Security and Privacy Concerns Associated with the Internet of Things(IoT) and the Role of Adapting Blockchain and Machine Learning - A Systematic Literature Review

Elva Leka[1,2], Enkeleda Hoxha[2], Genta Rexha[1,2]
[1]Polytechnic University of Tirana, Tirane, Albania
[2]Albanian University, Tirane, Albania
elva.leka@fgjm.edu.al; enkeleda.hoxha@student.albanianuniversity.edu.al; genta.rexha@albanianuniversity.edu.al

***Abstract* - The Internet of Things (IoT) is one of the most important technologies of our day, and it will continue to become more significant as more businesses realize the competitive advantages of having connected devices. Blockchain helps maintain correct data that is unaltered and permanent. At the same time, the Internet of Things (IoT), addresses hardware connected via the internet and may use machine learning to discover trends and produce accurate projections utilizing this data. Those three technologies have taken the place of the conventional methods that were previously employed for the design and architecture of new devices. Combining them yields a wide range of potential outcomes, some of which might result in the next great thing. We also contend that this convergence will speed up the development of autonomous models and information technology that aids companies in managing the security and privacy of their clients. We highlight and expose several challenges and upcoming research areas using machine learning algorithms and blockchain techniques to address security and privacy issues in the IoT space. In this paper, we thoroughly analyze the use of blockchain and machine learning technologies for IoT, focusing on security and privacy. Critical thoughtful writing has been heightened by examining research articles published in well-regarded magazines between 2018 and 2022. Finally, there are still challenges that can steer academics toward potential future advancements in IoT security and privacy.**

***Keywords* - Internet of Things; blockchain; machine learning; technologies; security; privacy**

I. INTRODUCTION

The internet of things (IoT), blockchain technology, and machine learning are now acknowledged as technologies that can enhance present procedures, develop innovative solutions, and disrupt numerous industries. A network of physical "things" that use software, sensors, and other technologies to connect and exchange data with other devices and systems through the internet is referred to as the "Internet of Things" [1]. IoT, which has brought about many technological advancements including voice assistants, smart homes, cars, and healthcare, has radically changed the way we live [2-4]. The recent rise of digital currency has sparked interest in blockchain, the technology that underpins it. Its advantages include decentralization, a distributed ledger, security, and information transparency [5].

Blockchain functions essentially as a list of all transactions made throughout time, much like a perpetual record book [6]. Blockchain primarily serves as a record of all prior transactions. Each participant's computer stores every piece of information as a long chain of linked data items, new items can only be added with the approval of the vast majority of users [7].

By utilizing complex algorithms to analyze vast amounts of data, machine learning can assist in demystifying the underlying patterns in IoT data. Automated systems that use statistically determined actions can supplement or entirely replace manual processes in critical activities [8]. We believe that ingesting images, video, and audio from data from IoT devices recorded on a decentralized ledger can aid machine learning in making predictions, identifying anomalies, and improving intelligence. Additionally, costs for data management, data transfer, and other essential services are decreased by assisting in the protection of data on IoT devices.

The research shows that using Blockchain to trade property between two devices, including smart contracts, offers a straightforward infrastructure [9]. Without the requirement for a centralized authority, autonomous device operation is possible with smart contracts. Blockchain can be used for interactions between people and platforms or objects in addition to IoT. On the other hand, millions of gadgets connected to the Internet of Things produce enormous amounts of data [10]. Machine learning, which extracts information from data, is fed by data.

The paper is organized as follows. In Section II, we give a background of The Internet of Things (IoT) and describe the security and privacy of IoT, further the Role of Adapting Blockchain and Machine Learning. In Section III we evaluate the Systematic Literature Review (SLR). Section IV presents the results of the SLR, and the final section describes the conclusions and future works.

II. BACKGROUND

The Internet of Things (IoT) is a network of physical devices, vehicles, home appliances, and other items that are embedded with sensors, software, and network connectivity, enabling these objects to collect and exchange data [11-12]. The IoT refers to the idea that everyday objects can be connected to the internet and can communicate with each other, without the need for human intervention. The impact of IoT can be seen in various aspects of daily life, including improved efficiency, convenience, and safety. For example, IoT-enabled devices can be used to monitor and control home appliances remotely, track the health and well-being of individuals, and optimize the use of energy in buildings [13]. IoT is also revolutionizing the way businesses operate by providing real-time data, improving decision-making, and enabling new business models. IoT is an important and rapidly growing field that is transforming the way we live, work, and interact with the world around us [14].

The security and privacy of IoT systems are critical concerns that must be addressed to ensure their widespread adoption and long-term viability. IoT devices generate and store large amounts of sensitive personal and commercial data, making them vulnerable to data breaches, hacking, and unauthorized access [15]. Some of the most common security threats to IoT systems include:

- *Data breaches*: IoT devices often collect and store sensitive personal information, making them a target for cybercriminals seeking to steal or misuse this information [16].
- *Hacking*: IoT devices can be easily hacked, especially if they are poorly secured or have outdated software. Hacked devices can be used to launch attacks on other systems, steal sensitive information, or control connected devices.
- *Unauthorized access*: IoT devices can be vulnerable to unauthorized access, which can occur when attackers gain access to devices through a weak password or by exploiting vulnerabilities in the system [17].
- *Malware*: IoT devices can be infected with malware, which can spread throughout the system and cause significant damage [18].

Securing large-scale IoT systems can be challenging, as many devices may have limited processing power, memory, and storage, making it difficult to implement traditional security solutions [19]. The need for effective and efficient security solutions is critical to ensure the security and privacy of IoT systems and the sensitive information they store and process. To address these security and privacy concerns, organizations must adopt a multi-layered approach to security, including the use of encryption, secure authentication, and regular software updates [20]. Additionally, the development of new security solutions, such as blockchain and machine learning, has the potential to enhance the security and privacy of IoT systems.

Blockchain technology has the potential to address some of the security and privacy issues associated with IoT [21]. Blockchain is a decentralized, distributed ledger that allows multiple parties to access and verify information without the need for a central authority [22]. This decentralized structure provides a number of benefits that could enhance the security and privacy of IoT systems, including:

- *Decentralization:* Blockchain technology eliminates the need for a central authority to control and manage data, reducing the risk of single points of failure and making it more difficult for attackers to compromise the system [23].
- *Immutability:* The data stored in a blockchain is tamper-proof, meaning that it cannot be altered or deleted once data is recorded on the blockchain. This feature provides a high level of trust in the data recorded on the blockchain, making it more difficult for attackers to manipulate or corrupt the information [24].
- *Transparency:* Blockchain technology provides a transparent and verifiable record of all transactions and data stored on the blockchain. This transparency helps to build trust and increases accountability, reducing the risk of data breaches or unauthorized access [25].
- *Smart Contracts:* Blockchains can support smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This can increase the security and privacy of IoT systems, as smart contracts can be used to automate the enforcement of security and privacy policies [26].

The use of blockchain technology in IoT has the potential to enhance the security and privacy of IoT systems by providing a decentralized, tamper-proof, transparent, and verifiable method of storing and managing data [27]. While there is still much research to be done in this area, the potential benefits of using blockchain in IoT are significant and could play a major role in addressing security and privacy concerns in IoT.

Machine learning algorithms have the potential to improve the security and privacy of IoT systems by providing real-time threat detection and response capabilities. Machine learning algorithms can learn from historical data and identify patterns that could indicate a security threat, such as unusual traffic patterns or attempts to access sensitive information [28]. This allows machine learning algorithms to detect and respond to threats in real time, reducing the risk of data breaches or unauthorized access to sensitive information [29].

Some of the benefits of using machine learning in IoT include:

- *Real-time Threat Detection*: Machine learning algorithms can detect threats in real-time, allowing for rapid response and mitigation of security incidents [30].

- *Predictive Analysis:* Machine learning algorithms can analyze historical data and identify patterns that could indicate a security threat. This allows for proactive and predictive security measures to be put in place, reducing the risk of data breaches or unauthorized access [31].

Machine learning algorithms in IoT have the potential to real-time the security and privacy of IoT systems by providing real-time threat detection and response capabilities, predictive analysis, personalized security measures, and improved accuracy [32]. While there are still challenges to be addressed in this area, such as privacy concerns and the need for large amounts of data to train machine learning algorithms, the potential benefits of using machine learning in IoT are significant and could play a major role in improving the security and privacy of IoT systems.

III. METHODOLOGY OF RESEARCH

In light of the quick advancements in science, an SLR locates and evaluates the pertinent research to respond to a developed research issue. For the researchers tackling that problem domain, the findings are an SLR that outlines potential solution options. By categorizing the papers and attempting to offer an overview of the study to detect deficiencies, SLR aids us in providing a visual summary and a map of outcomes.

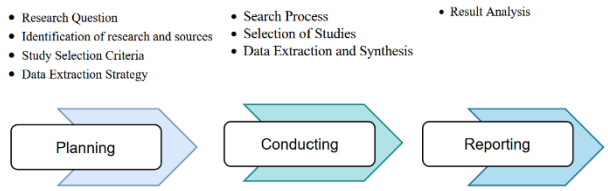

Figure 1. The Systematic Literature Review process

A. The Review's Planning

This analysis focuses on the benefits of integrating blockchain and machine learning technology into IoT devices and how they affect security and privacy. In this paper, the following research questions are especially addressed:

- **RQ1.** Could IoT devices potentially include blockchain and machine learning to further the technology?
- **RQ2.** How can we boost security by integrating blockchain and machine learning technologies into IoT devices?
- **RQ3.** What will be the effect on the cost of IoT security by combining other technologies?
- **RQ4.** Is the vulnerability assessment of IoT systems using blockchain and machine learning effective in identifying flaws?

B. Studying Techniques

A broad understanding of the literature was necessary for a thorough analysis. The relevant databases were rigorously reviewed to ensure that the information provided here is complete. We tracked down and collated relevant content. Not every exceptional work of literature met the search parameters for a variety of reasons.

TABLE I. DATABASE RESEARCH

Coverage	*Search terms*
Peer-reviewed journals, conferences, Articles	("IoT security, privacy " AND "blockchain")("IoT security, privacy " AND "machine learning")
Peer-reviewed journals, conferences, Articles	("IoT security challenges" AND "blockchain") OR ("Blockchain security" AND "machine learning privacy")
Peer-reviewed journals, conferences, Articles	("IoT privacy concerns" OR "blockchain for IoT security")
Peer-reviewed journals, conferences, Articles	("IoT privacy" AND "machine learning") ("IoT security challenges" OR "blockchain")
Peer-reviewed journals, conferences, Articles	("IoT privacy concerns" AND "blockchain for IoT security")

TABLE II. PAPER SELECTION RESULTS

Database	*Number of records retrieved*	*Number of studies selected*
Scopus	233	11
IEEE Xplore	324	10
ACM Digital Library	52	5
Science Direct	251	10
Google Scholar	124	4
Total	984	40

To accomplish this goal, a comprehensive literature search was carried out. We found 40 of the 984 papers from 5 databases to be interesting.

C. Primary Studies Chosen

The goal of the selection process is to find a group of studies that are relevant to the topic of the systematic literature review. By carefully evaluating primary publications, we seek to ensure that the review provides a strong and trustworthy interpretation of the research issue. The search string formulation was influenced by the study domain and themes, and the right content was discovered and gathered as a result.

We created the inclusion and exclusion criteria in order to perform selection on the collected material.

Inclusion Criteria:

- Peer-reviewed articles and conference papers that were published between 2018 and 2022.
- Studies that focus on the security and privacy challenges associated with the IoT.

Inclusion Criteria:

- Peer-reviewed articles and conference papers that were published between 2018 and 2022.
- Studies that focus on the security and privacy challenges associated with the IoT.
- Studies that discuss the role of blockchain and machine learning in enhancing the security and privacy of IoT systems.
- Empirical studies that provide quantitative and qualitative evidence to support their findings.

Exclusion Criteria:

- Grey literature such as thesis, dissertations, and technical reports.
- Non-English language Peer-reviewed, Journals, Conferences, and Articles.
- Studies that only focus on the technology and implementation of the IoT without addressing security and privacy concerns.
- Studies that only focus on the blockchain or machine learning without considering their application in the IoT context.

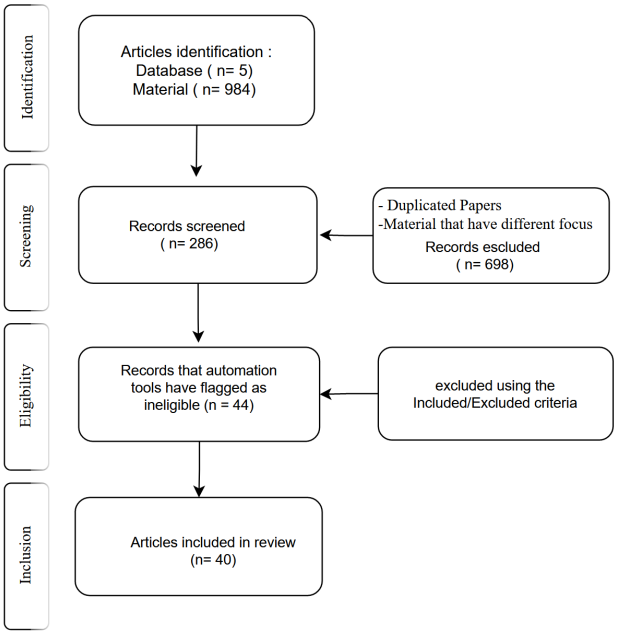

Figure 2. Diagram illustrating the research process [33]

IV. RESULTS

The number of articles generated in each year from 2018 through 2022 is shown in Figure 3. Over the past five years, the idea of incorporating blockchain technology and machines into the Internet of Things (IoT) and addressing concerns about security and privacy has developed and grown.

Table 4 below lists the words used most frequently by the authors. It should come as no surprise that "Blockchain", "Machine Learning", "Internet of Things", " Cryptography", and "Security" were the most often used terms.

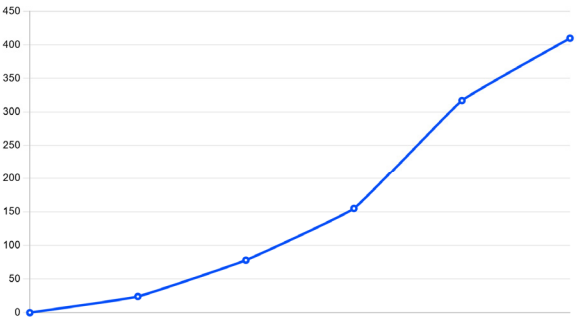

Figure 3. The number of articles published between 2018 and 2022

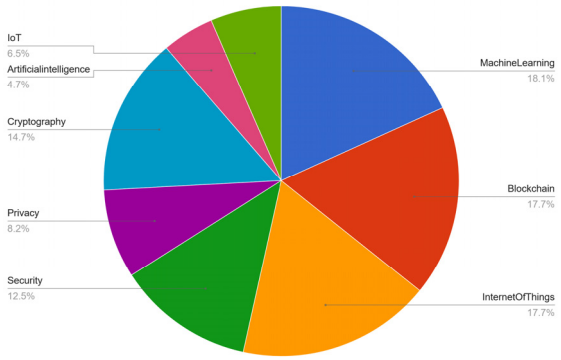

Figure 4. Frequently used subject words

The findings of our SLR with reference to each study question are presented ongoing.

RQ1. Could IoT devices potentially include blockchain and machine learning to further the technology?

To further improve the functionality and security of the IoT ecosystem, IoT devices may use blockchain and machine learning technology. Blockchain technology can provide a secure and decentralized platform for storing and managing the vast amounts of data generated by IoT devices, as stated by the authors of the article [6] [23]. We can assist in preventing data breaches and illegal access to sensitive information in this way. The massive amounts of data produced by IoT devices may be analyzed using machine learning algorithms to provide insights, discover patterns, and make predictions. This can lead to improved decision-making and automation in various industries and applications [28-29].

Incorporating these technologies presents new challenges, such as scalability, privacy, and security issues. Developers must carefully examine the benefits and drawbacks before integrating these technologies into IoT devices.

RQ2. How can we boost security by integrating blockchain and machine learning technologies into IoT devices?

Integrating blockchain and machine learning technologies into IoT devices can boost security in several ways, which have been analyzed in [34-37]:

- *Blockchain for data security:* Blockchain can provide a secure and decentralized ledger for storing and transmitting the vast amounts of data generated by IoT devices. The decentralized nature of blockchain ensures that the data is not controlled by any single entity, reducing the risk of data breaches or unauthorized access.
- *Blockchain for device authentication:* Blockchain can be used to authenticate IoT devices, ensuring that only authorized devices can access the network and the data stored on it. This helps prevent malicious actors from accessing and manipulating the network or its data.
- *Machine learning for threat detection:* Machine learning algorithms can be used to analyze the data generated by IoT devices in real-time, detecting anomalies and potential threats. This can improve the speed and accuracy of detecting and responding to security threats.
- *Machine learning for access control:* Machine learning algorithms can be used to control access to the network and its data, based on the behavior and characteristics of the devices and users. This can help prevent unauthorized access and increase the security of the network.

It is important to note that while integrating blockchain and machine learning technologies into IoT devices can significantly boost security, these solutions must be implemented with caution and proper security measures must be put in place to prevent new security risks from emerging.

RQ3. What benefits do ML and blockchain provide for the IoT privacy framework?

Machine learning (ML) and Blockchain technologies can provide several benefits for an IoT privacy framework:

- *Data protection:* ML algorithms can help in identifying and detecting unusual behaviour in the data, while blockchain can provide an immutable ledger of data transactions, thus making it difficult for unauthorized users to access the data [38].
- *Decentralization:* Blockchain allows for decentralized data storage, reducing the risk of single-point failure and enabling secure data sharing between multiple parties [23].
- *Trust and transparency*: The transparency and immutability of blockchain transactions can help to build trust between different parties involved in the IoT ecosystem, including consumers, manufacturers, and service providers [39].
- *Improved security:* ML algorithms can help in identifying security threats in real time and prevent them as analyzed in [40], while blockchain can provide an additional layer of security through cryptographic techniques [41].
- *Compliance:* The use of blockchain and ML can help organizations meet privacy regulations such as GDPR, as they enable organizations to securely manage and track personal data [42].

RQ4. Is the vulnerability assessment of IoT systems using blockchain and machine learning effective in identifying flaws?

Although it is crucial to keep in mind that no technology is impenetrable and all systems have some level of vulnerabilities, the usage of blockchain and machine learning (ML) for the security assessment of IoT systems can be successful in discovering faults. IoT devices create a lot of data, which ML algorithms may be used to analyze to find patterns and abnormalities that might point to security vulnerabilities. For example, an ML algorithm may be able to detect unusual network traffic patterns or identify unauthorized devices on a network. Similarly, blockchain can provide a secure and transparent platform for tracking and verifying data transactions, making it easier to identify and prevent unauthorized access to sensitive information, as the authors have highlighted in their paper [43]. The decentralized nature of blockchain also makes it more difficult for malicious actors to manipulate the system, which can help to increase the overall security of IoT networks.

V. CONCLUSION

This paper performed a Systematic Literature Review to provide an in-depth understanding of the current state of research on this topic. The review aims to identify the primary security and privacy issues associated with the IoT, as well as the strategies and technologies used to address these concerns.

We collected 984 papers and selected 40 papers as primary studies. The integration of blockchain and machine learning has the potential to address some of the security and privacy concerns associated with the Internet of Things (IoT). Blockchain provides a secure and transparent ledger of data transactions, which can prevent tampering and unauthorized access to sensitive information and help ensure the security of network-stored data. Machine learning algorithms can analyze large amounts of data generated by IoT devices to identify patterns and anomalies that may indicate security vulnerabilities, further as well as detect unusual network activity or identify devices that deviate from their normal behaviour.

However, there are also limitations and challenges associated with using blockchain and machine learning in IoT systems. These include the need for high computational power and data storage, the potential for data privacy breaches, and the need for a secure and reliable infrastructure. As the IoT continues to evolve and expand, it is important for organizations and individuals to be aware of these security and privacy concerns and to explore the potential benefits and limitations of integrating blockchain and machine learning into their IoT systems. In addition to ensuring the integrity and security of the IoT as a whole, this will also help protect private user information and sensitive data.

REFERENCES

[1] A. Banafa, "16 IoT, AI and Blockchain: Catalysts for Digital Transformation," in Secure and Smart Internet of Things (IoT): Using Blockchain and AI ", River Publishers, 2018, pp.113-120.

[2] A. Miglani, N. Kumar, "Blockchain Management and Machine Learning Adaptation for IoT environment in 5G and beyond Networks: A systematic review, Computer Communications, Volume 178, 2021, Pages 37-63, ISSN 0140-3664, DOI: https://doi.org/10.1016/j.com

[3] W. Choi, J. Kim, S. Lee, E. Park, "Smart home and internet of things: A bibliometric study", in Journal of Cleaner Production, Volume 301, 2021, 126908, ISSN 0959-6526, https://doi.org/10.1016/j.jclepro.2021.126908.

[4] Sh. Nazir, Y. Ali, N. Ullah, I. García-Magariño, "Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review", Wireless Communications and Mobile Computing, vol. 2019, Article ID 5931315, 20 pages, 2019. https://doi.org/10.1155/2019/5931315

[5] M. Banerjee, J. Lee, Kim-Kwang Raymond Choo, "A blockchain future for internet of things security: a position paperDigital Communications and Networks,Volume 4, Issue 3,2018,Pages 149-160,ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2017.10.006

[6] D. Shah, D. Patel, J. Adesara, "Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector", Vis. Comput. Ind. Biomed. Art 4, 18 (2021). https://doi.org/10.1186/s42492-021-00084-y.

[7] D. Lizcano, J. A. Lara, B. White, "Blockchain-based Approach to Create a Model of Trust in Open and Ubiquitous Higher Education" J Comput High Educ 32, 109–134 (2020). https://doi.org/10.1007/s12528-019-09209-y.

[8] Machine Learning (ML) for IoT, Available: https://www.softwareag.com/en_corporate/resources/what-is/machine-learning.html, (Accessed: Jan. 2023).

[9] G. Schmitt, A. Mladenow, Ch. Strauss, M. Schaffhauser-Linzatti, "Smart Contracts and Internet of Things: A Qualitative Content Analysis using the Technology-Organization-Environment Framework to Identify Key-Determinants", Procedia Computer Science, Volume 160, 2019, pp. 189-196, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.09.460.

[10] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, Volume 88, 2018.

[11] D. Mocrii, Y. Chen, P. Musilek, "IoT-based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security, Internet of Things, Vol. 1–2, 2018, pp. 81-98,ISSN 2542-6605, DOI: 10.1016/j.iot.2018.08.009.

[12] F. Sabrina, N. Li, S, Sohail, "Blockchain Based Secure IoT System Using Device Identity Management". *Sensors (Basel, Switzerland)*. 2022; 22(19):7535, DOI: 10.3390/s22197535.

[13] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem and K. Tepe, "Technical Issues on Cognitive Radio-Based Internet of Things Systems: A Survey," in *IEEE Access*, vol. 7, pp. 97887-97908, 2019, doi: 10.1109/ACCESS.2019.2929915.

[14] A. Banafa, "8 IoT Standardization and Implementation Challenges," in *Secure and Smart Internet of Things (IoT): Using Blockchain and AI* , River Publishers, 2018, pp. 53-58.

[15] B. K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial Intelligence and Blockchain technology, Internet of Things, Volume 11, 2020, 100227, ISSN 2542-6605, DOI: 10.1016/j.iot.2020.100227.

[16] G. Vojković, M. Milenkovic, T. Katulić, "IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law", *Business Systems Research*. 2020;11(3):167-185. doi:10.2478/bsrj-2020-0033.

[17] C. Hahn C, J. Kim, H. Kwon H, J. Hur, "Efficient IoT Management With Resilience to Unauthorized Access to Cloud Storage". *IEEE transactions on cloud computing*. 2022, 10(2):1008-1020. doi:10.1109/TCC.2020.2985046

[18] N. R. Nath, V. H. Nath, "Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges". Computers & Electrical Engineering. 2022; 100:107997-. doi:10.1016/j.compeleceng.2022.107997.

[19] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, I. Traore "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook". Energies (Basel). 2022; 15(19):6984-. doi:10.3390/en15196984.

[20] Y. Goh, J. Yun , D. Jung, JM. Chung JM, "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning", IEEE Access. 2022; 10:118498-118511. doi:10.1109/ACCESS.2022.3220852.

[21] R. Xu and Y. Chen, "μDFL: A Secure Microchained Decentralized Federated Learning Fabric Atop IoT Networks," In IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2677-2688, Sept. 2022, doi: 10.1109/TNSM.2022.3179892.

[22] A. Su. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, J. Li, Efficient Privacy-Preserving Authentication Protocol Using PUFs with Blockchain Smart Contracts, Computers & Security, Vol. 97, 2020, 101958, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101958.

[23] M. Alhejaz, R. Mohammad, "Enhancing the Blockchain Voting Process in IoT using a Novel Blockchain Weighted Majority Consensus Algorithm (WMCA)", Information Security Journal. 2022;31(2):125-143. Doi:10.1080/19393555.2020.1869356.

[24] Z. Rahman, X. Yi, I. Khalil I., "Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat", IEEE Internet of Things Journal. Published online 2022:1-1. Doi:10.1109/JIOT.2022.3147186.

[25] Y. Goh, J. Yun, D. Jung, J. Chung, "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning", in IEEE access. 2022; 10:118498-118511. doi:10.1109/ACCESS.2022.3220852.

[26] H. Mrabet, A. Alhomoud, A. Jemai, D. Trentesaux, "A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing". Applied sciences. 2022;12(9):4641-. doi:10.3390/app1209464.

[27] A Dorri, C. Roulin, S. Pal S, S. Baalbaki, R. Jurdak, S. Kanhere "Device Identification in Blockchain-Based Internet of Things". In IEEE Internet of Things Journal. 2022; 9(24): 1-1. doi:10.1109/JIOT.2022.3194671.

[28] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[29] U. Farooq, N. Tariq, M. Asim, T. Baker, A. Al-Shamma'a "Machine Learning and the Internet of Things Security: Solutions and open challenges". In Journal of Parallel and Distributed Computing, Vol. 162, 2022, pp. 89-104, ISSN 0743-7315, Doi: 10.1016/j.jpdc.2022.01.015.

[30] Y. Zhao, G. Cheng, Y. Duan, Z. Gu, Y. Zhu, L. Tang, "Secure IoT edge: Threat situation awareness based on network traffic" *Computer networks (Amsterdam, Netherlands : 1999)*. 2021;201:108525-. doi:10.1016/j.comnet.2021.108525.

[31] J. Cui, L. Wang, X. Zhao, H. Zhang, “Towards Predictive Analysis of Android Vulnerability Using Statistical Codes and Machine Learning for IoT applications. *Computer communications*. 2020; 155, pp. 125-131. doi:10.1016/j.comcom.2020.02.078.

[32] M. Ferrag, O. Friha, L. Maglaras, H. Janicke H, L. Shu, “Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis”, IEEE Access. 2021, pp. 138509-138542. DOI:10.1109/ACCESS.2021.3118642.

[33] M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ (Online), 372, n71–n71. https://doi.org/10.1136/bmj.n71.

[34] D. Liao, H. Li, W. Wang, X. Wang, M. Zhang, X. Chen, “Achieving IoT data security based blockchain”. In *Peer-to-peer networking and applications*, 2021, 14(5), 2694-2707. doi:10.1007/s12083-020-01042-w.

[35] M. Shen, H. Liu, L. Zhu, “Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT”. In *IEEE Journal on Selected Areas in Communications*. 2020, 38(5), pp. 942-954. doi:10.1109/JSAC.2020.2980916.

[36] D. Javeed D, U. Badamas, T Iqbal, A. Umar, C. Ndubuisi, “Threat Detection using Machine/Deep Learning in IOT Environments”. *International Journal of Computer Networks and Communications Security*. 2020, 8 (8), pp. 59-65.

[37] A. K. Istiaque, M. Tahir, H. M. Habaebi, S. L. Lun, A. Ahad “Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction”. *Sensors (Basel, Switzerland)*. 2021;21(15):5122-. doi:10.3390/s21155122.

[38] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, “Blockchain for the IoT: Privacy-preserving protection of sensor data”. In *Journal of the Association for Information Systems*. 2019, 20(9): 1271-1307, DOI:10.17705/1jais.00567.

[39] W. Liang W, N. Ji, “Privacy challenges of IoT-based blockchain: a Systematic Review”, *Cluster computing*. 2022, vol. 25, issue 3, pp. 2203-2221. doi:10.1007/s10586-021-03260-0

[40] S. Bharati, P. Podder, “Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions”, *Security and communication networks*. 2022, 2022:1-41. doi:10.1155/2022/8951961.

[41] N Y, P M. Radial kernelized regressive merkle–damgård cryptographic hash blockchain for secure data transmission with IoT sensor node. *Peer-to-peer networking and applications*. 2021;14(4):1998-2010. doi:10.1007/s12083-021-01135-0.

[42] A. Kounoudes, G. Kapitsaki, “A mapping of IoT user-centric privacy preserving approaches to the GDPR”. In *Internet of Things*. 2020;11:100179-. doi:10.1016/j.iot.2020.100179.

[43] C. Nartey C, E. Tchao, J. Gadze JD, “On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives”. In *Wireless communications and mobile computing*. 2021;2021:1-25. doi:10.1155/2021/6672482.