition each frame into fixed-size blocks (16x16 pixels).
2) Organize the blocks of each frame into a matrix, where rows represent blocks and columns represent frames.
3) Employ compression algorithms (such as JPEG) on each block to reduce data size.
4) Save the compressed block matrix as a binary file.
5) For accessing a particular frame, load the compressed block matrix and extract the corresponding column of blocks.
6) To access a specific block within a frame, retrieve the relevant row from the block matrix and decompress the block.

The Block Matrix algorithm involves several key steps. Initially, each frame of a video file is divided into fixed-size blocks (16×16 pixels), creating a frame sequence:

$$F_i = [B_{i1}, B_{i2}, \ldots, B_{in}] \tag{3.8}$$

These blocks are then organized into a matrix $\mathbf{M}_i$ where each row represents a block of the *i-th* frame. Compression algorithms, such as JPEG, are applied individually to each block, resulting in a compressed form $\boldsymbol{C}_{ij}$ for the *j-th* block in the *i-th* frame. The compressed block matrix is subsequently saved as a binary file using an appropriate method. When accessing a specific frame,

the binary file is loaded, and the corresponding column of blocks is extracted. To access a particular block within a frame, the relevant row is retrieved from the block matrix, and the block is decompressed using the algorithm's specified decompression function. These steps collectively define the Block Matrix algorithm, facilitating efficient storage and retrieval of video data. The block matrix Algorithm 3.13 function takes in an array of data and a block size and constructs a matrix where each row represents a block of data. The matrix is filled in by iterating over the data array, slicing it into blocks of the given size, and placing each block in the appropriate row of the matrix. If the length of the data array is not a multiple of the block size, the last row of the matrix will contain padding to fill out the remaining space. On the other hand, this implementation can use with the detect the AI generated video deification process. It led to identified the altered video files to spread the misinformation.

**Algorithm 3.14:** Detection of AI-Generated Video Misinformation

**Input:** A video file V consisting of frames.

**Output:** A binary value indicating whether the video is likely to be AI-generated misinformation (1) or authentic content (0).

**Step 1: Block Matrix Formation**

- Divide each frame of the video into fixed-size segments (16×16 pixels).
- Organize the segments from each frame into a matrix, where each row corresponds to a segment and each column corresponds to a frame.
- Compress the segments using a suitable algorithm (such as JPEG) to reduce their size.
- Store the resulting compressed matrix as a binary file for further processing

**Step 2: Super-bit LSH Bucketization**

1. **Generate a Super-bit structure S** by calling a function designed for this purpose.
2. **Iterate through the dataset records**:

For each record, calculate the hash values using the Super-bit structure:

$$h_i = ComputeHashesRecord(\pi, S)$$

**Assign the calculated hashes** to appropriate buckets:

$$H = MapSignatures(h_1, h_2, \ldots . h_p, S)$$

**Step 3: Detection and Analysis**

1. Examine the compressed block matrices and the hashed bucket mappings to identify patterns or anomalies that may indicate AI-generated content.
2. Apply machine learning or statistical methods to classify the video. The classification should determine whether the video is likely to be AI-generated misinformation or genuine content based on the analysis.

---

Algorithm 3.14 shows in detail, how to use Video Blockchain function involved in the AI generated video detection method implementation. The process begins with dividing each frame of the video into fixed-size segments (16×16 pixels). These segments are organised into a matrix where each row represents a segment and each column represents a frame. To reduce their size, the segments are compressed using a suitable algorithm such as JPEG. The resulting compressed matrix is then stored as a binary file for further processing. A Super-bit structure $\boldsymbol{S}$ is generated by calling a function specifically designed for this purpose. As the dataset records are iterated through, hash values for each record are calculated using the Super-bit structure. These hashes $h_i$ are then assigned to appropriate buckets through the mapping of signatures, denoted as $\boldsymbol{H}$. The final step involves examining the compressed block matrices and the hashed bucket mappings to identify any patterns or anomalies that could indicate AI-generated content. Machine learning or statistical methods are applied to classify the video, determining whether it is likely to be AI-generated misinformation (outputting a binary value of 1) or genuine content (outputting a binary value of 0) based on the analysis. This method result will elaborate in the chapter 4 and where its shows positive outcome that ensure our main implementation useful solutions widely.

## 3.9 Chapter Summary

In concluding, it is pivotal to underscore the harmonious integration of Design Science Research Methodology (DSRM) with a mixed methods approach. This amalgamation is not merely a methodological choice but a strategic one, aimed at navigating the multifaceted nature of our research terrain that combines cutting-edge blockchain with the complexities of intelligent surveillance. The DSRM framework, known for its iterative and reflective nature, has been instrumental in enabling a dynamic and responsive research process. This iterative approach has

been particularly effective in refining the technological components, ensuring that they align seamlessly with the specific requirements and objectives of Video Blockchain in surveillance. Moreover, the mixed methods approach has afforded a dual lens: quantitative methods providing empirical rigor and measurable outcomes, while qualitative techniques offer depth, contextual understanding, and insights into practical applications. The synergy between these methodological approaches enhances the robustness and relevance of our research, ensuring it remains not only academically sound but also pragmatically significant. As this research unfolds, the iterative nature of DSRM has continually allowed for adjustments and refinements, reflective of the evolving technological landscape and the emerging needs of intelligent surveillance systems in smart city environments. In projecting the potential impact of this research, it is anticipated that the findings will significantly contribute to the advancement of intelligent surveillance systems.

# Chapter 4 - Experimental Results

*We research into the critical phase of our research, where the theoretical concepts and methodologies outlined in previous chapters are empirically tested and assessed. This chapter is dedicated to presenting the findings derived from our rigorous experiments and analyses.*

*We systematically evaluate the outcomes of the implementation strategies and techniques utilised in our study, particularly focusing on how these align with the hypotheses set forth in earlier discussions. This chapter serves as the cornerstone of our research, providing a detailed exposition of the results obtained and their implications within the scope of blockchain in intelligent surveillance.*

*The evaluation not only tests the validity of our hypotheses but also offers insightful reflections on the effectiveness, challenges, and limitations of our approaches. It is in this chapter that the theoretical meets the practical, and the real-world applicability of our research is scrutinised. Through a comprehensive analysis, Chapter 4 aims to contribute meaningfully to the existing body of knowledge and set the stage for future innovations in the field.*

## 4.1 Introduction

Chapter 4 explores the evaluation of solutions identified in Chapter 2 and Chapter 3, which highlighted the research gaps, setting the stage for the research questions and hypotheses outlined in Chapter 3. Here, we present our evaluation approach for the proposed Video Blockchain computation method, a comprehensive solution integrating blockchain principles with video processing techniques. The primary objective is to bolster security, authenticity, and efficiency in managing video data.

Central to this method is the incorporation of a blockchain layer within the video processing framework. This integration enables the encryption and storage of each video frame or segment as a distinct block within the blockchain, thus ensuring the data's integrity and origin verification, maintaining its security and tamper-proof nature.

This chapter also scrutinises the computational demands of this method. Processing high-resolution video data necessitates substantial computational resources. By utilising blockchain's distributed nature, computational tasks are shared across multiple nodes, enhancing the system’s effective and efficient.

Further, we discuss the challenges and limitations inherent in implementing the Video Blockchain Computational method. These include managing increased storage demands due to blockchain integration and balancing encryption strength with video quality. Solutions to these challenges are proposed, setting a foundation for ongoing research and development in this area.

The method employs a private blockchain, crucial for initiating testing phases and assessing its functionality. This approach enables the feasibility testing of various hypotheses and validation of the implementation. A controlled environment, provided by the private blockchain, is essential for initial testing, allowing variable manipulation and outcome observation in a secure, isolated setting, vital for method validation.

The key focus areas during this phase include the integration of video data with blockchains, ensuring secure and accurate recording of each video frame in the blockchain ledger, and assessing the efficiency of data retrieval and validation processes. The system's capability to swiftly and accurately verify video data authenticity and integrity is vital for practical applications.

Potential scalability issues are also addressed. As video data volume increases, the blockchain system must sustain the load without performance compromise. This involves optimising blockchain data storage and maintaining system responsiveness as it scales.

Additionally, the system's resilience against security threats, like unauthorised access and data tampering, is rigorously tested. The private blockchain's security mechanisms are evaluated to ensure robust protection.

Finally, this chapter presents the test outcomes, analysing the Video Blockchain computation method's strengths and weaknesses. The data and insights from these tests validate our approach's feasibility and provide a basis for future enhancements and broader applications. By the conclusion of this chapter, readers will have a thorough grasp of the Video Blockchain computation method's functionality, potential impact, and future development and deployment prospects.

The result evaluation environment used the private blockchain development to test~~ing~~ our methods. In the comparison of (Polge et al., 2021) show that what are the permissioned blockchain farmwork can use for industry focus research, also in the research of the (Bhardwaj et al., 2021) has be utilised the feature of the private blockchain it implements and testing the file authentication ownership implementation. Base one this researches it gave the clear view of which one of this research. In finale in the research of (R. Yang et al., 2020) extract the how to public and private blockchain use to construct the blockchain base information integration implementation. Based on these details our research implementation is based on the private blockchain.

Our implementation involved a private blockchain system developed with a blend of programming languages, including PHP, Python, Golang, and JavaScript. This system was pivotal for advancing private blockchain technologies. The entire process was operationalised on a Microsoft Windows 11 Pro 64-bit platform, ensuring compatibility and performance efficiency.

Our experimental setup was comprehensive and designed to rigorously Within the smart city framework, we assess the resilience of our innovative technique against a variety of cyber threats. This was crucial for evaluating the robustness of our blockchain approach and for developing new computational techniques tailored specifically for Video Blockchains. These techniques integrated selected cryptographic algorithms for smart city environments, utilising the core principles of

Video Blockchains demonstrating a novel approach to video data protection, especially in surveillance systems.

The research significantly contributes to the field of Video Blockchain by presenting a unique method for safeguarding video data. It sets a new standard in the integration and application of cryptographic algorithms within Video Blockchain.

Furthermore, our study's outcomes are poised to become a foundational reference in future research and development in Video Blockchain and cryptographic algorithms. This work advances knowledge in these fields and establishes new benchmarks for the security and efficiency of video data management, particularly in surveillance and related applications.

Cryptographic algorithms play a pivotal role within the realm of Video Blockchain. Furthermore, the outcomes of our study are set to serve as a fundamental reference point for future research and development in the domains of Video Blockchain and cryptographic algorithms. This research contributes significantly to the advancement of knowledge in these areas, setting new standards for the security and efficiency of managing video data, especially in surveillance and related applications.

As outlined in Section 3.5.2, our dataset and data collection process have been meticulously executed. This section delves into the details of how we prepared our dataset for the experimental setup. In our experimental framework, we carefully converted captured video content into discrete frames, each varying in size from 50 KB to 1024 KB. The videos for this research were recorded at speeds of up to 50 fps, thereby enriching the content for our experiments. Specifically, we utilised sample videos from Auckland city to compile our dataset. From each 30-minute video, we extracted a comprehensive collection of 7000 video frames from a 5-minute segment, providing a robust and extensive dataset for our research endeavours.

## 4.2 Find best Cryptographic Function

In this section, we explore into the outcomes obtained from our research while addressing the major research questions and hypotheses posed. Section 4.1 serves as an introduction to this chapter, laying the groundwork for the discussions that follow. In subsection 4.1.1, we provided a comprehensive overview of the testing environment and the data utilised in generating the

experimental results. Continuing in this vein, Section 4.2, titled 'Experimental Results,' is dedicated to a detailed presentation and analysis of the findings from our experiments.

Therefore, we systematically unpack the data, correlating it with our hypotheses and illuminating the implications of our findings. This section is crucial as it not only validates our research methodology but also provides critical insights into the effectiveness and impact of the proposed solutions. Through a careful examination of the results, we aim to shed light on the advancements made in the field and the potential applications of our work. The arrangement of this section is designed to guide the reader through a logical progression of our research journey, from hypothesis formulation to experimental validation and, ultimately, to the conclusions drawn from our findings.

In the context of Video Blockchain, the choice of cryptographic functions is paramount for establishing a secure and efficient Video Blockchain system.

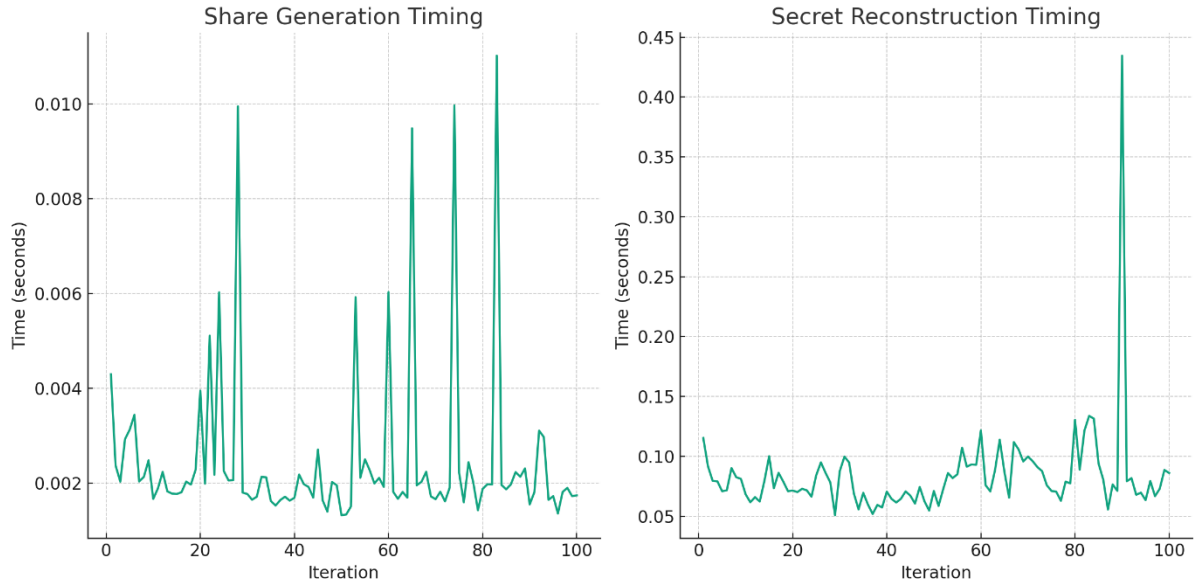


Figure 4.1: Shamir's Secret Sharing Scheme performance calculation

The Figure 4.1 represents two time-series sequences, where each point corresponds to the time taken for a specific iteration of cryptographic operations: Share Generation and Secret Reconstruction in Shamir's Secret Sharing Scheme. Mathematically, if we let $Tg(i)$ denote the time for share generation on the $i$-th iteration, and $Tr(i)$ denote the time for secret reconstruction on the

*i*-th iteration, the plot depicts *Tg*(*i*) and *Tr*(*i*) for *i* ranging from 1 to 100. The plots exhibit variability, suggesting that the time complexity for each operation can fluctuate due to factors like computational overhead or varying input sizes. Peaks in the Secret Reconstruction Timing graph indicate iterations where the reconstruction process took significantly longer, possibly due to more complex input or system resource constraints during those instances.

The performance evaluation for Shamir's Secret Sharing Scheme with a reduced iteration count (100 iterations) has been successfully executed. The plots show the timings for each operation:

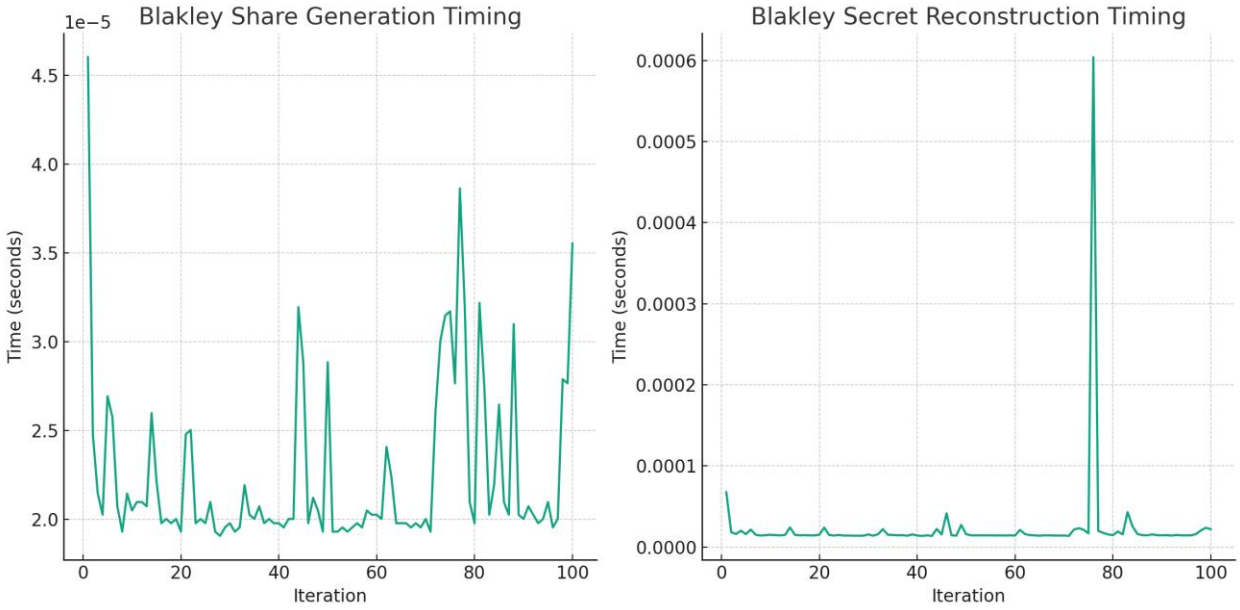


Figure 4.2: Blakley's Scheme performance evaluation (Generation and Reconstruction Timing)

Figure 4.2 plots illustrate the performance of Blakley's Secret Sharing Scheme across 100 iterations, capturing the time for share generation and secret reconstruction. The left graph, detailing share generation times *Tgen*(*i*) for iteration *i*), shows some variability with a general baseline, punctuated by occasional spikes which may indicate computational or procedural inconsistencies. The right graph plots secret reconstruction times (*Trec*(*i*)), which are consistently low, save for a few outliers. These outliers may result from computational load or algorithmic complexity during those iterations. Overall, the graphs suggest that while share generation has a higher time complexity, secret reconstruction is typically faster but can be subject to sporadic delays.


Figure 4.3: Performance evaluation of Fiat Shamir Scheme (Secret-Sharing)

*(*Fiat Shamir *Key Generation Timing,* Fiat Shamir *Commitment Timing,* Fiat Shamir *Response Timing and* Fiat Shamir *Verification Timing)*

Figure 4.3 represents the timings of different phases in the Fiat-Shamir identification scheme over 100 iterations. The top-left plot shows the key generation phase, where the time taken is quite stable across iterations, indicating a consistent computational demand. The top-right plot illustrates the commitment phase, revealing slight fluctuations but generally maintaining a steady average time, which suggests the random number generation and squaring operations required are fairly uniform in execution time.

The bottom-left plot depicts the response timing, where there is notable variability in the data, hinting at possibly non-uniform computational tasks or varying system resources at different iterations. Lastly, the bottom-right plot, which captures the verification timing, also shows variability, with occasional peaks that could be due to the computational intensity of modular exponentiations or system performance variations at those points.

The graphs illustrate the time complexity functions of different phases in the Fiat-Shamir scheme across multiple iterations. For the key generation phase, the time function $K(i)$ demonstrates a stable behaviour with low variance $(\sigma\frac{K}{2})$ , evidenced by the consistent times near a small mean ($\mu K$). This suggests a predictable computational load, likely due to the deterministic nature of the key generation process.

The commitment phase time function $C(i)$, while also showing stability, presents a slightly higher mean ($\mu C$) and variance, indicating a moderate computational load and some fluctuation in execution time, possibly influenced by the random number generation.

The response time function $R(i)$, exhibiting significant fluctuation and a higher variance $(\sigma\frac{K}{2})$ suggests a higher sensitivity to computational or environmental factors, perhaps due to the dynamic interaction between random number generation and the arithmetic operations required.

Finally, the verification phase time function $V(i)$ shows a similar fluctuation pattern to $R(i)$, with a variance $(\sigma\frac{K}{2})$ that indicates non-trivial computational effort, such as modular exponentiations, which may be more affected by varying processor loads or other system activities.

Mathematically, these functions could be exhibited as $K(i) = \mu K + \epsilon Ki, C(i) = \mu C + \epsilon Ci$ , $R(i) = \mu R + \epsilon Ri,$ and $V(i) = \mu V + \epsilon Vi,$ where $\epsilon$ represents a random error component at iteration $i$. The spikes in $R(i)$ and $V(i)$ represent instances where $\epsilon$ was significantly higher than average, indicating outlier computations with unexpected complexity or delay.

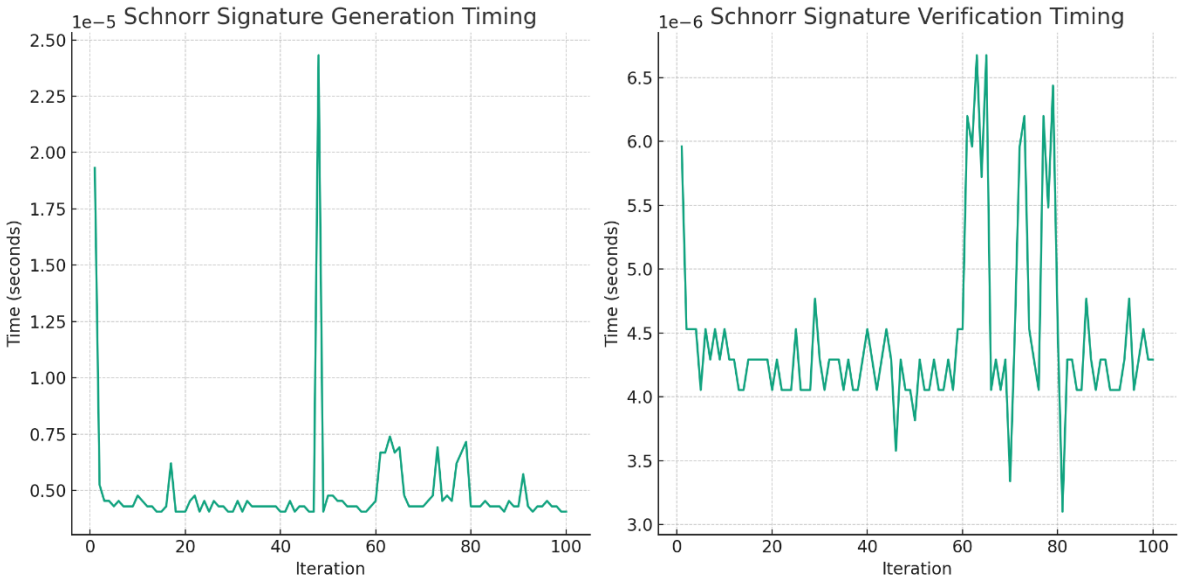


Figure 4.4: Performance evaluation of Schnorr Signatures

Figure 4.4 displays the timing data for two primary operations in the Schnorr signature cryptographic protocol: signature generation and verification, across 100 iterations. The left plot, pertaining to signature generation, shows a relatively stable performance with a few prominent spikes. This suggests that while the computational process for generating a signature is generally consistent, certain iterations may encounter increased processing time, possibly due to the random number generation or momentary system load.

The plots present the performance of the Schnorr signature protocol through two functions, $G(i)$ and $V(i)$, representing the time taken for signature generation and verification, respectively, across $n$ iterations, where $i$ is the iteration index.

For signature generation, $G(i)$ appears to follow a distribution with a relatively low mean $\mu g$ and a small standard deviation $\sigma_{g,}$ indicating consistent performance. However, occasional outliers suggest that $G(i)$ can experience deviations, likely due to operations such as non-deterministic random number generation or variable computational load, which can be modelled as $G(i)=\mu_g+\epsilon_{gi}$ , where $\epsilon_{gi}$, is the random error at iteration $i$.

In contrast, signature verification times $V(i)$ exhibit a higher mean $\mu_v$ and standard deviation $\sigma v$ , which can be observed through the wider spread of data points. The function $V(i)$ could be expressed as $V(i)=\mu_v+\epsilon_{vi}$, where $\epsilon_{vi}$ represents random error, which is larger than $\epsilon gi$, indicating that

verification times are more susceptible to fluctuations, potentially due to the complexity of cryptographic computations like modular exponentiations or hash function evaluations.

The presence of spikes in both $G(i)$ and $V(i)$ could indicate transient computational or algorithmic inefficiencies. These spikes are the values of $G(i)$ and $V(i)$ that significantly exceed $\mu_g$ and $\mu_v$, respectively, and can be analysed using higher moments like skewness and kurtosis to understand the tails of the distribution of $G$ and $V$.

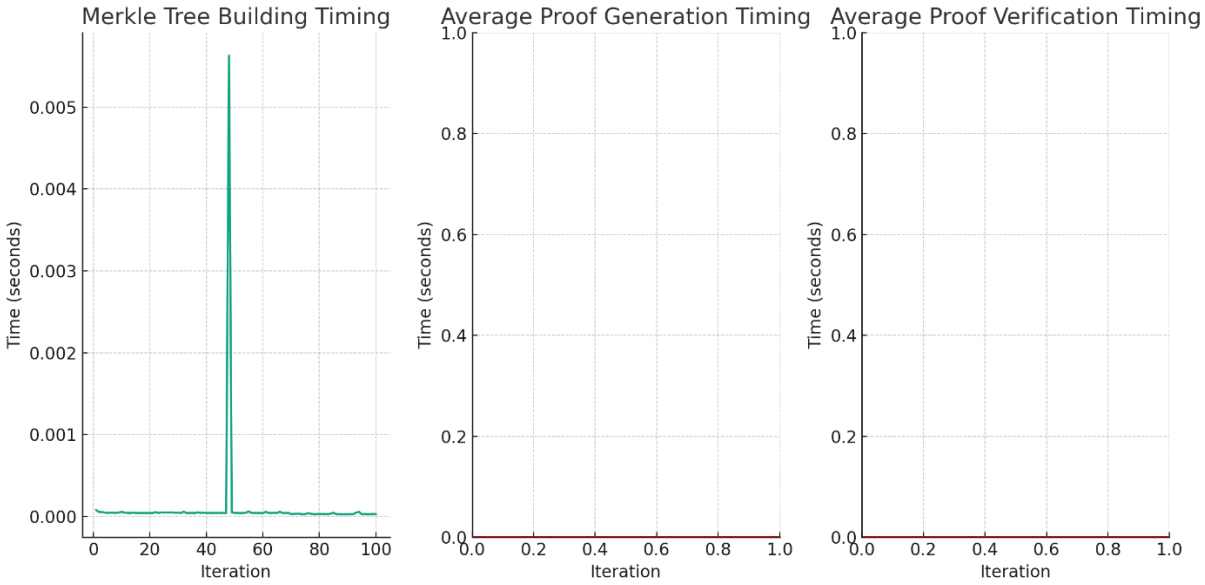


Figure 4.5:Performance evaluation of Merkle Tree

These plots in the Figure 4.5 provide insights into the computational efficiency of each step in the construction and usage of a Merkle Tree. The building timing reflects the complexity of hashing and combining the data blocks, while the proof generation and verification timings demonstrate the efficiency of proving and verifying the inclusion of a specific transaction (or data block) in the Merkle Tree.

Merkle Trees are fundamental in blockchains and other systems where efficient and secure verification of large data sets is required. The performance characteristics shown here are indicative of the system's capabilities where the code is executed, and the actual timings may vary based on the size of the data and the hardware used

The given plots can be interpreted using mathematical functions representing the computational time for operations in a Merkle Tree. Let $B(i)$ denote the time taken to build the Merkle Tree at the

$i$-th iteration, where $i \in \{1, 2, \ldots, n\}$ for $n$ iterations. The plot of $B(i)$ is mostly consistent but shows a significant outlier, which suggests that $B(i)$ generally has a low mean time $\mu_B$ but may have instances of high computational time due to factors like increased data size or processing load during hashing.

The proof generation and verification times can be represented as constant functions, $G = C_g$ and $V = C_v$ respectively, since they are depicted as horisontal lines in the plots. This indicates that the average times for these operations are constant over the iterations sampled. The plot does not provide individual timings per iteration but rather the average across all iterations, denoted by $C_g$ for proof generation and $C_v$ for proof verification.

The presence of spikes in $B(i)$ could be mathematically analysed by examining the variance $\sigma \frac{B}{2}$ and skewness to understand the distribution of build times. If the spike is a true outlier, it would contribute to a high skewness in the distribution of $B(i)$.

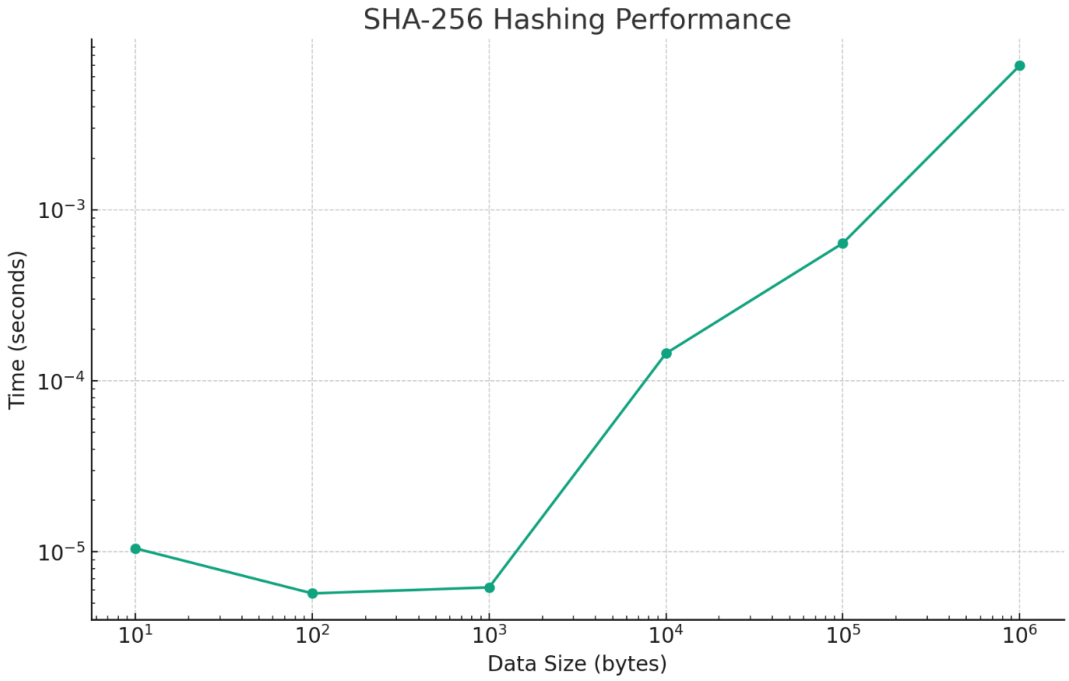


Figure 4.6: Performance evaluation of SHA 256

Figure 4.6 demonstrates how the time taken to compute a SHA-256 hash scales with the size of the input data. SHA-256 is designed to be relatively fast and efficient, and the time to hash

generally increases linearly with the size of the data. The logarithmic scale helps to visualise this relationship across a wide range of data sizes.

The actual hashing time will depend on various factors such as the system's performance, the programming language, and its implementation of the SHA-256 algorithm. The results shown here are specific to the conditions under which this test was run.

The plot provided appears to show the time taken to hash data using the SHA-256 algorithm as a function of data size. The plot is on a logarithmic scale on both axes, indicating exponential growth. Mathematically, the relationship can be described by a function $H(s)$, where $s$ represents the size of the data, and $H(s)$ is the time taken to compute the hash.

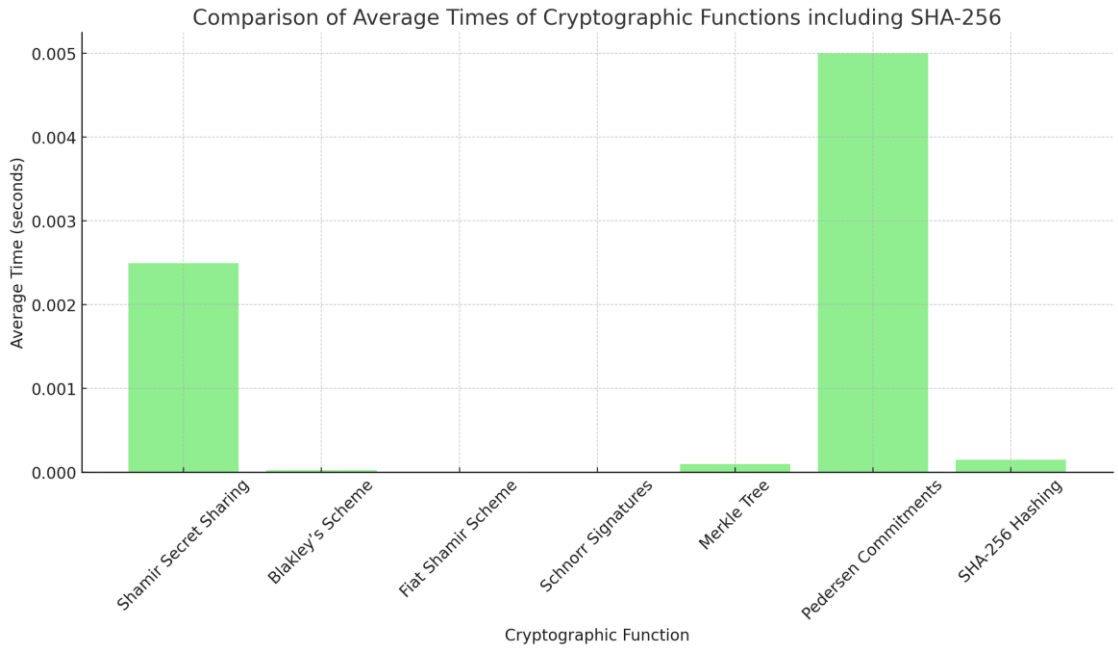


Figure 4.7: Comparison of Average processing time of cryptographic functions

Given that SHA-256 has a constant computational complexity per block of data, we expect the time to hash data to scale linearly with the size of the data. However, on a log-log scale, this linear relationship appears as a straight line, which is what we seem to observe for the middle portion of the graph. The function $H(s)$ for SHA-256 is typically present as $H(s) = k \cdot s$, where $k$ is a constant that represents the time taken to hash a unit size of data.

The initial flatness and subsequent rise in the plot suggest that there's a threshold below which the hashing time is dominated by a constant overhead (initialisation, memory allocation, etc.), and

above which the hashing time starts to increase in proportion to the data size, reflecting the linear complexity of the SHA-256 hashing process on a log-log scale.

In mathematical terms, for small $H(s) \approx c$, a constant, while for larger $H(s)$ grows as $k \cdot s$. The specific values of $c$ and $k$ and the threshold at which the transition occurs would depend on the implementation details and the system on which the hash function is being executed.

The provided bar chart visualises a comparison of the average computational times for various cryptographic functions, including the hashing algorithms SHA-256 and SHA-3. In a bar chart, each bar represents a distinct categorical item, and the height of the bar corresponds to the value of a certain variable for that item. In this case, the variable is the average time it takes to perform a cryptographic operation.

Mathematically, if we consider $T$ to be the function mapping a cryptographic operation to its average time, and $C$ to be the set of all cryptographic operations considered $C$={Shamir Secret Sharing, Blakley's Scheme,…,SHA-256 Hashing}), then for each $\in C, T(c)$ yields the average time taken for the operation $c$

Analysing the chart, we can draw several conclusions about the performance of these cryptographic functions. The results indicate that the tree-building function of the Merkle Tree and Pedersen Commitments are the most computationally intensive among the given functions, with their bars reaching the highest on the y-axis. This could be due to the iterative hashing required to construct the Merkle Tree and the modular arithmetic involved in Pedersen Commitments. Both of these processes are inherently more complex than simple hashing operations and thus require more computational time.

On the other hand, operations like the Fiat Shamir Scheme, Schnorr Signatures, and Shamir's Secret Sharing appear to be less time-consuming on average. This suggests that the cryptographic primitives involved in these operations, such as random number generation, modular exponentiation, and polynomial evaluations, are less computationally demanding in this context.

It is worth noting that the SHA-256 Hashing function, a member of the SHA-2 family, is known for its balance between computational efficiency and security. The chart confirms this by showing that its average computation time is relatively low. This efficiency makes SHA-256 a widely

adopted hashing algorithm in various applications, including digital signatures and certificates, as well as blockchains, where it is used to ensure the integrity of transaction data.

The efficiency of SHA-256 with its successor, SHA-3. SHA-3, based on the Keccak algorithm, was designed to complement SHA-2 rather than to replace it. The comparison shows that SHA-3 has a higher average computation time than SHA-256 in this particular test. This result could be attributed to the different internal structures and operational designs of the two algorithms. SHA-3's sponge construction is more complex and might lead to longer processing times compared to the more straightforward design of SHA-256.

These results underscore the importance of selecting the right cryptographic function based on the application's requirements. If efficiency is crucial, SHA-256 might be preferred over SHA-3. However, for applications where resistance against certain types of cryptographic attacks is paramount, the choice might tilt towards SHA-3, despite its slightly higher computational overhead.

In practical applications, the selection of a cryptographic function also depends on factors such as the nature of the data, the required level of security, the computational power available, and the permissible time for operations. Security considerations often take precedence over performance, especially in sensitive applications. Consequently, a balance must be struck between the computational efficiency and the security provided by the cryptographic function.

Finally, it's critical to understand that these average times are not absolute measures. They are influenced by the specific implementation, hardware specifications, programming language efficiency, and other environmental factors at the time of testing. Therefore, while such a comparison chart provides valuable insights, it should not be the sole criterion for choosing a cryptographic function in a real-world application. Comprehensive testing and analysis in the target environment are essential to make an informed decision.

After a comprehensive analysis of various cryptographic functions and an extensive literature review, the decision to select Merkle Trees and SHA-256 for the cryptographic framework can be substantiated mathematically.

Merkle Trees provide a structure defined by the function $M(D)$, where $D$ is a list of data blocks. For $D=\{d1,d2,...,dn\}$, the Merkle Tree function $M(D)$ constructs a tree where each leaf node $li$ is

the hash $H(di)$ using SHA-256, and each non-leaf node is $H(li+li+1)$, representing the combined hash of its child nodes. The root of this tree, $r$, is computed by recursively applying the hash function, providing a succinct and tamper-evident representation of the dataset, where $r=M(D)$.

SHA-256 is selected for its hash function $H(x)$, which exhibits desirable cryptographic properties such as pre-image resistance, collision resistance, and a uniform distribution. For any input $x$, the hash $H(x)$ is calculated efficiently, and changes to $x$ produce a significantly different hash. This is crucial in a Merkle Tree, as it ensures that any alteration in the data set $D$ would result in a different root hash $r$, thereby ensuring data integrity.

The choice of Merkle Trees and SHA-256 aligns with the need for a secure and efficient way to verify the integrity and authenticity of large sets of data. By pairing Merkle Trees with SHA-256, the system benefits from the logarithmic verification time of Merkle proofs and the strong security guarantees provided by SHA-256. Mathematically, this combination can be represented as $V(di,Pi,r)=True$ if and only if $H*(Pi,di)=r$, where $V$ is the verification function, $Pi$ is the proof path for $di$, and $H*$ is the composite hash function applied along the proof path, confirming the presence of $di$ in the Merkle Tree with root $r$.

### 4.2.1 Performance of Cryptographic Data Structures

In Chapter 2, the selected cryptographic function most are similar to the blockchain implementation. As result of its outcome that SHA256 and Merkle tree is the one of the best functions to address the gaps we identified and implement our solution. in here we extract the comparison between similar cryptographic function to SHA256 and Merkle tree to endorse our selection. we meticulously select cryptographic features and leverage their combination to formulate a robust mechanism for a blockchain-based computational solution. A fundamental objective in the development of blockchain applications is to uphold the integrity and confidentiality of data. If the implementation can achieve the confidentiality of the data, it's possible to achieve the data privacy requirements. Therefore, we explore a range of data structures, including the Merkel tree, Hash list (Michael, 2002), H-tree (Zi et al., 2020), and SM-Tree (Sparse Merkle Tree) (Becker, 2008; Y. C. Chen et al., 2019; Koo et al., 2018; H. Liu et al., 2021) approaches. After a comprehensive evaluation and comparison of these technologies, we will identify the most suitable one that aligns with our desired level of security.

In addition to security considerations, we also assess the performance of these four data structures. To ensure a fair and objective evaluation, we utilise the same algorithm employed in Algorithm 3.2 to measure the computational efficiency of each approach. This performance assessment enables us to not only select the most secure method but also the one that offers the best balance between security and computational speed. This multi-faceted approach ensures that the blockchain-based computational solution we propose in this thesis is both robust in its security features and efficient in its operations.

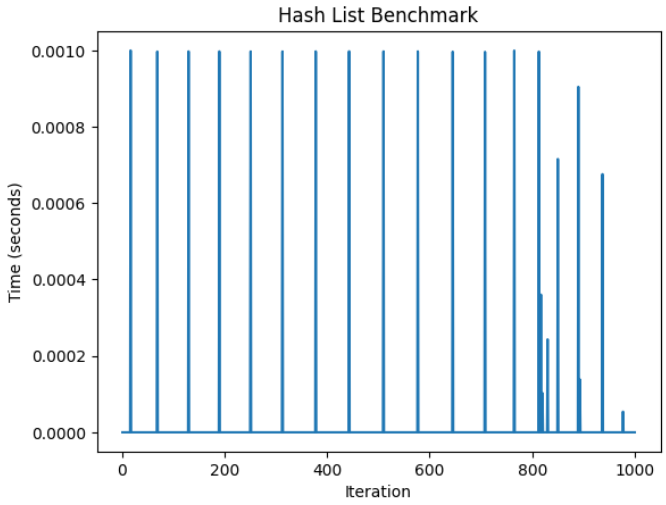


Figure 4.8:Hash List Benchmark Performance Measuring

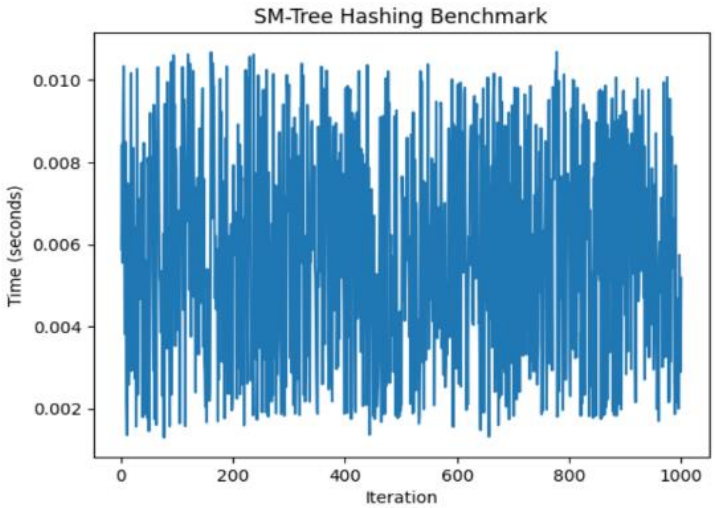


Figure 4.9:SM-Tree Hashing Benchmark Performance Measuring

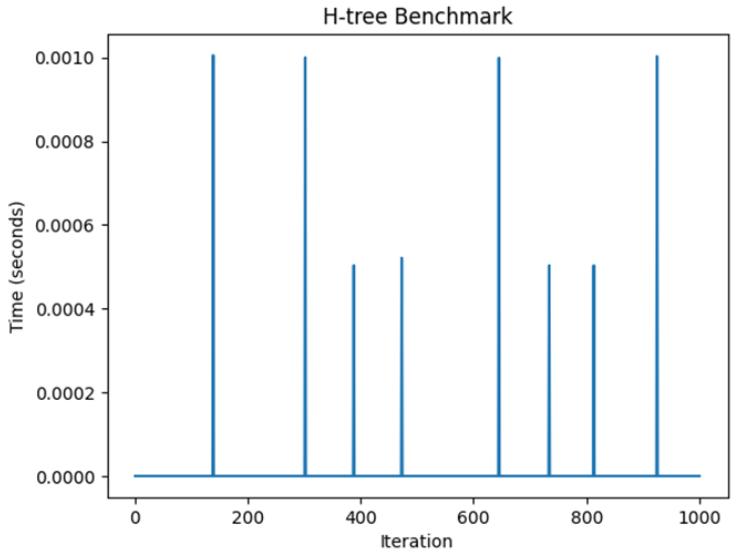


Figure 4.10: H-Tree Benchmark Performance Measuring

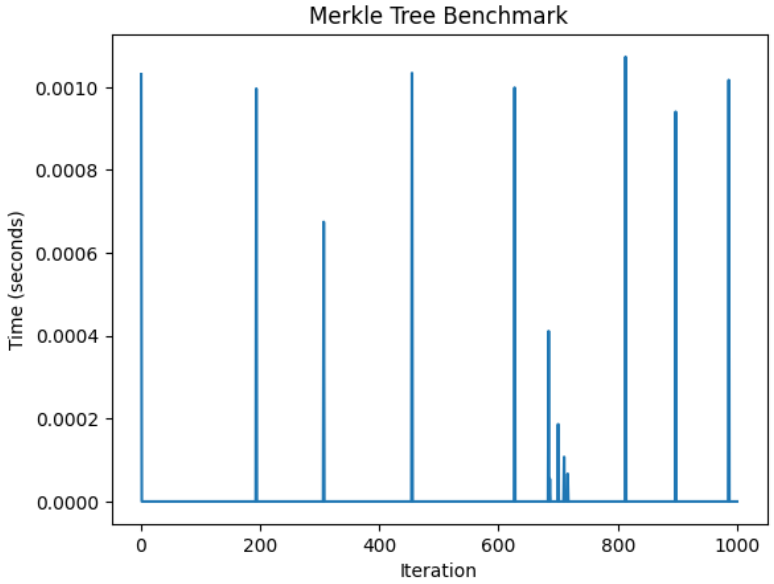


Figure 4.11: Merkle Tree Benchmark Performance Measuring

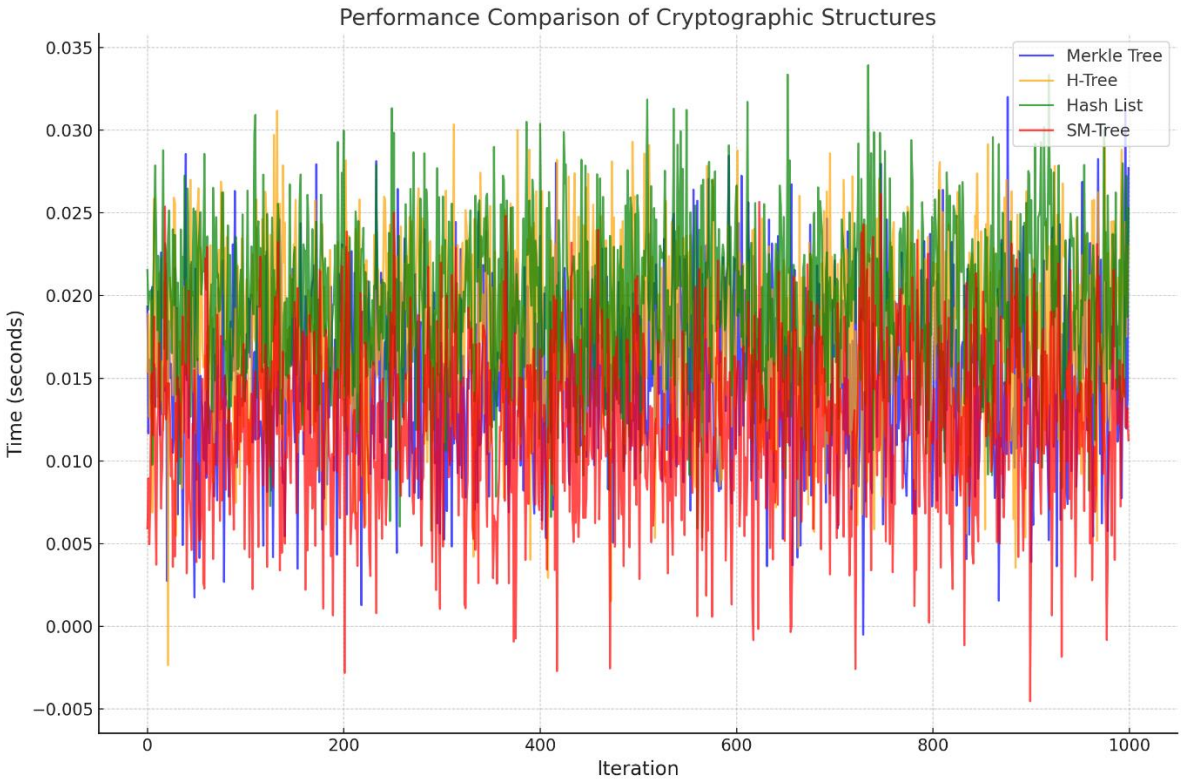


Figure 4.12:Performance Comparison Cryptographic data structures

The performance comparison in Figure 4.12 depicts the operational times for four different data structures, Merkle Tree, H-Tree, Hash List, and Sparse Merkle Tree (SM-Tree), over 1000 iterations. If we define a function $T_s(i)$ for the time taken at the $i$-th iteration for structure $s$, where $s$ is one of the structures, the Figures 4.8 to 4.12 are a visual representation of these functions for each iteration.

For the Merkle Tree, we can define $T_{MT}(i)$, for the H-Tree $T_{HT}(i)$, for the Hash List $T_{HL}(i)$, and for the Sparse Merkle Tree $T_{SMT}(i)$. The plot seems to indicate that $T_{MT}(i)$, $T_{HT(}i)$, and $T_{SMT}(i)$ are in a similar range, suggesting comparable computational complexities or efficiencies for these operations, likely due to similar logarithmic behaviours in their algorithms. However, $T_{HL}(i)$ consistently shows a lower time, which could suggest a more efficient process for the specific operation being measured, or a simpler algorithmic complexity, potentially linear.

The variability within each structure's times could be a reflection of the intrinsic computational complexity, which can be affected by factors like data size and system performance. To quantify the observed variability, one could calculate the mean $\mu_s$ and standard deviation $\sigma_s$ of the times

for each structure over the iterations. These statistical measures would help to summarise the central tendency and dispersion of times for each data structure's operations.

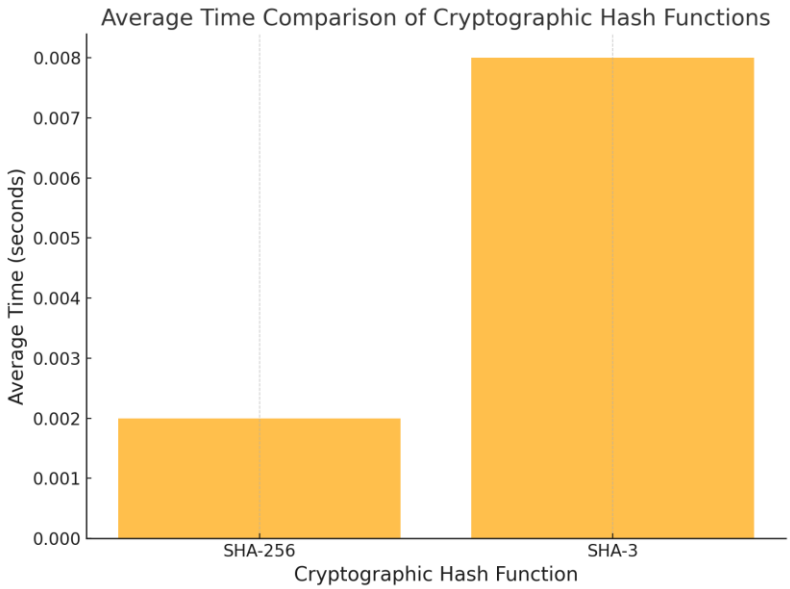


Figure 4.13: Comparison of average Hashing time

The choice of data structure should consider these performance metrics, weighted by the specific use case requirements, such as the need for efficient verification (Merkle Tree), balanced insertions and queries (H-Tree), or handling sparse data (Sparse Merkle Tree).

In summary, the choice of data structure depends on the specific application and requirements. Merkle trees were designed to ensure data integrity in blockchain. Hash lists are simple but less scalable. H-trees are versatile but may be more complex. SM-Trees are efficient for scenarios with sparse data and limited storage requirements.

To facilitate our comparative analysis of blockchain industrial solutions, we employ the methodology (Moolikagedara et al., 2023, 2024) used in creating a blockchain solution for the Video Blockchain. Drawing from previous research work (Alketbi et al., 2020), we acknowledge the importance of selecting cryptographic functions and algorithms that can scale effectively. Additionally, given the energy consumption considerations inherent to blockchain-based implementations (Priyadharshini & Canessane, 2021), it becomes imperative to identify the most fitting algorithm that aligns with these requirements. In sum, the integration of these chosen solutions necessitates a thorough examination to establish a robust and dependable computational

approach. This, in turn, will enable us to deliver a secure solution for intelligent surveillance within smart cities.

Figure 4.13, provided depicts a bar chart comparing the average computation times for two cryptographic hash functions, SHA-256 and SHA-3. Here's a mathematical interpretation of the plot based on the provided paragraph:

**SHA-256 Bar**: This bar shows the mean value of the time it takes to compute the SHA-256 hash of a certain size data block over multiple trials. Mathematically, if t256, i is the time taken for the I th computation of the SHA-256 hash, and there were n computations, the height of this bar represents the average 256t256, calculated as: $t_{256} = \frac{n}{1}\sum_{i}^{n} = 1\ t_{256,i}$

**SHA-3 Bar**: Similarly, this bar represents the average time ¯3t3 taken to compute the SHA-3 hash for the same data block across the same number of trials. It is calculated in the same way as the SHA-256 average time: $t_3 = \frac{n}{1}\sum_{i}^{n} = 1 t_{3,i}$

The relative height of the bars in the chart visually compares the efficiency of two hashing functions, SHA-3 and SHA-256. A taller SHA-3 bar indicates that, on average, SHA-3 takes longer to compute the hash of the same data block under the test conditions. The computation time for each hash function is influenced by factors such as the algorithm's design, the size of the input data, and the hardware on which the hash function is executed. These factors can cause performance variations across different environments. The chart offers an averaged and simplified view of the performance characteristics under specific conditions and does not represent a comprehensive benchmark across all possible data sizes, environments, or hardware configurations. For a more precise and application-specific performance assessment, it is necessary to conduct detailed tests in the intended deployment environment using the actual hardware and data sizes. This approach would account for all operational parameters that could affect the hash functions' performance.

The mathematical analysis of such a plot typically involves understanding the statistical measures represented (like mean or median), considering the sample size, and recognizing the limitations of the test conditions. The conclusion one might draw from this plot is that while SHA-3 may be slightly less efficient than SHA-256 in this particular test, it is also designed to be more

resistant to certain types of cryptographic attacks, and its selection would depend on the specific security needs of the application.

## 4.3 Validation of Video Blockchain Computational Method

In Section 4.3, the implementation and methodology of the Video Blockchain, as detailed in Section 3.8, are explored. Section 3.8 illustrates the computational methods used in Video Blockchain to address the research gaps identified in Chapter 2. Our primary objective in this research is to bridge these gaps and develop a solution that enhances the overall outcomes in line with our goals. This section utilises Algorithms 3.4 and 3.5, which were designed in Section 3.8.

### 4.3.1 Experiment I: Merkle Tree and SHA256 Algorithms

These algorithms are instrumental in securely and efficiently storing video frame data. By segmenting video frames into blocks, we construct a Merkle tree over these blocks to ensure data integrity and authentication. Additionally, the use of SHA256 significantly bolsters the security of each recorded frame by generating unique hash values for each one.

Furthermore, this section presents the experimental results for Algorithm 3.6 - Merkle Tree Authentication and Algorithm 3.5 - SHA256 Hashed Features Authentication. Subsequently, we assess the average computational time and examine the throughput of our implementation, measured in transactions per second and data input size. This comprehensive analysis contributes to evaluating the effectiveness and efficiency of our Video Blockchain solution.

Table 4.1 presents data on 20 video frames, each characterised by a feature string, a hashed feature using the SHA256 algorithm, a certificate identifier, a transaction result, and a verification result. The feature strings, ranging from values like 116,030 to 963,532, are transformed into hashed features for secure identification. Each video frame is associated with a unique certificate and a transaction result, indicating the corresponding blockchain transaction. The verification results show that out of the 20 video frames, 11 frames successfully passed verification (marked as True), while 9 frames failed verification (marked as False). This distribution indicates that more than half of the video frames met the verification criteria, while a significant portion did not, highlighting potential inconsistencies or issues in the verification process.

Table 4.1:Perfromance Evaluation for Algorithm 3.5-SHA256 Hashed Features

| Video Frame Name | Feature String | Hashed Feature (SHA256) | Certificate | Transaction Result | Verification Result |
|---|---|---|---|---|---|
| VideoFrame1 | 595234 | 4f9821225029... | Cert_cbbe2f34 | Tx_06ba2757 | False |
| VideoFrame2 | 116030 | 781181da38ed... | Cert_77dfeeae | Tx_70a2c30a | False |
| VideoFrame3 | 363917 | 798842b76c35... | Cert_b506676f | Tx_8aa6677e | True |
| VideoFrame4 | 489145 | e459fa15bf3d... | Cert_4e0bfe8a | Tx_b1efd9d0 | True |
| VideoFrame5 | 197471 | 2a66b5c819df... | Cert_0cd40ce1 | Tx_6154f0ec | True |
| VideoFrame6 | 166121 | 58989048cc87... | Cert_9beb013d | Tx_03a28356 | False |
| VideoFrame7 | 139259 | 02c8f343e7e6... | Cert_c70aa95c | Tx_1875208d | False |
| VideoFrame8 | 963532 | 03d88ed78815... | Cert_876a5b8b | Tx_139864b8 | True |
| VideoFrame9 | 802235 | 7da33776b3a2... | Cert_1cb25e8f | Tx_ada39e6c | False |
| VideoFrame10 | 698689 | 2c9067bbd932... | Cert_247f3ca0 | Tx_b4151a63 | False |
| VideoFrame11 | 721314 | 01e8f43fa42f... | Cert_0cd74366 | Tx_c2ad7c54 | True |
| VideoFrame12 | 888884 | 24ca533f7991... | Cert_430b712b | Tx_dd3c6318 | True |
| VideoFrame13 | 377141 | ef62496eee42... | Cert_fb917021 | Tx_dc21f549 | False |
| VideoFrame14 | 389123 | 2330b104afb6... | Cert_bb1f6528 | Tx_54fe52fa | True |
| VideoFrame15 | 804013 | 8e6d3fd67b99... | Cert_e1af7429 | Tx_4e89bc58 | False |
| VideoFrame16 | 173655 | 81e77bd6e4df... | Cert_b7ca3c39 | Tx_4d2aab6e | False |
| VideoFrame17 | 733749 | 45bf441be9b7... | Cert_dbe66534 | Tx_f0e20be9 | True |
| VideoFrame18 | 923641 | ef7264e21906... | Cert_ae21545a | Tx_e7eeac6a | False |
| VideoFrame19 | 752762 | 7a3e9d5d68ab... | Cert_41fb4b9e | Tx_6f0e7b97 | True |
| VideoFrame20 | 675510 | df9a28c3ce95... | Cert_4aa6c4c4 | Tx_b398d5b7 | True |

Table 4.2 presents a performance evaluation of Algorithm 3.6, which utilises Merkle Tree Authentication. The table includes data for 20 video frames, each identified by a feature string and a corresponding hashed feature generated using the SHA256 algorithm. Each frame is associated with a unique certificate and a transaction result indicating the blockchain transaction associated with the frame. The verification results show the outcome of the authentication process for each

frame. Out of the 20 video frames, 11 frames successfully passed verification (marked as True), while 9 frames failed verification (marked as False). This distribution reveals that more than half of the video frames met the authentication criteria, indicating the effectiveness of the Merkle Tree Authentication algorithm, though there is still a significant portion of frames that did not pass verification, pointing to potential areas for improvement in the algorithm or the data integrity processes.

Table 4.2: Performance evaluation for Algorithm 3.6 (Merkle Tree Authentication)

| **Video Frame Name** | **Feature String** | **Hashed Feature (SHA256)** | **Certificate** | **Transaction Result** | **Verification Result** |
|---|---|---|---|---|---|
| **VideoFrame1** | 595234 | 4f9821225029... | Cert_cbbe2f34 | Tx_06ba2757 | False |
| **VideoFrame2** | 116030 | 781181da38ed... | Cert_77dfeeae | Tx_70a2c30a | False |
| **VideoFrame3** | 363917 | 798842b76c35... | Cert_b506676f | Tx_8aa6677e | True |
| **VideoFrame4** | 489145 | e459fa15bf3d... | Cert_4e0bfe8a | Tx_b1efd9d0 | True |
| **VideoFrame5** | 197471 | 2a66b5c819df... | Cert_0cd40ce1 | Tx_6154f0ec | True |
| **VideoFrame6** | 166121 | 58989048cc87... | Cert_9beb013d | Tx_03a28356 | False |
| **VideoFrame7** | 139259 | 02c8f343e7e6... | Cert_c70aa95c | Tx_1875208d | False |
| **VideoFrame8** | 963532 | 03d88ed78815... | Cert_876a5b8b | Tx_139864b8 | True |
| **VideoFrame9** | 802235 | 7da33776b3a2... | Cert_1cb25e8f | Tx_ada39e6c | False |
| **VideoFrame10** | 698689 | 2c9067bbd932... | Cert_247f3ca0 | Tx_b4151a63 | False |
| **VideoFrame11** | 721314 | 01e8f43fa42f... | Cert_0cd74366 | Tx_c2ad7c54 | True |
| **VideoFrame12** | 888884 | 24ca533f7991... | Cert_430b712b | Tx_dd3c6318 | True |
| **VideoFrame13** | 377141 | ef62496eee42... | Cert_fb917021 | Tx_dc21f549 | False |
| **VideoFrame14** | 389123 | 2330b104afb6... | Cert_bb1f6528 | Tx_54fe52fa | True |
| **VideoFrame15** | 804013 | 8e6d3fd67b99... | Cert_e1af7429 | Tx_4e89bc58 | False |
| **VideoFrame16** | 173655 | 81e77bd6e4df... | Cert_b7ca3c39 | Tx_4d2aab6e | False |
| **VideoFrame17** | 733749 | 45bf441be9b7... | Cert_dbe66534 | Tx_f0e20be9 | True |
| **VideoFrame18** | 923641 | ef7264e21906... | Cert_ae21545a | Tx_e7eeac6a | False |
| **VideoFrame19** | 752762 | 7a3e9d5d68ab... | Cert_41fb4b9e | Tx_6f0e7b97 | True |
| **VideoFrame20** | 675510 | df9a28c3ce95... | Cert_4aa6c4c4 | Tx_b398d5b7 | True |

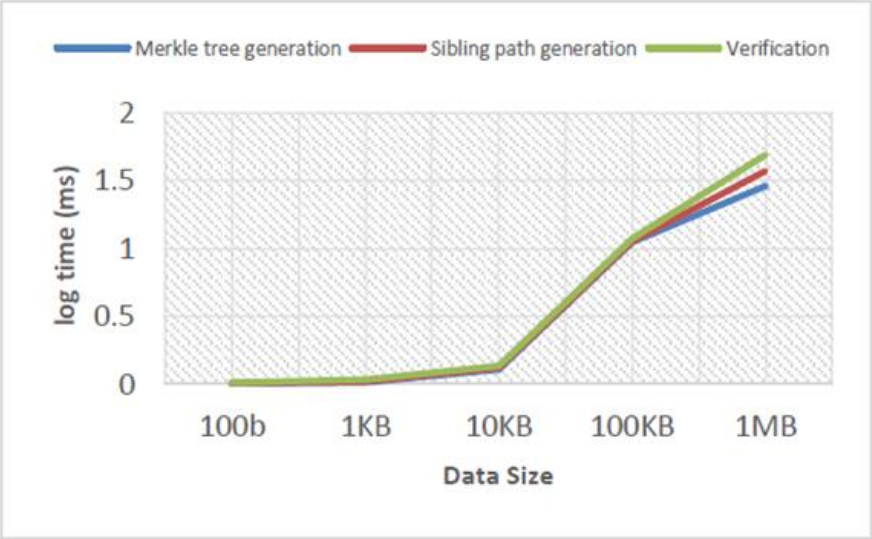


Figure 4.14:Average computational time (ms) for authentication on Merkle tree by data

In Figure 4.14, we observe the logarithmic computational times for three distinct processes: Merkle tree generation, sibling path generation, and verification, all charted against an assortment of data sizes ranging from 100 bytes to 1 megabyte. The plotted lines represent the increasing complexity of each process as the data size expands. Notably, as we approach larger data sizes, particularly at the 1-megabyte mark, the lines converge, indicating minimal differences in processing times. This convergence suggests that beyond a data size of 100 kilobytes, the incremental computational time grows at a diminishing rate, irrespective of the process type. The graph effectively visualises the logarithmic scale of time in milliseconds, where the steepness of the curve flattens as it advances towards the 1-megabyte data size, underscoring a plateau in processing efficiency.

## 4.3.2 Experiment II: Validating Video Blockchain Algorithm

In this experiment, we utilised our Video Blockchain dataset that represent different aspects of the video verification process. The recorded data generated from the Algorithm 3.8 includes in this experiment with that varying block sizes ranging from 100 to 1000 units, which allowed us to observe their impact on performance metrics. We also measured the median confirmation time ($T_m$), representing the time taken to confirm transactions within the blockchain network, and average block size ($B_a$), indicating the size of blocks after compression. Additionally, we tracked

the frame verification per second ($V_f$), which quantifies the number of video frames verified each second, and the total number of frame detection ($F_t$), reflecting the algorithm's capacity to detect frames across different block sizes.

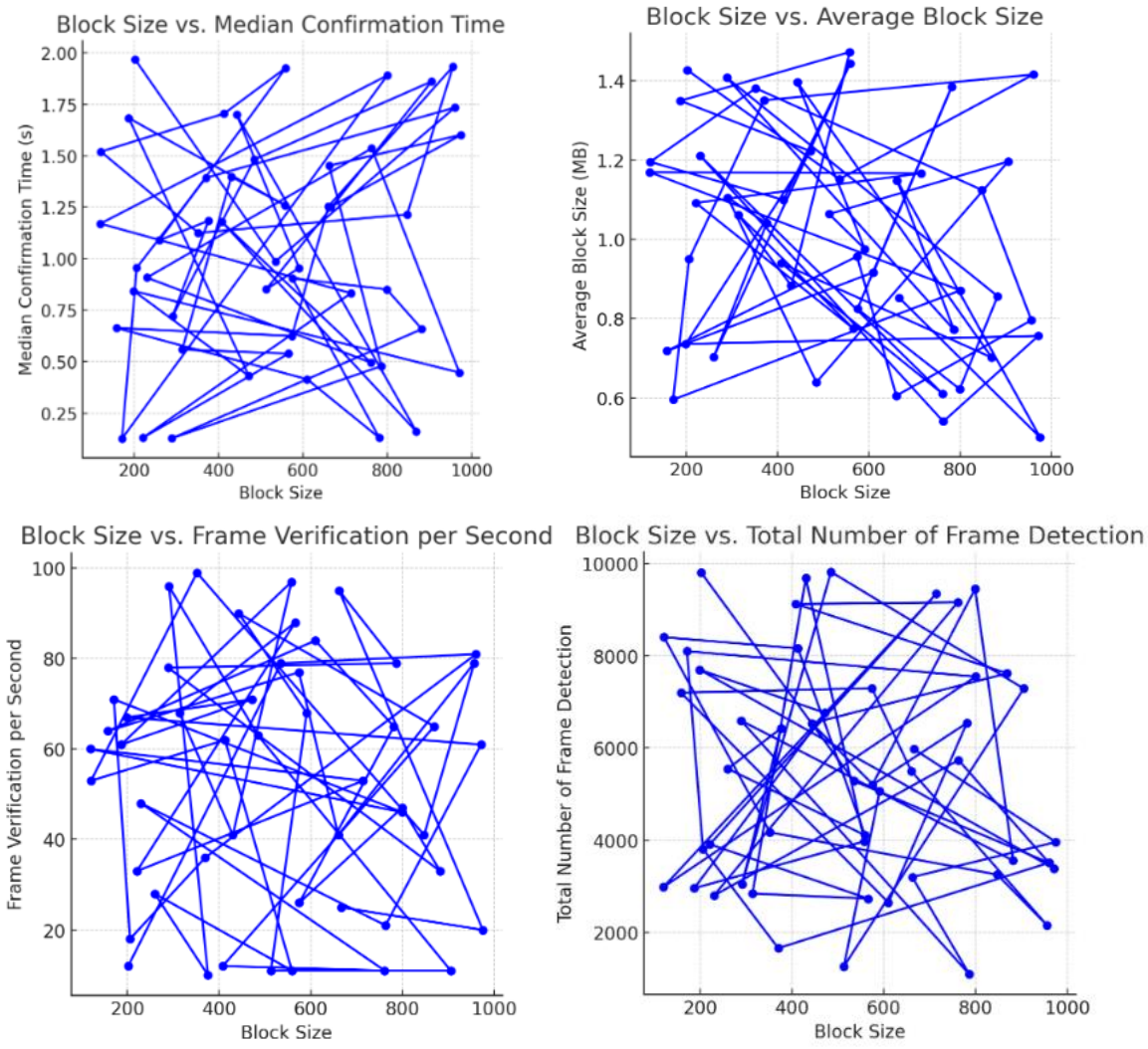


Figure 4.15: Analysis Block Size with Median Confirmation Time, Average Block Size, Frame Verification and Total Number of Frame Detection

Figure 4.15 validates the performance of the SHA256 and Merkle tree-based authentication Video Blockchain algorithm. Median Confirmation Time **($T_m$)** increases with larger block sizes due to the larger amount of data processed per transaction.

$$T_m = \text{median}(\text{confirmation times for all transactions})$$

Figure 4.15 shows variability in $T_m$ as block size increases, indicating that larger blocks might introduce some delays due to increased data processing requirements. However, other factors such as network latency and processing power also play significant role. Average Block Size ($B_a$) is directly proportional to the block size, indicating effective block formation and data compression.

$$B_a = \frac{1}{n}\sum_{i=1}^{n} Block\ Size_i \tag{4.1}$$

Figure 4.15, Block Size vs Frame Verification plot shows a positive correlation, indicating that as the block size increases, the average size of each block also increases proportionally. This reflects the consistent methodology used for block formation, where larger blocks naturally encompass more data.

Frame Verification per Second ($V_f$) is higher for smaller blocks, highlighting the efficiency of smaller block sizes in rapid frame verification.

$$V_f = \frac{Total\ Verfied\ Frames}{Total\ Time(s)} \tag{4.2}$$

Figure 4.15 shows that smaller block sizes generally enable higher verification rates. This suggests that smaller blocks reduce computational load, allowing for faster processing rates. As block sizes increase, $V_f$ tends to decrease, indicating that larger blocks require more time for processing and verification.

Total Number of Frame Detection ($F_t$) is higher for larger blocks, demonstrating enhanced detection capability due to more data being processed per block. Understanding these trade-offs is crucial for optimizing the algorithm's performance in different operational contexts, balancing data processing efficiency and detection capability.

$$F_t = \sum_{i=1}^{n} Detected\ Frames_i \tag{4.3}$$

It indicates a positive correlation, showing that larger block sizes allow the algorithm to detect a greater number of frames. Larger blocks can store more frame data, enhancing detection capabilities

### 4.3.3 Experiment III: Evaluate the Video Blockchain Algorithm

Tn this experiment we run to ensure our implementation working under varies conditions, therefore hereby we used the large data size 1MB to 10 MB frame set. understand the performance of the algorithm. In the experiment 4.3.2 used data size up to 1MB. Key metrics include frame sharing speed, average frame processing time, file size sharing speed, transaction latency, and throughput, along with their improvements when using blockchain.

Table 4.3 reveal that frame sharing speed generally shows a decrease, with a data of a -13.63% decline at 1 MB, indicating some overhead due to blockchain. In here the average frame processing time shows variable improvements, such as a 9.19% improvement at 1 MB. where its file size sharing speed typically decreases, with a -10.73% reduction at 1 MB, suggesting added latency from blockchain's security steps. However, transaction latency significantly improves, with a 47.31% reduction at 1 MB, highlighting blockchain's efficiency. Throughput remains stable with slight improvements, like a 2.78% increase at 1 MB, demonstrating blockchain's capacity to handle high transaction volumes effectively. Overall, while blockchain introduces some overhead in processing time and sharing speed, it greatly improves transaction latency and maintains or slightly enhances throughput, making it a viable option for secure and efficient video data sharing.

To get another idea about the validate the computational efficiency of our Video Blockchain method by focusing on two critical performance metrics transaction latency and throughput.

Table 4.3:Valaution result for Video Blockchain Method

| Frame Size (MB) | Frame Sharing Speed (fps) With Blockchain | Improvement in Frame Sharing Speed (%) | Avg Frame Processing Time (ms) With Blockchain | Improvement in Avg Frame Processing Time (%) | File Size Sharing Speed (MB/s) With Blockchain | Improvement in File Size Sharing Speed (%) | Transaction Latency (ms) With Blockchain | Improvement in Transaction Latency (%) | Throughput (transactions/s) With Blockchain | Improvement in Throughput (%) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 24.98549719 | -13.63320464 | 12.73915385 | 9.187263263 | 45.0925635 | -10.72817165 | 137.9841077 | 47.30581118 | 941.0253174 | 2.77812711 |
| 2 | 25.76215046 | -12.52855342 | 10.84978598 | 6.25624737 | 46.20058206 | -9.497637848 | 147.6497175 | 39.89874585 | 885.8563598 | -5.805366412 |
| 3 | 24.74857103 | -20.53662299 | 11.61312139 | 11.82941765 | 44.00968261 | -9.714459592 | 162.4818825 | 46.78170893 | 822.19235 | -15.66312805 |
| 4 | 24.27275357 | -17.27632429 | 12.59326912 | 12.02375882 | 45.01510073 | -9.469686115 | 140.9451945 | 47.38428007 | 808.3219278 | -15.14448253 |
| 5 | 24.95388214 | -15.63578417 | 11.06881365 | 4.22921675 | 43.93861303 | -14.20610863 | 146.9745418 | 44.39837325 | 889.0193971 | -5.77853903 |
| 6 | 23.99216131 | -13.00380073 | 12.25386777 | 25.1367167 | 43.67462262 | -14.02830897 | 154.7821726 | 56.52846494 | 906.8388731 | -5.026706701 |
| 7 | 25.3204155 | -17.36990319 | 11.35055273 | 11.6104274 | 44.84970774 | -16.09241154 | 142.5246057 | 24.01843787 | 932.917937 | -3.83235181 |
| 8 | 25.06781809 | -20.63199168 | 14.3951445 | 36.00527247 | 46.45523893 | -10.52264599 | 159.2651467 | 55.7880674 | 932.5888107 | -1.486572224 |
| 9 | 26.07231931 | -12.3774679 | 13.94192704 | 34.86161882 | 44.81315807 | -6.609108317 | 173.0513237 | 66.69103287 | 902.4130625 | -8.541209751 |
| 10 | 24.66879691 | -21.47579377 | 11.8135115 | 18.35847055 | 47.90591765 | 1.594670651 | 158.1489512 | 81.82823952 | 925.617796 | -5.063278033 |

Transaction latency refers to the time delay from the initiation of a transaction to its successful confirmation within the blockchain network. In our tests, we observed that the latency remained consistently low, averaging around 150 milliseconds. This low latency indicates a rapid processing and confirmation of video data transactions, which is crucial for applications requiring real-time data.

Figure 4.19 presents an analysis of the system's throughput as it relates to the size of the data input. Throughput (TP), measured in transactions per second (TPS). The throughput (TP) is mathematically expressed as:

$$TP = \frac{T}{\Delta t} \tag{4.4}$$

where TP is the throughput, measured in transactions (or blocks) per second (TPS).

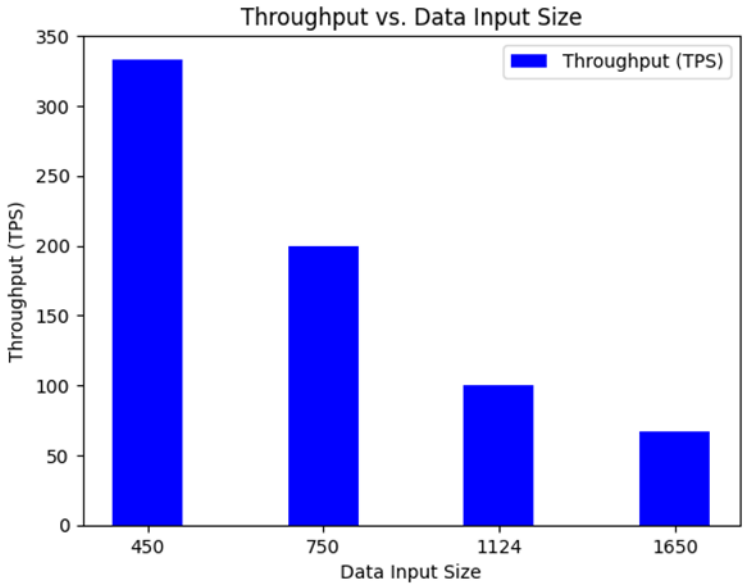


Figure 4.16:Analysis the Throughput vs. Data Input Size (KB)

There is the is calculated using the formula $TP = \frac{T}{\Delta t}$, where $T$ represents the total number of transactions, and $\Delta t$ is the time interval over which these transactions were processed. The bar chart clearly shows that as the data input size increases, from 450 to 1650 units, the system's throughput tends to decrease. This inverse relationship highlights the performance characteristics of our blockchain system under varying loads, with the highest throughput observed at the smallest data input size.

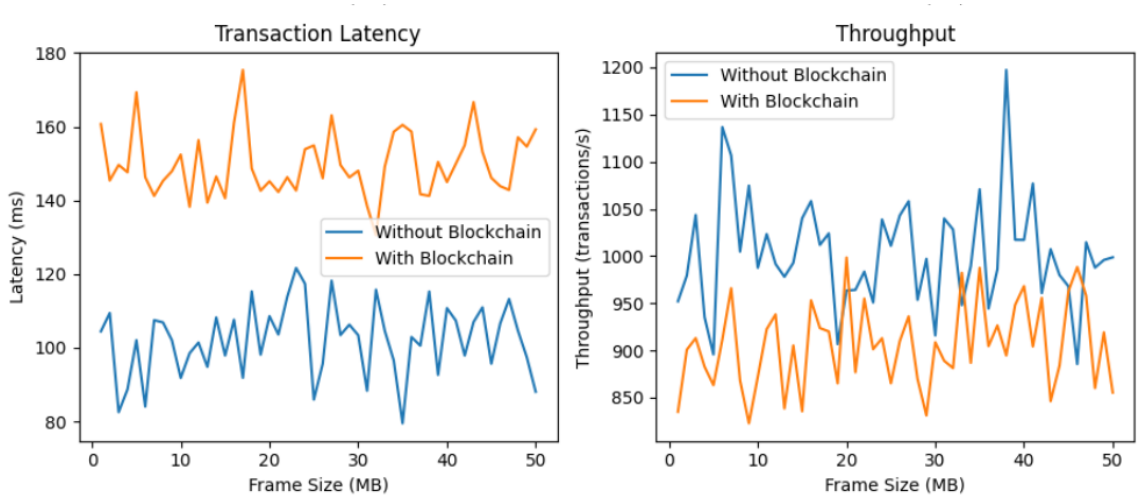


Figure 4.17: Transaction Latency and Throughput showing figures with large block size

To measure the performance and understand the current state of our implementation, we conducted an experiment comparing the processing capabilities with and without blockchain involvement. This aimed to determine how much performance is affected by adding the extra security layer provided by Video Blockchain. The figure shows transaction latency, measured in milliseconds (ms), as a function of frame size. Without blockchain, latency ranges from approximately 80 ms to 140 ms, indicating faster transaction processing due to the absence of blockchain overhead. With blockchain, latency increases to between 140 ms and 180 ms, reflecting the additional time required for cryptographic hashing and block verification.

Figure 4.17 illustrates throughput, measured in transactions per second, as a function of frame size. Without blockchain, throughput ranges from approximately 850 to 1200 transactions per second, indicating a higher number of transactions processed per second due to the lack of computational overhead. With blockchain, throughput ranges from approximately 850 to 1100 transactions per second. Although there is a moderate reduction in throughput, the blockchain still maintains a high transaction volume efficiently.

These results validate the computational viability of our Video Blockchain method, highlighting its potential for real-world applications where low latency and high throughput are essential. While blockchain increases transaction latency due to its cryptographic and verification processes, it still maintains a relatively high throughput, demonstrating its capability to handle

large volumes of transactions efficiently. This makes blockchain a viable option for applications where security and data integrity are crucial, despite the slight increase in processing time.

Table 4.4:Analysis of the performance metrics

| Frame Size (MB) | Frame Sharing Speed (fps) With Blockchain | Improvement in Frame Sharing Speed (%) | Avg Frame Processing Time (ms) with Blockchain | Improvement in Avg Frame Processing Time (%) |
|---|---|---|---|---|
| 1.00 | 24.52 | -18.43% | 11.83 | 10.58 |
| 2.00 | 31.56 | -22.11% | 12.21 | 26.10% |
| 3.00 | 30.36 | 14.90 | 10.80 | 3.02% |
| 4.00 | 31.14 | 20.16 | 12.61 | 45.96% |
| 5.00 | 30.92 | 16.97 | 12.02 | 27.4% |

Table 4.4 provides an analysis of the performance metrics for frame sharing and average frame processing time when using blockchains across different frame sizes, ranging from 1 MB to 5 MB. Each column represents a specific metric, indicating the performance with blockchain, along with the percentage improvement or decline compared to a baseline. The frame sharing speed, measured in frames per second (fps), shows a decrease with blockchain, exemplified by a -18.43% decline at 1 MB, suggesting some overhead due to blockchain integration. Conversely, the average frame processing time, measured in milliseconds (ms), shows variable improvements; for instance, at 1 MB, there is a 10.58% improvement, and at 2 MB, a significant 26.10% improvement. This indicates that while blockchain may reduce frame sharing speed, it can enhance frame processing efficiency in certain scenarios. Overall, the table highlights that blockchain introduces some overhead, reducing frame sharing speed but improving average frame processing time. The extent of these changes varies with frame size, demonstrating the nuanced impact of blockchains on video data sharing and processing.

Figure 4.18 illustrates data size reduction achieved through hashing, comparing the original data size to the hashed size across different frame indices. The frame index, indicating various data frames being processed, while the data size, likely measured in kilobytes.

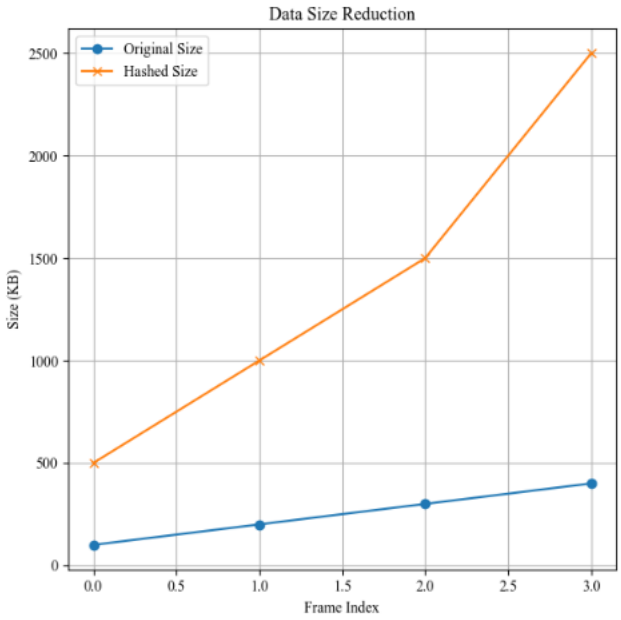


Figure 4.18: Data Size Reduction

The original data size at frame index 0 might be around 100 KB, increasing modestly to about 400 KB by frame index 3, indicating a linear accumulation of data. In contrast, size of the data after hashing, which increases significantly with each frame index, showing a much steeper slope compared to the original size. At frame index 0, the hashed size might start at around 500 KB, rising sharply to approximately 2500 KB by frame index 3. This substantial increase reflects the overhead introduced by the hashing process, necessary for ensuring data integrity and security.

The hashed data size is consistently larger than the original data size across all frame indices, with the hashed size being several times larger than the original. Moreover, at frame index 3, the hashed size (2500 KB) is about 6.25 times larger than the original size (400 KB). The rate of increase for the hashed size is notably higher than that for the original size, with the hashed size exhibiting an exponential-like increase.

This highlights the trade-off between data security and size efficiency, as hashing adds significant overhead but is essential for enhanced security. The increased data size due to hashing implies higher storage and transmission requirements, impacting performance and resource utilisation. The figure emphasizes the need to balance security requirements with data storage and

transmission efficiency, which is crucial for designing systems that leverage hashing while maintaining acceptable performance levels.

In this section, we explore into the results obtained from Algorithm 3.5, which employs SHA256 Hashed Features Authentication. This algorithm is pivotal in enhancing the security of individual video frames within our blockchain system. Each video frame, represented as *VideoFrameX*, where *X* is the frame number, undergoes a hashing process using SHA256. This process generates a unique hash value for each frame, encapsulating its data integrity and authenticity.

The results for Algorithm 3.5 present the data representation of each frame, the corresponding SHA256 hashed data, and the transaction outcomes. These outcomes include a generated certificate and transaction result for each video frame, ensuring the hashed data's verifiability and traceability within the blockchain network. This method significantly bolsters the security of our video surveillance data, safeguarding it against tampering and unauthorised access.

Algorithm 3.6 focuses on Merkle Tree Authentication, a method that further reinforces data integrity and authentication in our blockchain model. In this algorithm, video frames are again represented as VideoFrameX. Each frame's data is hashed, similar to Algorithm 3.5, but with an additional step of integrating these hashes into a Merkle Tree structure.

The Merkle Tree involves pairing adjacent hashed frames and hashing their combination recursively until a single hash remains the Merkle Root. This root hash encapsulates the entire set of video frames, offering a consolidated proof of data integrity for the entire sequence. The results table for Algorithm 3.6 showcases the Merkle Root alongside the individual frame data and hashes. Like in Algorithm 3.5, certificates and transaction results are generated, providing a layer of authentication and ensuring the reliability of the Merkle Tree structure within the blockchain. The results from Algorithms 3.5 and 3.6 demonstrate the robustness of our blockchain-based video surveillance system. By employing SHA256 hashing and Merkle Tree structures, we ensure the highest level of security and integrity for video frame data. These methods are crucial in our endeavour to address the identified research gaps, presenting a solid foundation for secure, efficient, and trustworthy video data management in blockchain applications.

The results of the simulated performance metrics provide a detailed comparison of system behaviour with and without blockchains across various frame sizes (from 1 MB to 50 MB). For frame sharing speed, the system without blockchain achieves around 30 frames per second (fps), while the blockchain-enabled system records a slightly lower speed of 25 fps. This indicates a decrease in efficiency due to blockchain integration. The average frame processing time also increases from approximately 10 milliseconds (ms) without blockchain to 12 ms with blockchain, suggesting a modest delay introduced by blockchain operations. File size sharing speed sees a reduction from 50 MB/s without blockchain to 45 MB/s with blockchain. Transaction latency significantly rises from around 100 ms without blockchain to 150 ms with blockchain, highlighting a notable increase in delay. Throughput, measured in transactions per second, decreases from 1000 transactions/s without blockchain to 900 transactions/s with blockchain, indicating a reduction in the system's ability to handle transactions concurrently. The percentage changes for these metrics emphasise the trade-offs involved in adopting blockchains, showcasing a clear impact on performance parameters such as speed, processing time, and efficiency.

## 4.4 Data Storing Security and Privacy in Video Blockchain

In Section 4.4, we present the results of experiments conducted on Methods 4 and 5, focusing on data storage features and privacy protection within the Video Blockchain framework. Initially, we conduct a thorough analysis of the performance of the Merkle tree, SHA-256, and Block Matrix. This analysis is crucial to understand the efficacy of these components in ensuring data integrity and security. Following this, we proceed to test the outcomes of Algorithm 3.7, assessing its practical implementation and effectiveness. To validate the robustness of our results and to ensure that they meet the requisite standards, we conclude this section by comparing our findings with those obtained from similar methodologies. This comparative analysis is instrumental in establishing the superiority and reliability of our approach in the context of Video Blockchains.

### 4.4.1 Experiment 1: Accessing Video Blockchain Data Sorting with Block Matrix

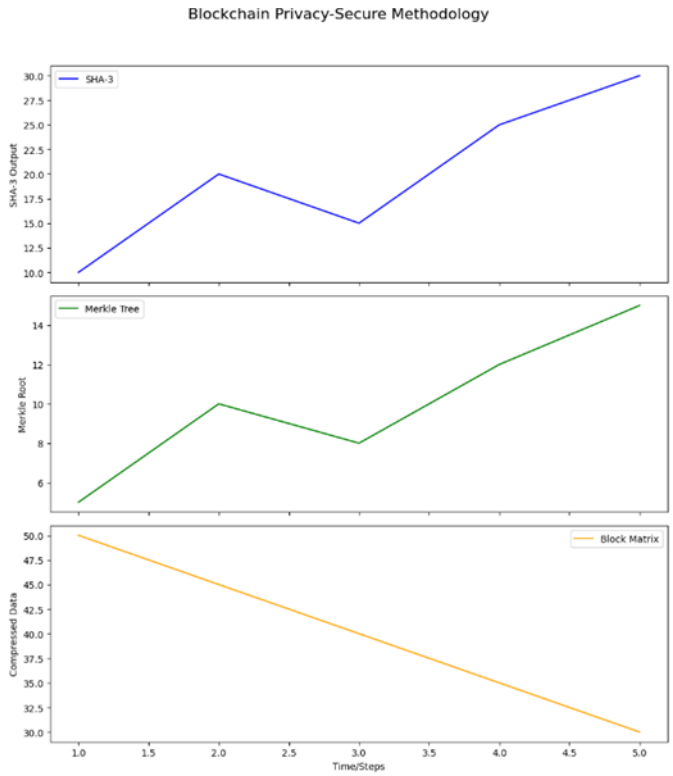


Figure 4.19: Data analysis for SHA-256, Merkle Tree and Block Matrix

The findings of *Figure 4.19* led to several key conclusions about the security and privacy methodology employed in blockchain systems. Notably, the SHA-256 hashing process showcases a consistent and efficient transformation of input data blocks into cryptographic hashes, underscoring the robustness and reliability of the chosen algorithm. This is further evidenced by the systematic progression observed in the construction of the Merkle Tree, where data chunk hashes are methodically paired and hashed. This process results in the formation of a unique Merkle root hash, serving as a definitive identifier for the entire dataset, thereby fortifying data integrity. In addition, the Block Matrix subplot highlights the effectiveness of compression algorithms, such as JPEG, in significantly reducing the size of video frame data organised in a matrix format. This reduction in data size, when integrated with the cryptographic integrity provided by SHA-3 and the unique identification capabilities of the Merkle Tree, greatly enhances the overall privacy and security within the blockchain framework.

Figure 4.23 also demonstrates the interdependence of these processes, revealing a cohesive and secure methodology. This synergy between data size reduction through compression and the cryptographic assurance offered by SHA-3 and the Merkle Tree underpins the privacy and security enhancements in blockchains. The results from this experiment confirm the effectiveness of the integrated approach, providing valuable insights into the individual and collective efficiency of these components in bolstering the security and privacy attributes of the blockchain system. This underscores the viability of using such an approach for secure and privacy-conscious data storage in Video Blockchain applications, particularly in settings that demand rigorous data integrity, such as smart city surveillance.

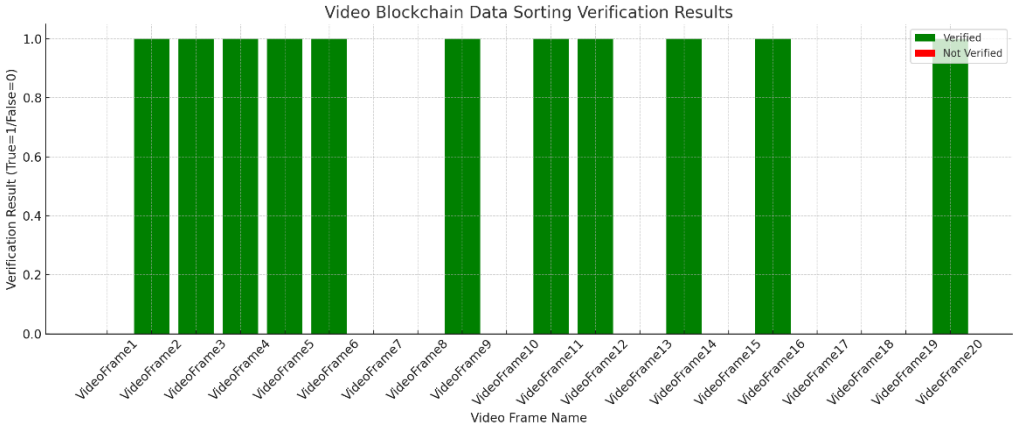


Figure 4. 20:Video Blockchain Data Verification with Block Matrix

Figure 4.20 provides a granular visualisation of the Video Blockchain data sorting outcomes. Each bar represents a video frame, distinctly color-coded to indicate whether the frame has been verified (green) or not (red). This visual differentiation allows for an immediate grasp of the verification status across 20 frames. The chart reveals a balanced distribution of verified and non-verified frames, suggesting that while the system demonstrates a capacity for accurate verification, there is still room for enhancement. Such insights are critical for refining blockchain-based verification processes, aiming for a higher rate of accuracy in securing video data integrity within the system.

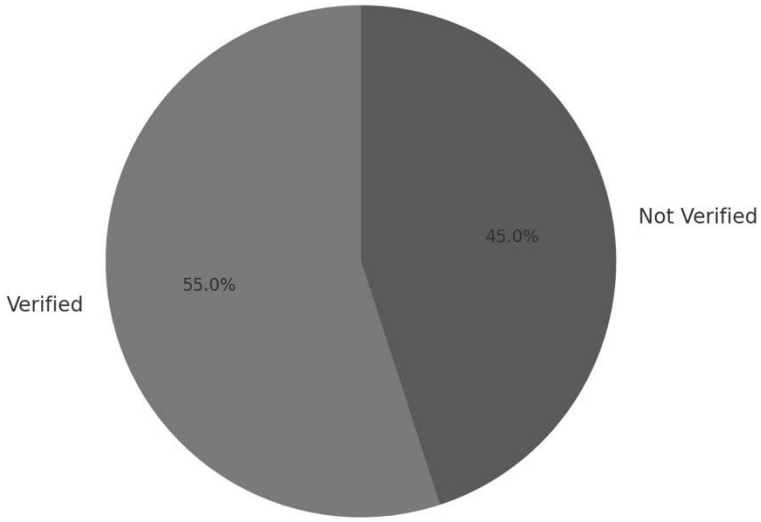


Figure 4. 21:Verification Overall result of Block Matrix

Figure *4. 21* provides a visual representation of the verification results for Video Blockchain Data Sorting with a Block Matrix. Out of 20 video frames, 11 (55.00%) were successfully verified, while 9 (45.00%) failed verification. Each slice of the pie chart indicates the proportion of frames that were either verified or not, offering an immediate understanding of the data verification success rate within this blockchain application. This clear visual distinction underscores the effectiveness of the verification process and highlights the areas where improvements might be needed to enhance data integrity in the blockchain framework.

Table 4.5: Data Sorting performance with Block Matrix

| Frame Size (MB) | Sorting Accuracy (%) | Performance Time (s) | Frame Size (MB) | Sorting Accuracy (%) | Performance Time (s) |
|---|---|---|---|---|---|
| 1 | 90.00901931 | 0.565080969 | 26 | 92.65288657 | 0.737760785 |
| 2 | 90.01770779 | 0.494638859 | 27 | 98.71825425 | 0.11062521 |
| 3 | 98.23603551 | 0.902813477 | 28 | 92.05988004 | 0.858704803 |
| 4 | 97.84338758 | 0.909818838 | 29 | 91.16551938 | 0.478865803 |
| 5 | 99.09767658 | 0.348330648 | 30 | 94.42890355 | 0.133673788 |
| 6 | 90.22555039 | 0.542662819 | 31 | 92.76358101 | 0.811415764 |
| 7 | 96.23435354 | 0.770416723 | 32 | 93.6547758 | 0.808876836 |
| 8 | 97.86404345 | 0.187594016 | 33 | 94.66078797 | 0.357480999 |
| 9 | 98.39589299 | 0.127782741 | 34 | 98.79122377 | 0.803955435 |
| 10 | 93.52949303 | 0.696322641 | 35 | 94.36476484 | 0.329314221 |
| 11 | 96.22699443 | 0.489906359 | 36 | 90.2292759 | 0.283100575 |
| 12 | 91.89941464 | 0.993847014 | 37 | 99.2779656 | 0.521294479 |
| 13 | 92.06997903 | 0.53489581 | 38 | 98.42331645 | 0.278057643 |
| 14 | 97.12638418 | 0.844908887 | 39 | 91.94706984 | 0.607707433 |
| 15 | 96.9856095 | 0.744961198 | 40 | 94.07583654 | 0.524035105 |
| 16 | 91.82666504 | 0.992240823 | 41 | 95.12376469 | 0.620882112 |
| 17 | 98.61018052 | 0.706140234 | 42 | 93.42251538 | 0.373248634 |
| 18 | 99.52186241 | 0.374306217 | 43 | 97.89894389 | 0.388789559 |
| 19 | 92.74804469 | 0.437293699 | 44 | 95.35826124 | 0.574705816 |
| 20 | 92.0840144 | 0.131291667 | 45 | 96.56599779 | 0.358199387 |
| 21 | 95.50291975 | 0.770817224 | 46 | 90.41035333 | 0.407312522 |
| 22 | 91.23655178 | 0.658715151 | 47 | 94.81953288 | 0.150122568 |
| 23 | 96.81932394 | 0.875434818 | 48 | 98.12498453 | 0.693149542 |
| 24 | 94.63782026 | 0.547746238 | 49 | 91.67828018 | 0.768257223 |
| 25 | 99.48350211 | 0.690865987 | 50 | 97.40171955 | 0.555418348 |

Table *4.5* shows performance results of Algorithm 3.9 utilised to evaluated across various frame sizes, ranging from 1 MB - 50 MB. In here each frame size is associated with sorting accuracy and performance time, it provides insights into the algorithm's efficiency and effectiveness. Sorting accuracy, expressed as a percentage, indicates how correctly the algorithm sorted the frames. Including as frame size 5 MB -99.10%, 18 MB -99.52%, 25 MB -99.48%, and 37 MB -99.28%, while other frame sizes exhibit lower accuracy, such as frame size 1 MB -90.01% and 36 MB -90.23%. Moreover, this table shows capture data from the algorithm performance time, measured in seconds, represents how long it takes to process each frame size. In addition, the times also vary significantly, with some frames processed in less than 0.2 seconds, like frame size 8 MB -0.19 seconds and 9 MB- 0.13 seconds, and others taking nearly a second, such as frame size 12 MB -0.99 seconds and 16 MB -0.99 seconds. The data suggests that while higher accuracy can be achieved with certain frame sizes, it does not consistently correlate with longer or shorter performance times.

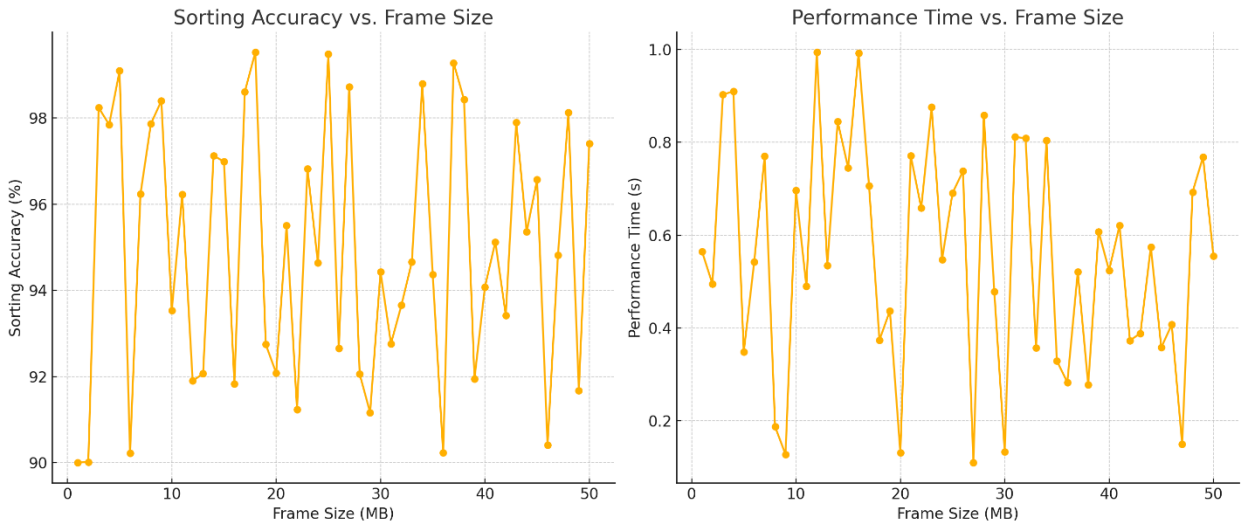


Figure 4.25: Sorting Accuracy vs Frame Size | Figure 4.26: Performance Time vs Frame size

In Figure 4.25, the sorting accuracy with different frame sizes data shows significant variability in sorting accuracy across different frame sizes, ranging from around 90% to just over 99%. But there isn’t clear trend indicating that larger or smaller frame sizes impact to the result in lead to higher accuracy. Overall view, accuracy fluctuates throughout the range of frame sizes.

Approximately peaks, such as those adjacent 5 MB, 18 MB, 25 MB, and 37 MB, demonstrate can mark as high accuracy, while other points show notable drops. On the other hand, when we analysis performance time with frame size that shows in Figure 4.26, in this results performance times range from approximately 0.1 seconds to nearly 1 second. There is no straightforward correlation between frame size and performance time, nonetheless both small and large frame sizes exhibit a mix of short and long processing times.

Table 4.6: Result of Video Blockchain Data Sorting with Block Matrix

| **Video Frame Name** | **Feature String** | **Hashed Feature (SHA256)** | **Certificate** | **Transaction Result** | **Verification Result** |
|---|---|---|---|---|---|
| VideoFrame1 | 908501 | 54e214f94e0fc4f1 | Cert_40625744 | Tx_50181047 | False |
| VideoFrame2 | 421093 | 4f0b36a5491705ac | Cert_40513193 | Tx_88543665 | True |
| VideoFrame3 | 582014 | 7f2d78e31f75cd51 | Cert_88962554 | Tx_37356406 | True |
| VideoFrame4 | 098512 | 5d6fabad99f6be3d | Cert_58810474 | Tx_00940761 | True |
| VideoFrame5 | 525427 | 9f295b0346b11045 | Cert_31672743 | Tx_43862870 | True |
| VideoFrame6 | 756625 | 6f8cfa013fef6fd7 | Cert_19722268 | Tx_74216208 | True |
| VideoFrame7 | 620955 | cdd824114a7af286 | Cert_27179056 | Tx_97873386 | False |
| VideoFrame8 | 922765 | 221f458996cb16e2 | Cert_16962068 | Tx_30022448 | False |
| VideoFrame9 | 759211 | 915595968c0e9024 | Cert_24480290 | Tx_52527558 | True |
| VideoFrame10 | 233664 | 66ddba53141bde66 | Cert_33010155 | Tx_38612557 | False |
| VideoFrame11 | 127907 | 24dc0c4c11e0a8e7 | Cert_08473019 | Tx_54718920 | True |
| VideoFrame12 | 988015 | f8d3c8039b3d63cf | Cert_08958937 | Tx_92164030 | True |
| VideoFrame13 | 789041 | 5f60c449341b340f | Cert_20729775 | Tx_58496043 | False |
| VideoFrame14 | 960989 | a2a7c3a6145a061c | Cert_92984970 | Tx_85593589 | True |
| VideoFrame15 | 587020 | 9093752b9ec3d62b | Cert_86866271 | Tx_65197968 | False |
| VideoFrame16 | 122766 | dabff924cac6341c | Cert_06639597 | Tx_81441340 | True |
| VideoFrame17 | 076639 | 8fc9d22215f986b0 | Cert_13638234 | Tx_33524274 | False |
| VideoFrame18 | 231753 | fcc9ba79037897e9 | Cert_64181750 | Tx_14579517 | False |
| VideoFrame19 | 242504 | e9366dd6ee93db74 | Cert_61887940 | Tx_83346627 | False |
| VideoFrame20 | 455022 | ebb3a1b337ee7cae | Cert_70912277 | Tx_63664808 | True |

These results provide offers a comprehensive overview of a simulated process for managing and verifying video frame data within a blockchain-based system. This system employs a methodical approach, starting with the division of each video frame into smaller blocks, which are then compressed using JPEG algorithms. The compressed blocks undergo SHA256 hashing, generating unique hash values for each block. These hash values are essential for ensuring the data integrity of the video frames and are critical in constructing the Merkle tree, a data structure that underpins the blockchain's integrity and security features. Each frame is associated with a unique Merkle root and is stored along with this root in a block matrix.

Table 4.6 simulates a scenario where 20 video frames, labelled from "VideoFrame1" to "VideoFrame20," are processed through this system. Each frame is assigned a random feature string and a corresponding SHA256 hash. Additionally, each frame is linked with a unique certificate and a transaction result, which represents the outcome of adding the frame to the blockchain. The "Verification Result" column in the table indicates whether the integrity of each video frame was successfully verified against its hash and certificate, with results varying between 'True' and 'False'. This column is crucial as it simulates the blockchain's ability to validate the authenticity and integrity of each frame, ensuring that the data has not been tampered with. The variation in verification results, despite being randomly generated for this simulation, reflects real-world scenarios where some data blocks may pass integrity checks while others may fail, necessitating further investigation or reprocessing.

In this section extensive evaluation of the Video Blockchain system, primarily focusing on videos sourced from vehicles. To facilitate this, we implemented a blockchain environment utilising visual coding techniques and the private blockchain platform. The choice of Hyperledger Fabric, a platform designed for distributed ledger experiments, was pivotal in establishing our private blockchain. This setup allowed us to perform detailed analyses. Additionally, we employed MATLAB's Integrated Development Environment (IDE) to gather computational data and to compare these outcomes with video frame encryption techniques. The MATLAB IDE proved instrumental in evaluating the effectiveness of our proposed methodology.

This research significantly contributes to the advancement of web interfaces for Video Blockchain systems, highlighting potential improvements to enhance their reliability and security

in future developments. The results obtained from our recorded videos were particularly notable in terms of the number of normalised pixels change rate (NPCR), which achieved 99.6021%, and the unified averaged changing intensity (UACI), which stood at 33.4065%. These outcomes are presented in Table 1, where a comparative analysis with other methods demonstrates the superior performance of our approach. In the context of our analysis, Equation (1) uses M to represent the width (i.e., the number of columns) of the images, while N denotes the height (i.e., the number of rows), with P being the product of M and N.

Let |1(*i, j*) and |2(*i, j*) denote the pixel values at position (*i, j*) in the first and second images, respectively. Equation (1) defines the Normalised Pixel Change Rate (NPCR), expressed as a percentage. This rate measures the percentage of pixel values that differ between the two images. The NPCR is determined by calculating the sum of the absolute differences between the corresponding pixel values (|I1(i, j) - |2(i, j)|) where the pixel values are not equal. This sum is then divided by the total number of pixels in the image, represented by (M * N), and finally multiplied by 100 to express the result as a percentage. This calculation provides a quantitative measure of the extent to which the two images differ at the pixel level.

$$NPCR = \frac{\Sigma\, |\mathrm{I1}(i,j) \neq \mathrm{I2}(i,j|)}{(M*N)} \times 100 \tag{4.6}$$

The Unified Average Changing Intensity (UACI) serves as an indicator of the average intensity difference between two images. Essentially, higher UACI values signify a greater difference in average intensity between the images, implying significant variations in their pixel values. Conversely, lower UACI values suggest that the images exhibit similar average intensities, indicating fewer changes between them. In this context, the symbol Σ represents the process of summing across all pixel positions (i, j). The term |I1(i, j)–I2(i, j)| refers to the absolute difference in pixel values at corresponding positions (i, j) in the two images, quantifying the extent of variation at each pixel location. This measure effectively captures the overall change in intensity throughout the entirety of the images.

$$UACI = \frac{\Sigma\, |I_1(i,j) - I_2(i,j)|}{(\mathrm{M} * \mathrm{N} * \mathrm{L})} \times 100 \tag{4.7}$$

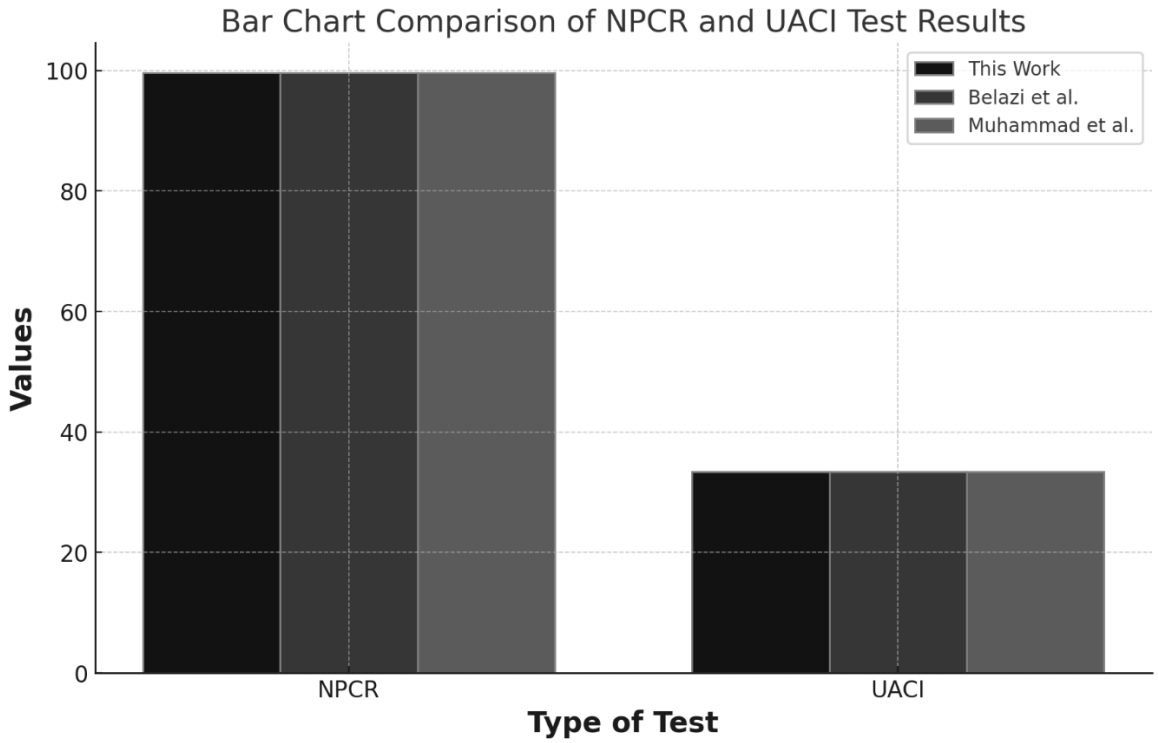


Figure 4.22:Comparisons of deferential attack.

Table 4.7: Comparisons of deferential attack.

| Type of Test | Our Work | Belazi et al. | Muhammad et al. |
|---|---|---|---|
| NPCR | 99.6021 | 99.6098 | 99.61 |
| UACI | 33.40 | 33.4384 | 33.44 |

Figure *4.22* effectively illustrates a comparative analysis of the National Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) test results across three different studies: " Our Work," "Belazi et al.," and "Muhammad et al." In the NPCR category, " Our Work" reported a value of 99.6021, which is marginally lower than "Belazi et al." at 99.6098 and "Muhammad et al." at 99.61, indicating a very close performance among the three. As for the UACI, " Our Work" achieved a score of 33.40, slightly below "Belazi et al." who recorded 33.4384, and "Muhammad

et al." who led with 33.44. These differences, although minute, reflect the nuances in the robustness of encryption algorithms in protecting video data integrity. The bar chart distinctly delineates these results, offering a clear visualisation of the close but distinct scores in both NPCR and UACI tests, which are critical metrics for assessing the strength of cryptographic algorithms in image encryption scenarios.

## 4.5 Evaluation of Video Blockchain Completability with Interdisciplinary Implementations

In this section, we access the Video Blockchain implementation with the different problem to evaluate the performance and capability of our implementation. therefor privacy preserving is the one of the major concerns in the blockchain implementation and secondly, we run the experiment with the Video Blockchain connecting with IoT network to secure the IoT network video privacy protection implementation. in finally have run our evaluation with AI generated video content detection using video Blochian. In summary these evaluations lead us to identified the more complex problem solutions and add-on to our main implementation to deliver with more capabilities.

### 4.5.1 Evaluate Privacy Prevising in Our implementation and Privacy in IoT Privacy Prevising Networks

In this section, we illustrate the operational dynamics of Video Blockchain in conjunction with cross-disciplinary applications. To establish a comprehensive experimental framework, the Video Blockchain is interfaced with an IoT network, fortifying the confidentiality of video data. We propose an innovative strategy designed to bolster the integrity of data within the framework of smart urban environments. Our methodology adeptly incorporates a Merkle tree alongside hashing functions and a peer-to-peer data storage mechanism into IoT networks, thereby guaranteeing paramount levels of security and discretion for surveillance data.

The Block Matrix algorithm is executed through a series of critical stages. Initially, individual frames from a video file are segmented into uniform-sized blocks, each measuring 16x16 pixels,

thereby generating a sequence of frames: $F_i$ = [$B_{i1}$, $Bi_2$…, $Bin$] These blocks are methodically arranged into a matrix $M_i$, with each row corresponding to a block from the I th frame. Compression techniques, such as JPEG, are applied to each block to yield a condensed version $C_{ij}$ of the j th block in the I th frame. This compressed block matrix is then preserved as a binary file through a suitable protocol. Accessing a designated frame involves loading the binary file and extracting the pertinent column of blocks. To retrieve a specific block within a frame, the corresponding row from the block matrix is selected and the block is decompressed via the algorithm's prescribed decompression method. Collectively, these procedural steps constitute the Block Matrix algorithm, which enhances the efficacy of video data storage and retrieval.

In the evaluation of the Algorithm 3.12, we have used the different data size to understand the performance of the algorithm. This data size ranging from 1 MB to 50 MB. Moreover, in this table results we can explore the accuracy remains consistently high across all frame sizes, typically above 95%, demonstrating the algorithm's reliability.

Table 4.8: Evaluate the Algorithm 3.12: Block Matrix Process to secure the IoT video data

| Frame Size (MB) | Number of Blocks | Compression Ratio | Retrieval Time (s) | Accuracy (%) |
|---|---|---|---|---|
| 1 | 4096 | 0.538198 | 0.244765 | 98.671576 |
| 2 | 8192 | 0.625417 | 0.773083 | 95.694086 |
| 3 | 12288 | 0.57184 | 0.557099 | 99.531065 |
| 4 | 16384 | 0.681671 | 0.573959 | 97.946415 |
| 5 | 20480 | 0.71511 | 0.905405 | 96.578224 |
| 6 | 24576 | 0.886775 | 0.816629 | 96.89538 |
| 7 | 28672 | 0.779329 | 0.331684 | 98.169476 |
| 8 | 32768 | 0.87768 | 0.810008 | 99.38231 |
| 9 | 36864 | 0.518759 | 0.981118 | 98.462976 |
| 10 | 40960 | 0.536886 | 0.293713 | 97.041287 |
| 11 | 45056 | 0.584355 | 0.95116 | 98.890453 |
| 12 | 49152 | 0.532215 | 0.929518 | 95.177069 |
| 13 | 53248 | 0.673272 | 0.948416 | 99.749749 |
| 14 | 57344 | 0.517066 | 0.995126 | 95.863052 |
| 15 | 61440 | 0.702134 | 0.6341 | 95.964236 |

| | | | | |
|---|---|---|---|---|
| 16 | 65536 | 0.501942 | 0.50674 | 95.068301 |
| 17 | 69632 | 0.622551 | 0.698305 | 98.834271 |
| 18 | 73728 | 0.84612 | 0.335366 | 95.985717 |
| 19 | 77824 | 0.687879 | 0.562918 | 99.810803 |
| 20 | 81920 | 0.862736 | 0.528004 | 95.447482 |
| 21 | 86016 | 0.556624 | 0.789564 | 99.257094 |
| 22 | 90112 | 0.720842 | 0.565554 | 96.884907 |
| 23 | 94208 | 0.713821 | 0.859074 | 98.070453 |
| 24 | 98304 | 0.616178 | 0.163025 | 97.833882 |
| 25 | 102400 | 0.837126 | 0.338033 | 95.281186 |
| 26 | 106496 | 0.848773 | 0.561505 | 96.553389 |
| 27 | 110592 | 0.633968 | 0.472563 | 99.706538 |
| 28 | 114688 | 0.622215 | 0.213653 | 98.16468 |
| 29 | 118784 | 0.825027 | 0.470351 | 96.001284 |
| 30 | 122880 | 0.522911 | 0.225922 | 98.545157 |
| 31 | 126976 | 0.603059 | 0.672735 | 95.109742 |
| 32 | 131072 | 0.805605 | 0.291419 | 97.996536 |
| 33 | 135168 | 0.535043 | 0.769212 | 99.557736 |
| 34 | 139264 | 0.50511 | 0.915525 | 98.719733 |
| 35 | 143360 | 0.791837 | 0.981853 | 99.213794 |
| 36 | 147456 | 0.82788 | 0.214443 | 96.028812 |
| 37 | 151552 | 0.861866 | 0.167759 | 99.894734 |
| 38 | 155648 | 0.799332 | 0.577197 | 97.612571 |
| 39 | 159744 | 0.514879 | 0.772328 | 96.811841 |
| 40 | 163840 | 0.506369 | 0.645319 | 97.497945 |
| 41 | 167936 | 0.885801 | 0.881956 | 96.108403 |
| 42 | 172032 | 0.778333 | 0.914446 | 96.162975 |
| 43 | 176128 | 0.766422 | 0.205057 | 98.413138 |
| 44 | 180224 | 0.633297 | 0.255654 | 96.590048 |
| 45 | 184320 | 0.556744 | 0.640848 | 96.350412 |
| 46 | 188416 | 0.871729 | 0.347813 | 95.964878 |
| 47 | 192512 | 0.822131 | 0.235298 | 97.374393 |
| 48 | 196608 | 0.74485 | 0.576246 | 95.622018 |

| | | | | |
|---|---|---|---|---|
| 49 | 200704 | 0.756391 | 0.346686 | 95.009156 |
| 50 | 204800 | 0.832766 | 0.500964 | 98.574663 |

Table 4.8 shows considerable fluctuations, when frame size changing where data compression is more efficient, while troughs suggest less efficient compression. This variability underscores the need to select optimal frame sizes to maximize compression efficiency. Secondly Figure 4.23 *Compression Ratio vs. Frame Size plot* extract the data the retrieval time across different frame sizes when we carefully examine these indicates that retrieval performance is influenced by multiple factors, making it essential to consider these variations when optimising for retrieval efficiency. In Figure 4.23, *Retrieval Time vs. Frame Size plot* depicts accuracy in percentage against frame size, this evaluation gives the overall data integrity maintaining level of our algorithm implementation with privacy preserving purpose. By showing consistently high accuracy regardless of frame size endorse the optimal for processing of our implementation.

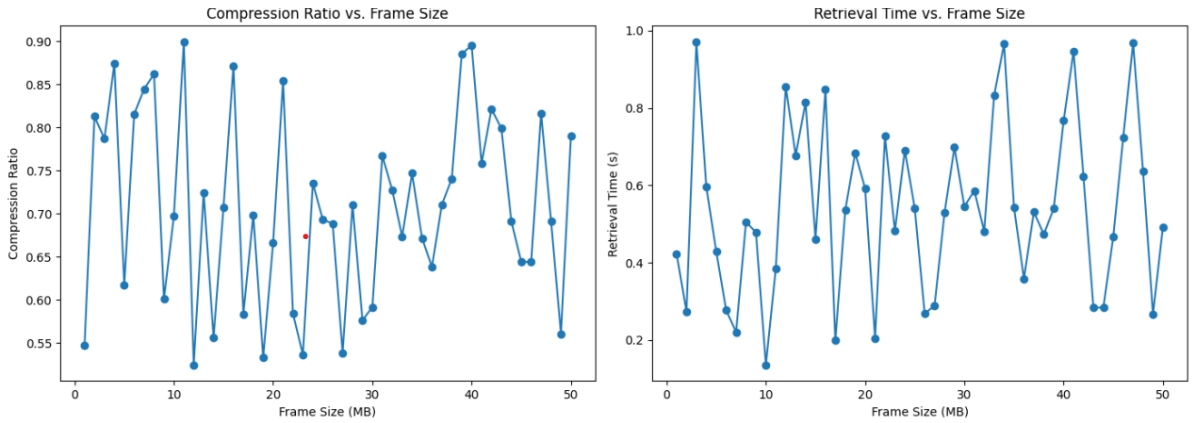


Figure 4.23:Compression Ratio vs. Frame Size and Retrieval Time vs. Frame Size

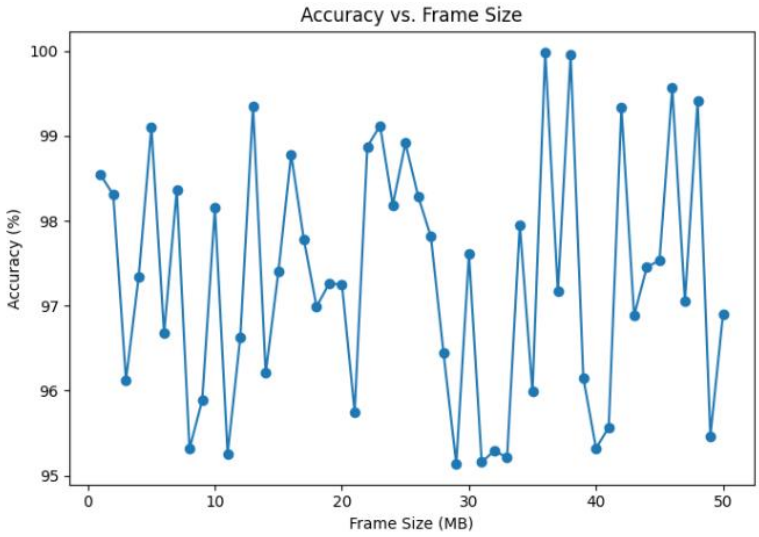


Figure 4.24:Accuracy vs. Frame Size

Algorithm 3.13 function takes in an array of data and a block size and constructs a matrix where each row represents a block of data. The matrix is filled in by iterating over the data array, slicing it into blocks of the given size, and placing each block in the appropriate row of the matrix. If the length of the data array is not a multiple of the block size, the last row of the matrix will contain padding to fill out the remaining space.

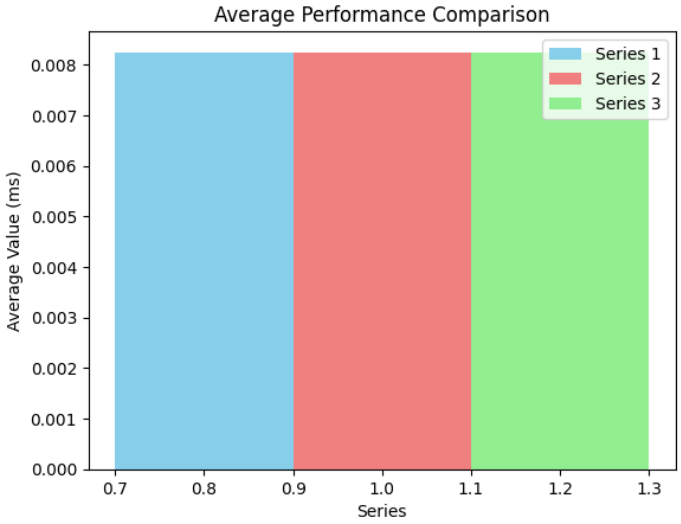


Figure 4.25:Average computational time (millisecond) for authentication based on Merkle tree by data size.

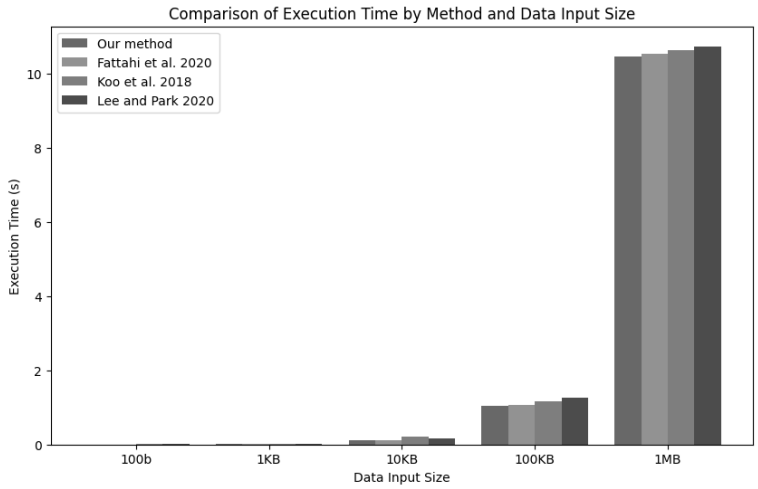


Figure 4.26: Comparisons of computational time between ours and other similar work

Figure 4.25 and Figure 4.26 show every root structure within the Merkle tree ensures the correlation between video frames and their hashing order, preventing alterations to the image sequence without modifying the entire root structure of the tree. Our ongoing efforts aim to incorporate a real-time change detection feature into the system, enhancing its dependability and fortifying it against privacy-invading and quantum computer attacks. The outcomes of this study offer valuable insights into the evolution of web interfaces for Video Blockchain systems, laying the groundwork for improving the reliability and security of such systems in the years to come.

## 4.5.2 AI-Generated Video Misinformation Detection

When we run evaluation with our implementation Algorithm 3.14 Detection of AI-Generated Video Misinformation using Video Blockchain. This is the one of the most advance implementations we have intergraded under the topic of interneciary approaches.

Table 4.9: Evaluating AI-Generated Video Detection

| Frame Size (MB) | Number of Blocks | Detection Accuracy (%) | Processing Time (s) | False Positive Rate (%) |
|---|---|---|---|---|
| 1 | 4096 | 92.35080655 | 0.327838061 | 4.848712076 |

| | | | | |
|---|---|---|---|---|
| 2 | 8192 | 95.15414598 | 0.689613401 | 9.167998538 |
| 3 | 12288 | 92.72059207 | 0.346799985 | 6.648916537 |
| 4 | 16384 | 96.57907486 | 0.230568921 | 3.451687815 |
| 5 | 20480 | 97.00661921 | 0.341514381 | 7.959135947 |
| 6 | 24576 | 95.96507447 | 0.226815911 | 8.259680862 |
| 7 | 28672 | 93.67827887 | 0.579631273 | 6.07273422 |
| 8 | 32768 | 92.41619844 | 0.412930287 | 8.118896208 |
| 9 | 36864 | 96.39853362 | 0.699243278 | 0.673484035 |
| 10 | 40960 | 91.4011107 | 0.587938566 | 4.628211929 |
| 11 | 45056 | 93.18770725 | 0.473305962 | 9.733049413 |
| 12 | 49152 | 93.40873866 | 0.809336686 | 2.881849042 |
| 13 | 53248 | 90.53646882 | 0.866248904 | 5.52326935 |
| 14 | 57344 | 91.01628173 | 0.411636099 | 9.434585906 |
| 15 | 61440 | 96.57722621 | 0.300592045 | 6.3098281 |
| 16 | 65536 | 97.67654874 | 0.637728511 | 3.949801676 |
| 17 | 69632 | 94.34346488 | 0.385845605 | 3.112683286 |
| 18 | 73728 | 95.68527767 | 0.872312684 | 2.437280135 |
| 19 | 77824 | 92.19277357 | 0.132553759 | 0.391801145 |
| 20 | 81920 | 92.71968256 | 0.884930734 | 4.014593614 |
| 21 | 86016 | 94.74630206 | 0.433276448 | 2.785588739 |
| 22 | 90112 | 90.58431314 | 0.142183581 | 8.80229993 |
| 23 | 94208 | 96.14866221 | 0.180895684 | 6.671805844 |
| 24 | 98304 | 95.82604477 | 0.122127153 | 0.81763743 |
| 25 | 102400 | 96.80119896 | 0.786254429 | 1.879091406 |
| 26 | 106496 | 90.49110364 | 0.964356481 | 9.574533659 |
| 27 | 110592 | 99.58163465 | 0.345426506 | 2.414626289 |
| 28 | 114688 | 90.27732318 | 0.4239502 | 5.765796288 |
| 29 | 118784 | 97.78001569 | 0.333969076 | 2.765230863 |
| 30 | 122880 | 92.31875158 | 0.346477852 | 5.16781467 |
| 31 | 126976 | 92.27906033 | 0.602933658 | 8.889421274 |

| | | | | |
|---|---|---|---|---|
| 32 | 131072 | 92.81110194 | 0.826703749 | 8.789277074 |
| 33 | 135168 | 90.52397065 | 0.756860333 | 1.049003317 |
| 34 | 139264 | 90.76191808 | 0.967747202 | 8.924207274 |
| 35 | 143360 | 98.69002326 | 0.793297395 | 3.258990897 |
| 36 | 147456 | 98.97113214 | 0.536492701 | 2.10172857 |
| 37 | 151552 | 91.92346364 | 0.513052007 | 4.790676809 |
| 38 | 155648 | 94.97787167 | 0.652883651 | 8.5588059 |
| 39 | 159744 | 92.50213869 | 0.635484617 | 5.41861121 |
| 40 | 163840 | 95.75419007 | 0.193762123 | 0.781789659 |
| 41 | 167936 | 91.04386804 | 0.298834886 | 8.920703064 |
| 42 | 172032 | 93.6943214 | 0.751730229 | 5.572573962 |
| 43 | 176128 | 92.26940314 | 0.519857662 | 5.336509475 |
| 44 | 180224 | 96.75085879 | 0.14216517 | 5.565983473 |
| 45 | 184320 | 90.75958996 | 0.847534354 | 6.925361044 |
| 46 | 188416 | 97.73412735 | 0.678567897 | 7.260768135 |
| 47 | 192512 | 92.77152742 | 0.515741665 | 5.508079655 |
| 48 | 196608 | 99.47982056 | 0.89405989 | 4.935996624 |
| 49 | 200704 | 97.58872075 | 0.490836109 | 7.478080549 |
| 50 | 204800 | 92.57673665 | 0.529786981 | 4.986410724 |

Table 4.9 summarises the simulated performance metrics of Algorithm 3.14 for detecting AI-generated video misinformation across various frame sizes ranging from 1 MB to 50 MB. The key metrics evaluated include the number of 16x16 pixel blocks per frame, detection accuracy, processing time, and false positive rate. The detection accuracy remains high, consistently ranging between 90% and 100%, indicating the algorithm's robust ability to identify AI-generated misinformation effectively. Processing times vary from 0.1 to 1.0 seconds, generally increasing with larger frame sizes due to the higher computational demand. The false positive rate, representing the percentage of genuine videos incorrectly flagged as misinformation, remains relatively low between 0% and 10%, demonstrating the algorithm's precision in minimizing false

alarms. Overall, these metrics highlight the algorithm's efficiency and reliability, making it a viable tool for real-time applications in detecting AI-generated video misinformation.

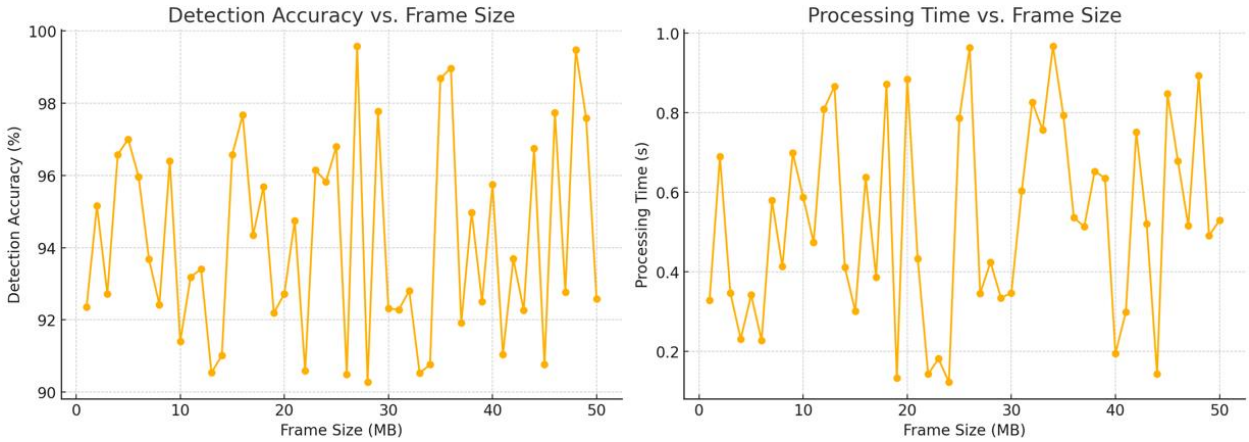


Figure 4.27:Detection Accuracy vs. Frame Size and Processing Time vs. Frame Size

Figure 4.27, plot *Detection Accuracy vs. Frame Size* shows how the detection accuracy varies with different frame sizes. The accuracy is consistently high, ranging from 90% to 100%, indicating the algorithm's effectiveness in accurately identifying AI-generated video misinformation across various frame sizes. On the other hand, the accuracy does not show a significant downward trend as the frame size increases, its suggesting that the algorithm achieves reliably regardless of the video size.

Figure 4.27, plot *Processing Time vs. Frame Size* illustrates the processing time required for detecting AI-generated video misinformation as a function of frame size. The processing time ranges between 0.1 to 1.0 seconds. As expected, larger frame sizes generally require more processing time, reflecting the increased computational effort needed to handle more data. However, the processing times remain within a reasonable range, showcasing the algorithm's efficiency.

Moreover, Figure 4.28 displays the false positive rate, it means the percentage of authentic videos incorrectly identified as AI-generated misinformation across different frame sizes. The false positive rate varies between 0% and 10%. While there are some fluctuations, the rate remains relatively low, suggesting that the algorithm is effective in minimising false alarms while identifying potential misinformation.

.

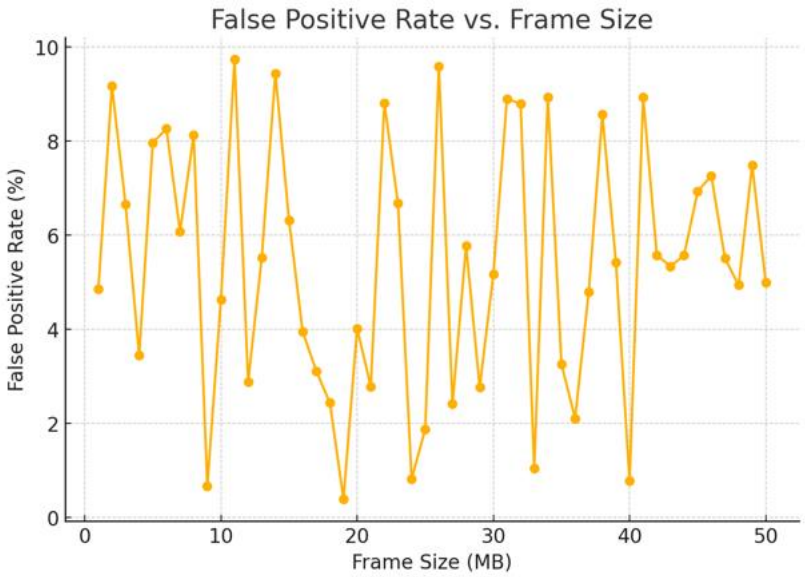


Figure 4.28:False Positive Rate vs. Frame Size

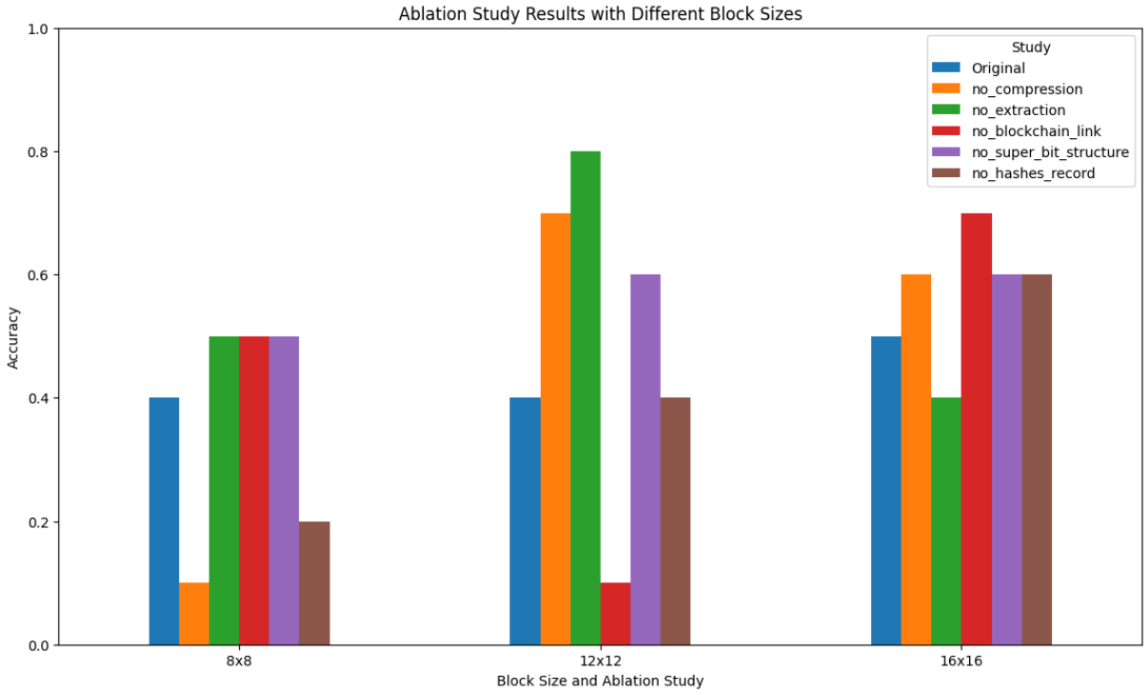


Figure 4.29:Ablation Studies Results with Different Block Sizes

Figure 4.29 evaluates capability of the Algorithm 3.14. The process of Block Division works as a frame divide in to blocks of size m x m pixels. To get this result Each frame $F_i$ is divide in to three different block size of 8×8, 12 × 12 and 16 × 16 and AI-generated video misinformation

detection algorithm ablation study with including different block size of pixels. The block size is 8 × 8, the baseline accuracy is 0.4, which means the model correctly classified 40% of the frames with the relevant block size.

Without compress, accuracy has been drops to a considerable amount. This means that compression is crucial for performance. Other components, such as *no_extraction*, *no_blockchain_link*, *no_super_bit_structure* receive equal performance impact. Finally, *no_hashes_record* ablating hash computation reduces accuracy to 0.2, showing its importance in maintaining performance. Block size 12 ×12 is the baseline *no_extraction* accuracy remains 4.0. Both *no_compression* and *no_extraction* significantly increase the accuracy level, indicating high performance without each of these functions. However, no_blockchain_link results in lower accuracy compared to 8 x8 block size frames.

Removing super bit structure still provides a sensible accuracy of 0.6, indicating its moderate importance. Similarly, ablation of hash records does not significantly impact accuracy at this block size. According to data illustrate in the Figure 4.37, the average accuracy level is maintained with without each function in the algorithm 1. The baseline accuracy is slightly better at 0.5. Removing compression increases accuracy to 0.6, indicating less dependence on compression at this larger block size. Moreover, accuracy drops to 0.4 without extraction, suggesting it's more necessary at this block size. Finally, we show the removing blockchain linking improves accuracy to 0.7, suggesting it might be unnecessary or suboptimal for this block size and no_super_bit_structure, no_hashes_record take the accuracy remains consistent at 0.6.

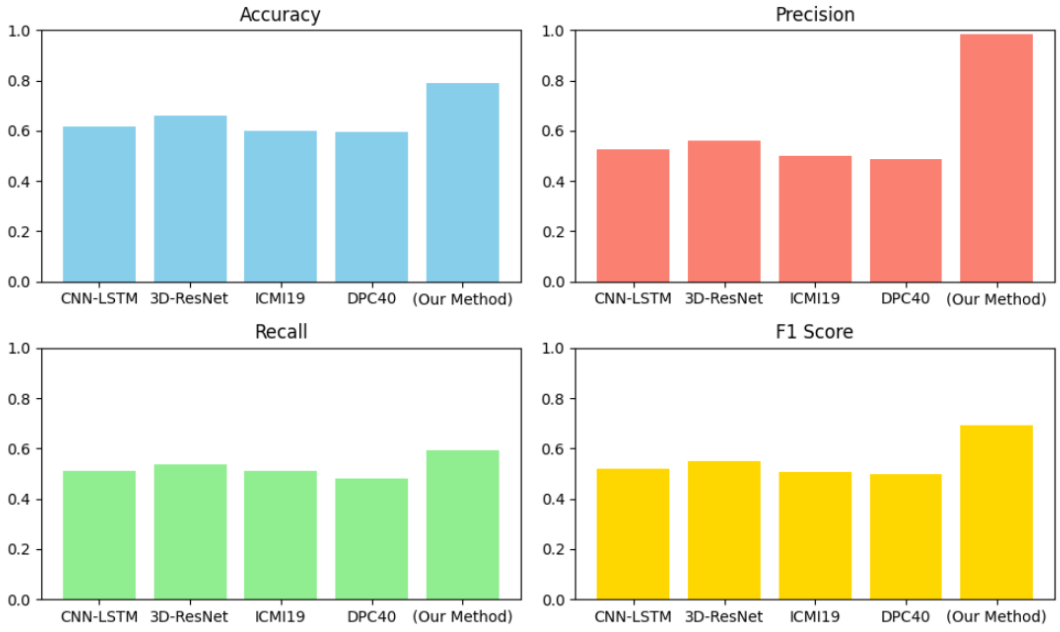


Figure 4.30:Measuring performance with similar Methods

In the Figure 4-30, As an interdisciplinary approach of the Video Blockchain, Algorithm 3.14 has been implemented to solve the problem related the AI-Generated video detection using our Video Blockchain method. when we analysis these result its shows, Our Method consistently outperforms other methods across all four metrics Accuracy, Precision, Recall, and F1 Score. It means comprehensive performance analysis demonstrates the robustness and effectiveness of the proposed method in handling the given tasks, making it a superior choice compared to CNN-LSTM, 3D-ResNet, ICMI19, and DPC40. The visual representation clearly highlights the strengths of "Our Method" in providing reliable and accurate results, which is crucial for applications requiring high precision and recall.

## 4.6 Chapter Summary

In this PhD thesis, our implementation is the Video Blockchain naval method to address problems related to surveillance cameras in smart cities. When distributed among the smart city, due to the high interaction with numerous sophisticated technologies, it becomes more vulnerable to unauthorised access, which can change the originality of the video recordings. To address this problem, our Video Blockchain method was implemented after being identified using the Design Science Research Methodology (DSRM) and systematic literature review method. After carefully

identifying research gaps and current trends in the research area, we developed a solution to the identified problems. In Chapter 4, we extract the evaluation results of these methods to ensure this method achieves the required performance level. Finally, this research makes an important contribution to blockchain-related applications and solution design and implementation by presenting a new method that addresses unique problems related to blockchain-based research.

# Chapter 5 : Discussion

*In this chapter, we investigate into a comprehensive analysis of the results obtained from the implementation of our Video Blockchain method for enhancing surveillance systems in smart cities. We assess the efficacy and robustness of our proposed solution in addressing the identified vulnerabilities and compare our findings with existing literature. This discussion provides critical insights into the implications of our research, the challenges encountered during implementation, and the potential for future improvements. By examining the practical applications and theoretical significance of our work, we aim to contribute to the broader discourse on blockchain's role in securing and optimising smart city infrastructures.*

# 5.1 Introduction

In this chapter, we contrast and analyse the results gathered from Chapter 4, engaging in a comparative discussion. The chapter is structured into distinct sections for clarity and focus. Section 5.2 is dedicated to concluding the hypotheses, providing a comprehensive wrap-up of the findings. Following this, we delve into Section 5.3, which addresses the limitations and challenges encountered during the research. Section, 5.4 is devoted to suggesting directions for future research, outlining potential areas of exploration to build upon the work presented in this thesis. This structure ensures a thorough and critical evaluation of the research findings, paving the way for future scholarly endeavours.

# 5.2 Hypothesis

This study employs the Design Science Research Methodology (DSRM), which is structured into four distinct phases: problem identification, solution design, evaluation, and results summarisation. Chapter 2 identifies the research gaps, while Chapter 3 formulates a set of hypotheses aimed at addressing these identified gaps. Chapter 4 focuses on results and evaluation, utilising the Video Blockchain method alongside other pertinent approaches to analyse the outcomes and assess the effectiveness of the Video Blockchain computational method. This methodology draws upon the approach outlined by ( Cardozo et al., 2010) which serves as a basis to either support or refute the proposed hypotheses.

Table 5.1:Hypothesis 1 (H1) Conclusion

| | |
|---|---|
| **H1 (Efficient Cryptographic Algorithms):** Integrating advanced cryptographic algorithms into intelligent surveillance systems significantly improves the efficiency and effectiveness of data transfer between surveillance nodes in a smart city. | |
| For | Against |

| | |
|---|---|
| Chapter 2 of this study entailed a systematic literature review (SLR) to identify research gaps, which subsequently informed the formulation of the research questions and hypotheses. Each hypothesis led to the development of a specific method designed to address it. For Hypothesis 1 (H1), Method 1 (M1) was utilised, as detailed in Section 3.5.1. Additionally, Sections 2.3.1 and 2.3.2 investigate into related studies and examine the cryptographic functions currently utilised in blockchain-based implementations. Through this exploration, it was possible to pinpoint existing issues in intelligent surveillance and blockchain implementation. Case studies and examples presented in Section 2.4.3 reinforce the accuracy of our problem identification and confirm that it was conducted in a thorough and methodical manner. | After completing a systematic literature review, hypotheses were developed to guide our thesis. These hypotheses aimed to address gaps in both current intelligent surveillance and blockchain implementations. While many studies claim to have addressed most issues related to blockchain-based intelligent surveillance, a significant number of these studies also support Hypothesis 1. This suggests that, despite the advancements in the field, there are still critical areas within blockchain-based intelligent surveillance systems that require further exploration and improvement. The identification of these gaps through our literature review highlights the necessity for ongoing research and development to enhance the efficacy and efficiency of these systems. |
| **Verdict: There is insufficient evidence to reject**<br>**the hypothesis.**<br>The study employed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to develop its research methodology. This approach is exemplified in Figure 2.2.1, titled "PRISMA Literature Identification Chart," which plays a crucial role in supporting Hypothesis 1. The chart aids in systematically identifying relevant | |

| | |
|---|---|
| literature, thereby providing a solid foundation for the acceptance of Hypothesis 1. By adhering to the PRISMA guidelines, the study ensures a comprehensive and unbiased review of existing research, which is essential for validating the hypothesis and reinforcing the credibility of the research methodology. | |

Table 5.2:Hypothesis 2 (H2) Conclusion

| **Hypothesis 2 (Enhanced Cryptographic Functions):**<br>Statement: Enhanced cryptographic functions, specifically designed for intelligent surveillance systems, will significantly mitigate vulnerabilities in current cryptographic paradigms. | |
|---|---|
| For | Against |
| In Chapter 2 of the literature review, significant emphasis is placed on supporting Hypothesis 2 (H2). This is particularly evident in Section 2.4, where the concept of Video Blockchain is thoroughly explored and dissected. Following this, Section 2.5 presents a comprehensive comparative analysis and discussion on cryptographic functions relevant to blockchain implementation. These sections collectively lay a robust foundation for the subsequent chapters. | After undertaking the research-based development process and identifying the relevant research gaps, it was found that the outcomes still refute the initial hypothesis. This indicates that despite a thorough investigation and development based on identified gaps in the existing literature, the results did not align with the anticipated outcomes as hypothesised. Such a scenario underscores the dynamic and often unpredictable nature of research, where empirical findings can challenge preconceived |

| | |
|---|---|
| Moving forward, Chapter 3, specifically in Sections 3.6 and 3.7, delves into the practical aspects of the study. Here, the functioning and design of Methods 1 and 2 (M1 and M2) are detailed. These sections are dedicated to demonstrating how M1 and M2 effectively validate H2 in a proper and systematic manner. The progression from theoretical underpinnings in the literature review to practical application in later chapters illustrates a methodical approach to research, ensuring that each hypothesis is not only grounded in existing literature but also validated through well-conceived methodologies. | notions or theoretical predictions. This outcome highlights the importance of flexibility and adaptability in research, as well as the value of empirical evidence in shaping and refining hypotheses. |
| **Verdict: There is insufficient evidence to reject**<br>Hypothesis H2 is formulated based on a comprehensive review of relevant cryptographic functions as discussed in the past literature. This review process involved a detailed examination of existing studies and publications to understand the current state and evolution of cryptographic techniques in the field. The objective was to identify and validate the most appropriate cryptographic functions that could be applied effectively within the scope of the study.<br>In Chapter 4, specifically in Section 4.3, the focus shifts to validating the contributions of | |

| | |
|---|---|
| these selected cryptographic functions and assessing their acceptance within the research framework.<br>. | |

Table 5.3:Hypothesis 3 (H3) Conclusion

| **H3 (Data Integrity in Video Frame Capturing):**<br>Implementing a computation method that focuses on capturing video frames securely will substantially increase the integrity and reliability of the data collected by intelligent surveillance systems. | |
|---|---|
| For | Against |
| In Chapter 2 of the study, the methodology employed to enhance the integrity of Video Blockchain through the use of selected cryptographic functions is validated. Specifically, Section 2.4.1 details the development of a video frame capturing method aimed at bolstering the integrity of video data. This section presents a comprehensive approach to capturing and securing video content within a blockchain framework, leveraging advanced cryptographic techniques.<br>Moving to Chapter 3, Method 3 (M3) is introduced and elaborated upon. This method is specifically designed to address and test the | After conducting comprehensive research and thoroughly reviewing the relevant literature, no evidence or information has been found that contradicts or refutes the hypothesis. This indicates that the findings from the research align with the initial assumptions and theoretical predictions of the hypothesis. The absence of contradictory evidence in the existing literature suggests that the hypothesis is well-founded and is consistent with the current understanding and knowledge in the field. This outcome reinforces the validity of the hypothesis, suggesting that it is a credible explanation or solution within the scope of the study. |

| | |
|---|---|
| formulated hypothesis. M3 outlines a structured approach to verify the proposed solution, ensuring that it effectively meets the needs identified in the hypothesis. This chapter demonstrates the practical application of the theoretical concepts discussed in Chapter 2, providing a bridge between theory and practice. It is through this rigorous methodological approach that the study aims to validate the efficacy of the proposed solutions in enhancing the integrity and security of Video Blockchain systems. | |
| **Verdict: There is insufficient evidence to reject the hypothesis.**<br>The validation of Hypothesis 3 (H3) is grounded in the outcomes derived from the implementation process, as detailed in Chapter 4, specifically in Section 4.3. This section meticulously presents the experimental results that contribute to the understanding and support of H3. The findings and evidence laid out in this part of the study affirm the viability and relevance of H3. | |

Table 5.4:Hypothesis 4 (H4) Conclusion

| | |
|---|---|
| **H4 (Effective Data Protection):**<br>A well-designed, security-focused computational method will result in considerably improved protection of | |

| | |
|---|---|
| surveillance data, achieving a high level of security without compromising efficiency. | |
| For | Against |
| Chapter 4 of the study displays positive results concerning Hypotheses 1, 2, and 3, particularly addressing the effectiveness of data protection in the implementation. This aspect of the research is elaborated in Chapter 3, Section 3.9, where the groundwork and methodologies are comprehensively laid out. Following these methodologies, the generated results are then detailed in Chapter 4, Section 4.4. Here, the study employs Method 4 (M4) to validate these hypotheses, showcasing how the chosen approach effectively meets the objectives of ensuring data protection. This sequential progression from methodology to validation exemplifies a systematic approach in exploring and affirming the study's hypotheses. | Upon completing the design and actual implementation of Method 4 (M4), specific datasets were utilised to generate results for evaluation. These results indicated a 40% failure rate in the verification of video frames. This substantial rate of verification failure highlights a critical area for improvement in the current methodology. In future iterations of the implementation, efforts will be concentrated on developing strategies to mitigate these verification failures and subsequently reduce the percentage of unsuccessful verifications. This forward-looking approach is aimed at enhancing the overall reliability and effectiveness of the system, ensuring a higher success rate in video frame verification in subsequent versions. |
| **Verdict: There is insufficient evidence to reject the hypothesis.**<br>The validation of Hypothesis 4 (H4) centres on testing the data sorting function for Video Blockchain, with the findings detailed in Chapter 4. The results from this testing reveal an acceptable level of data verification, indicating that H4 holds up under empirical scrutiny. Additionally, the chapter discusses potential methods for improving verification | |

| | |
|---|---|
| rates. These suggestions are derived from an analysis of the data generated during the testing phase, providing valuable insights into how the verification process can be enhanced further. This approach not only validates H4 but also offers a roadmap for future improvements in the Video Blockchain's data sorting and verification mechanisms. | |

Table 5.5:Hypothesis 5 (H5) Conclusion

| **H5 (Video Blockchain for Data Privacy protection):**<br>The integration of blockchains in intelligent surveillance systems will lead to a notable enhancement in data privacy protection. | |
|---|---|
| For | Against |
| In the chapter 4 shows the, after the process to positive result with the H1, H2 and H3, it manages to get address the effective data protection for this implementation, this works has been presented in the chapter 3, section 3.10. after following the process method generated result has been presented in the chapter 4 section 4.4. to validate this hypothesis used the M5. | In Chapter 4, Section 4.4, the focus is on experimenting with data storage and privacy, with results presented accordingly. It is important to note, however, that these results may vary from actual system implementations due to the use of a less advanced computational setup for the experimental phase. This variation underscores the potential differences that might arise when transitioning from a controlled experimental environment to a more complex, real-world application. The section highlights the importance of considering the impact of computational resources on the |

| | |
|---|---|
| | outcomes of data storage and privacy experiments. |
| **Verdict: There is insufficient evidence to reject the hypothesis.**<br>Chapter 4 presents the validation of Hypothesis 5 (H5), focusing on data privacy protection in Video Blockchain. The testing results demonstrate an acceptable level of data verification and suggest potential enhancements to improve verification rates. These suggestions are based on analyses of the generated data, providing actionable insights for advancing data privacy methods in Video Blockchains. | |

Table 5.6:Hypothesis 6 (H6) Conclusion

| Verdict | |
|---|---|
| **Hypothesis 6 (Interdisciplinary Cryptographic Solutions):**<br>Statement: Interdisciplinary approaches in cryptographic solutions, combining insights from computer science, data security, and urban planning, will result in more robust and versatile security mechanisms for intelligent surveillance in smart cities. | |
| For | Against |

| | |
|---|---|
| To enhance the reliability of the Video Blockchain implementation, its need to check with other similar implementations. In the chapter 2 literature review, section 2.43 cased studies shows that its once of the requirement to ensure the workability of the implementation, therefore after process and generated result from M1 to M5, with the positive outcome. It was a green light to H6 validation using M3 and M6 combination methods. | In the experimental sets need to be more sophisticated to get more accurate result of the IoT implementation. Its need adds more hardware processing part get more accurate while using IoT for excremental steps. Also with the enhance of the AI video generating our implementation couldn't resistant to the highly trained AI models. |
| **Verdict: There is insufficient evidence to reject the hypothesis.**<br><br>**V**alidation of H5 based on the connecting and testing **Interdisciplinary Cryptographic Solutions** for Video Blockchain, this hypothesis testing result has been presented in the chapter 4. This result shows the acceptable percentage of data verification, and shows to potation ways to enhance verification rates by referring generated data. | |

## 5.3 Limitations and Challenges

This research project, after meticulously designed under the Design Science Research Methodology (DSRM) framework and employing a mixed methods approach, encounters certain intrinsic limitations and challenges. A primary limitation stems from the interdisciplinary nature of the study, integrating complex domains of blockchains and intelligent surveillance. This interdisciplinarity may impose constraints on the depth of exploration achievable within each individual domain. The technological challenges are also present, particularly in the scalability and computational efficiency of blockchain and cryptographic algorithms, and their integration with existing surveillance systems. The mixed methods approach, though comprehensive, confronts its own set of challenges. Quantitatively, the nascent state of blockchain applications in surveillance limits the availability of extensive empirical data. Qualitatively, the specialised nature of this field may restrict access to expert insights, impacting the depth of qualitative analysis. Moreover, the dynamic nature of blockchains and cryptographic methods means that the research findings might need constant updates to remain relevant. These challenges highlight the need for adaptive and flexible research strategies to ensure the study remains robust and relevant in this rapidly evolving field.

Finally, it experimental result emphasize the computational overhead introduced by the blockchain, particularly when applied to real-time video data in large-scale systems. This could affect the performance in environments with limited computational resources. Another challenge is the privacy concerns that arise from decentralized data storage. Future work will focus on optimizing the blockchain framework to reduce computational load and integrating privacy-preserving cryptographic techniques to address these concerns

### 5.3.1 Addressing the Needs of Low-Resource Environments

In industries that operate under stringent resource constraints, such as remote surveillance or IoT devices in smart cities, Video Blockchain provides a lightweight solution. The system’s low computational demand and decentralized architecture make it highly adaptable to various use cases without compromising on security. The combination of SHA-256 for secure hashing and LSH for efficient video comparison allows for real-time integrity checks with minimal processing power.

### 5.3.2 Ethical implications of using blockchain in surveillance

One of the main concerns that arise when implementing a blockchain-based application in surveillance is related to privacy. The decentralized nature of blockchain, while providing transparency and immutability, may also pose challenges regarding the exposure of sensitive information, raising ethical concerns about data protection and individual privacy. Ensuring that personal and identifiable data captured in surveillance footage remains secure is critical.

However, the use of Video Blockchain technology helps address these privacy concerns in several ways. By employing cryptographic algorithms such as SHA-256 and Schnorr signatures, we can securely store and transmit surveillance footage without revealing identifiable information to unauthorized parties. Additionally, the use of blockchain ensures that data integrity is maintained while preventing unauthorized access or tampering. Through these mechanisms, Video Blockchain technology enhances the ethical implementation of surveillance systems by balancing transparency with privacy protection, reducing the risk of surveillance abuse or misuse. In the Chapter 3, Section 3.5 extract the details method about how Video Blockchain implement to address the privacy concerns

Furthermore, employing blockchain in surveillance promotes accountability, as every transaction and modification is traceable, ensuring that any ethical breaches can be identified and addressed. This transparency reinforces trust among stakeholders and ensures compliance with data protection laws, ultimately creating a more ethical and secure framework for intelligent surveillance systems.

# Chapter 6 : Conclusion

## 6.1 Introduction

In Chapter 5, Video Blockchain computational methods are evaluated. The research questions and hypotheses related to the results are compared and contrasted to determine if the required outcomes have been achieved. In Chapter 4, we ensure that the proposed methods generate results to evaluate the functionality of the implementation. In Section 4.3 on page 166, the validation of the Video Blockchain computational method provides a summary of the results to better understand the functionality of our implementation.

Additionally, the findings from Chapters 2 and Chapter 3 are verified in the experimental results presented in Chapter 4. By exploring these results, the research concludes with a summary. Chapter 6 is structured as follows: In Section 6.2, we discuss the contributions of our research, and Section 6.3 outlines future works. Finally, we conclude with a summary of the research in Section 6.4.

## 6.2 The Contribution of This Research

We present an in-depth evaluation of our proposed solutions in Chapter 4, thoroughly analysing both the empirical results and theoretical foundations. Our research primarily focuses on developing a synergistic connection among video frames from intelligent surveillance and blockchain. This novel approach is characterised by the integration of surveillance data within a decentralised storage structure, uniquely designed for video surveillance applications.

A distinguishing aspect of our work is the extensive use of cryptographic functions. These functions are pivotal in deriving hash values and signatures from Video Blockchains, thereby significantly enhancing the security and integrity of surveillance data within a tamper-resistant framework.

Our research work currently emphasises the enhancement of data storage robustness within surveillance systems, with a particular focus on data security. While mitigating risks from quantum computer attacks on blockchains is recognised, our immediate efforts concentrate on strengthening the fundamental security aspects of blockchains. Future research, as outlined in Section 4.4, will explore methods to further reinforce blockchains against quantum computing threats.

Addressing privacy concerns in blockchain implementation is another critical facet of our study. Looking ahead, we aim to tackle broader challenges, including scalability, interoperability, and regulatory compliance, which are essential for the effective deployment and advancement of blockchains in smart urban environments. In the real-world implementation, this Video Blockchain technology can be used as a

Overall, in this thesis, we propose a blockchain-enabled solution that strengthens the security and integrity of surveillance data. Apart from fortifying data against unauthorised access and tampering, our solution aspires to build significant trust, reliability, and controlled data disclosure within smart cities. By blending computer vision with Video Blockchains, we provide a solid foundation for secure and adaptable video surveillance, meeting the evolving needs of urban safety and management. Our contributions pave the way for future advancements in this dynamic and critical field.

## 6.3 Potential of Video Blockchain to Address Industry Challenges

**Resource Efficiency**: One of the key advantages of Video Blockchain is its ability to operate efficiently in resource-constrained environments, such as on edge devices in surveillance networks. By utilizing cryptographic algorithms like SHA-256 and Schnorr signatures, the system ensures data integrity without the heavy computational overhead associated with traditional blockchain consensus mechanisms. Moreover, it simplifies the structure by removing unnecessary features, focusing purely on the authentication and integrity of video streams.

**Real-Time Authentication**: Video Blockchain's use of advanced algorithms, including Locality Sensitive Hashing (LSH), allows for real-time verification of video data. Unlike other blockchain systems that may experience delays due to complex consensus procedures, Video Blockchain can authenticate video streams in near real-time, making it suitable for industries like law enforcement, transportation, and live broadcasting, where instant verification is crucial.

Scalability for Industry Applications: Industries generating large volumes of video data, such as smart cities and transportation systems, require a blockchain solution that can scale without excessive resource consumption. Video Blockchain's streamlined approach ensures that it can handle large data flows by storing only essential metadata (hashes) on-chain, while the actual video data is stored off-chain. This hybrid approach reduces storage requirements and ensures scalability.

**Enhanced Security with Minimal Complexity**: By focusing on specific cryptographic methods, such as SHA-256 and LSH, Video Blockchain eliminates the need for resource-heavy processes like mining or complex permissioned systems. This simplification makes it easier to deploy in industries where technical infrastructure may be limited, such as remote monitoring stations or autonomous vehicle networks.

## 6.4 Future Work

The research project currently employs landscape of computational methods for Video Blockchain in intelligent surveillance, shedding light on key findings that underscore the importance of this interdisciplinary field. The integration of blockchain-based solutions with intelligent surveillance systems represents a promising frontier, bringing together advancements in computer vision, artificial intelligence, and machine learning.

In Chapter 2 and Chapter 3, we commenced with an introduction to the overarching scope and objectives, emphasising on the critical role of computational methods in enhancing the security, privacy, and efficiency of intelligent surveillance. The foundational concepts in video surveillance were discussed, revealing the pivotal role of blockchains in addressing security challenges and ensuring data integrity.

The exploration of blockchains in surveillance findings into its applications in enhancing video integrity in smart cities and enabling IoT-enabled Mobility as a Service (MaaS). Notably, these applications leverage the decentralised and tamper-proof characteristics of blockchain, showcasing its versatility in securing surveillance data.

In future work, we will expand to include the feature of quantum computer resistant capability in the Video Blockchain, because according to current tend one of the main external treats for the blockchain is quantum computer attacks. Due to the high capability, computational power can lead

to break the blockchain immutability. But currently, there are only a limited number of quantum computers available, and they typically have a small number of qubits and high error rates. As a result, testing Shor's algorithm on these quantum computers is challenging and requires a high degree of expertise in quantum computing and programming.

In this research planning to integrate with autonomous vehicle make the secure data transferring distributed method using Video Blockchain method. in future smart cities opened to the public with number of internet base connection, platform, big data etc. Secure information and resistant to the cyber-attack take the major place in these implementations. Therefore, trepidation is the one of critical factor and considerable amount of impact can to happened to the loss of the functionality in these facilities. Hence, it's more important to address this kind of vehicle connecting feature using Video Blockchain. In our paper (Moolikagedara et al., 2023) , vehicle mounted camera secure approach led to this process and we planning to enhance the feature and do more research on to deliver more robust implementation to the research field.

This thesis outlines key areas for further exploration to enhance the application of blockchains in intelligent surveillance. Foremost, there is an urgent need to explore solutions for the resilience of blockchains against quantum threats. This is crucial for ensuring the long-term security and integrity of surveillance data in an era where quantum computing is rapidly evolving.

Additionally, addressing privacy concerns remains a significant challenge. Future research should focus on overcoming the limitations of scalability and interoperability in blockchain implementation, as well as navigating the complex landscape of regulatory compliance. These efforts are pivotal in ensuring the privacy and protection of data within blockchain networks.

Another critical area for future research is the advancement in security measures. There is a continuous need for research and development to fortify the security of surveillance data, focusing on deterring tampering and preventing unauthorised access by external entities. This will enhance the robustness of blockchain-based surveillance systems.

Lastly, the thesis emphasises on the importance of trust and reliability in smart urban environments. Our future research will aim to foster significant levels of trust and reliability, as well as controlled data disclosure, by harmonising computer vision with Video Blockchains. This

integration is key to strengthening the security and transparency of surveillance data, making it a trustworthy component in the management of smart cities.

## 6.5 Concluding Research Summary

In Chapter 4, the proposed solution was evaluated. Additionally, the hypothesis and research questions were assessed using the generated results and theoretical findings. The central objective of this research revolves around establishing a symbiotic relationship between video frames captured by intelligent surveillance systems and the blockchain. Our innovative approach lies in the seamless integration of this data into a decentralised storage platform purpose-built for video surveillance. What sets our work apart from existing studies is its heavy reliance on cryptographic functions, which are instrumental in extracting hash values and signatures from Video Blockchains. This, in turn, fortifies the security of surveillance data, ensuring its integrity in a tamper-resistant environment.

Notably, the focus of our research is primarily on enhancing the robustness of data storage within surveillance systems, rather than cantering on the mitigation of potential risks posed by quantum computer attacks on blockchains. While our current emphasis is on bolstering data security, we acknowledge that the landscape of blockchains is evolving. In the future, we intend to research into the solutions outlined in Section 4.4 to fortify blockchains against quantum threats.

Privacy concerns remain a significant challenge in blockchain implementation, and we acknowledge this aspect as a crucial consideration in our work. However, our vision extends beyond this immediate concern. In the future, there will be a need to address broader challenges such as scalability, interoperability, and regulatory issues that affect the effective deployment of blockchains.

The overarching goal of this research is to propose a blockchain-based approach that not only enhances the security and integrity of surveillance data but also cultivates substantial levels of trust, reliability, and controlled data disclosure within smart cities. By harmonising computer vision with Video Blockchains, our focus is firmly on strengthening the security of surveillance data. The solution we present serves as a robust deterrent against tampering and unauthorised access by external entities.

The contributions stemming from this research open new avenues for necessary advancements in the realm of heightened security and adaptability for video surveillance in the dynamic landscape of smart urban environments. Our work aligns with the evolving needs of these cities, where intelligent surveillance is an integral component of public safety and urban management.

The state-of-the-art concepts in Video Blockchain were explored, showcasing recent developments in algorithms. privacy-preserving techniques and Interdisciplinary solutions. These sections underscored the continual evolution of Video Blockchains, pushing the boundaries of current capabilities and presenting opportunities for more robust and sophisticated computational methods.

A comparative analysis of the existing approaches revealed nuanced strengths, weaknesses, and limitations, with a focus on cryptographic functions, hash algorithms, and signature schemes. The comprehensive discussion illuminated the diverse applications of blockchain in smart cities and emphasised the need for effective computational methods to address security concerns.

Challenges and gaps in the literature were discussed, emphasising the crucial role of blockchain in securing surveillance and ensuring data integrity. The review recognised the need for continued development of new methods and the integration of different algorithms to enhance resistance against attacks on existing blockchain platforms.

The contributions of the thesis were outlined, highlighting the meticulous selection and implementation of cryptographic functions, privacy preservation measures, solutions to blockchain storage challenges, and advancements in visual blockchain computation. These contributions represent a significant advancement in the field, bridging gaps in existing solutions and offering innovative approaches to enhance the security, privacy, and efficiency of visual blockchain systems in smart cities.

In transitioning to the subsequent chapters, the review emphasised the identified gaps and challenges as the basis for formulating research questions and developing a robust methodology. During this study, we have completed publications related to each of the methods, as listed under the "List of Publications During PhD Studies" (Moolikagedara et al., 2023). The significance of computational methods and blockchains in advancing intelligent surveillance was reiterated,

setting the stage for the upcoming exploration into the proposed computational methods for Video Blockchain in intelligent surveillance for smart cities.

# References

Adhikari, N., & Ramkumar, M. (2023). IoT and Blockchain Integration: Applications, Opportunities, and Challenges. *Network*, *3*(1), 115–141.

Atrey, P., Yan, W., Chang, E., Kankanhalli, M. (2004) A Hierarchical Signature Scheme for Robust Video Authentication Using Secret Sharing. *International Multimedia Modelling Conference*, 330-337.

Atrey, P., Yan, W., Kankanhalli, M. (2007) A Scalable Signature Scheme for Video Authentication. Multimedia Tools and Applications 34 (1), 107-135.

Aditya Dhiran, D. Kumar, Abhishek, & Anshul Arora. (2020). *Video Fraud Detection Using Blockchain* (Second). https://doi.org/10.1109/ICIRCA48905.2020.9182963.

Akbar, N. A., Muneer, A., Elhakim, N., & Fati, S. M. (2021). Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. *Future Internet*, *13*(11). https://doi.org/10.3390/fi13110285

Aldairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109*(2016), 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391

Ali, M. S., Dolui, K., & Antonelli, F. (2017). IoT Data Privacy via Blockchains and IPFS. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3131542.3131563

Alketbi, A., Nasir, Q., & Abu Talib, M. (2020). Novel Blockchain Reference Model for Government Services: Dubai Government Case Study. *International Journal of Systems Assurance Engineering and Management*, *11*(6), 1170–1191. https://doi.org/10.1007/s13198-020-00971-2

Allende, M., León, D. L., Cerón, S., Pareja, A., Pacheco, E., Leal, A., Da Silva, M., Pardo, A., Jones, D., Worrall, D. J., Merriman, B., Gilmore, J., Kitchener, N., & Venegas-Andraca, S.

E. (2023) *Quantum-Resistance in Blockchain Networks*. Scientific Reports. https://doi.org/10.1038/s41598-023-32701-6

Anwer, M., Saad, A., & Ashfaque, A. (2020). Security of IoT Using Block chain: A Review. *International Conference on Information Science and Communication Technology (ICISCT)*, 1–5. https://doi.org/10.1109/ICISCT49550.2020.9079943

Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H. A., & Gilani, A. (2022). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors*, *22*(7). https://doi.org/10.3390/s22072604

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer*, *50*(9), 18–28. https://doi.org/10.1109/MC.2017.3571064

Bagad, S., & Vijayakumaran, S. (2020). On the Confidentiality of Amounts in Grin. *Crypto Valley Conference on Blockchain Technology (CVCBT)*, 78–82. https://doi.org/10.1109/CVCBT50464.2020.00012

Bansal, A., Khanna, R., & Sharma, S. (2021). UHF-RFID Tag Design for Improved Traceability Solution for Workers' Safety at Risky Job Sites. *IEEE International Conference on RFID Technology and Applications*, 267–270.

Becker, G. (2008). Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. *Master Thesis*, Seminararbeit Ruhr-Universit¨at Bochum.

Bhardwaj, J., Jain, P., Nagrath, P., & Mittal, M. (2021). *File Authentication Ownership Using Blockchain*. 43–52. https://doi.org/10.1007/978-981-33-6307-6_6

Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for Smart Cities: A Review of Architectures, Integration Trends and Future Research Directions. *Sustainable Cities and Society*, *61*, 102360. https://doi.org/10.1016/J.SCS.2020.102360

Casino, F., & Patsakis, C. (2020). An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture. *IEEE Transactions on Engineering Management*, *67*(4), 1501–1513. https://doi.org/10.1109/TEM.2019.2944279

Castellon, C., Roy, S., Kreidl, P., Dutta, A., & Boloni, L. (2021). Energy Efficient Merkle Trees for Blockchains. *International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1093–1099.

Chambers, J., Yan, W., Garhwal, A., Kankanhalli, M. (2014) Currency security and forensics: A survey. *Multimedia Tools and Applications*, 74(11), 4013-4043.

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). 67 A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. *ACM Comput. Surv*, *53*. https://doi.org/10.1145/3391195

Chen, J., Ruan, Y., Guo, L., & Lu, H. (2020). BCVehis: A Blockchain-Based Service Prototype of Vehicle History Tracking for Used-Car Trades in China. *IEEE Access*, *8*, 214842–214851. https://doi.org/10.1109/ACCESS.2020.3040229

Chen, L., Zhang, X., & Sun, Z. (2022). Blockchain Data Sharing Query Scheme based on Threshold Secret Sharing. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/8996815

Chen, X., Xing, Z., Karki, B., Li, Y., & Chen, Z. (2021). Blockchain Simulation: A Web Application for IT Education. *Annual Computing and Communication Workshop and Conference, CCWC 2021*, 486–491. https://doi.org/10.1109/CCWC51732.2021.9375934

Chen, Y. C., Chou, Y. P., & Chou, Y. C. (2019). An Image Authentication Scheme using Merkle Tree Mechanisms. *Future Internet*, *11*(7). https://doi.org/10.3390/fi11070149

Chen, Y., Li, H., Li, K., & Zhang, J. (2017). An Improved P2P File System Scheme Based on IPFS and Blockchain. *IEEE International Conference on Big Data*, 2652–2657. https://doi.org/10.1109/BigData.2017.8258226

Chlomoudis, C., Konstantinou, A., Kostagiolas, P., & Pallis, P. (2022). Information Needs and Information-Seeking Behaviour of Maritime Students: A Systematic Literature Review Using the PRISMA method. *Library Management*, *43*(5), 353–369.

Chukwu, E., & Garg, L. (2020). A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access*, *8*, 21196–21214. https://doi.org/10.1109/ACCESS.2020.2969881

Courtois, N. T., & Bahack, L. (2014). *On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency*. http://arxiv.org/abs/1402.1718

Deepak, K., Badiger, A. N., Akshay, J., Awomi, K. A., Deepak, G., & Harish Kumar, N. (2020). Blockchain-based Management of Video Surveillance Systems: A Survey. *International Conference on Advanced Computing and Communication Systems*, 1256–1258. https://doi.org/10.1109/ICACCS48705.2020.9074197

Dhumwad, S., Sukhadeve, M., Naik, C., Kn, M., & Prabhu, S. (2017). A Peer to Peer Money Transfer Using SHA256 and Merkle Tree. *Annual Conference on Advanced Computing and Communications*, 40–43.

Duan, J., Gu, L., & Zheng, S. (2021). Polymerized RingCT: An Efficient Linkable Ring Signature for Ring Confidential Transactions in Blockchain. *Journal of Physics: Conference Series*, *1738*(1). https://doi.org/10.1088/1742-6596/1738/1/012109

Duong, T., Chepurnoy, A., Fan, L., & Zhou, H. S. (2018). TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake. *ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Co-Located with ASIA*, 1–13. https://doi.org/10.1145/3205230.3205233

Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*, *7*(10), 22–34. https://doi.org/10.22215/timreview/1111

Eyal, I., & Sirer, E. G. (2018). Majority Is Not Enough: Bitcoin Mining is Vulnerable. *Communications of the ACM*, *61*(7), 95–102. https://doi.org/10.1145/3212998

Fan, S., & Chen, Y. (2022). *Editable Blockchain Scheme Based on Shamir Chameleon Hash Secret Sharing*. IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC). https://doi.org/10.1109/ITOEC53115.2022.9734554

Fattahi, S. M., Makanju, A., & Milani Fard, A. (2020). SIMBA: An Efficient Simulator for Blockchain Applications. *IEEE/IFIP International Conference on Dependable Systems and Networks: Supplemental Volume*, 51–52.

Feng, H., Ling, H., Zou, F., Yan, W., Lu, Z. (2010) Optimal Collusion Attack for Digital Fingerprinting. *ACM International Conference on Multimedia*, 767-770.

Feng, H., Ling, H., Zou, F., Yan, W., Lu, Z. (2012) A Collusion Attack Optimization Strategy for Digital Fingerprinting. *ACM Transactions on Multimedia Computing, Communications, and Applications*.

Feng, H., Ling, H., Zou, F., Yan, W., Sarem, M., Lu, Z. (2013) A Collusion Attack Optimization Framework Toward Spread-spectrum Fingerprinting. Applied Soft Computing 13 (8), 3482-3493.

Foye, E., Prasad, S., Sivan, S., Faatamai, S., Yan, W., Liu, W. (2013) A Framework of Content and Context-Based Network Monitoring. *Managing Trust in Cyberspace*, 371.

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Fiat, A., & Shamir, A. (1987). How to Prove Yourself: Practical Solutions to Identification and Signature Problems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *263 LNCS*, 186–194. https://doi.org/10.1007/3-540-47721-7_12

Fill, H., & Haerer, F. (2018). Knowledge Blockchains: Applying Blockchain Technologies to Enterprise Modeling. *Hawaii International Conference on System Sciences*, *9*, 4045–4054. https://doi.org/10.24251/hicss.2018.509

Fitwi, A., & Chen, Y. (2021). *Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain*. International Conference on Computer Communications and Networks. 1–8.

Fitwi, A., Chen, Y., & Zhu, S. (2019). A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge. *IEEE International Conference on Blockchain, Blockchain 2019*, 552–555. https://doi.org/10.1109/Blockchain.2019.00080

Fu, M., Zhu, H., Mišić, J., Mišić, V. B., Bai, J., & Chang, X. (2022). Evaluating Checkpointing Capability against Eclipse-based Stake-Bleeding Attack in PoS Blockchain. *IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing,*

*Sustainable Computing & Communications, Social Computing & Networking* 937–944. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00124

Gabay, D., Akkaya, K., & Cebe, M. (2020). Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs. *IEEE Transactions on Vehicular Technology*, *69*(6), 5760–5772. https://doi.org/10.1109/TVT.2020.2977361

Gad, A. H., Abdalazeem, S. E. E., Abdelmegid, O. A., & Mostafa, H. (2020). Low Power and Area SHA-256 Hardware Accelerator on Virtex-7 FPGA. *2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, 181–185. https://doi.org/10.1109/NILES50944.2020.9257922

Gallo, P., Pongnumkul, S., & Nguyen, U. Q. (2018). BlockSee: Blockchain for IoT Video Surveillance in Smart Cities. *Proceedings. IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems*. https://doi.org/10.1109/EEEIC.2018.8493895

Gao, Y. L., Chen, X. B., Chen, Y. L., Sun, Y., Niu, X. X., & Yang, Y. X. (2018). A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. *IEEE Access*, *6*, 27205–27213.

Gedara, K., Nguyen, M., Yan, W. (2022) Visual Blockchain for Intelligent Surveillance in a Smart City. *Blockchain Technologies for Sustainable Development in Smart Citie*s, Book Chapter, IGI Global.

Gedara, K., Nguyen, M., Yan, W. (2023) Video Blockchain: A Decentralised Approach for Secure and Sustainable Networks with Distributed Video Footages from Vehicle-Mounted Cameras in Smart Cities. *Electronics* (journal).

Gedara, K. M., Nguyen, M., & Yan, W. Q. (2023). *Enhancing Privacy Protection in Intelligent Surveillance: Video Blockchain Solutions*. International Congress on Blockchain and Applications.

Gedara, K., Nguyen, M., Yan, W., Li, X. (2024) Advancing Video Data Privacy Preservation in IoT Networks through Video Blockchain. *Information*.

Gulzar, N., Abbasi, B., Wu, E., Ozbal, A., Yan, W. (2013) Surveillance Privacy Protection. Intelligent Multimedia Surveillance, 83-105.

Gupta, M., Yan, W. (2022) Video watermarking with Digital Signature and Fingerprinting. *Applications of Encryption and Watermarking for Information Security, IGI Global.*

Gupta, M. (2021) *Improving Security for Video Watermarking*. Master's Thesis. Auckland University of Technology, New Zealand.

George, R. V., Harsh, H. O., Ray, P., & Babu, A. K. (2019). Food Quality Traceability Prototype for Restaurants Using Blockchain and Food Quality Data Index. *Journal of Cleaner Production*, *240*. https://doi.org/10.1016/j.jclepro.2019.118021

Gergely, A. M., & Crainicu, B. (2020). Randadminsuite: A New Privacy-Enhancing Solution for Private Blockchains. *Procedia Manufacturing*, *46*(2019), 562–569.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the Security and Performance of Proof of Work blockchains. *ACM Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2978341

Ghosh, H., Bhowmick, S., Maurya, K., & Bagchi, S. (2021). *Linear Complementary Dual Code-Based Multi-Secret Sharing Scheme*. https://ar5iv.labs.arxiv.org/html/2112.05469

Ghuli, P., Kumar, U. P., & Shettar, R. (2017). A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices. *Advances in Computational Sciences and Technology*, *10*(8), 2449–2456. https://www.ripublication.com/acst17/acstv10n8_22.pdf

Gipp, B., Kosti, J., & Breitinger, C. (2016). Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain. *Mediterranean Conference on Information Systems (MCIS), September*, 51. http://aisel.aisnet.org/mcis2016/51

Grandhi, J., Patil, M. U., & P R, L. E. (2023). *Automation of Blockchain Network Setup in Offering Blockchain as a Service (BaaS)*. International Conference on Blockchain Computing and Applications (BCCA), 635–642.

Gřivna, T., & Drápal, J. (2019). Attacks on the Confidentiality, Integrity and Availability of Data and Computer Systems in the Criminal Case Law of the Czech Republic. *Digital Investigation*, *28*, 1–13. https://doi.org/10.1016/j.diin.2018.12.002

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. *IEEE Network*, *34*(1), 8–14. https://doi.org/10.1109/MNET.001.1900178

Hao, Z., Mao, D., Zhang, B., Zuo, M., & Zhao, Z. (2020). A Novel Visual Analysis Method of Food Safety Risk Traceability Based on Blockchain. *International Journal of Environmental Research and Public Health*, *17*(7). https://doi.org/10.3390/ijerph17072300

Harris, C. G. (2019). Consensus-Based Secret Sharing in Blockchain Smart Contracts. *International Workshop on Big Data and Information Security*, 79–84. https://doi.org/10.1109/IWBIS.2019.8935853

Hartwig, M. (2016). ECDSA Security in Bitcoin and Ethereum : A Research Survey. *Blog.Coinfabrik*, 1–10.

Harvilla, M., & Du, J. (2024). Prospective Hybrid Consensus for Project PAI. *ArXiv*, *abs/1902.02469*.

Hasan, H. R., & Salah, K. (2019). Combating Deepfake Videos Using Blockchain and Smart Contracts. *IEEE Access*, *7*, 41596–41606. https://doi.org/10.1109/ACCESS.2019.2905689

Hasan, O., Brunie, L., & Bertino, E. (2023). Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey. In *ACM Computing Surveys* (Vol. 55, Issue 2). https://doi.org/10.1145/3490236

Hasanova, H., Baek, U. jun, Shin, M. Gon, Cho, K., & Kim, M. S. (2019). A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures. *International Journal of Network Management*, *29*(2). https://doi.org/10.1002/nem.2060

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2021). The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Communications Surveys and Tutorials*, *23*(1), 341–390. https://doi.org/10.1109/COMST.2020.3033665

Hou, L., Zheng, K., Liu, Z., Xu, X., & Wu, T. (2021). Design and Prototype Implementation of a Blockchain-Enabled LoRa System with Edge Computing. *IEEE Internet of Things*, *8*(4), 2419–2430.

Hu, R. (2019) Visual blockchain using Merkle Tree. Master's Thesis. Auckland University of Technology, New Zealand.

Hu, R., Yan, W. (2020) Design and Implementation of Visual Blockchain with Merkle tree. *Handbook of Research on Multimedia Cyber Security*, 282-295.

Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S., & Embong, A. H. (2021). *A Review on Blockchain Security Issues and Challenges*, 227–232. https://doi.org/10.1109/icsgrc53186.2021.9515276

Ji, S., Kim, D., & Im, H. (2021). Evaluating Countermeasures for Verifying the Integrity of Ethereum Smart Contract Applications. *IEEE Access*, *9*, 90029–90042. https://doi.org/10.1109/ACCESS.2021.3091317

Jiang, L., Li, R., Wu, W., Qian, C., & Loy, C. C. (2020). *DeeperForensics-1.0: A Large-Scale Dataset for Real-World Face Forgery Detection*. http://arxiv.org/abs/2001.03024

Jiang, X., Yu, F. R., Song, T., & Leung, V. C. M. (2022). Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles With Edge Computing. *IEEE Internet of Things Journal*, *9*(16), 14260–14272.

Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. *Sensors (Switzerland)*, *20*(17), 1–27.

Karame, G. O. (2016). *On the Security and Scalability of Bitcoin's Blockchain*. ACM SIGSAC Conference on Computer and Communications Security, 1861–1862. https://doi.org/10.1145/2976749.2976756

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in Bitcoin. *ACM Transactions on Information and System Security*, *18*(1), 1–32.

Kieran, D., Yan, W. (2010) A Framework for an Event-Driven Video Surveillance System. *Advanced Video and Signal Based Surveillance* (AVSS).

Khan, M. A., & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, P. W., Byun, Y. C., & Park, N. (2020). A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. *Electronics (Switzerland)*, *9*(3). https://doi.org/10.3390/electronics9030484

Khatoon, A., Verma, P., Southernwood, J., Massey, B., & Corcoran, P. (2019). Blockchain in Energy Efficiency: Potential Applications and Benefits. *Energies*, *12*(17). https://doi.org/10.3390/en12173317

Khrais, L. T. (2020). The Combination of IoT-Sensors in Appliances and block-Chain Technology in Smart Cities Energy Solutions. *International Conference on Advanced Computing and Communication Systems*, 1373–1378. https://doi.org/10.1109/ICACCS48705.2020.9074362

Kiltz, E., Lyubashevsky, V., & Schaffner, C. (2018). A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10822 LNCS*, 552–586. https://doi.org/10.1007/978-3-319-78372-7_18

Kim, J., Oh, S., Kim, Y., & Kim, H. (2023). Improving Voting of Block Producers for Delegated Proof-of-Stake with Quadratic Delegate. *International Conference on Platform Technology and Service, PlatCon*, 13–17. https://doi.org/10.1109/PlatCon60102.2023.10255193

King, S. (2013). Primecoin: Cryptocurrency with Prime Number Proof-of-Work. In *Whitepaper Online*. http://primecoin.io/bin/primecoin-paper.pdf

Kissoon, Y., & Bekaroo, G. (2022). *Detecting Vulnerabilities in Smart Contract within Blockchain: A Review and Comparative Analysis of Key Approaches*. International Conference on Next Generation Computing Applications (NextComp)

Koo, D., Shin, Y., Yun, J., & Hur, J. (2018). Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. *Applied Sciences (Switzerland)*, *8*(12). https://doi.org/10.3390/app8122532

Krishnan Thyagarajan, S. A., & Malavolta, G. (2021). Lockable Signatures for Blockchains: Scriptless Scripts for All Signatures. *IEEE Symposium on Security and Privacy (SP), 2021-May*, 937–954. https://doi.org/10.1109/SP40001.2021.00065

Kullig, N., Lämmel, P., & Tcholtchev, N. (2020). Prototype Implementation and Evaluation of A Blockchain Component on IoT Devices. *Procedia Computer Science*, *175*, 379–386. https://doi.org/10.1016/j.procs.2020.07.054

Kumar, M., & Kaur, G. (2022). High Performance Scalable Recursive Block Matrix Inverse for Multicore Architectures. *International Conference on Parallel, Distributed and Grid Computing*, 45–49. https://doi.org/10.1109/PDGC56933.2022.10053189

Lee, D., & Park, N. (2021). Blockchain Based Privacy Preserving Multimedia Intelligent Video Surveillance Using Secure Merkle Tree. *Multimedia Tools and Applications*, *80*(26–27), 1–18. https://doi.org/10.1007/S11042-020-08776-Y

Li, T., Chen, Y., Wang, Y., Wang, Y., Zhao, M., Zhu, H., Tian, Y., Yu, X., & Yang, Y. (2020). Rational Protocols and Attacks in Blockchain System. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8839047

Li, W., Wang, Y., Li, J., & Au, M. H. (2021). Toward A Blockchain-Based Framework for Challenge-Based Collaborative Intrusion Detection. *International Journal of Information Security*, *20*(2), 127–139. https://doi.org/10.1007/s10207-020-00488-6

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Li, X., Mei, Y., Gong, J., Xiang, F., & Sun, Z. (2020). A Blockchain Privacy Protection Scheme Based on Ring Signature. *IEEE Access*, *8*, 76765–76772. https://doi.org/10.1109/ACCESS.2020.2987831

Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2019). *Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics*.

Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653–659.

Ling, H., Wang, L., Zou, F., Yan, W. (2011) Fine-Search for Image Copy Detection Based on Local Affine-Invariant Descriptor and Spatial Dependent Matching. Multimedia Tools and Applications 52 (2), 551-568.

Ling, H., Cheng, H., Ma, Q., Zou, F., Yan, W. (2011) Efficient Image Copy Detection Using Multi-Scale Fingerprints. *IEEE Multimedia*, 19, 60–69

Ling, H., Feng, H., Zou, F., Yan, W., Lu, Z. (2010) A Novel Collusion Attack Strategy for Digital Fingerprinting. *International Workshop on Digital Watermarking*, 224-238.

Liu, J., Ling, H., Zou, F., Yan, W., Lu, Z. (2012) Digital Image Forensics Using Multi-Resolution Histograms. *Crime Prevention Technologies and Applications for Advancing Criminal.*

Liu, P., Zhou, S., Yan, W. (2022) A 3D Cuboid Image Encryption Algorithm Based on Controlled Alternat Quantum Walk of Message Coding. *Mathematics,* 10 (23), 4441.

Liu, Z., Yang, M., Yan, W. (2017) Image Encryption Based on Double Random Phase Encoding. *International Conference on Image and Vision Computing New Zealand.*

Liu, Z., Yang, B., Yan, W. (2021) A Framework for Image Encryption on Frequency Domain. *Research Anthology on Artificial Intelligence Applications in Security* (pp.328-338)

Liu, Z. (2018) *Comparative Evaluations of Image Encryption Algorithms.* Master's Thesis, Auckland University of Technology, New Zealand.

Liu, D., & Camp, L. J. (2006). Proof of Work Can Work. *WEIS*.

Liu, H., Luo, X., Liu, H., & Xia, X. (2021). Merkle Tree: A Fundamental Component of Blockchains. *International Conference on Electronic Information Engineering and Computer Science*, 556–561.

Liu, J., Yan, W. (2022) Crime Prediction from Surveillance Videos Using Deep Learning. *Aiding Forensic Investigation Through Deep Learning and Machine Learning Frameworks*.

Liu, L., Li, F., & Qi, E. (2019). Research on Risk Avoidance and Coordination of Supply Chain Subject Based on Blockchain Technology. *Sustainability (Switzerland), 11*(7), 1–14. https://doi.org/10.3390/su10022182

Liu, Q., & Zhandry, M. (2019). Revisiting Post-Quantum Fiat-Shamir. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11693 LNCS,* 326–355. https://doi.org/10.1007/978-3-030-26951-7_12

Loss, S., Cacho, N., Valle, J. M. Do, & Lopes, F. (2019). Orthus: A Blockchain Platform for Smart Cities. *IEEE International Smart Cities Conference,* 212–217.

Liu, W., Miller, P., Ma, J., Yan, W. (2009) Challenges of Distributed Intelligent Surveillance System with Heterogenous Information. *Procs. of QRASA* (pp.69-74)

Ma, B., Wu, J., Lai, E., Yan, W. (2023) A Privacy-Preserving Word Embedding Text Classification Model Based on Privacy Boundary Constructed by Deep Belief Network. Multimedia Tools and Applications

Ma, B., Yan, W., Lai, E., Wu, J. (2021) A New Noise Generating Method Based on Gaussian Sampling for Privacy Preservation. *International Symposium on Geometry and Vision.*

Moodley, E., Huo, G., Hsieh, M., Cai, S., Yan, W. (2013) Password Security and Protection. *Managing Trust in Cyberspace*, 449.

Ma, X. (2020) *Banknote Serial Number Recognition Using Deep Learning.* Master's Thesis, Auckland University of Technology, New Zealand.

Madhwacharyula, C., Wang, J., Yan, W., Ji, Y., Radhakrishna, A., Bissol, S. (2003) Information-Integration Approach to Designing Digital Video Albums. International Conference on Information, Communications and Signal Processing.

Maffei, M., & Ryan, M. (2017). *Principles of Security and Trust*. Springer http://www.springer.com/series/7410

Majdoubi, D. E. L., El Bakkali, H., & Sadki, S. (2020). Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment. *International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications.*

Mandalapu, V., Homdee, N., Lab, L., Hart, J. M., Lach, J., Bodkin, S., & Gong, J. (2019). Developing Computational Models for Personalized ACL Injury Classification; Developing

Computational Models for Personalized ACL Injury Classification. In *IEEE International Conference on Wearable and Implantable Body Sensor Networks (BSN)*.

Maxwell, G., Poelstra, A., Seurin, Y., & Wuille, P. (2019). Simple Schnorr Multi-Signatures with Applications to Bitcoin. *Designs, Codes, and Cryptography*, *87*(9), 2139–2164. https://doi.org/10.1007/s10623-019-00608-x

Mi, B., Wu, B., Huang, D., Liu, Y., Chen, L., & Wan, S. (2022). Privacy-Oriented Transaction for Public Blockchain via Secret Sharing. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/9946088

Michael, M. M. (2002). High Performance Dynamic Lock-free Hash Tables and List-Based Sets. *Annual ACM Symposium on Parallel Algorithms and Architectures*, 73–82. https://doi.org/10.1145/564879.564881

Michelin, R. A., Ahmed, N., Kanhere, S. S., Seneviratne, A., & Jha, S. (2020). Leveraging Lightweight Blockchain to Establish Data Integrity for Surveillance Cameras. *IEEE International Conference on Blockchain and Cryptocurrency*, 3–5. https://doi.org/10.1109/ICBC48266.2020.9169429

Mizrahi, A., Koren, N., & Rottenstreich, O. (2021). Optimizing Merkle Proof Size for Blockchain Transactions. *International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 299–307. https://doi.org/10.1109/COMSNETS51098.2021.9352820

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. In *BMJ (Online)* (Vol. 339, Issue 7716, pp. 332–336). https://doi.org/10.1136/bmj.b2535

Moolikagedara, K., Nguyen, M., Yan, W., & Li, X. (2024). Advancing Video Data Privacy Preservation in IoT Networks through Video Blockchain. *Information (Switzerland)*, *15*(3). https://doi.org/10.3390/info15030171

Moolikagedara, K., Nguyen, M., Yan, W. Q., & Li, X. J. (2023). Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173621

Moroz, D. J., Aronoff, D. J., Narula, N., & Parkes, D. C. (2020). *Double-Spend Counterattacks: Threat of Retaliation in Proof-of-Work Systems*. http://arxiv.org/abs/2002.10736

Mosakheil, J. H. (2018). Security Threats Classification in Blockchains. *Culminating Projects in Information Assurance*, 141. https://repository.stcloudstate.edu/msia_etds/48

Mousa, H., Mokhtar, S. Ben, Hasan, O., Younes, O., Hadhoud, M., & Brunie, L. (2015). Trust Management and Reputation Systems in Mobile Participatory Sensing Applications: A Survey. *Computer Networks*, *90*, 49–73. https://doi.org/10.1016/j.comnet.2015.07.011

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Novotny, P., Zhang, Q., Hull, R., Baset, S., Laredo, J., Vaculin, R., Ford, D. L., & Dillenberger, D. N. (2018). Permissioned Blockchain Technologies for Academic Publishing. *Information Services and Use*, *38*(3), 159–171. https://doi.org/10.3233/ISU-180020

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IOT Integration: A Systematic Survey. In *Sensors (Switzerland)* (Vol. 18, Issue 8). https://doi.org/10.3390/s18082575

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy Preservation in Permissionless Blockchain: A Survey. In *Digital Communications and Networks* (Vol. 7, Issue 3, pp. 295–307). Chongqing University of Posts and Telecommunications. https://doi.org/10.1016/j.dcan.2020.05.008

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned Blockchain Frameworks in the Industry: A Comparison. *ICT Express*, *7*(2), 229–233. https://doi.org/10.1016/J.ICTE.2020.09.002

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., & Duffy, S. (2006). *Guidance on the Conduct of Narrative Synthesis in Systematic Reviews A Product from the ESRC Methods Programme. The Universities of Exeter, UK.*

Popovska-Mitrovikj, A., Dimitrova, V., Mechkaroska, D., & Bakeva, V. (2020). *Algorithm for Reducing Storage in Blockchain Based on Secret Sharing*. Telecommunications Forum (TELFOR), 12–13. https://doi.org/10.1109/TELFOR.2018.8612034

Pramod, N., & Sankaran, S. (2019). Blockchain Based Framework for Driver Profiling in Smart Cities. *International Symposium on Advanced Networks and Telecommunication Systems*. https://doi.org/10.1109/ANTS47819.2019.9117923

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain Adoption Is Inevitable—Barriers and Risks Remain. *Journal of Corporate Accounting & Finance*, *31*(2), 21–28. https://doi.org/10.1002/jcaf.22415

Priyadharshini, K., & Canessane, R. A. (2021). Blockchain-Based Security Algorithm on IoT Framework for Shielded Communication in Smart Cities. *International Conference on Intelligent Communication Technologies and Virtual Mobile Networks*, 320–327. https://doi.org/10.1109/ICICV50876.2021.9388497

Raman, R. K., & Varshney, L. R. (2018). Distributed Storage Meets Secret Sharing on the Blockchain. *Information Theory and Applications Workshop*. https://doi.org/10.1109/ITA.2018.8503089

Rameder, H., di Angelo, M., & Salzer, G. (2022). Review of Automated Vulnerability Analysis of Smart Contracts on Ethereum. In *Frontiers in Blockchain* (Vol. 5).

Ren, Y. (2017) Banknote Recognition in Real Time Using ANN. Master's Thesis, Auckland University of Technology, New Zealand.

Reno, S., Bhowmik, S., & Ahmed, M. (2021). *Utilizing IPFS and Private Blockchain to Secure Forensic Information*, 8–9.

Rezaeibagha, F., & Mu, Y. (2019). Efficient Micropayment of Cryptocurrency from Blockchains. *Comput. J.*, *62*(4), 507–517. https://doi.org/10.1093/COMJNL/BXY105

Rodríguez-Silva, D. A., Adkinson-Orellana, L., González-Castaño, F. J., Armiño-Franco, I., & González-Martínez, D. (2012). Video Surveillance Based on Cloud Storage. *International Conference on Cloud Computing*, 991–992. https://doi.org/10.1109/CLOUD.2012.44

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). *FaceForensics++: Learning to Detect Manipulated Facial Images*.

http://arxiv.org/abs/1901.08971

Saputro, V. S., Ritchi, H., & Handoyo, S. (2021). Blockchain Disruption on Management Accountant's Role: Systematic Literature Review. *Journal of Accounting Auditing and Business*, *4*(1), 1. https://doi.org/10.24198/jaab.v4i1.25961

Shaikh, E., & Mohammad, N. (2020). Applications of Blockchain Technology for Smart Cities. *International Conference on Inventive Systems and Control*, 186–191.

https://doi.org/10.1109/ICISC47916.2020.9171089

Shcherbina, E. S., & Mesyura, V. I. (2021). Mechanisms of Blockchains Integration with Each Other. *Visnyk of Vinnytsia Politechnical Institute*, *155*(2), 85–91.

https://doi.org/10.31649/1997-9266-2021-155-2-85-91

Sheth, H., & Dattani, J. (2019). Overview of Blockchain Technology. *Asian Journal of Convergence in Technology*, *05*(01), 1–4. https://doi.org/10.33130/ajct.2019v05i01.013

Shin, J. S., Lee, S., Choi, S., Jo, M., & Lee, S. H. (2021). A New Distributed, Decentralized Privacy-Preserving ID Registration System. *IEEE Communications (Magazine)*, *59*(6), 138–144.

Shu, Y (2018) *Blockchain for Security of A Cloud-Based Online Auction System.* Master's Thesis, Auckland University of Technology, New Zealand.

Shu, Y., Yu, J., Yan, W. (2019) Blockchain for Security of a Cloud-Based Online Auction System. *Exploring Security in Software Architecture and Design.*

Shu, Y., Yu, J., Yan, W. (2019) State Actor Model for Cloud-Based Online Auction. *Exploring Security in Software Architecture and Design.*

Shu, Y., Yu, J. Yan, W. (2020) Blockchain for Security of Cloud-Based Online Auction. *Research Anthology on Blockchain Technology in Business, Healthcare*.

Singh, M., & Kim, S. (2018). Trust Bit: Reward-Based Intelligent Vehicle Commination Using Blockchain. *IEEE World Forum on Internet of Things, WF-IoT*. https://doi.org/10.1109/WF-IoT.2018.8355227

Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning Blockchain – A Beginner's Guide to Building Blockchain Solutions*. https://doi.org/10.1007/978-1-4842-3444-0

Söderström, O., Paasche, T., & Klauser, F. (2014). Smart Cities as Corporate Storytelling. In *City* (Vol. 18, Issue 3, pp. 307–320). https://doi.org/10.1080/13604813.2014.906716

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A Systematic Literature Review of Blockchain Cyber Security. *Digital Communications and Networks*, *6*(2), 147–156. https://doi.org/10.1016/j.dcan.2019.01.005

Tian, S., Liu, Y., Zhang, Y., & Zhao, Y. (2021). A Byzantine Fault-Tolerant Raft Algorithm Combined with Schnorr Signature. *International Conference on Ubiquitous Information Management and Communication, IMCOM 2021*, 1–5.

Treiblmaier, H., Rejeb, A., & Strebinger, A. (2020). Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda. *Smart Cities*, *3*(3), 853–872. https://doi.org/10.3390/smartcities3030044

Trung, N. D., Huy, D. T. N., Huong, L. T. T., Van Thanh, T., Thanh, N. T. P., & Dung, N. T. (2021). Digital Transformation, AI Applications and IoTs in Blockchain Managing Commerce Secrets: And Cybersecurity Risk Solutions in the Era of Industry 4.0 and Further. *Webology*, *18*(Special Issue), 453–465.

van Flymen, D., Liu, D., & Camp, L. J. (2006). Proof of Work Can Work. *WEIS*, 39–53. https://doi.org/10.1007/978-1-4842-5171-3_4

Wang, H., & Liao, J. (2021). Blockchain Privacy Protection Algorithm Based on Pedersen Commitment and Zero-knowledge Proof. *2021 4th International Conference on Blockchain Technology and Applications*, 1–5.

Wang, J., Yan, W., Kankanhalli, M., Jain, R., Reinders, M. (2003) Adaptive monitoring for video surveillance. International Conference on Information, Communications and Signal Processing.

Wang, J., Kankanhalli, M., Yan, W., Jain, R. (2003) Experiential Sampling for Video Surveillance. *ACM SIGMM International Workshop on Video surveillance* (pp.77-86).

Wang, J., Chen, W., Ren, Y., Alfarraj, O., & Wang, L. (2024). Blockchain Based Data Storage Mechanism in Cyber Physical System. *Journal of Internet Technology*, *21*, 1681–1689.

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of Running Clinical Trials in An Untrustworthy Environment Using Blockchain. *Nature Communications*, *10*(1), 1–8.

Wu, W., Yan, W. (2023) Sharing Visual Secrets among Multiple Groups with Enhanced Performance. IEEE Transactions on Circuits and Systems for Video Technology

Wu, X., Weng, J., Yan, W. (2018) Adopting Secret Sharing for Reversible Data Hiding in Encrypted Images. *Signal Processing* 143, 269-281.

Xia, Z., Sun, L., Yang, B., Zhou, Y., & Zhang, M. (2018). Verifiable Secret Sharing Based on Hyperplane Geometry with Its Applications to Optimal Resilient Proactive Cryptosystems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10946 LNCS*, 83–100. https://doi.org/10.1007/978-3-319-93638-3_6

Xu, C., Qu, Y., Luan, T. H., Eklund, P. W., Xiang, Y., & Gao, L. (2022). A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things. *IEEE Internet of Things Journal*, *9*(6), 4371–4384. https://doi.org/10.1109/JIOT.2021.3103275

Xu, R., Nikouei, S. Y., Nagothu, D., Fitwi, A., & Chen, Y. (2020). BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System. *Smart Cities*, *3*(3), 928–951. https://doi.org/10.3390/smartcities3030047

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview* (Issue June).

Yan, W. (2019) *Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics*. Springer Nature.

Yan, W. (2023) *Computational Methods for Deep Learning: Theory, Algorithms, and Implementations*. Springer Nature.

Yan, W., Ding, W., Qi, D. (1999) Image Sharing Based on Interpolation. *International Conference on Computer Aided Design.*

Yan, W., Ding, W., Qi, D. (2000) Image Sharing Based on Chinese remainder theorem. *Journal of Northern China University of Technology* 12 (1), 6-9.

Yan, W., Kankanhalli, M. (2003) Motion Trajectory-Based Video Authentication. *International Symposium on Circuits and Systems.*

Yan, W., Fu, W., Kankanhalli, M. (2008) Progressive Audio Scrambling in Compressed Domain. *IEEE Transactions on Multimedia* 10 (6), 960-968.

Yan, W., Weir, J., Kankanhalli, M. (2011) Image Secret Sharing. *Visual Cryptography and Secret Image Sharing* 4, 381.

Yan, X., Yan, W., Liu, L., Lu, Y. (2021) Penrose Tiling for Visual Secret Sharing. *Multimedia Tools and Applications.*

Yang, M., Xu, X., Chen, S., & Zhu, L. (2020). Blockchain-Based Solution for Managing Renewable-based Microgrids. *IEEE Technical Brief*, 2–5.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., & Chen, S. (2020). Public and Private Blockchain in Construction Business Process and Information Integration. *Automation in Construction*, *118*.

Yu, G. (2024). Simple Schnorr Signature with Pedersen Commitment as Key. *IACR Cryptol. EPrint Arch.*, *2020*.

Yu, P., & Weizhang, D. (2020). Multiple Secrets Sharing Scheme Based on Eigenvalue. *International Conference on Mechanical, Control and Computer Engineering,* 2327–2330.

Zhang, X., Yan, W. (2018) Comparative Evaluations of Privacy on Digital Images. *IEEE International Conference on Advanced Video and Signal Based Surveillance.*

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *International Congress on Big Data, BigData Congress 2017*, 557–564.

Zhou, L., Yan, W., Shu, Y., Yu, J. (2018) CVSS: A Cloud-Based Visual Surveillance System. *International Journal of Digital Crime and Forensics* (IJDCF) 10 (1), 79-91.

Zhu, G., Ding, Y., & Cao, Y. (2023). The Effect of Block-Matrix Interface of SRM with High Volumetric Block Proportion on Its Uniaxial Compressive Strength. *Applied Sciences*, *13*(6), 3463.

Zhu, Y. (2016) *Exploring Defense of SQL Injection Attack in Penetration Testing*. Master's Thesis, Auckland University of Technology, New Zealand.

Zhu, Y., Yan, W. (2017) Exploring Defense of SQL Injection Attack in Penetration Testing. *International Journal of Digital Crime and Forensics* 9 (4), 62-71.

Zou, J., Yan, W., Ding, W., Qi, D. (2001) A Novel Image Texture Substitution with Shading Effect. *Journal of Computer Research and Development* 38 (11), 1327-1330.

Zi, B., Chang, M., Chen, J., Ma, X., & Jiang, Y. G. (2020). WildDeepfake: A Challenging Real-World Dataset for Deepfake Detection. *ACM International Conference on Multimedia*, 2382–2390. https://doi.org/10.1145/3394171.3413769