Securing Smart City Health Services Using Blockchain Technology

doc. Ing. Hana Kopáčková, Ph.D., Ing. Suraj Belludi
Faculty of Economics and Administration
Institute of System Engineering and Informatics (40530), University of Pardubice
Pardubice, the Czech Republic
hana.kopackova@upce.cz, suraj.belludi@student.upce.cz

***Abstract* — In smart city environments cyber security is a major issue that must be addressed across different smart service domains while delivering quality of life for citizens. Smart healthcare is an important area that ensures quality health services delivery which is reliable and effective. Smart health is an important requirement for smart city services. To explore the nuances of smart city healthcare services, the paper presents a systematic literature review using current research. The focus of this study is to highlight the important issues surrounding s-healthcare services. There are multiple issues related to data security and privacy, since smart city infrastructures are complex and make use of multiple components in exchange of information resulting in security vulnerabilities. The use of blockchain technology in tackling the security and privacy issues in smart city healthcare are explored and analysed. The paper presents the role and importance of blockchain in healthcare, issues faced by health care services and the impact of blockchain in smart healthcare services to highlight the need for secured health information exchange in smart cities.**

Keywords—Blockchain, technology, Healthcare, Smart-health, Smart city, Systematic review

I. INTRODUCTION

The growth of urbanization and technology developments in recent years has continuously created the need for more efficient services and living standards for people. The concept of smart city implies the use of information and communication technologies to connect diverse physical components to improve information flow resulting in overall efficiency of city operations. Further smart city development also takes into account the creation of an operational environment using emerging technologies to address urban issues and provide citizens with quality living. Smart healthcare services make use of emerging smart technologies in smart city infrastructures to deliver quality healthcare [1].

Smart city services include healthcare service delivery as one of the major components. Healthcare services is a subject of innovation. For instance, health services are possible in the form of mobile-health (m-health) using wireless communications to support remote patients [2]. Further advances have led to the development of smart health (s-health) where health services were provisioned using smart city infrastructure [3]. Rather s-health focuses on improving m-health by adding smart sensing capabilities in the infrastructure.

Exploring the use of technologies for smart healthcare, it is noted that, remote health monitoring of patients makes use of different technologies to cater to health needs of people in remote locations [4]. According to Deloitte Research, smart healthcare is an important area for sustainability in smart cities as more and more people are moving to urban areas as found in cities such as Lisbon, Singapore, and Shiraz to mention a few [5]. Chicago in USA is another example of smart healthcare implementation that makes use of inter-connected technologies for health and wellness eco-system towards smart health initiatives.

In the USA, Louisville and Kentucky are focusing on optimal use of technology to facilitate information generation to take informed decisions on healthcare services [6]. In all these initiatives it is noted that optimization of service delivery significantly utilizes technologies such as Internet of Things (IoT), big data, blockchain, ICT applications and so on. For example, South Korea makes use of mobile data, bank cards and video surveillance to track people with health conditions. Israel also makes use of mobile location data coordinates to track patients with special healthcare needs. There are many countries that make use of mobile data, GPS and other technologies to monitor and track patients to note their current location [7].

Healthcare implementations and technology developments have led to the phenomenal increase in healthcare medical data where large volumes of information are shared between patients, healthcare providers, medical experts and insurance companies. This scenario has led to the development of data driven healthcare models which gave rise to significant levels of data and privacy risks [8]. To overcome data and privacy risks blockchain technology is considered for its security and privacy protection mechanisms. Blockchain can integrate with other smart city components and healthcare data available in other systems and networks such as internet of things (IoT), cloud and fog computing systems.

Blockchain is a decentralized platform with immutable security and privacy protection mechanisms that can address privacy and data security concerns in healthcare domain. Technical experts and smart city developers view blockchain as a potential technology to preserve privacy and confidentiality of patient's information in delivering health services [9]. Blockchain platforms can use patient health data from other applications and tackle issues surrounding data protection to deliver smart health services to citizens in smart city environments.

The research aims to investigate the role of blockchain technology in overcoming data vulnerabilities in s-health services in a smart city environment. A systematic literature review process is conducted in the study. The contributions of this study are as follows,

- To obtain a detailed view of data security and privacy related problems in s-health services in smart city environment.

- To analyse how blockchain in s-health services can resolve data security and privacy issues thus ensuring overall confidentiality of data for patients.
- Gain understanding on how blockchain technology can contribute in achieving s-health goals in smart cities.

II. Blockchain in Healthcare Services

Significant number of studies were identified on the topic of blockchain implementation for smart healthcare services in smart city environment. [10] provides a review of blockchain in smart city healthcare to address the issues surrounding the problems related to connecting disparate systems and poor interoperability in connecting patient health records with other systems. The use of blockchain is highlighted in interoperability in conjunction with address issues related to privacy, security, validation and authentication. [11] provided an investigation on the value co-creation of blockchain for healthcare services to highlight patient centered care, trust, enhanced service quality, secured information sharing, effective collaboration and dialogue with focus on patients' role. At this juncture the role of blockchain as a facilitator for interactions between patients and healthcare stakeholders in smart city environment was assessed. The aspect of improved trust through blockchain is highlighted for its ability to mitigate privacy and security risks related to patient sensitive data. However, the investigation is considerable on blockchain as a facilitator for information exchange between healthcare entities and patient with lack of adoption in a smart city environment. [12] presented a case study to highlight the issues faced in healthcare notably missing data, data security and privacy problems and inaccessibility of information for patients and healthcare specialists to make informed decisions. The case study was examined and based on analysis of interviews; the article reviews a framework for blockchain adoption to address issues in effective healthcare delivery. Architecture for fraud detection system using blockchain and artificial intelligence (AI) in healthcare sector is of great significance. In this study conducted by [13] focus was on health insurance fraud detection and highlights the different security threats and risks that can be overcome using blockchain technology. However, the study does not provide a demonstration of blockchain implementation to explain its usage in real time scenario. A comprehensive review on security challenges for healthcare data in smart city environment was undertaken by [14]. A security architecture based on AI and blockchain was proposed to handle malware and other network attacks. The study discussed commonly available security solutions along with open issues on smart healthcare environments.

It is noted that smart healthcare systems are susceptible to security risks and attacks on healthcare software applications and networks thus endangering patient lives. An exploration of literature highlights reviews many gaps related to blockchain implementation, issues in integrating different data sources and technologies to overcome security and privacy issues in smart healthcare environments.

III. Methodology

A systematic literature review was conducted in the research to examine the application of blockchain technology in smart healthcare environment. The articles used in the review were identified from search on the Web of Science Database as it is one of the authentic research databases in the world. The Web of Science database has a comprehensive repository of scholarly journals and conference proceedings. The other sources include online databases such as IEEE, Google Scholar and Elsevier.

The search was conducted using the following Boolean expressions:

- Blockchain for health data security and privacy
- Blockchain AND smart city healthcare
- Blockchain AND smart health services review

The search of literature was performed and the title and abstract were screened to shortlist articles for review. The selection criteria were applied to include articles from 2021 to 2024. The articles were categorized to provide answers for the research questions. The total number of articles finalized were 22 that falls within the scope of this research. In the next step the articles were categorized according to blockchain technology in the context of smart city healthcare services to address the challenges in smart healthcare domain as depicted in Figure 1.

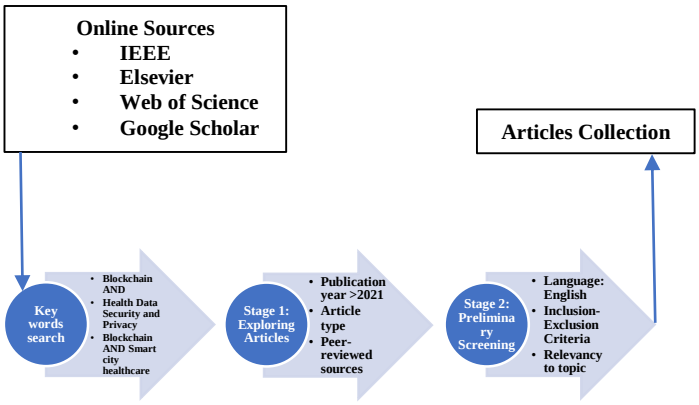


Figure 1: Data collection

The findings and discussions from literature on the use of blockchain in smart city health services provided significant publications related to blockchain for data security in smart city healthcare services. The publications further provide focus on the implementation of blockchain technology in areas of healthcare to create and facilitate smart healthcare services in smart city environment.

A. *Research Questions:*

The following research questions were addressed in this study:

RQ1: What challenges were found in data security for delivery of s-health services?

RQ2: How can blockchain technology resolve data related challenges in s-health services delivery?

RQ3: What is the impact of blockchain in s-healthcare in a smart city environment?

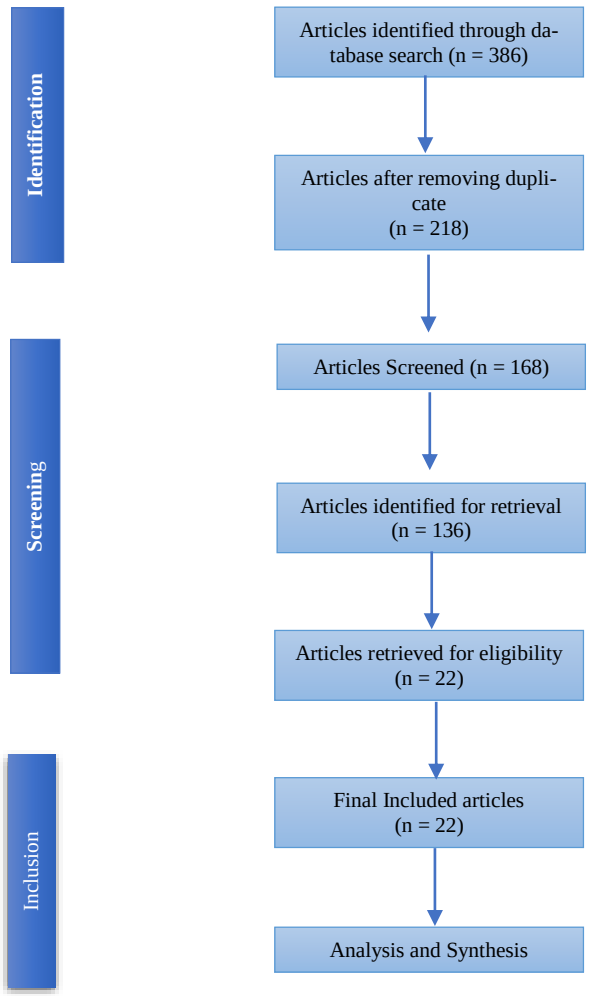
The analysis in this research has a comprehensive understanding of the role of blockchain technology in protecting s-health services data in a smart city environment. The research questions were developed to achieve this goal.

IV. Analysis

In the past decade healthcare domain has evolved as a major area in the development of smart cities. Healthcare services provide significant amounts of data that is mostly

private information and is vulnerable to privacy and security attacks, risks as main challenges .

The following flow chart was used in the study for systematic review of the litertaire, depicted as Chart 1



Charts 1: Flow chart for systematic analysis of literature

Results of PRISMA as flow chart are discussed and the key findings related to security challenges and possible solutions from papers reviewed are depicted in Table 1

Table 1: Key findings from papers reviewed based on criterion

Criterion	Description	Reference
Challenge	Information exchange between insurance companies, hospitals, medical experts and patients. Usually health insurance companies are required to avoid fraud claims and hence thee is a need to have a secured business model . In addition there are security attacks like phishing attacks, distributed denial of service attacks, and so on that target patient data.	[13] [15]
	Cyber crime impacts different entities involved in healthcare and where the patient's confidentiality and privacy is compromised	[16]
	leakage, intenal attacks and unauthoprised disclosue of data to third parties	[17], [18], [19]
Measures	Need for a comprehensive system that can authenticate and authorise the exact users for healthcare data acess. There are a variety of security solutions for access controls, however when data is shared between mutiple entities during different stages in diagnosis and treatment of patients, the existing encryption-decrypion systems tends to be a bit overwhelming.	[16]
Blochchain solves securityand privacy problems	To address common security and privacy issues in smart healthcare environments	[20], [21], [22], [23]
	Works as a distributed ledger that allows peers to collaborate and have accesss to data on a decentralised network. The consensus mechanisms in blockchains will support information sharing and communication between peers or only authorised users. Blockchain technology ensures data though decentralised protection from corruption or misuse or other malicious activities that are common challenges in healthcare information systems	[24]

RQ1: What challenges were found in data security in delivery of s-health services?

Many studies that highlight various challenges related to smart healthcare were explored. Since healthcare data contains sensitive data one of the major challenges is the inter-linked structure of electronic healthcare records (EHR)

[25]. EHR contains crucial patient data shared by physicians, healthcare workers, insurance companies and patients and hence the linked records pose security issues. Due to the inter-linking of records, the data is vulnerable to attacks where attackers can access patient data by stealing information [26]. This further complicates the overall data protection as networks share and transmit data between different users leading to network vulnerabilities.

The next challenge is the weaknesses in regulations that allow the sharing and exchange of healthcare data between healthcare provider and other entities such as health insurance companies and physicians. Recent trends indicate the use of smart devices such as Apple watches, fitness wearables, etc., that exchange healthcare data between the user and healthcare service provider. Usually, the exchange is unsecured that leads to compromised data [27].

Cyber security attacks are a major challenge in smart healthcare service delivery. Cyberattacks are targeted usually against systems and networks that contain sensitive data such as healthcare information. There are a variety of attacks that aims to compromise databases, software applications, networks and devices. Numerous studies highlight a variety of attacks targeting software, networks and communications, and databases to compromise healthcare systems and infrastructures.

RQ2: How can blockchain technology resolve data related challenges in s-health services delivery?

As noted in different studies blockchain for its immutable data structure in a shared healthcare service infrastructure is ideal for healthcare service delivery. Blockchain enabled health care systems ensure interoperability of data between disparate systems and data integrity of health data, authenticate insurance claims, in addition to offering quality health services for patients. Blockchain helps to overcome the issues related to distributed patient records stored in silos and are often inaccessible or not immediately available. Healthcare information exchanges need patient historical data quickly for services. In these scenarios, blockchain supports in developing smart healthcare by consolidating and securing health records and provides ease of access or exchange of patient health records [28].

In smart healthcare environments there is a need for customized and effective healthcare assistance for people. Blockchain due to its high reliability and in the absence of central authority will secure patients' EHR and medical reports and make them accessible to authorized medical personnel during serious illness or emergency situations. Blockchain technology for its cryptographic techniques will ensure only approved users have access to certain data stored in blocks thus preventing data misuse or other malicious activity. Further, blockchain ensures that existing data once saved through consensus cannot be modified or deleted thus enabling traceability of records in the chain. This implies, if a malicious user has access to a block, the information in a block the data cannot be modified or erased without consensus from all users in the chain. In this manner security challenges are usually addressed with blockchain. Furthermore, blockchain guarantees trust and reliability of data due to its immutability characteristic to enable new applications that are trust worthy in a smart healthcare environment.

RQ3: What is the impact of blockchain in s-healthcare in a smart city environment?

The role of blockchain in s-health services is significant. Due to the growing demand of patient health requirements and the need to have better control of patients' individual health records the need for secured data exchange mechanisms is highly important. To handle these areas blockchain implementation in healthcare services provide seamless data exchange across multiple healthcare systems. Another important area where blockchain plays a major role is in value co-creation. Value co-creation is important in resource and data sharing that involves participation of patients, healthcare service providers and health care professionals. Blockchain implementation in such scenarios improves service interactions along with enhancing engagement of involved parties [11]. This was demonstrated during the Covid-19 pandemic that involved data sharing between multiple entities and users to facilitate research. During reviews many blockchain platforms were identified, highlighted in studies. The s-healthcare must review existing platforms to select the most feasible blockchain platform that can improve data accessibility and standardization in the given healthcare ecosystem. There are numerous studies that highlight the use of blockchain technology for addressing data security and accessibility challenges, studies highlight the need for blockchain in fraud prevention and data misuse. It is noted that in smart healthcare data is more vulnerable to threats and risks that can impact other components in smart city environments. In view of these aspects, blockchain along with AI has the ability to mitigate security threats, however open issues facing smart city health services must be addressed using a more holistic approach.

V. Conclusion

The systematic literature review presents the growing attention of blockchain technology in smart healthcare services in smart city environments. Blockchain due to its potential in handling data and application issues in healthcare domain is widely considered for implementation in s-health services. The report provides the methodology followed in the systematic review and mainly focuses on the areas of data security and privacy related issues in s-health environments, problems related to patient privacy preservation and confidentiality in exchanging health data and to have more clarity on the use of blockchain technology implementation to achieve s-health initiatives.

The systematic review provides reviews and consensus related to blockchain in healthcare from existing work. The research highlights existing ideas and challenges along with gaps identified for the topic. The research questions were framed and answers to research questions were identified from existing research and presented in the analysis. It is noted that the use of blockchain in s-health will certainly improve patient privacy and security of data in complex smart city infrastructures. Blockchain will also enable smart healthcare solutions while ensuring trust and reliability of information exchanges in smart city environments. However, the open issues related to blockchain platform selection and implementation in smart city environments must be addressed.

Further research on this topic can be undertaken by using survey- based approach for data collection to understand the effectiveness of blockchain implementation in overcoming information protection issues in smart city environment.

REFERENCES

[1] M. Kamruzzaman, B. Yan , M. Sarker and I. Alruwa, "Blockchain and fog computing in IoT-driven healthcare services for smart cities," *Journal of Healthcare Engineering,* vol. 2022, 2022.

[2] R. Rayan , I. Zafar,, C. Tsagkaris , A. Papazoglou and D. Moysidis, "Pervasive m-health for chronic diseases," *Computational Intelligence for Medical Internet of Things (MIoT) Applications,* vol. 14, pp. 301-314, 2023.

[3] P. Mishra and G. Singh, "Smart Healthcare in Sustainable Smart Cities," in *Sustainable Smart Cities: Enabling Technologies, Energy Trends and Potential Applications,* 2023.

[4] D. Sangeetha, M. V. Rathnam, R. Vignesh, J. S. Chaitanya and V. Vaidehi, "MEDIDRONE—A Predictive Analytics-Based Smart Healthcare System," Singapore, Springer, 2020, p. 19–33.

[5] M.-. E. Antunes, "Deloitte Insights: Smart cities, smarter public health," Deloitte, 06 2022. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/smart-city/building-a-smart-city-with-smart-digital-health.html. [Accessed 28 02 2024].

[6] M. F. Antunes, D. G. OliveiraJean and G. Barroca, "Urban Future. 12 trends shaping the future," Deloitte Research, 2021.

[7] Z. Kalpaeva, E. Rodionova and I. Dominiak, "The role of smart cities in countering health threats: A review of practices," *E3S Web of Conferences,* vol. 435, 2023.

[8] A. Pise , B. Yoon and S. Singh, "Enabling Ambient Intelligence of Things (AIoT) healthcare system architectures," *Computer Communications,* vol. 198, 2023.

[9] P. Sharma , S. Namasudra , N. Chilamkurti and B. Kim, "Blockchain-based privacy preservation for IoT-enabled healthcare system," in *ACM Transactions on Sensor Networks,* 2023.

[10] H. ,. D. Zubaydi, Y. W. Chong, K. Ko, S. M. Hanshi and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electronics,* vol. 8, no. 6, 2019.

[11] T. Russo-Spena, C. Mele, Y. Cavacece, S. Ebraico, C. Dantas, P. Roseiro and W. van Staalduinen, "Enabling Value Co-Creation in Healthcare through Blockchain Technology," *International Journal of Environmental Research and Public Health,* vol. 20, no. 1, 2022.

[12] I. Azogu, A. Norta, I. Papper, J. Longo and D. Draheim, "A framework for the adoption of blockchain technology in healthcare information management systems: A case study of Nigeria," in *12th International Conference on Theory and Practice of Electronic Governance*, 2019.

[13] K. Kapadiya, U. Patel, R. Gupta, M. D. Alshehri, S. Tanwar, G. Sharma and P. N. Bokoro, "Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects," *IEEE Access,* vol. 10, pp. 79606-79627, 2022.

[14] A. Alabdulatif, I. Khalil and M. Saidur Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis.," *Applied Sciences,* vol. 12, no. 21, 2022.

[15] A. B. de Neira, B. Kantarci and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks,* vol. 222, 2023.

[16] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar and R. Ahmad Khan, "Healthcare data breaches: insights and implications," *Healthcare, MDPI,* vol. 8, no. 2, 2020.

[17] Z. Sultana and D. Kumar, "Medical Data Privacy Representation with Improved Encryption Algorithm," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 12, no. 8s, pp. 581-591, 2024.

[18] I. Boumezbeur and K. Zarour, "Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption," *Acta Informatica Pragensia,* vol. 11, no. 3, pp. 361-379, 2022.

[19] S. R. Oh, Y. D. Seo, E. Lee and Y. G. Kim, "A comprehensive survey on security and privacy for electronic health data," *International Journal of Environmental Research and Public Health,* vol. 18, no. 8, 2021.

[20] A. Ali, H. A. Rahim, M. F. Pasha, N. Dowsley, M. Masud, J. Ali and M. Baz, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics,* vol. 10, no. 16, 2021.

[21] J. ,. B. Awotunde, C. Chakraborty and S. ,. O. Folorunso, "A secured smart healthcare monitoring systems using blockchain technology," in *Intelligent Internet of Things for Healthcare and Industry (pp. 127-143).*, 2022.

[22] M. Sookhak, M. R. Jabbarpour, N. S. Safa and F. R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," *Journal of Network and Computer Applications,* vol. 178, 2021.

[23] M. Younis, W. Lalouani, N. Lasla, L. Emokpae and M. Abdallah, "Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access," *IEEE Systems Journal,* vol. 16, no. 3, pp. 3746-3757, 2021.

[24] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri and Q. N. Nguyen, "Blockchain technology: security issues, healthcare applications, challenges and future trends," *Electronics,* vol. 12, no. 3, 2021.

[25] H. B. Mahajan, A. S. Rashid, A. A. Junnarkar, N. Uke, S. D. Deshpande, P. R. Futane, A. Alkhayyat and B. Alhayani, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience,* vol. 13, no. 3, 2023.

[26] M. Nalin, I. Baroni, G. Faiella, M. Romano, F. Matrisciano, E. Gelenbe, D. ,. M. Martinez, J. Dumortier, P. Natsiavas, K. Votis, V. Koutkias, D. Tzovaras and F. Clemente, "The European cross-border

health data exchange roadmap: Case study in the Italian setting," *Journal of Biomedical Informatics,* 2019.

[27] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *International Journal of Healthcare Management,* vol. 15, no. 1, pp. 70-83, 2022.

[28] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble and R. A. Dziyauddin, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *Sustainability,* vol. 15, no. 8, 2023.