JOURNAL OF THE AMERICAN INSTITUTE
ISSN: 3066-3776
United States

Data Security in Internet of Things Systems Based on Distributed Blockchain

Vina Ardelia Effendy[1]

Email Correspondent: vinaardelia@unj.ac.id

Keywords:
E-Service Quality, E-Trust, E-Loyalty.

Abstract

The development of digital technology has driven major changes in consumer behavior, especially in the use of e-commerce platforms such as Shopee. This study was conducted to examine the effect of e-service quality and e-trust on e-loyalty with e-satisfaction as an intervening variable on Shopee users in Indonesia. The main objective of this study is to understand how e-service quality and e-trust indirectly affect user satisfaction and loyalty through user satisfaction with the service. The research method used is a quantitative approach with data collection techniques through distributing questionnaires to 130 respondents who are active Shopee users. Data processing was carried out using the Structural Equation Modeling (SEM) method based on Partial Least Squares (PLS). The results of the study show that e-service quality and e-trust have a positive and significant effect on e-satisfaction. Furthermore, e-satisfaction also has a positive effect on e-loyalty. However, e-trust does not have a significant direct effect on e-loyalty, although it has an indirect effect through e-satisfaction. This research provides an important contribution to the understanding of digital consumer behavior and how to build loyalty through improving service quality and trust in e-commerce platforms. These findings are useful for e-commerce companies to design more effective marketing and service strategies.

INTRODUCTION

The development of Internet of Things (IoT) technology has brought about significant transformations in various sectors, from the manufacturing industry to healthcare (Atzori et al., 2010; Gubbi et al., 2013). IoT allows physical devices to communicate with each other and exchange data automatically via the internet network (Perera et al., 2013). However, behind its benefits, IoT systems have major challenges related to security aspects, especially in terms of privacy and integrity of data sent and stored (Jing et al., 2014; Roman et al., 2013). This vulnerability can be exploited by irresponsible parties to carry out cyber attacks such as data theft or system manipulation (Alrawais et al., 2017; Weber, 2010).

The Internet of Things (IoT) is a network ecosystem that connects physical devices to the internet, allowing them to collect and exchange data in real-time without direct human intervention. IoT integrates sensors, software, and communication technologies to create intelligent environments in areas such as homes, industry, healthcare, and transportation. In the past five years, there has been

[1] Universitas Negeri Jakarta, Indonesia, vinaardelia@unj.ac.id

significant progress in the integration of technologies such as artificial intelligence (AI), blockchain, and quantum cryptography to enhance the security and efficiency of IoT systems, especially in industrial or Industrial Internet of Things (IIoT) scenarios. These technologies not only improve operational efficiency but also pave the way for large-scale automation and data-driven decision-making in vital sectors of the modern world (Ali et al., 2025).

In addition, recent developments show that the application of IoT is increasingly widespread, including in remote health monitoring, smart energy management, and smart city management. For example, in the context of healthcare, IoT devices are used to monitor patient conditions in real time, transmit data to doctors, and reduce the need for hospital visits. In the energy sector, smart meters and automated distribution systems facilitate more efficient and sustainable energy use. However, challenges such as interoperability between devices, big data management, and security and privacy remain major concerns in the widespread implementation of IoT. Therefore, current research continues to focus on the application of supporting technologies such as edge computing and AI to address these issues (Ali et al., 2025).

Security issues in IoT are largely due to the centralized system architecture, where a single point of failure can result in the failure of the entire system (Lin & Bergmann, 2016; Wu et al., 2017). In addition, many IoT devices have limitations in terms of computing power and storage capacity, making it difficult to implement complex traditional security mechanisms (Conti et al., 2018; Sicari et al., 2015). Therefore, new approaches are needed that can increase the resilience of IoT systems to attacks, especially those that are able to distribute trust and integrity evenly across the network (Dorri et al., 2017; Reyna et al., 2018).

One technology that offers a potential solution to this problem is blockchain, a decentralized digital record-keeping system that is resistant to manipulation and transparent (Crosby et al., 2016; Nakamoto, 2008). The integration of blockchain into IoT systems enables secure data storage, transaction validation without intermediaries, and high traceability of network activity (Christidis & Devetsikiotis, 2016; Zhang & Wen, 2017). With smart contract and distributed consensus features, blockchain can help strengthen authentication, access control, and data tracking in IoT systems (Dai et al., 2019; S. Li, 2018).

The implementation of blockchain in IoT not only solves security issues but also opens up opportunities for the development of a more autonomous, efficient, and trustworthy system architecture for all stakeholders (Novo, 2018; Salman et al., 2018). Distributed blockchain systems eliminate dependence on third parties in data management, which can indirectly reduce operational costs and increase service speed (Ferrag et al., 2016; Ouaddah et al., 2016). However, challenges still remain, especially in terms of scalability, transaction speed, and adaptation of blockchain technology to the limitations of IoT devices (Conoscenti et al., 2016; J. Li et al., 2017).

The urgency of this research lies in the increasing dependence of society on IoT devices that store and process personal and operational data in real-time. With increasingly complex cybersecurity threats, there needs to be a system design that can guarantee data security from upstream to downstream. Therefore, further exploration of blockchain integration in IoT is important in order to formulate sustainable and adaptive technological solutions to future threats.

Several previous studies have explored the integration of IoT and blockchain, such as research by Dorri et al. (2017) which suggests a lightweight blockchain-based architecture for smart homes (Dorri et al., 2017), and by Reyna et al. (2018) which discusses the potential and challenges of the synergy of these two technologies (Reyna et al., 2018). However, the study is still limited to conceptual introduction and small-scale case studies. The need for a more in-depth analysis of the systemic data security aspects in a distributed blockchain-IoT environment is still an unanswered gap.

The purpose of this study is to analyze and propose a distributed blockchain-based data security system approach in the context of the Internet of Things. This study will evaluate the reliability, effectiveness, and challenges of implementing blockchain technology in ensuring data security in IoT systems, with a focus on authentication, encryption, consensus, and access management mechanisms.

METHOD

This study uses a qualitative approach with a literature review research type, which aims to identify, analyze, and synthesize various scientific findings related to data security in distributed blockchain-based Internet of Things (IoT) systems. Literature studies were chosen because they are in accordance with the needs of exploratory and conceptual research in understanding the security approaches that have been developed and their potential application in complex IoT architectures (J. Li et al., 2017; Snyder, 2019). This study does not involve experiments or primary data collection, but rather focuses on a systematic review of academic publications and relevant scientific sources.

Data sources in this study were obtained from secondary literature in the form of scientific journal articles, conference proceedings, reference books, and technical reports published in the last ten years (2013–2023). The literature used was obtained through leading academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. The inclusion criteria used include publications that focus on IoT security, the application of blockchain technology in distributed systems, and the integration of the two technologies in the context of data protection. Meanwhile, exclusion criteria include non-peer reviewed articles, opinions without scientific basis, and publications with irrelevant technological contexts.

Data collection techniques were carried out through digital document searches using relevant keywords such as "IoT security", "blockchain-based IoT", "distributed security system", and "data protection in IoT". This process was carried out systematically using the snowballing technique to find literature that references each other and strengthens the study base. All collected documents were analyzed to find the main themes related to security challenges and solutions in blockchain-based IoT systems, as well as technology integration patterns that have been proposed or tested previously (Okoli & Schabram, 2015).

The data analysis methods used in this study were content analysis and thematic synthesis. Content analysis was carried out to identify important elements in each literature, such as security architecture frameworks, authentication protocols, encryption schemes, and consensus methods in blockchain that support integration with IoT (Krippendorff, 2018). Next, the analysis results are categorized into key themes and arranged narratively to form a comprehensive understanding of the data security landscape in blockchain-based IoT systems. Thematic synthesis is conducted to draw conclusions and develop evidence-based recommendations on the most effective, efficient, and adaptive security approaches to IoT characteristics.

RESULT AND DISCUSSION

The following is a bibliography table that is the result of a selection of 10 recent and relevant scientific articles discussing the topic of "Data Security in Internet of Things Systems Based on Distributed Blockchain". These articles were selected based on their contributions in identifying security challenges, technical solutions, and future research directions in the integration of blockchain technology to improve data security in IoT systems.

Table 1. Literature Review

No	Title	Author	Research Focus

1	Blockchain Technology for IoT Security and Trust: A Comprehensive SLR	Alzahrani et al. (2024)	Identify key challenges in IoT security and trust and how blockchain technology can address them.
2	Cybersecurity for Blockchain-Based IoT Systems: A Review	Alzahrani et al. (2023)	Highlight challenges in IoT device security, blockchain security, and network integration, and potential solutions for each.
3	Integration of Blockchain and Edge Computing in Internet of Things: A Survey	Xue et al. (2022)	Present a general architecture of blockchain and edge computing integration, as well as the benefits and challenges of such integration.
4	Redactable Blockchain Solutions for IoT: A Review of Mechanisms and Applications	Solanki (2024)	Review redaction mechanisms in blockchain and their applications in IoT to meet data protection requirements.
5	Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques	Zhang et al. (2023)	Propose a multi-level security architecture with an adaptive cluster approach to enhance the security and efficiency of IoT networks.
6	Privacy, Security and Policies: A Review of Problems and Solutions with Blockchain-Based Internet of Things Applications in Manufacturing Industry	Smith et al. (2021)	Identify general trends and the need to further explore data security issues in the convergence of IoT and blockchain in the manufacturing industry.
7	Research on Distributed Blockchain-Based Privacy-Preserving and Data Security Framework in IoT	Tian et al. (2020)	Present a framework that uses the PBFT consensus mechanism to achieve fast and efficient data authentication in IoT systems.
8	Towards Blockchain-based Auditable Storage and Sharing of IoT Data	Shafagh et al. (2017)	Propose a blockchain-based design for distributed access control and data management in IoT, enabling secure and tamper-resistant data sharing.
9	Blockchain Technologies for the Internet of Things: Research Issues and Challenges	Ferrag et al. (2018)	Present a comprehensive survey of blockchain protocols for IoT networks and classify current threat models and solutions.
10	Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions	Kumar et al. (2023)	Provide a holistic evaluation of the application of blockchain technology in securing IoT devices and identify future research directions.

Based on the literature data that has been collected and filtered from ten recent scientific articles on data security in distributed blockchain-based Internet of Things (IoT) systems, a number of important findings were obtained that indicate the direction of development of this technology in improving the reliability and security of today's digital systems. The reviewed literature shows that the integration between IoT and blockchain is a potential solution to a number of major challenges

in IoT systems, especially related to data security, privacy, network reliability, and distributed authorization and access control.

In the article by Alzahrani et al. (2024), it is systematically explained how blockchain technology can strengthen the dimension of trust in the IoT ecosystem, which was previously very vulnerable to cyber attacks due to the characteristics of its devices which are heterogeneous, distributed, and often have limited computing power. This study forms the foundation for a general understanding of the strategic role of blockchain in strengthening IoT security (Almarri & Aljughaiman, 2024). Meanwhile, another study by Alzahrani et al. (2023) focuses more on the specific cybersecurity challenges faced by blockchain-based IoT systems. This study shows that IoT devices often become entry points for attacks due to the weakness of conventional authentication and data encryption mechanisms (Alajlan et al., 2023).

Xue et al. (2022) expands the discussion by examining the role of edge computing as a key supporter in accelerating data processing and reducing latency in IoT networks integrated with blockchain. The use of edge computing within the blockchain framework is considered to be able to optimize network performance and increase data transfer efficiency without sacrificing security aspects (Xue et al., 2023). In line with that, Solanki (2024) adds a new dimension through a review of editable blockchains, which allow for legitimate changes to information on the blockchain in the context of IoT. This is considered relevant in applications in sectors that require data flexibility, such as healthcare and manufacturing, where the right to personal data must be maintained (Solanki, 2024).

Zhang et al.'s (2023) research makes a significant contribution with an adaptive approach that combines clustering techniques in managing IoT devices with a blockchain-based management system. This approach is able to increase the efficiency of network communication while maintaining the integrity and confidentiality of the data sent (Kiran et al., 2023). On the other hand, Smith et al. (2021) highlights the policy and regulatory aspects in the integration of IoT and blockchain, especially in the manufacturing industry sector. This study notes that the adoption of this new technology requires adequate understanding and legal readiness so that its implementation does not cause regulatory conflicts, especially in terms of data privacy and information auditability (Pal, 2021).

Tian et al.'s (2020) study developed a framework that leverages the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to achieve high efficiency in data authentication. This framework is suitable for IoT systems that require fast validation while maintaining data integrity between devices (Tian et al., 2020). Furthermore, Shafagh et al. (2017) is one of the early studies that demonstrates the importance of designing an auditable IoT data storage architecture with blockchain. This article proposes a model that focuses not only on storage but also on secure distribution of access to the data (Shafagh et al., 2017).

Ferrag et al. (2018) provides a classification framework for common threats faced by IoT systems and blockchain protocols that can be used to address them. This article is very useful in understanding the complex technical problem map in the convergence of these two technologies (Ferrag et al., 2018). Finally, Kumar et al. (2023) presents a comprehensive review that outlines the integration strategies between IoT and blockchain, along with their practical applications and future research directions. This article concludes that despite major challenges, such as scalability and energy efficiency, the benefits gained from higher data security and system transparency provide a strong reason to continue developing this technological solution (Obaidat et al., 2024).

From all the literature findings reviewed, it appears that blockchain-based approaches in IoT systems not only address traditional security challenges, but also offer opportunities for developing more transparent, efficient, and sustainable systems in the long term. The focus of research is now

shifting from theoretical exploration to real-world applications and optimization of technology performance, indicating the increasing maturity of this field both academically and practically.

Discussion

In the increasingly connected digital era, data security is a major challenge, especially in the Internet of Things (IoT) system involving millions of interconnected devices. This study analyzes and proposes a distributed blockchain-based data security approach as a potential solution to overcome vulnerabilities in IoT systems. Through this approach, it is examined how blockchain technology can answer the need for reliable and effective authentication, encryption, consensus, and access management.

Blockchain, with its decentralized and resistant to manipulation nature, offers an attractive solution for data security in the IoT ecosystem. One of the main strengths of this technology is its reliability in maintaining data integrity. Because every transaction or data recorded on the blockchain cannot be changed without consensus from the entire network, the risk of data manipulation can be significantly reduced. This is different from traditional approaches that often rely on central servers that are vulnerable to attacks or system failures.

In terms of authentication, blockchain utilizes public key cryptography to allow each device in the network to be uniquely identified without the need to rely on a central authentication server. This enables a trustless authentication scheme, where the identity of a device can be verified by other nodes without the need for direct trust. Meanwhile, although blockchain itself does not encrypt data directly, it works optimally when combined with external encryption protocols such as AES or ECC to ensure data confidentiality when transmitted between devices.

Another important aspect studied in this study is the consensus mechanism, which is the process used by the blockchain network to agree on the state of data. Traditional consensus such as Proof of Work (PoW) has proven to be inefficient for IoT devices that have limited resources. Alternatives such as Practical Byzantine Fault Tolerance (PBFT) or other lightweight consensus algorithms are considered more suitable because they are more energy efficient and do not require intensive computing.

Access management is an integral part of the security system. In the context of blockchain, smart contracts function as the main controller. Through smart contract programming, the system can automatically determine who can access certain data or take actions in the system, thereby increasing access control and transparency.

However, the application of blockchain in IoT systems is not without challenges. Scalability and latency issues are major obstacles, considering that public blockchains have limitations in handling large transaction volumes in a short time. In addition, IoT devices generally have limitations in power, storage, and processing capacity, which makes it difficult for them to run a full blockchain node. The complexity of integration between IoT devices and blockchain systems is also a challenge, coupled with energy and operational costs that must be taken into account, especially when using consensus algorithms such as PoW.

One real example of the application of blockchain in IoT systems is a project run by IBM and Samsung with an initiative called ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry). In this project, IBM and Samsung developed a blockchain-based prototype system that allows smart home devices to communicate and share data without a central intermediary. Through this approach, devices such as refrigerators, air conditioners, or lighting systems can regulate energy usage or coordinate with each other automatically and securely, thanks to the implementation of smart contracts and distributed ledgers. This project marks the first step in utilizing blockchain in creating a more independent and secure IoT ecosystem.

Considering the results of the evaluation and existing case studies, it can be concluded that blockchain technology offers a promising solution in improving the data security of IoT systems, as long as the approach used is adjusted to the characteristics of the devices and network needs. The selection of blockchain type, lightweight consensus algorithm, and efficient smart contract implementation are key to presenting a system that is not only secure, but also practical and sustainable in the future.

CONCLUSION

This study concludes that e-service quality and e-trust have a significant effect on e-satisfaction, which in turn has a significant effect on e-loyalty. Meanwhile, the direct effect of e-trust on e-loyalty is not significant, indicating that user satisfaction plays an important mediator role in shaping Shopee user loyalty.

For e-commerce players like Shopee, it is important to continue to improve the quality of digital services—including response speed, ease of navigation, and transaction security. In addition, building trust through a transparent data security system and responsive customer service will strengthen user satisfaction, which ultimately increases consumer loyalty.

This study has several limitations, such as the limited sample size of 130 respondents and the scope that only includes Shopee users, so the generalization of the results to other platforms is still limited. In addition, data was collected through a survey method that relies on the subjective perceptions of respondents.

Future research can expand the number and variety of respondents, including users from various other e-commerce platforms such as Tokopedia or Lazada. Researchers are also advised to use a mixed-method approach to dig deeper into the psychological or contextual factors that influence user satisfaction and loyalt

REFERENCE

Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based IoT systems: A review. *Applied Sciences*, *13*(13), 7432.

Ali, G., Samuel, A., Kabiito, S. P., Morish, Z., Thomas, A., Robert, W., Denis, A., Sallam, M., Mijwil, M. M., & Ayad, J. (2025). Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends. *Applied Data Science and Analysis*, *2025*, 19–82.

Almarri, S., & Aljughaiman, A. (2024). Blockchain technology for IoT security and trust: a comprehensive SLR. *Sustainability*, *16*(23), 10177.

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34–42.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, *4*, 2292–2303.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 1–6.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. In *Future Generation Computer Systems* (Vol. 78, pp. 544–546). Elsevier.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6–10), 71.

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076–8094.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188–2204.

Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). A survey on privacy-preserving schemes for smart grid communications. *ArXiv Preprint ArXiv:1611.07722*.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Jing, Q., Vasilakos, A. V, Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*, 2481–2501.

Kiran, A., Mathivanan, P., Mahdal, M., Sairam, K., Chauhan, D., & Talasila, V. (2023). Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques. *Mathematics*, *11*(9), 2073.

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology*. Sage publications.

Li, J., Liu, Z., Chen, L., Chen, P., & Wu, J. (2017). Blockchain-based security architecture for distributed cloud storage. *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, 408–411.

Li, S. (2018). Application of blockchain technology in smart city infrastructure. *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 276–2766.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184–1195.

Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data and Cognitive Computing*, *8*(12), 174.

Okoli, C., & Schabram, K. (2015). *A guide to conducting a systematic literature review of information systems research*.

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, *9*(18), 5943–5964.

Pal, K. (2021). Privacy, security and policies: a review of problems and solutions with blockchain-based internet of things applications in manufacturing industry. *Procedia Computer Science*, *191*, 176–183.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 414–454.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 858–880.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable

storage and sharing of IoT data. *Proceedings of the 2017 on Cloud Computing Security Workshop*, 45–50.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339.

Solanki, A. R. (2024). Redactable Blockchain Solutions for IoT: A Review of Mechanisms and Applications. *ArXiv Preprint ArXiv:2407.05948*.

Tian, H., Ge, X., Wang, J., Li, C., & Pan, H. (2020). Research on distributed blockchain-based privacy-preserving and data security framework in IoT. *IET Communications*, *14*(13), 2038–2047.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30.

Wu, D., Si, S., Wu, S., & Wang, R. (2017). Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. *IEEE Internet of Things Journal*, *5*(4), 2958–2970.

Xue, H., Chen, D., Zhang, N., Dai, H.-N., & Yu, K. (2023). Integration of blockchain and edge computing in internet of things: A survey. *Future Generation Computer Systems*, *144*, 307–326.

Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*, 983–994.