A REVIEW OF ISSUES IN HEALTHCARE INFORMATION MANAGEMENT SYSTEMS AND BLOCKCHAIN SOLUTIONS

AT Litchfield
Auckland University of Technology
alitchfi@aut.ac.nz

A Khan
Auckland University of Technology
arshad.khan@aut.ac.nz

March 26, 2019

Abstract

Healthcare is a data-driven domain where a large volumes of data are created, accessed, stored, and disseminated daily. In this paper, issues such as security, privacy, data transparency, interoperability, data accessibility, user interface issues in healthcare information management systems are presented. In addition, blockchain technology related studies in healthcare information systems are discussed with the aim to find what issues in healthcare system present research opportunities using blockchains.

Keywords: Healthcare data, Healthcare Information Management System issues, blockchain technology.

1 Introduction

In this paper socio-technical issues that are related to Healthcare Information Management Systems (HIMS) and how those issues are addressed by applications of blockchain technologies in current research are discussed. Opportunities for further research and the development of new architectures in HIMS are also addressed. The range of applications to which blockchain technology may be applied tends to focus on problems related to authorisation, authentication, privacy of data, security, auditability, and data immutability. The blockchain uses byzantine fault tolerant consensus algorithms to validate transactions through proofing methods such as Proof of Stake and Proof of Work. These processes can have the effect of making systems complex and so the type of problem resolved with a blockchain needs to be carefully considered.

The paper presents the results of a review of literature that involved 71 unique high quality articles published between 2008 and 2018. To provide a high level of rigour tot he review process, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method is used (Moher, Liberati, Tetzlaff, & Altman, 2009). The review identifies a number of consistent issues in HIMS: weaknesses in security and privacy, lack of data transparency, drug prescription and supply chain errors, lack of accessibility, lack of data integrity, lack of knowledge interpretation. From these, there are common potential areas for investigation for the adoption of a blockchain solution.

2 Issues in HIMS

In this section, core issues identified from the review are presented. The principal issues are focussed around socio-technical factors, particularly relating to understandings of data ownership and rights of access or privileges.

Inappropriate sharing of patient data without permission presents as a key issue. To alleviate a patient's concerns about data sharing, a system must demonstrate how data are shared and what purpose the data are used for (Kelman, Bass, & Holman, 2002). For example, a system ought to provide an option for patients and stakeholders to decide who is responsible for a transaction (Mashima & Ahamad, 2012; Miriovsky, Shulman, & Abernethy, 2012). At other times, patient data are accessed by external service providers so better decisions can be made on behalf of patients, but without their knowledge. This affects the patient's perception of the organisation and therefore, the level of trust in its capability. A further instance that affects trust is the transparency or availability of data, which also affects reliability and visibility (Kelman et al., 2002; Colijn, Jones, Johnston, Yaliraki, & Barahona, 2017; Das, Holla, Mohpal, & Muralidharan, 2016) and limited capability of the organisation to perform effective analytics on data (Shortliffe et al., 2000).

Recent developments in technology has seen a rapid growth of digital devices and technologies to improve HIMS and reduce cost (Kaye, 2000). However, (Goslee & Conte, 1998) identifies a number of groups of people that cannot afford devices or have limited access to digital infrastructure, these people have long term medical or disability issues and face cultural or language problems. An additional issue in rural areas is low Internet speed that limits access to technology. In all these cases, the social impact arises from an unequal level of access to digital platforms, which now can lead to unequal levels of healthcare delivery.

A frequent concern for sensitive data are security and privacy, especially in HIMS that are integrated with third party devices (Tsai, Chiang, Ksentini, & Chen, 2016; Viceconti, Hunter, & Hose, 2015). The increased threat footprint is also observable when patients' personal data are accessible through an Internet connection. (Cardenas, Manadhata, & Rajan, 2013; Terry, 2000) claim that healthcare providers have put patient data online for financial gain without any concern for the privacy of the patient. In addition, McGuire et al. (2008) argue that there is no regulation or policy that restricts online vendors and providers. The use of the Internet for medical purposes concerns many people, for example, patients fear that insurance companies might change their coverage after finding out what is online. While sensitive private data is the norm among healthcare providers and it is distributed as a matter of course (Cartwright-Smith, Gray, & Thorpe, 2016), due to privacy concerns, provider access to data is increasingly limited (Meng, Tischhauser, Wang, Wang, & Han, 2018; Liu, Zhu, Mundie, & Krieger, 2017; Raghupathi & Raghupathi, 2014).

Drug prescription errors occur when visually similar names of drugs and patients, or similar generic drugs are preferred (Campbell, Sittig, Ash, Guappone, & Dykstra, 2006; Campbell, Guappone, Sittig, Dykstra, & Ash, 2009). Visually similar drug names and patient names may be indistinguishable in a line of text (Ash et al., 2007). So it may be that a visual display presents ambiguous, complicated, and unordered data, and that user interface issues and create additional problems due to a reduction of cognitive processing, loss of visibility, confusion, time delays, and frustration (Horsky, Kuperman, & Patel, 2005; Saleem et al., 2005), as well as poor skill levels and lack of adequate training that leads errors.

3 Blockchain in healthcare system

Naturalness, consistency, error prevention, minimisation of cognitive load, interaction efficiencies, feedback mechanisms, effective use of language, and customisability or flexibility are factors considered when improving HIMS (Howe, Adams, Hettinger, & Ratwani, 2018), which give more time for individual patients (Alshamari, 2016). Authentication or veracity of data can be accepted using smart contracts with third party notarisation. For example, the assurance of data when a biomedical database receives a query from the enquirer (Kleinaki, Mytis-Gkometh, Drosatos, Efraimidis, & Kaldoudi, 2018). Although while records in a blockchain cannot be altered easily (Di Vimercati, Foresti, Jajodia, & Samarati, 2007; Meng et al., 2018), which prevents unauthorised changes, records that contain inaccurate data may require a new record to be appended to the chain.

The decentralised blockchain architecture handles security and tamper resistance as a matter of its design, thus establishing trust in HIMS. However a continuing issue relates to the speed at which blockchains are able to process transactions, therefore there is effort around finding more time-efficient solutions (Han, Huang, Zhang, & Bhatti, 2018). Addressing the issue of inappropriate data sharing, and authenticity and privacy Jiang et al. (2018) present BlocHIE, a blockchain solution that links multiple sources of healthcare data and uses two blockchains to manage various types of data. In addition, decentralised systems offer no single point of failure (Abouelmehdi, Beni-Hessane, & Khaloufi, 2018).

While intrusion detection is an important step in overall data security (Al Omar, Rahman, Basu, & Kiyomoto, 2017), it is the human factor that is the greater risk, for example, poor passwords lead to weakened control policies (Dias, Reis, Ferreira, & Martins, 2018). (J. Zhang, Xue, & Huang, 2016) propose a Pervasive Social Network (PSN) based HIMS in which two protocols establish secure links for mobile devices with unbalanced computational requirements and the distribution of healthcare data among PSN devices. Alternatively, smart contracts provide controls for access privileges (Dagher, Mohler, Milojkovic, & Marella, 2018) using cryptographic signatures (Xia, Sifah, Smahi, Amofa, & Zhang, 2017). Further, patient data tracking may be provided (Dorri, Steger, Kanhere, & Jurdak, 2017; Brodersen et al., 2016; Han et al., 2018).

The timeliness of data availability for sufficient healthcare outcomes (Gokalp, Gokalp, Çoban, & Eren, 2018) and the transfer of patient data between healthcare providers (Yang, Li, & Niu, 2015; Peterson, Deeduvanu, Kanjamala, & Boles, 2016) have been identified as issues. These are addressed as a relationship between provider and MedRec, where relevant data are stored on a ledger. Patients are empowered by ownership of their personal information and allowed to accept or reject patient-provider relationships (Azaria, Ekblaw, Vieira, & Lippman, 2016; Ekblaw, Azaria, Halamka, & Lippman, 2016). it is assumed that the level of data accuracy improves when patient are able to access information about themselves (Sujansky, Faus, Stone, & Brennan, 2010; Wu, Zhang, Xie, Alelaiw, & Shen, 2017; Sadiku, Eze, & Musa, 2018).

HIMS typically store large volumes of complicated and composite data. Poorly integrated independent/dependent HIMS result in inconsistent data representation. This may occur as a consequence of frequent updates to existing data, but the result is difficulty in knowledge discovery (Hosseinkhah, Ashktorab, & Veen, 2009). A blockchain solution provides an enterprise bus or service-based search (Gokalp et al., 2018; P. Zhang, White, Schmidt, & Lenz, 2017; Jiang et al., 2018). In cases where supply management and provenance tracking for counterfeit drugs that find their way into the drug supply chain (Bell, Buchanan, Cameron, & Lo, 2018), the blockchain provides a platform for the analysis of drugs using a chain of protection to trace where are the drugs have been (Sylim, Liu, Marcelo, & Fontelo, 2018).

4 Conclusion

This paper presents issues in healthcare information management system and opportunities for further research. A number of issues are identified in HIMS: Security, privacy, data transparency, accountability, data sharing, analytics, knowledge generation, interoperability, data accessibility, and storage. While blockchain technology focuses on financial systems, it provides other solutions such as identity management, risk management, auditing functions, security, and privacy.

Still, blockchain technology is difficult to use in HIMS. Studies propose solutions to solve issues, but these are still small in relation to the healthcare system. Currently, blockchain solutions focus on data accessibility to improve retrieval, strengthening security measures through the application of authentication and identification applications, creating an interoperability layer between providers, enabling data tracking to improve outcomes for patients, empowering patients by transferring data ownership, providing third party records verification, improving the accuracy of healthcare services invoicing, and supply chain management for patient management, drugs tracking, and so on.

References

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1.

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 534–543). Guangzhou, China.

Alshamari, M. (2016). Usability factors assessment in health information system. *Intelligent Information Management*, *8*(06), 170.

Ash, J. S., Sittig, D. F., Poon, E. G., Guappone, K., Campbell, E., & Dykstra, R. H. (2007). The extent and importance of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association*, *14*(4), 415–423.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *Open and big data (OBD), international conference on* (pp. 25–30). Vienna, Austria.

Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. *Blockchain in Healthcare Today*, *1*, 1-7. Retrieved from `https://doi.org/10.30953/bhty.v1.8`

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. (2016). *Blockchain: Securing a new health interoperability experience.* Retrieved from `https://bit.ly/2Hj5BjO`

Campbell, E. M., Guappone, K. P., Sittig, D. F., Dykstra, R. H., & Ash, J. S. (2009). Computerized provider order entry adoption: implications for clinical workflow. *Journal of general internal medicine*, *24*(1), 21–26.

Campbell, E. M., Sittig, D. F., Ash, J. S., Guappone, K. P., & Dykstra, R. H. (2006). Types of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association*, *13*(5), 547–556.

Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. *IEEE Security & Privacy*, *11*(6), 74–76.

Cartwright-Smith, L., Gray, E., & Thorpe, J. H. (2016). Health information ownership: legal theories and policy implications. *Vand. J. Ent. & Tech. L.*, *19*, 207.

Colijn, C., Jones, N., Johnston, I. G., Yaliraki, S., & Barahona, M. (2017). Toward precision healthcare: context and mathematical challenges. *Frontiers in physiology*, *8*, 136.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297.

Das, J., Holla, A., Mohpal, A., & Muralidharan, K. (2016). Quality and accountability in health care delivery: audit-study evidence from primary care in india. *American Economic Review*, *106*(12), 3765–99.

Dias, J. a. P., Reis, L., Ferreira, H. S., & Martins, A. (2018). Blockchain for access control in e-health scenarios. *CoRR ArXiv*. Retrieved from `https://arxiv.org/abs/1805.12267`

Di Vimercati, S. D. C., Foresti, S., Jajodia, S., & Samarati, P. (2007). Access control policies and languages in open environments. In *Secure data management in decentralized systems* (pp. 21–58). Springer.

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, *55*(12), 119–125.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data. In *Proceedings of ieee open & big data conference* (Vol. 13, p. 13). china.

Gokalp, E., Gokalp, M. O., Çoban, S., & Eren, P. E. (2018). Analysing opportunities and challenges of integrated blockchain technologies in healthcare. In *Eurosymposium on systems analysis and design* (pp. 174–183).

Goslee, S., & Conte, C. (1998). *Losing ground bit by bit: Low-income communities in the information age. what's going on series.* Wahington DC: Benton Foundation.

Han, H., Huang, M., Zhang, Y., & Bhatti, U. A. (2018). An architecture of secure health information storage system based on blockchain technology. In *International conference on cloud computing and security* (pp. 578–588). Nature Switzerland.

Horsky, J., Kuperman, G. J., & Patel, V. L. (2005). Comprehensive analysis of a medication dosing error related to cpoe. *Journal of the American Medical Informatics Association*, *12*(4), 377–382.

Hosseinkhah, F., Ashktorab, H., & Veen, R. (2009). Challenges in data mining on medical databases. In *Database technologies: Concepts, methodologies, tools, and applications* (pp. 1393–1404). IGI Global.

Howe, J. L., Adams, K. T., Hettinger, A. Z., & Ratwani, R. M. (2018). Electronic health record usability issues and potential contribution to patient harm. *Jama*, *319*(12), 1276–1278.

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018). Blochie: a blockchain-based platform for healthcare information exchange. In *2018*

ieee international conference on smart computing (smartcomp) (pp. 49–56). Taormina, Italy.

Kaye, H. S. (2000, July). Disability and the digital divide. *Disability Statistics Abstract*(22).

Kelman, C. W., Bass, A. J., & Holman, C. (2002). Research use of linked health data—a best practice protocol. *Australian and New Zealand journal of public health*, *26*(3), 251–255.

Kleinaki, A.-S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2018). A blockchain-based notarization service for biomedical knowledge retrieval. *Computational and structural biotechnology journal*, *16*, 288–297.

Liu, W., Zhu, S., Mundie, T., & Krieger, U. (2017). Advanced block-chain architecture for e-health systems. In *e-health networking, applications and services (healthcom), 2017 ieee 19th international conference on* (pp. 1–6). Dalian, China.

Mashima, D., & Ahamad, M. (2012). Enabling robust information accountability in e-healthcare systems. In *Proceedings of the 3rd usenix conference on health security and privacy* (pp. 14–14). USENIX Association. Retrieved from https://www.usenix.org/system/files/conference/healthsec12/health

McGuire, A. L., Fisher, R., Cusenza, P., Hudson, K., Rothstein, M. A., McGraw, D., ... Henley, D. E. (2008). Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. *Genetics in Medicine*, *10*(7), 495.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. *IEEE Access*, *6*, 10179–10188.

Miriovsky, B. J., Shulman, L. N., & Abernethy, A. P. (2012). Importance of health information technology, electronic health records, and continuously aggregating data to comparative effectiveness research and learning health care. *Journal of Clinical Oncology*, *30*(34), 4243–4248.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the prisma statement. *Annals of internal medicine*, *151*(4), 264–269.

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). *A blockchain-based approach to health information exchange networks* [White paper]. Retrieved 04 dec 2018, from https://pdfs.semanticscholar.org/c1b1/89c81b6fda71a471adec11cfe72

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. *Health information science and systems*, *2*(1), 3.

Sadiku, M. N., Eze, K. G., & Musa, S. M. (2018). Block chain technology in healthcare. *IJASRE*, *4*, 154–159.

Saleem, J. J., Patterson, E. S., Militello, L., Render, M. L., Orshansky, G., & Asch, S. M. (2005). Exploring barriers and facilitators to the use of computerized clinical reminders. *Journal of the American Medical Informatics Association*, *12*(4), 438–447.

Shortliffe, E. H., Altman, R., Brennan, P., Davie, B., Detmer, W., Florance, V., ... Huffman, J. (2000). *Networking health: Prescriptions for the internet*.

Sujansky, W. V., Faus, S. A., Stone, E., & Brennan, P. F. (2010). A method to implement fine-grained access control for personal health records through standard relational database queries. *Journal of biomedical informatics*, *43*(5), S46–S50.

Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *JMIR research protocols*, *7*(9).

Terry, N. P. (2000). Structural and legal implications of e-health. *Journal of health law*, *33*(4), 605–614.

Tsai, C.-W., Chiang, M.-C., Ksentini, A., & Chen, M. (2016). Metaheuristic algorithms for healthcare: open issues and challenges. *Computers & Electrical Engineering*, *53*, 421–434.

Viceconti, M., Hunter, P. J., & Hose, R. D. (2015). Big data, big knowledge: big data for personalized healthcare. *IEEE J. Biomedical and Health Informatics*, *19*(4), 1209–1215.

Wu, L., Zhang, Y., Xie, Y., Alelaiw, A., & Shen, J. (2017). An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. *Wireless Personal Communications*, *94*(4), 3371–3387.

Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, *8*(2), 44.

Yang, J.-J., Li, J.-Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems*, *43*, 74–86.

Zhang, J., Xue, N., & Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access*, *4*, 9239–9250.

Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *CoRR ArXiv*. Retrieved from `https://arxiv.org/abs/1706.03700`