J Inf Process Syst, Vol.19, No.1, pp.118~129, February 2023
https://doi.org/10.3745/JIPS.03.0182

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Recent Trends on Smart City Security: A Comprehensive Overview

Hyuk-Jun Kwon[1], Mikail Mohammed Salim[2], and Jong Hyuk Park[2,*]

Abstract

The expansion of smart cities drives the growth of data generated from sensor devices, benefitting citizens with enhanced governance, intelligent decision-making, optimized and sustainable management of available resources. The exposure of user data during its collection from sensors, storage in databases, and processing by artificial intelligence-based solutions presents significant security and privacy challenges. In this paper, we investigate the various threats and attacks affecting the growth of future smart cities and discuss the available countermeasures using artificial intelligence and blockchain-based solutions. Open challenges in existing literature due to the lack of countermeasures against quantum-inspired attacks are discussed, focusing on post-quantum security solutions for resource-constrained sensor devices. Additionally, we discuss future research and challenges for the growing smart city environment and suggest possible solutions.

Keywords

Blockchain, Security, Post Quantum, Privacy, Smart City

1. Introduction

The increasing human migration from rural to urban areas has rapidly increased data transmission from wired and wireless sensor devices used for traffic monitoring, lighting, parking, waste, water, and energy management [1-3]. The sustainability and growth of each smart city require dependence on the optimized implementation of available resources and intelligent services provided to each citizen. Artificial intelligence (AI) has been deeply explored to improve decision-making for collaborative services using big data collected from citizens. The collaboration between intelligent applications, such as energy management with smart building and smart homes, collectively enables the government to monitor energy distribution throughout the city, manage its storage, and fair allocation to all citizens during peak hours [4-6]. Smart factory and logistics collectively enable organizations to control distribution channels of goods and services and prevent unavailability. The quality-of-experience is directly correlated with the quality-of-service, where the continual service of intelligent applications is required for effective governance, innovative data management, and inter-smart application sharing of data. However, the reliability of smart cities relies on the security of data and devices to prevent user privacy and confidentiality violation.

Manuscript received October 25, 2022; first revision November 22, 2022; second revision December 14, 2022; accepted January 6, 2023.

* **Corresponding Author:** Jong Hyuk Park (jhpark1@seoultech.ac.kr)
[1] Dept. of Economics & Finance, Soonchunhyang University, Asan, Korea (gloryever@gmail.com)
[2] Dept. of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea (mikail@seoultech.ac.kr, jhpark1@seoultech.ac.kr)

Cyber-attacks such as distributed denial-of-service (DDoS), ransomware, malware, replay, and delay attacks are some common forms of attacks launched on the smart city environment. Various cloud, fog, and edge-based attacks present unique challenges to securing smart city networks. Poor encryption of sensor devices due to weak computation and low battery prevents direct implementation of computing-intensive security solutions. Furthermore, the transition of networks from classical systems to quantum mechanics-inspired networks exposes the network to several open vulnerabilities threatening data security, integrity, confidentiality, and user privacy.

The existing literature studies focus on limited technologies for securing smart city networks resulting in an obsolete proposal for the next-generation quantum computing-supported smart city environment. In the future, attack vectors are expected to increase from quantum-based attacks, threatening existing blockchain and AI-based security solutions in data management, storage, and transmission. Addressing the lack of investigation of security solutions inspired by quantum science, this paper proposes a new and holistic study of solutions using blockchain and AI. Furthermore, we discuss and present post-quantum-based solutions using lattice cryptography present in existing studies to defend against quantum-era attacks. The contributions of our research are as follows:

- We discuss the recent state-of-the-arts and surveys conducted on smart city security and cyber-threats.
- An overview of existing cyber-attacks and post-quantum attacks executed on a smart city environment.
- We present the technologies essential for the security of the Smart City environment and include studies for managing post-quantum-based attacks.

The remainder of this paper is as follows. Section 2 discusses the existing literature on smart city security and privacy-based studies. Section 3 outlines the attacks and threats facing the next-generation smart city network. Section 4 presents the countermeasures and security solutions for each attack and threat proposed in existing studies. Section 5 presents future research and challenges, and finally, in Section 6, we conclude our paper.

2. Related Works

The smart city environment has evolved to include several technologies enabling efficient energy management, optimized task collection, reduced financial costs, and improved quality of service to its citizens. The merits of a smart city have introduced new cyber-attack vectors threatening data confidentiality, data integrity, device availability, and user privacy. In this section, we discuss existing literature surveys addressing security and privacy threats and solutions for the smart city environment. A summary of comparison between the existing literature and the proposed survey paper are illustrated in Table 1 [7-13].

An in-depth study of security for smart city applications including smart grid, smart transportation, smart building, and smart healthcare is presented by Ma et al. [7]. The research discusses various solutions to detect, prevent and mitigate the effects of fraud detection, malware analysis, and ransomware identification, however, the study limits itself to solutions using deep learning. The limitations of this paper restrict users to studying only a singular approach as a solution against a wide variety of attack

Table 1. Comparison of proposed survey and existing studies

Study	Year	Security and privacy	Blockchain	Artificial intelligence	Post quantum solutions
Ma et al. [7]	2021	Yes	No	Yes	No
Ismagilova et al. [8]	2020	Yes	Yes	No	No
Al-Turjman et al. [9]	2019	Yes	Yes	Yes	No
Bhushan et al. [10]	2020	No	No	No	No
Khan et al. [11]	2020	No	No	No	No
Singh et al. [12]	2020	Yes	Yes	Yes	No
Magaia et al. [13]	2020	Yes	No	Yes	No
Proposed survey	-	Yes	Yes	Yes	Yes

vectors. Ismagilova et al. [8] focused on security and privacy for smart city environment focusing on connected mobile devices and smart city applications, which include healthcare, energy systems, and protocols. Security challenges are discussed from the perspective of the smart citizens such as data security, integrity, confidentiality, and privacy. However, the study presents very little detail of counter measures against cyber-attacks and does not include Quantum based attacks on the smart city environment. Al-Turjman et al. [9] focused on security and privacy attacks on information security of smart city applications and presents various countermeasures against attacks. Future research challenges discuss measures to improve the performance of smart cities. The study presents blockchain, AI, and cryptography-based solutions. However, the study does not address future quantum computing based attacks that are nullify existing security protocols. Moreover, the proposed architecture is not presented in detail and does not discuss modern attack vectors and solutions. Bhushan et al. [10] presented a review of the blockchain based solutions focusing on architecture, trends and future research directions for resolving security challenges in the smart city environment. The focus of the paper is primarily on implementing blockchain for resolving security challenges in intelligent applications such as transportation, healthcare, financial systems, transportation, energy, and supply chain management. The study lacks a detailed description of security threats on the smart city environment and focuses on only a single technology for resolving smart city security challenges. The study on edge-enabled in smart city is presented by Khan et al. [11] focusing on computing resources, latency in task execution, and mobility support for devices. Intelligent applications such as autonomous vehicle crash reporting system, environment disaster identification, vehicle parking, and smart homes are discussed from the perspective of improving quality of services by bringing intelligence to the edge layer. The introduction of edge intelligence for future smart cities resents a new set of cyber-attacks which are not discussed in this study. The lack of study of countermeasures against attacks further restricts the study from a presenting a holistic approach to defending and maintaining an edge intelligence based smart city.

The convergence of two technologies, blockchain and AI presents a unique solution for ensuring the security and sustainability of smart city environments. Singh et al. [12] presented a detailed study on the deployment of combined blockchain and AI based approach for securing the smart transportation application in smart cities. Furthermore, the study proposes the need for standardization of data management and consensus algorithms in blockchain to reduce challenges in implementation of the decentralized technology. The threat to smart cities from quantum computing-based attacks are not discussed in the study, thereby resulting in a lack of post quantum-based solutions for securing future

smart cities. Magaia et al. [13] presented a survey on the security of the Industrial Internet of Things (IIoT) in a smart city environment. The study focuses on the applications of deep learning technology, including reinforcement learning and convolutional neural networks, and recurrent neural networks to secure IIoT environments. A five-layer IIoT architecture illustrates the general design of IIoT networks, and an in-depth study of its security challenges include lack of standardized hardware, physical device security, sensor device operating system isolation, and authentication. The limitations of the study are its restriction to the study and comparison of only deep learning models for securing the IIoT environment. The growth of new attack vectors requires focus on other technologies including blockchain and post-quantum solutions such as cryptography.

3. Cyber-Attacks on Smart City Method

The heterogeneous and complex nature of smart cities make it prone to critical cyber threats. As discussed in the above sections, smart city encloses several applications such as smart transportation, smart healthcare system, smart infrastructure, smart home, smart industry, and so on. A cyber-attack on these applications may result to serious damages both economically and can go to the extent of threatening human lives as well. Based on the study conducted by Cynerio and Ponemon companies [14], over 50% of cyber-attacks on smart healthcare system are found to be indirectly linked for increased mortality rates. Moreover, Kaspersky company has detected more than 100 million cyber-attacks on IoT devices in smart homes during the first half of 2019 [15]. Based on the report, 39% of the attacks were executed using Mirai malware. Another example on the vulnerabilities of smart cities, San Francisco Municipal Transportation Agency (SFMTA) went under critical cyber-attack in 2016. The attack manipulated the agency's network to open the entry gates free of charge. Although this attack was controlled and only resulted in financial losses, it caused worrisome both for the agency and security executives about their train operation system and traffic signals. If an attacker could easily control their entry doors, it is highly possible using the same method and through the same network, attacked may control a more critical system that can affect human lives.

In this era of IoT devices, cyber-attacks and malware are becoming cyber-terror due to its critical impacts on users and governments [16,17]. In this section, we depict different types of cyber-attacks on smart cities and their impact. Moreover, we discuss various countermeasures that security requirements that should be deployed to create a safer and secure smart city environment.

Ransomware: Giving the fact that smart cities are mainly built using IoT devices and communication networks, ransomware attacks are the most common cyber threats on smart cities. While a ransomware cannot affect all the component of smart city at once, it is still a critical attack on smart city applications. As illustrated in Fig. 1, Bajpai and Enbody [18] divided the ransomware attacks objectives on smart cities into four main tiers, Denial-of-Data, where attackers maintain data as hostage until a ransom is received. Denial-of-service is achieved threatening several applications until demands such as financial incentives are not satisfied. Denial of Access prevents citizens in a smart city from accessing smart applications such as their personal smart home security protocols. Finally, Denial of Privacy aims at acquiring user personal information such as credit card information, medical records, and contact information until a ransom is not received.

Although ransomware attacks mainly target large companies or individuals, they can be critical for smart cities. In the study of Hamid et al. [19], it was depicted that 64% of cyber-attacks on smart networks and industrial control system in smart cities were executed through a ransomware. Moreover, 17% of data breach in smart healthcare system were due to ransomware attacks as well. Large number of cyber-attacks and cyber terror on critical smart cities' applications such as transportation systems, healthcare, networks, and e-Government are due to ransomwares. Thus, securing smart city applications against ransomware is an urgent step to be executed before any further development on smart cities.

Zero-day attack: Zero-day attacks are one of the main security challenges on smart cities. Zero-day attacks are critical cyber threats as they are executed using undiscovered system vulnerabilities, thus, the attacks comes unexpectedly and the deployed firewalls or antivirus software cannot detect it, resulting in longer time for discovery as described by Bilge and Dumitras [20] were the authors studied various zero-day attacks from 2008 to 2011. The research founds that the median time to discover the attack is between 8 to 10 months. Attackers often try to find vulnerabilities in wildly used software such as Microsoft Office to grant access to as many users as possible. Zero-day attacks menace smart city security since they are hard to detect. It can lead to critical data breach and private information leakage from sensitive applications such as smart healthcare and smart government systems. Fig. 1 outlines the motivation for zero-day attacks in a smart city environment, including a smart city's data collection, storage, and management schemes. Security breaches aim at Data breaches to compromise data, steal confidential data affecting data privacy, and modify stored affecting data integrity and compromising the performance of smart city applications.

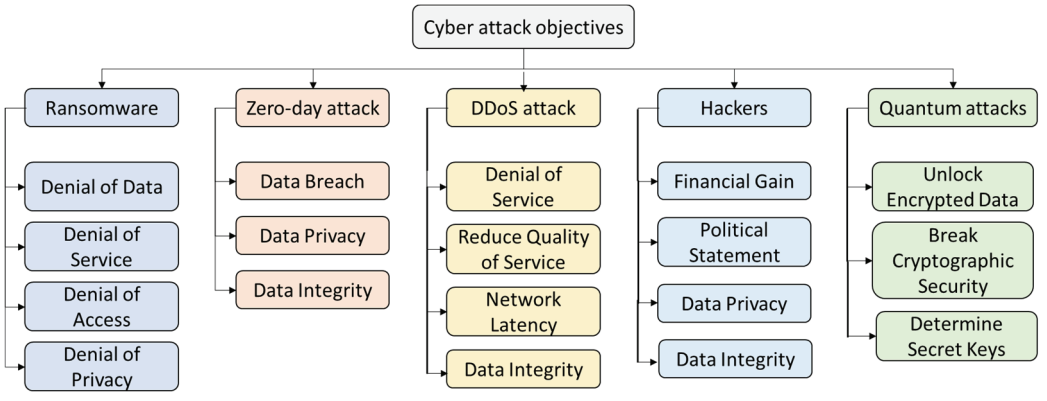

Fig. 1. Cyberattack objectives in the smart city environment.

DDoS Attack: Network systems are the most vulnerable applications in smart cities to DDoS attacks. DDoS attacks are one of the oldest yet most critical cyber-attacks capable of preventing the availability of the targeted server. Thus, authenticated devices and users would loss the access to the desirable service. In case of companies and smart manufacturing, this would result in large-scale disruption in a production line. However, DDoS attacks may lead to serious damages, including human lives in more latency-intolerant applications such as smart healthcare and smart transportation. Fig. 1 outlines the cyber-attack motivations using DDoS attacks where the attacker's primary objective is to disable the target application from providing service to local smart city citizens. Smart healthcare, transportation, and energy are

frequent targets of DDoS attacks. The cyberattack floods server with several request packets resulting in increased network latency and reduced quality of service. Furthermore, upon failing to respond to request packets, a server is exposed to data manipulation and theft affecting data integrity.

Hackers: Besides the well-known attacks discussed above, hackers can still initialize personalized attacks of smart city applications. For example, a personalized cyber-attack launched in 2016 on MedStar hospital chain in Los Angeles has reportedly paralyzed the and system leading to severe surgery delays. This type of attack is possible due to the several vulnerabilities in IoT devices such as medical wearable devices and the weak security measurements in the network systems. The motivation of a hacking attack, as illustrated in Fig. 1, aims at achieving financial gains by holding critical data such as smart healthcare breached data as ransom. Patient data stolen is sold to insurance companies for marketing campaigns resulting in breach of data privacy. Tampered data in smart energy applications leads to data integrity concerns as it impacts all energy distribution algorithms for the entire smart city environment. Lastly, hackers aim to deface prominent applications frequented by citizens to voice their political opinions and get mass attention to their agenda.

Quantum-based attacks: Classical computing using RSA (Rivest-Shamir-Adleman) encryption successfully secures blockchain blocks using digital signatures against attacks relying on mathematical complexity. However, quantum computers with higher computational power are known to break RSA, AES, and elliptic curve cryptography-based security methods. Shor's algorithm, published in 1994, uses an input length as a polynomial to break classical security methods. The algorithm transforms the Factoring problem into a period-finding problem that breaks AES security when solved in polynomial time. Another quantum attack using Grover's algorithm breaks blockchain encryption using two approaches. The first method modifies the nonce value during the block creation, thus affecting the mainchain integrity. Subsequent block creations use modified nonce values, reducing the security of blockchain networks. The second approach by Grover's algorithm identifies hash collisions and then proceeds to alter block data without affecting the integrity of the entire blockchain network. As shown in Fig. 1, the primary objective of an attacker using the vast computing power of quantum systems is to break existing cryptographic security protocols by decrypting private and public keys. Furthermore, loss of control over individual secret keys enables attackers to access confidential information, rendering secret key-based security protocols as weak security measures. Critical data shared, such as military data, are exposed to attackers using vast computing power to break decryption keys and convert ciphertext to plaintext.

4. Existing Solutions

Several research studies have investigated multiple technologies as potential solutions to cyber threats on smart city's environment. Enhancing the security of the smart city and its applications is the most advisable remedy as it can prevent current and future cyber-attacks. To this end, the most studied technologies are blockchain, AI, machine learning (ML), and post-quantum cryptography to secure smart cities. In this section, we discuss the technologies mentioned above and explain how they can be deployed to improve the security measurements of smart city and detect cyber-attacks.

Blockchain: In recent studies and real-world applications, blockchain has been used as a secure and private infrastructure for smart cities. This is generally due to the fast development of blockchain and the amount of interest it gained during the recent years. Currently, blockchain is used in several sectors including data management, smart energy, smart education, smart transportation, smart healthcare, and so on. Blockchain is capable of bringing the desired privacy and required security measurement to smart city. We can divide this into several tiers: authentication, data verification, data validation, and access control. Since blockchain is a distributed ledger operating in a peer-to-peer mechanism and illuminating by those centralized authorities, ensuring the privacy and security of smart cities is possible. A blockchain network in a smart city application is capable of verifying the users, grating access control to authenticated users only, validating the source of data, recording transactions, verifying the validity of data, and communicated information, all while keeping the transparency, security, and anonymity of the network, granting by that the security and privacy levels required.

Artificial intelligent and machine learning: AI and ML can be used both as a mitigation method and prevention method for smart city security. AI has been investigated to detect ongoing attacks and prevent future ones based on the pattern similarity of attacks. Moreover, other AI categories such as deep learning and natural language processing are also used as a proactive and predictive security methods. Xin et al. [21] explained that ML for cyber security can be depicted into four main phases: first extracting the features, second selecting the appropriate ML algorithm, third training the model, and finally classification and prediction phase. AI techniques applied on cyber-security can be deployed to increase network situation awareness, monitor dangerous behavior in the system both from users and system managers, detect abnormal traffic generated by malicious users, and predict future attacks based on the current network status and the trained models. AI is an essential technology in smart city's development, and it is fundamental for its security.

Post-quantum cryptography: With the fast development of quantum information technology (QIT), quantum computers will soon be available to classical users. Quantum computers are capable of solving complex mathematical problems exponentially faster than today's most powerful computers. And since today's cryptography mainly relies on the hardness of mathematical problems such as prime number factorization problem, a quantum computer could theoretically break it in few seconds, which create a critical threat to the current security system used by smart cities. Moreover, even blockchain could not resist a quantum attack, thus, there is an urgent need to secure future smart cities using post-quantum cryptography methods to be ready for the quantum era and enhance the privacy and security of smart city users.

Blockchain technology secures data management and storage for smart cities. Resistance to quantum attacks requires designing post-quantum solutions for securing the smart city environment. Thus, a post-quantum lattice-based cryptography is recommended due to its high resistance to elliptic curve cryptography-based attacks. A one-time linkable ring signature based on lattice cryptography was proposed in a study by Alberto Torres et al. [22], where several digital signatures are verified using a common signatory. A second lattice cryptography-based signature scheme proposed by Gao et al. [23] implements stochastic values to design secret keys. A preimage sampling algorithm first securely signs the message and finally applies a digital signature to hide the relationship between the original message and its initial signature.

5. Future Research and Challenges

In this paper, we described several security threats to the smart city environment based on varying attack vectors and discussed their associated defense strategies, models, methods, architectures, and frameworks. However, open issues and challenges affect the security and privacy of smart cities. In this section, we discuss the various open research challenges to help direct future research directions.

IoT device limitations: Existing IoT devices are restricted with limited computation capabilities, battery capacity, and low data storage availability. Therefore, it is not possible to implement complex and secure security protocols natively on IoT devices. In a smart city environment, the weakness of IoT devices presents an exploitable opportunity for cyber-attackers to comprise network security. For a native security protocol that is locally operated on devices, a lightweight security system is essential and thus presents itself as a promising area for future security research direction. A lightweight authentication protocol presented in [24] uses a hardware-oriented authentication protocol based on device signatures generated using voltage over scaling to deploy lightweight security protocols for resource-constrained IoT devices. RFID tags and smart cards are extensively used in smart cities in factories, logistics, and manufacturing systems. As discussed in [25], they require a lightweight cryptography-based algorithm to ensure data security, privacy, and availability. The study presented 57 varying algorithms, submitted as part of a contest for IoT device security. Traditional cryptography-based algorithms require powerful computation systems and thus for IoT devices, research in short encryption keys is implemented in resource-constrained environments.

Cyber security: The massive growth of IoT devices in smart cities presents serious security vulnerabilities on edge computing systems. DDoS attacks prevent real-time service-based operations that negatively affect critical smart city-based intelligent applications such as healthcare, transportation, and logistics. The study proposed in [26] presents lightweight deep learning-based solutions for DDoS attack detection with low processing overhead and the ability to address various attack vectors that are suitable for edge computing devices due to their comparatively fewer available resources than with the cloud. Furthermore, the concentration of DDoS attacks on edge devices requires extensive research that addresses various attack vectors and is not limited to a few attack approaches. Several effective authentications and reliable access control challenges exist for edge computing-enabled smart cities and require a low-complexity solution for quick identification between two nodes. A lightweight solution presented in [27] provides a secure authentication protocol for mobile edge computing and wireless body area networks providing low computation, communication, and storage costs. Lightweight solutions for edge nodes ensure low energy consumption, as presented in [28], ensure reliability and reduced service latency. As the amount of data grows and devices are added regularly in smart cities, future research should focus on energy-efficient solutions that provide a combination of power-efficient and efficient security protocols.

Data storage: Open research challenges for the growing data in smart city systems require research focus on securing the data collection process, its sharing protocols, and storage management systems. Data confidentiality, non-repudiation, security, and privacy are the key areas of consideration for future research directions. The study in [29] describes that none of the existing literature focusing on edge-IoT addresses all four key areas of consideration and therefore presents a major research direction. Furthermore, cloud-based security systems are not suitable for protecting data stored at edge nodes due to the vast difference in security, computation, and data storage protocols. Moreover, edge nodes' heterogeneity and distributed nature present a challenge for cloud-based security mechanisms to ensure

efficiency and maintain user privacy. The limitation of computation power of edge nodes requires focus on computation and lightweight operational solutions for secure data processing and ensuring the correctness of data collected for analytical purposes. Data redundancy presents the challenge of maintaining edge nodes' computational and storage efficiency due to similar data collected by different nodes for a single mobile user in a distributed environment. Future research directions include designing secure, mobility-friendly caching and resource management methods for smart cities.

Blockchain based solutions: The security of smart city environment can be improved by introducing blockchain technology for fine-grained access control measures preventing malicious nodes from interacting with benign IoT and edge devices. Future research directions using the decentralized technology include designing a permissioned blockchain for the edge-IoT environment. While SDN-enabled handover authentications for mobile IoT devices are an area for future research direction for smart cities, the study in [30] suggests a hybrid blockchain-enabled SDN system presents a research opportunity in the field of distributed and security architectures. A blockchain-based secure SDN architecture at the edge is secured from the single point of failure vulnerability of centralized SDN-based systems. The SDN monitors the network for anomalous activity and the blockchain technology ensures security at the edge layer. Non-repudiation and trust management can be secured using blockchain-based edge-IoT smart city environments, presenting another future area of research.

6. Conclusion

The fast and continuous development of IoT and communication networks led to an exponential growth in smart cities. Currently, numerous advanced countries are adopting smart cities as current and future projects with an annual budget over billions of dollars. Smart citizen are the main users of smart cities applications such as smart homes, smart hospitals, and smart transportation. However, the security and privacy issues are arising with the continuous growth and heterogeneity of IoT devices. Cyber-criminals are targeting these vulnerabilities to attack smart city system. Moreover, the developments of quantum computers create a novel security issue as it threatens the current encryption techniques and protocols. To this end, in this paper, we investigate the various threats and attacks affecting the growth of future smart cities and discuss the available countermeasures using AI and blockchain-based solutions. Open challenges in existing literature due to the lack of countermeasures against quantum-inspired attacks are discussed, focusing on post-quantum security solutions for resource-constrained sensor devices. Additionally, we discuss future research and challenges for the growing smart city environment and suggest possible solutions.

Acknowledgement

This work was supported by the Soonchunhyang University Research Fund (No. 10220011).

References

[1] S. K. Singh, C. Lee, and J. H. Park, “CoVAC: a P2P smart contract-based intelligent smart city architecture for vaccine manufacturing,” *Computers & Industrial Engineering*, vol. 166, article no. 107967, 2022. https://doi.org/10.1016/j.cie.2022.107967

[2] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications*, vol. 57, article no. 102686, 2021. https://doi.org/10.1016/j.jisa.2020.102686

[3] S. K. Singh and J. H. Park, "TaLWaR: blockchain-based trust management scheme for smart enterprises with augmented intelligence," *IEEE Transactions on Industrial Informatics*, vol. 19, n. 1, pp. 626-634, 2023.

[4] S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-enabled secure framework for energy-efficient smart parking in sustainable city environment," *Sustainable Cities and Society*, vol. 76, article no. 103364, 2022. https://doi.org/10.1016/j.scs.2021.103364

[5] A. E. Azzaoui, S. K. Singh, and J. H. Park, "SNS big data analysis framework for COVID-19 outbreak prediction in smart healthy city," *Sustainable Cities and Society*, vol. 71, article no. 102993, 2021. https://doi.org/10.1016/j.scs.2021.102993

[6] S. K. Singh, A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "DeepBlockScheme: a deep learning-based blockchain driven scheme for secure smart city," *Human-centric Computing and Information Sciences*, vol. 11, article no. 12, 2021. https://doi.org/10.22967/HCIS.2021.11.012

[7] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, vol. 7, pp. 7999-8012, 2021.

[8] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework," *Information Systems Frontiers*, vol. 24, pp. 393-414, 2022.

[9] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, article no. e3677, 2022. https://doi.org/10.1002/ett.3677

[10] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for smart cities: a review of architectures, integration trends and future research directions," *Sustainable Cities and Society*, vol. 61, article no. 102360, 2020. https://doi.org/10.1016/j.scs.2020.102360

[11] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: a comprehensive survey," *IEEE Internet of Things*, vol. 7, no. 10, pp. 10200-10232, 2020.

[12] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I. H. Ra. "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, article no. 102364, 2020. https://doi.org/10.1016/j.scs.2020.102364

[13] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. L. Neto, and V. H. C. Albuquerque, "Industrial Internet-of-Things security enhanced with deep learning approaches for smart cities," *IEEE Internet of Things*, vol. 8, no. 8, pp. 6393-6405, 2021.

[14] CISION PR Newswire, "Cynerio and Ponemon Study Finds Frequent Cyber Attacks and Insufficient Accountability in Healthcare Adversely Impact Patient Care," 2022 [Online]. Available: https://www.prnewswire.com/news-releases/cynerio-and-ponemon-study-finds-frequent-cyber-attacks-and-insufficient-accountability-in-healthcare-adversely-impact-patient-care-301604539.html

[15] Kaspersky, "IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019," 2019 [Online]. Available: https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019.

[16] Y. Kim, H. Lee, and D. Hwang, "IoT malware detection and family classification using entropy time series data extraction and recurrent neural networks," *KIPS Transactions on Software and Data Engineering*, vol. 11, no. 5, pp. 197-202, 2022.

[17] R. Yumlembam, B. Issac, S. M. Jacob, and L. Yang, "IoT-based Android malware detection using graph neural network with adversarial defense," *IEEE Internet of Things*, 2022. https://doi.org/10.1109/JIOT.2022.3188583

[18] P. Bajpai and R. Enbody, "Preparing smart cities for ransomware attacks," in *Proceedings of 2020 3rd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, 2020, pp. 127-133.

[19] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, "Cyber security issues and challenges for smart cities: a survey," in *Proceedings of 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Karachi, Pakistan, 2019, pp. 1-7.

[20] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, NC, 2012, pp. 833-844.

[21] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365-35381, 2018.

[22] W. A. Alberto Torres, R. Steinfeld, A. Sakzad, J. K. Liu, V. Kuchta, N. Bhattacharjee, M. H. Au, and J. Cheng, "Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1. 0)," in *Information Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 558-576.

[23] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205-27213, 2018.

[24] J. Zhang, C. Shen, H. Su, M. T. Arafin, and G. Qu, "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 323-336, 2022.

[25] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177-28193, 2021.

[26] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "LUCID: a practical, lightweight deep learning solution for DDoS attack detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876-889, 2020.

[27] X. Yang, X. Yi, I. Khalil, J. Luo, E. Bertino, S. Nepal, and X. Huang, "Secure and lightweight authentication for mobile-edge computing enabled WBANs," *IEEE Internet of Things*, vol. 19, no. 14, pp. 876-889, 2022.

[28] K. Cao, S. Hu, Y. Shi, A. W. Colombo, S. Karnouskos, and X. Li, "A survey on edge and edge-cloud computing assisted cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7806-7819, 2021.

[29] M. Yahuza, M. Y. I. B. Idris, A. W. N. A. Wahab, A. T. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, "Systematic review on security and privacy requirements in edge computing: state of the art and future research opportunities," *IEEE Access*, vol. 8, pp. 76541-76567, 2020.

[30] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761-1804, 2020.

Hyuk-Jun Kwon **https://orcid.org/0000-0002-0408-9001**

He is a professor of Economics and Finance at Soonchunhyang University, Korea. He received his Ph.D. in Information System from Graduate School of Information at Yonsei University, Korea. He has published many research papers in international journals and conferences and serves as program committee for international conferences and workshop.

Mikail Mohammed Salim **https://orcid.org/0000-0001-7870-9368**

He received his bachelor's in Computer Applications from Garden City College, India in 2011. Currently he is pursuing his Ph.D. degree under the supervision of Prof. Jong Hyuk Park at the UCS Lab, Seoul National University of Science and Technology, Seoul, South Korea.

Jong Hyuk (James J.) Park **https://orcid.org/0000-0003-1831-0309**

He received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December 2002 to July 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co. Ltd., Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology, Korea. Dr. Park has published about 400 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences—MUE, FutureTech, CSA, CUTE, BIC, World IT Congress-Jeju. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) and The Journal of Information Processing Systems (JIPS) by KIPS. He is Associate Editor/Editor of international journals including JoS, JIT, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: IEEE, Springer, Elsevier, John Wiley, MDPI, etc., got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from SeoulTech, 2014, 2020, and 2021. He was listed as one of the World's Top 2% Scientists by Stanford University, 2021. His research interests include IoT, cloud computing, blockchain, quantum information, information security, metaverse, etc.