Securing edge-enabled smart healthcare systems with blockchain: A systematic literature review

Žiga Kodrič, Simon Vrhovec, and Luka Jelovčan*
University of Maribor, Ljubljana, Slovenia
ziga.kodric@student.um.si, {simon.vrhovec, luka.jelovcan}@student.um.si

Received: September 7, 2021; Accepted: October 30, 2021; Published: November 30, 2021

Abstract

As edge computing applications in smart healthcare systems are becoming increasingly more popular, security issues are on the rise as well. Blockchain is emerging as one of the most popular solutions for securing edge-enabled smart healthcare systems however the extent to which blockchain has been applied to those systems is unclear. To fill in this gap, we conducted a systematic literature review focusing on blockchain-based edge-enabled smart healthcare systems. The results of our review show that this is a novel field as the number of publications seems to grow exponentially each year. Blockchain is mostly utilized for ensuring access control and data transmission security albeit several papers emphasize the importance of node security in such systems too. Most edge-enabled smart healthcare systems support creating and reading data, and approximately half of them support updating data while deleting is rarely supported.

Keywords: smart health, edge, blockchain, SLR

1 Introduction

Healthcare is one of the sectors that has been highly affected by digitization. Smart healthcare system are complete system that can perform automated medical and other health-related tasks locally and remotely. Such systems present an efficient opportunity to newly empower physicians, nurses and other staff in healthcare institutions which warrants better performance and treatment quality for patients. For smart healthcare systems to perform efficiently, certain functional criteria, such as high quality service, low running costs, capability of executing remote and wireless tasks, and task automation, need to be met [14].

Among many industries in which it is crucial to ensure data security, healthcare is probably the most critical one [49, 51]. Although the internet of things (IoT) is a crucial part of smart healthcare systems, it is still inherently insecure in its nature [15] while the identification of its vulnerabilities remains one of the most tedious challenges [46]. In recent years, the edge computing paradigm evolved. The key benefit of edge-enabled compared to cloud-based smart systems is its decentralized nature [23]. Edge computing brings data processing to the very edge of smart systems [6, 21], i.e., close to IoT devices which collect patient health data (e.g., blood pressure, body temperature, pulse). IoT devices may be thus relieved from certain security-related overhead and run more smoothly and without interruptions [48, 19]. Among various methods that have been used to resolve security and privacy challenges in edge-enabled smart healthcare systems, few received as much attention as solutions involving the blockchain technology [1, 48].

Journal of Internet Services and Information Security (JISIS), volume: 11, number: 4 (November), pp. 19-32
DOI:*10.22667/JISIS.2021.11.30.019*

*Corresponding author: University of Maribor, Faculty of Criminal Justice and Security, Kotnikova 8, 1000 Ljubljana, Slovenia, Tel: +386-41-290-854

Several literature reviews on the use of blockchain in the context of healthcare can be found in the literature. For example, [45] and [49] review the use of blockchain in the context of IoT in healthcare, [47] reviews the use of blockchain in the context of electronic health records, and [41] and [35] review the use of blockchain for ensuring IoT security in general. To the best of our knowledge, none of the published reviews focus on the use of blockchain in the context of edge-enabled smart healthcare systems beyond mentioning it as a potential future trend [47]. The aim of this paper is to fill in this gap by identifying the current trends for blockchain-based security solutions for edge-enabled smart healthcare systems.

This paper is organized as follows. Theoretical background is introduced in Section 2 and followed by the description of the used research method for conducting our literature review in Section 3. In Section 4, we present the results of our study, namely, some general observations, results related to the three identified security areas, and core data management operations (i.e., create, read, update, delete). Section 5 is dedicated to the discussion and study limitations. Finally, Section 6 concludes the paper with outlining its core ideas.

2 Theoretical background

Modern healthcare systems need to be highly efficient as well as cost effective. They need to offer high quality service, have low running costs and be possibly automated [14]. To achieve this, smart healthcare systems that use IoT devices were developed. A smart healthcare system is a complete system that enables remote healthcare activities, such as diagnosing, monitoring, treatment and even surgeries [8, 60]. Smart healthcare systems thus effectively extend healthcare services from hospitals to patients' homes. Healthcare staff therefore do not need to be in contact with patients physically which may save both time and funds [40]. However, such systems do not come with benefits only.

The scalability of centralized smart healthcare systems (e.g., network bandwidth, response time) is a key operational challenge [48]. To deal with this issue, the edge computing paradigm moves the processing of data towards the data producers at the edges of networks, such as smart healthcare systems [48]. Edge-enabled smart healthcare systems can thus achieve shorter response times, more efficient data processing and smaller pressure on the system as a whole [48, 19]. A key benefit of edge computing is therefore its decentralized nature [23], and computer clouds in such smart systems turn towards becoming more or less storehouses for raw data [3]. Although edge computing offers some advantages over pure cloud computing, it does not address the security and privacy issues *per se*.

Data security and privacy challenges are one of the most significant threats to smart healthcare systems [51]. Information collected with IoT devices is vulnerable and thus needs to be secured prior to uploading [10]. Data must be first securely delivered from IoT devices to edge nodes where they are processed [17]. Since data theft and tampering remain a key challenge in smart healthcare systems, securing edge nodes is crucial [2]. Security challenges of edge-enabled smart healthcare systems can be categorized into three groups: network and service, data and IoT devices [51]. *Network and service* includes challenges related to verification of identity, access control, lightweight protocol design, intrusion detection, trust management, privacy-conserving forwarding, and rogue node detection [51]. *Data* includes challenges related to data identification, aggregation and integrity, secure content distribution, distributed computation ledgers, big data analysis, verifiable computations, and secure data computations [51]. *IoT devices* challenges include lightweight trust management, and confidentiality preservation [51]. The latter can be further divided into authentication and privacy (i.e., identity, data, usage, and location privacy).

To address some of these security and privacy challenges of edge-enabled smart healthcare systems, the blockchain technology may be used. Blockchain is a decentralised distributed ledger where no single authority can endorse transactions secretly [1, 29]. The ledger is distributed, immutable, transparent, secure, and auditable [43]. Blockchain has four key benefits, namely authorization, authentication, non-repudiation, and integrity [10]. Blockchain-enabled systems are scalable, offer mutual authentication, trustworthiness, privacy, and data integrity therefore offering an attractive opportunity for ensuring security and privacy in smart healthcare systems ([2].

3 Methods

First, we collected relevant records from the Web of Science and Scopus bibliographic databases. The same search query was used for querying both databases: (”edge” OR ”iot healthcare” OR ”iot-based healthcare” OR ”iot healthcare” OR ”edgecare”) AND (”healthcare” OR ”health care” OR ”hospital*” OR ”patient*” OR ”medical”) AND (”blockchain”) AND (”cybersecurity” OR ”cyber-security” OR ”security” OR ”privacy”). Both bibliographic databases were queried on 22 March 2021 resulting in 123 records (39 in Web of Science and 84 in Scopus). Second, after excluding duplicates, 90 papers were suitable for further analysis. Third, we excluded articles which did not meet our inclusion and exclusion criteria presented in Table 1 by reviewing the titles and abstracts of the considered papers.

Table 1: Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
Article is available in English.	Article is not available in English.
Full text is available.	Full text is not available.
Research article or conference paper.	Poster, book, book chapter, review, editorial or note.
Paper proposes a novel smart healthcare data management system, framework, or architecture.	Paper does not use blockchain for security or privacy purpose.
Paper utilizes blockchain in at least one security- or privacy-related application.	

Fourth, two researchers independently identified research methods, security areas, and data management functionalities they investigate by reviewing the full texts of papers. All disparities were consolidated by consulting a third researcher. After reading the full texts, 9 papers were additionally excluded. The research process is presented on Figure 1.

4 Results

4.1 General observations

The distribution of papers over the years is presented in Figure 2. The presented data suggests that the number of papers which address blockchain-enabled solutions for security in smart healthcare is increasing as half of all analysed papers ($N = 18$) were published in 2020. The projection for 2021 suggests that the growth of indexed papers in this field may continue to be close to exponential in the foreseeable future indicating a growing interest among researchers in this topic.

4.2 Security areas

Based on the reviewed papers, three security areas were identified. The security areas were determined based on the purpose for which blockchain technology is used for security in the papers. A summary of security areas and their aims, key functions, and related literature is provided in Table 2.

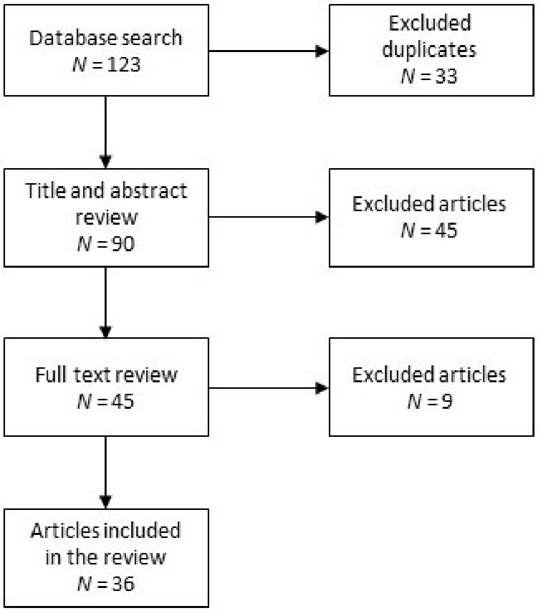

Figure 1: Systematic literature review process.

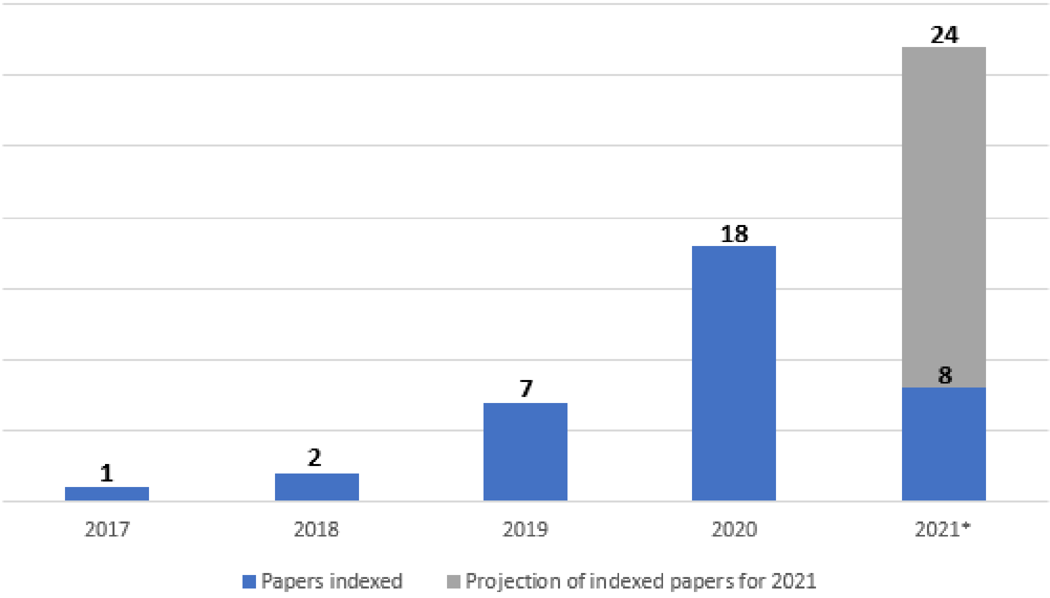

Figure 2: Publication years.

Table 2: Security areas.

Security area	**Aim**	**Key functions**	**Literature**
Access control	Blockchain is used to restrict the access to certain data or nodes.	(1) Preventing the access to healthcare data from unauthorised entities. (2) Designating the end users and their respective rights. (3) Maintaining the privacy of the patients.	[2, 3, 4, 5, 10, 11, 16, 17, 18, 20, 22, 25, 26, 27, 31, 32, 36, 37, 44, 50, 53, 56, 57, 59, 61, 62, 63]
Node security	Maintaining the integrity of healthcare data which is used in a blockchain-supported system.	(1) Maintaining the integrity and authenticity of healthcare data input. (2) Ensuring interoperability of nodes across the network.	[5, 10, 20, 22, 44, 53, 56, 61]
Data transmission security	Blockchain is used to secure the transmission of healthcare data between two nodes.	(1) Granting the access to the healthcare data. (2) Ensuring the integrity of the transmitted data packages of healthcare data. (3) Preventing man-in-the-middle attacks. (4) Preventing eavesdropping. (5) Maintaining the privacy of the patients.	[2, 4, 7, 9, 10, 11, 17, 20, 22, 24, 25, 26, 27, 28, 31, 34, 36, 38, 39, 42, 50, 53, 54, 56, 57, 59, 61, 62]

In Figure 3, security areas covered by individual papers over the years are presented. In total, data transmission security has been covered by the most papers ($N = 28$), with access control following ($N = 27$). Node security was covered in eight papers. Both access control and data transmission security were covered in the oldest paper identified, while node security was first covered in 2019.

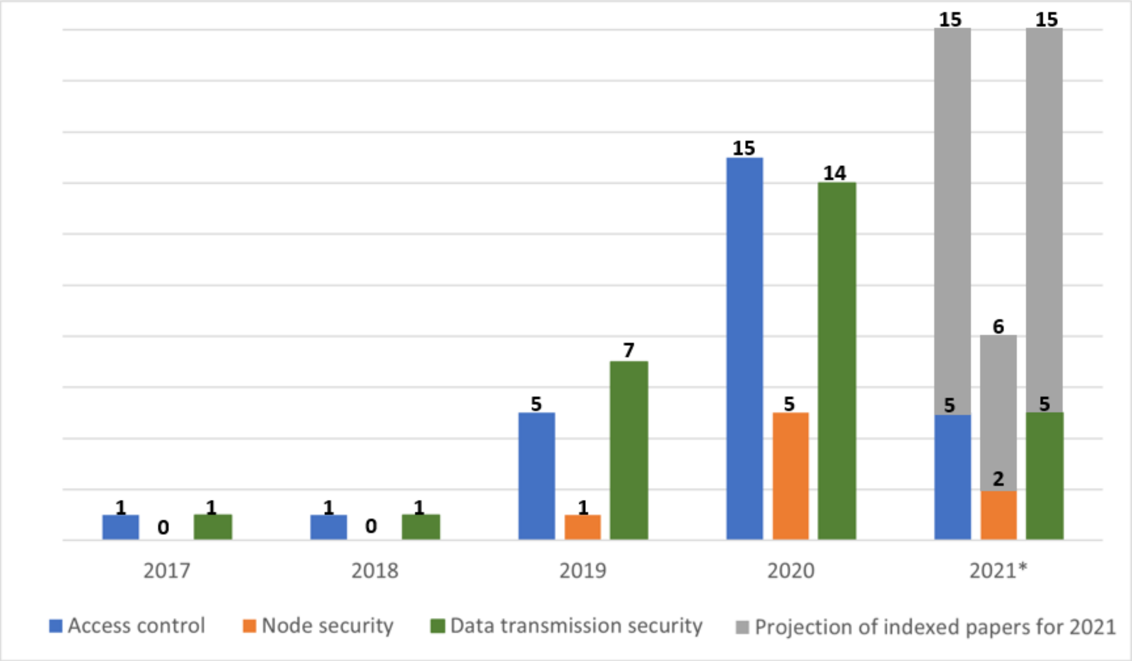

Figure 3: Security areas covered by years.

All papers included in our review propose a novel framework, approach, solution, or system utilizing the blockchain technology in edge-enabled smart healthcare. Papers however differ on the research methodology used. Based on the review of the papers, three main research methodologies were identified. Most papers employed an experimental method ($N = 26$), nine papers were theoretical, and one paper provided a use case. Papers that employed an experimental method generally consisted of a proposed theoretical framework, and an empirical test of the proposed framework. The main purpose of such papers is to show the empirical value and to evaluate the performance of proposed systems [20, 31, 36]. Simulations using either self-generated data or existing data from different healthcare-related databases were conducted in most cases [3, 5, 7, 11, 16, 18, 20, 22, 26, 27, 28, 31, 32, 34, 37, 42, 54, 57, 61]. Four quasi-experiments were also conducted [25, 36, 39, 56] and three experiments [38, 44, 62]. Theoretical papers mostly focused on developing theoretical models without empirically testing them. Frameworks were built either on findings from previous studies or on authors' assumptions. Although some papers [9, 50] provide a security or a performance evaluation, the conditions under which evaluations were performed are unclear judging from the data provided in papers and were thus considered as theoretical papers since the majority of paper was of a theoretical nature. Along with a theoretical model, one paper also provided a use case [2]. This paper demonstrated the usability of the proposed framework in a use case scenario showing how the framework could be used in practice.

Figure 4 shows which security areas were studied with which research methodologies. The shares of all three research methodologies for access control, node security, and data transmission security are comparable, favouring experiments (70%, 75% and 68%, respectively) over theoretical papers (26%, 25% and 29%, respectively), and use cases (4%, 0% and 4%, respectively).

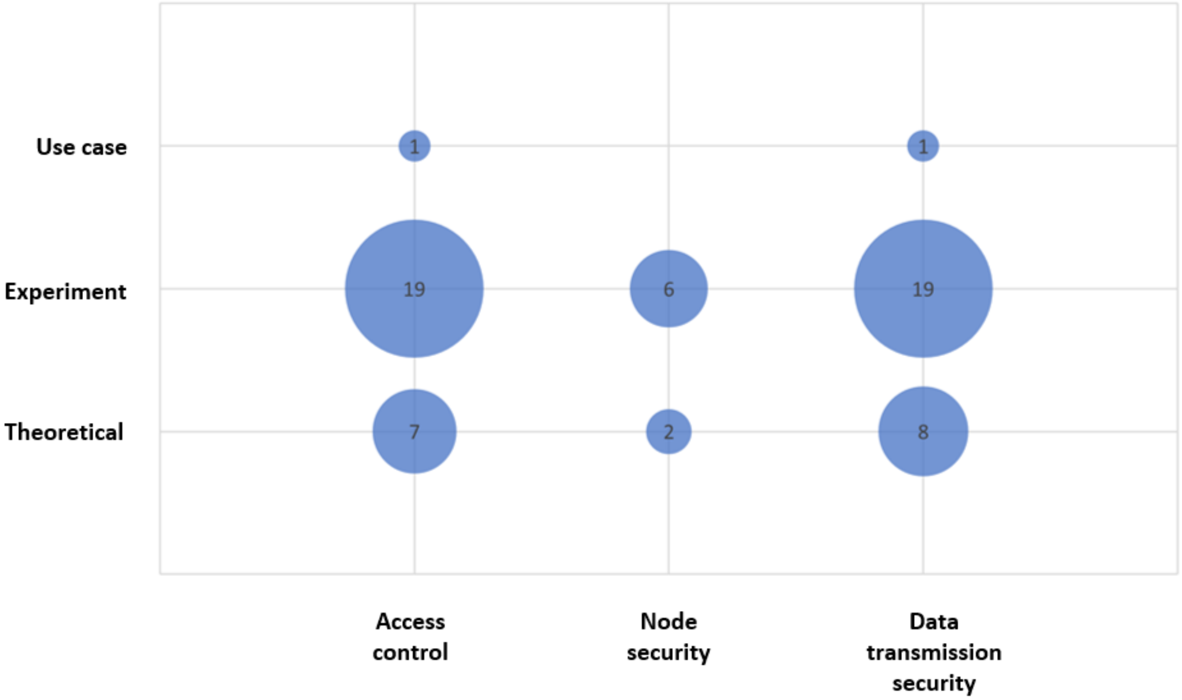

Figure 4: Distribution of employed research methodologies for different security areas.

4.3 Data management

Data management involves four key data operations, namely Create, Read, Update and Delete – CRUD. The papers were reviewed to determine which CRUD operations their proposed systems / frameworks support. Most proposed systems support create ($N = 32$) and read ($N = 31$) operations. Roughly half of the proposed systems / frameworks support the update operation ($N = 19$) and only four support the delete operation. Four frameworks did not provide any indication on which CRUD operations they support. Figure 5 presents a bubble chart showing which research methodologies were used for different CRUD operations. Again, the shares of all three research methodologies for create, read, update, and delete are comparable, favouring experiments (72%, 71%, 74% and 75%, respectively), over theoretical papers (25%, 26%, 26% and 25%, respectively), and use cases (3%, 3%, 0%, 0%, respectively).

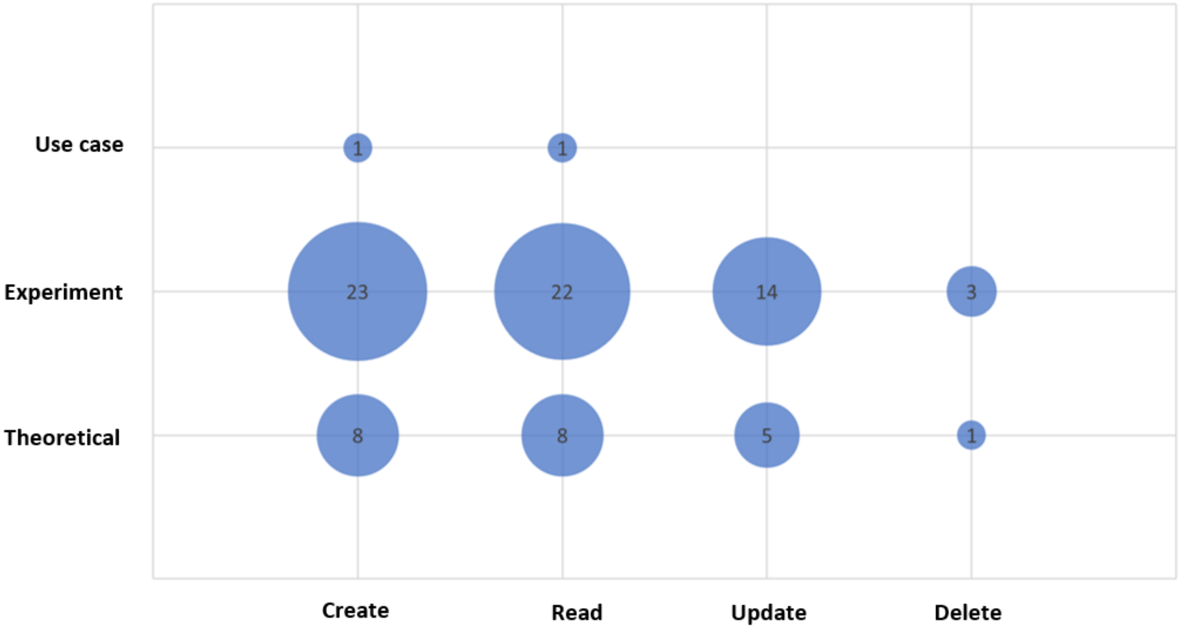

Figure 5: Distribution of employed research methodologies for different CRUD operations.

Figure 6 presents the distribution of papers investigating CRUD operations with respect to different security areas. All three security areas as most often connected to create and read operations (data transmission security 89%; node security 63% and 50%, respectively; access control 85% and 81%, respectively). Proportionally, the share of papers investigating the update operation in relation to node security (38%) was comparable with the share for data transmission security (42%) and access control (35%), unlike the shares for the create and read operations. All papers, which included delete function also included access control and three of them also included data transmission security.

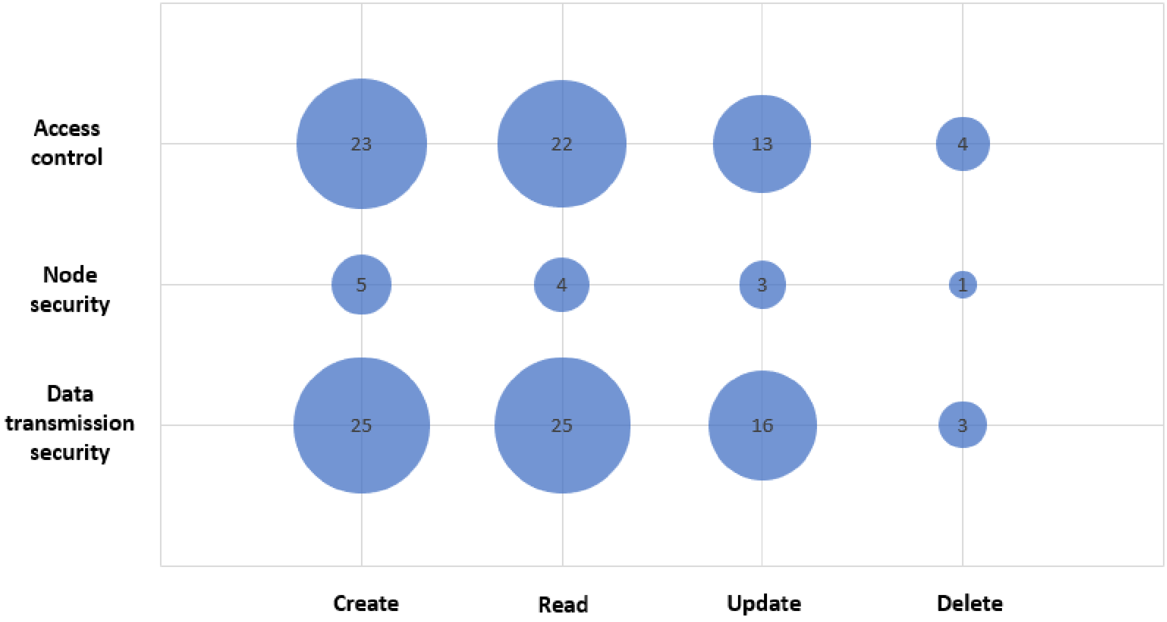

Figure 6: Distribution of CRUD operations over different security areas.

5 Discussion

The conducted a systematic literature review offers several interesting insights and implications. First, the distribution of papers over the years and the fact that the first paper published in this field was in 2017 [57] suggests that this is a fairly new field of study. Research on blockchain-based applications and systems started being published in 2014, and first connection of blockchain to the health sector in 2016 [13] suggesting that the application of blockchain to edge-enabled smart healthcare systems started in a timely manner. Although not as high as in some related areas, the number of papers almost tripled every year from 2017 to 2020. Eight papers published and indexed in the first three months of 2021 suggest that a similar trend will continue in 2021.

Second, due to the relative novelty of the research field, most papers provide a theoretical model which is often supported by simulations in experimental settings. This indicates a need for real-world empirical evidence that would provide more insights into the applicability of proposed frameworks and related security challenges. Although one paper employed a use case [2], it used a non-real world example to present the usability of the system. Use cases based on real-world examples would provide some useful insights although not as rich as case studies of real-world applications. The lack of such case studies and real-world use cases can be partially contributed to the novelty of the research field as testing smart healthcare systems in real world settings presents a complex task [58]. This may also be partially contributed to the fact that most healthcare institutions are relatively slow in adopting smart healthcare and IoT solutions [55]. This makes it even harder to currently implement proposed systems in a real-world case study. Nevertheless, insights from case studies of some of the first implemented smart healthcare systems would be invaluable.

Third, the identified papers mostly focus on data transmission security and access control. Those concepts specifically apply to the security of data during the transfer between two nodes and ensuring that only authorised users can create, read, update, and delete the data. In contrast, node security that focuses on security of the data in the proximity of its entry into the smart healthcare system is far less investigated than the other two security areas. Node security presents a prerequisite for the security of a smart healthcare system as a whole as it ensures the integrity and authenticity of healthcare data. Out of 23 papers that propose blockchain-enabled support systems, only four also consider node security [5, 10, 44, 61]. While this may be somewhat understandable since some papers primarily focus on using blockchain for security operations, it would be highly beneficial to investigate more node security.

Fourth, research on several aspects of smart healthcare is growing [52]. Although our structured literature review captured several technical security challenges of edge-enabled smart healthcare systems, there seems to be a large research gap regarding the human aspects of their security. It may be important to consider attitudes of healthcare workers and patients towards use of IoT devices, edge nodes and the blockchain technology in healthcare. Research suggests that healthcare workers are hesitant to use smart healthcare systems which may be mainly attributed to their perceived usefulness, ease of use and perceived risks [33]. Patients' perceptions on the other hand are largely unexplored. Besides the hesitation to adopt smart healthcare systems, privacy laws, such as GDPR regulating ownership and sharing of the healthcare data [12], which vary over different countries can also present a security challenge with wider adoption of smart healthcare systems.

5.1 Limitations

Like most research, this paper has a number of limitations that should be considered. First, we only considered research articles and conference papers indexed in two databases, which could eliminate some relevant publications in this field. Second, only publicly available full texts in English language were included in our research. It is possible that our research thus left out some relevant publications, which were not available publicly or were not published in English language. Third, only two researchers reviewed the papers independently. While the third researcher consolidated all inconsistencies, involving more researchers in the review process would ensure even higher validity of results.

6 Conclusion

Smart healthcare systems enable remote healthcare activities [8, 60]. Edge computing can be applied to deal with scalability and other issues in centralized cloud-based healthcare systems [48]. Edge computing moves the processing of data to the edges of data network systems which improves user experience by reducing response time, increasing the efficiency of data processing, and relieving the whole systems from extra pressure [48, 19].

To deal with security and privacy challenges researchers proposed several solutions. The most frequent one is blockchain which is a decentralized distributed ledger originally introduced for cryptocurrencies, specifically, Bitcoin [1, 30]. Its key benefits are immutability, transparency, security and auditability [43].

In this paper, we conducted a systematic literature review of published literature on the use of blockchain in edge-enabled smart healthcare systems. The results of our study indicate that the number of publications is growing almost exponentially. Approximately half of the analyzed papers were published in 2020. We identified three security areas, namely, access control, node security, and data transmission security. Most papers focused on access control and data transmission security. Considering the research methods used, most studies employed an experimental method, and the second most frequently employed method was theoretical. A single paper employed the use case research method calling for more implementations of proposed blockchain-based edge-enabled smart healthcare systems in practice. Only implementing edge-enabled smart healthcare systems in the real world may help to identify and deal with any practical issues and hidden vulnerabilities that may show up during everyday operations.

Furthermore, we explored the coverage of data management operations (i.e., create, read, update, and delete) in published literature. Most reviewed papers support creating ($N = 32$) and reading ($N = 31$) data, roughly half of them support updating ($N = 19$), and only a few ($N = 4$) deleting data. Future works may focus more on solutions related to deleting data to ensure edge-enabled smart healthcare systems are able to delete data if required to do so. Only smart healthcare systems that fully support all CRUD data management operations can be considered as complete.

References

[1] N. Abdullah, A. Hakansson, and E. Moradian. Blockchain based approach to enhance big data authentication in distributed environment. In *Proc. of the 9th International Conference on Ubiquitous Future Networks (ICUFN'17), Milan, Italy*, pages 887–892. IEEE, July 2017.

[2] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. Y. Song, A. K. Bashir, and A. A. El-Latif. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, 8:111223–111238, June 2020.

[3] R. Akkaoui, X. Hei, and W. Cheng. EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. *IEEE Access*, 8:113467–113486, June 2020.

[4] B. Alamri, I. T. Javed, and T. Margaria. Preserving Patients' Privacy in Medical IoT Using Blockchain. In *Proc. of the 4th International Conference Edge COmputing (EDGE'20), Honolulu, Hawaii, USA*, volume 12407 of *Lecture Notes in Computer Science*, pages 103–110, Honolulu, HI, 2020. Springer, Cham.

[5] J. A. Alzubi. Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. *Computer Communications*, 170:200–208, March 2021.

[6] M. Amiri-Zarandi, R. A. Dara, and E. Fraser. A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Computers & Security*, 96(101921), September 2020.

[7] G. S. Aujla and A. Jindal. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE Journal on Selected Areas in Communications*, 39(2):491–499, February 2021.

[8] S. B. Baker, W. Xiang, and I. Atkinson. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access*, 5:26521–26544, November 2017.

[9] M. Bampatsikos, C. Ntantogian, C. Xenakis, and S. C. Tomopoulos. BARRETT blockchain regulated remote attestation. In *Proc. of the 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI'19), Thessaloniki, Greece*, pages 256–262. ACM, October 2019.

[10] A. Banerjee, B. K. Mohanta, S. S. Panda, D. Jena, and S. Sobhanayak. A Secure IoT-Fog Enabled Smart Decision Making system using Machine Learning for Intensive Care unit. In *Proc. of the 2020 International Conference on Artificial Intelligence and Signal Processing (AISP'20), Amaravati, India*, pages 2–7. IEEE, April 2020.

[11] R. Bosri, A. R. Uzzal, A. Al Omar, M. Z. A. Bhuiyan, and M. S. Rahman. HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices. In *Proc. of the 2020 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'20), Toronto, Ontario, Canada*, pages 376–381. IEEE, July 2020.

[12] J. Bowles, J. Mendoza-Santana, and T. Webber. Interacting with Next-Generation Smart Patient-Centric Healthcare Systems. In *Proc. of the 28th ACM Conference on User Modeling, Adaptation and Personalization (UMAP'20), Genoa, Italy*, pages 191–192, Genoa, Italy, July 2020. ACM.

[13] F. Casino, T. K. Dasaklis, and C. Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36:55–81, November 2019.

[14] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone. An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal*, 2(6):515–526, March 2015.

[15] I.-R. Chen, J. Guo, D.-C. Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You. Trust-Based Service Management for Mobile Cloud IoT Systems. *IEEE Transactions on Network and Service Management*, 16(1):246–263, 2019.

[16] Y. Ding and H. Sato. Derepo: A Distributed Privacy-Preserving Data Repository with Decentralized Access Control for Smart Health. In *Proc. of the 7th IEEE International Conference on Cyber Security and Cloud Computing and the 6th IEEE International Conference on Edge Computing and Scalable Cloud (CSCloud-EdgeCom'20), New York, New York, USA*, pages 29–35. IEEE, August 2020.

[17] B. S. Egala, S. Priyanka, and A. K. Pradhan. SHPI: Smart Healthcare System for Patients in ICU using IoT. In *Proc. of the 2019 International Symposium on Advanced Networks and Telecommunication Systems (ANTS'19), Goa, India*, pages 1–6. IEEE, December 2019.

[18] Y. Gao, H. Lin, Y. Chen, and Y. Liu. Blockchain and SGX-enabled Edge Computing Empowered Secure IoMT Data Analysis. *IEEE Internet of Things Journal*, 8(21):15785–15795, January 2021.

[19] T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen. Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction. In *Proc. of the 2015 IEEE International Conference on Computer and Information Technology (CIT'15), Liverpool, England, UK*, pages 356–363. IEEE, October 2015.

[20] H. Guo, W. Li, E. Meamari, C. C. Shen, and M. Nejad. Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution. In *Proc. of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC'20), Toronto, Ontario, Canada*, pages 1–5. IEEE, 2020.

[21] X. Hei, X. Yin, Y. Wang, J. Ren, and L. Zhu. A trusted feature aggregator federated learning for distributed malicious attack detection. *Computers & Security*, 99(102033), 2020.

[22] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage. Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. In *Proc. of the 2020 IEEE Global Communications Conference (GLOBECOM'20), Taipei, Taiwan*, pages 1–6. IEEE, May 2020.

[23] X. Huang, R. Yu, J. Kang, and Y. Zhang. Distributed reputation management for secure and efcient vehicular edge computing and networks. *IEEE Access*, 5:25408–25420, November 2017.

[24] S. Ismail, R. Almayouf, S. Chehab, S. Alghamdi, A. Almutairi, B. Alasmari, and R. Altherwy. Edge IoT-cloud Framework based on Blockchain. In *Proc. of the 2nd International Conference on Computer and Information Sciences (ICCIS'20), Sakaka, Saudi Arabia*, pages 1–7. IEEE, October 2020.

[25] D. Krishnaswamy, P. Jundre, A. Bhatnagar, K. Chauhan, D. Bhamrah, S. Srivastava, S. Thakur, S. Bisht, S. Narula, and K. Jangid. A microservices-based virtualized blockchain framework for emerging 5G data networks. In *Proc. of the 2019 IEEE Globecom Workshops (GC Wkshps'19), Waikola, Hawaii, USA*, pages 1–6. IEEE, December 2019.

[26] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access*, 8:118433–118471, June 2020.

[27] X. Li, X. Huang, C. Li, R. Yu, and L. Shu. EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access*, 7:22011–22025, February 2019.

[28] P. Lin, Q. Song, F. R. Yu, D. Wang, and L. Guo. Task Offloading for Wireless VR-Enabled Medical Treatment with Blockchain Security Using Collective Reinforcement Learning. *IEEE Internet of Things Journal*, 4662:1–13, January 2021.

[29] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88(101653), 2020.

[30] A. Murko and S. L. R. Vrhovec. Bitcoin adoption. In *Proc. of the 3rd Central European Cybersecurity Conference (CECC'19), Munich, Germany*, pages 1–6, New York, NY, USA, 2019. ACM.

[31] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne. Blockchain and Edge Computing for Decentralized EMRs Sharing in Federated Healthcare. In *Proc. of the 2020 IEEE Global Communications Conference (GLOBECOM'20), Taipei, Taiwan*, pages 1–6. IEEE, December 2020.

[32] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne. BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. *IEEE Internet of Things Journal*, 8(14):11743–11757, July 2021.

[33] J. Pan, S. Ding, D. Wu, S. Yang, and J. Yang. Exploring behavioural intentions toward smart healthcare services among medical practitioners: a technology transfer perspective. *International Journal of Production Research*, 57(18):5801–5820, November 2018.

[34] S. Parvin, S. F. Nimmy, S. Venkatraman, S. Abed, and A. Gawanmeh. A KNN Approach for Blockchain Based Electronic Health Record Analysis. In *Proc. of the 27th International Conference on Systems Engineering (ICSEng'20), Las Vegas, Nevada, USA*, pages 455–464. Springer, Cham, January 2021.

[35] P. Patil, M. Sangeetha, and V. Bhaskar. Blockchain for IoT Access Control, Security and Privacy: A Review. *Wireless Personal Communications*, 117(3):1815–1834, 2021.

[36] L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos. SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits. *IEEE Transactions on Consumer Electronics*, 67(1):20–29, February 2021.

[37] A. Rahman, E. Hassanain, M. Rashid, S. J. Barnes, and M. Shamim Hossain. Spatial Blockchain-Based Secure Mass Screening Framework for Children with Dyslexia. *IEEE Access*, 6:61876–61885, October 2018.

[38] A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. *IEEE Access*, 6:72469–72478, November 2018.

[39] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access*, 8:205071–205087, November 2020.

[40] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 78(2):641–658, January 2018.

[41] A. Raj and S. D. Shetty. IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey. *Wireless Personal Communications*, 2021.

[42] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 79(15-16):9711–9733, June 2020.

[43] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88:173–190, November 2018.

[44] M. Shamim Hossain, G. Muhammad, and N. Guizani. Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. *IEEE Network*, 34(4):126–132, July 2020.

[45] A. Sharma, S. Kaur, and M. Singh. A comprehensive review on blockchain and Internet of Things in healthcare. *Transactions on Emerging Telecommunications Technologies*, 32(10):1–53, 2021.

[46] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho. BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems. *IEEE Access*, 7:118556–118580, 2019.

[47] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, 97(101966), 2020.

[48] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5):637–646, October 2016.

[49] R. Soni and G. Kumar. A Review on Blockchain Urgency in the Internet of Things in Healthcare. In *Proc.of the 2019 International Conference on Intelligent Sustainable Systems (ICISS'19), Palladam, India*, pages 578–583. IEEE, February 2019.

[50] H. Tan, P. Kim, and I. Chung. Practical homomorphic authentication in cloud-assisted vanets with blockchain-based healthcare monitoring for pandemic control. *Electronics*, 9(10):1–21, October 2020.

[51] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir. The security of big data in fog-enabled iot applications including blockchain: A survey. *Sensors*, 19(8):1–33, April 2019.

[52] G. L. Tortorella, F. S. Fogliatto, A. Mac Cawley Vergara, R. Vassolo, and R. Sawhney. Healthcare 4.0: trends, challenges and research directions. *Production Planning and Control*, 31(15):1245–1260, December 2019.

[53] G. Tripathi, M. A. Ahad, and S. Paiva. Sms: A secure healthcare model for smart cities. *Electronics (Switzerland)*, 9(7):1–18, July 2020.

[54] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian. A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring. In *Proc. of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'19), Barcelona, Spain*, pages 207–214. IEEE, October 2019.

[55] M. Umair, M. A. Cheema, O. Cheema, H. Li, and H. Lu. Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT. *Indian Journal of Computer Science*, 21(11), June 2021.

[56] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang. Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment. *Journal of Systems Architecture*, 115(January), May 2021.

[57] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani. MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access*, 5:1–10, July 2017.

[58] W. Yaïci, K. Krishnamurthy, E. Entchev, and M. Longo. Recent Advances in Internet of Things (IoT) Infrastructures for Building Energy Systems: A Review. *Sensors*, 21(6):2152, March 2021.

[59] Q. Yang, Q. Liu, and H. Lv. A decentralized system for medical data management via blockchain. *Journal of Internet Technology*, 21(5):1335–1345, September 2020.

[60] Y. Yin, Y. Zeng, X. Chen, and Y. Fan. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, 1:3–13, March 2016.

[61] Y. Zhen and H. Liu. Distributed privacy protection strategy for MEC enhanced wireless body area networks. *Digital Communications and Networks*, 6(2):229–237, May 2020.

[62] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. *Journal of Medical Internet Research*, 21(6), June 2019.

[63] H. D. Zubaydi, Y.-W. Chong, G.-S. Ham, K.-M. Ko, and S.-C. Joo. A Decentralized Consensus Secure and Authentication Framework for Blockchain-Based Healthcare Application. In *Proc. of the 2018 International Conference on Ubiquitous Information Technologies and Applications (CUTE'18), Kuala Lumpre, Malaysia*, pages 550–556. Springer, Singapore, December 2019.

Author Biography

Žiga Kodrič is a Master's degree student at Faculty of Criminal Justice and Security, University of Maribor. His research intrests are cybersecurity, cloud computing and crypto currencies.

Simon Vrhovec is Associate Professor at the University of Maribor, Slovenia. He received his PhD degree in Computer and Information Science from the University of Ljubljana (Slovenia) in 2015. He is editorial board member of the Journal of Cyber Security and Mobility, Frontiers in Computer Science, EUREKA: Social and Humanities, and International Journal of Cyber Forensics and Advanced Threat Investigations (CFATI). He serves or has served as guest editor for IEEE Security & Privacy, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and Journal of Universal Computer Science (J.UCS). He is in the steering committee of the European Interdisciplinary Cybersecurity Conference (EICC) since 2019, and co-chaired the Central European Cybersecurity Conference (CECC) in 2018 and 2019. His main research interests are in human factors in cybersecurity, secure software development, agile methods, and change management.

Luka Jelovčan is a Master's degree student at Faculty of Criminal Justice and Security, University of Maribor. His research interests are in human factors in cybersecurity, corporate risk management and enterprise information systems management.