Toward Using Blockchain as a Promised Solution for Security Issues in IOT

Salah M. Ahmed and Aiman A. Samra

Salah M. Ahmed
Computer Engineering Dep.
Islamic Univeristy of Gaza
Gaza, Palestine
Salah@ait.ps

Aiman A. Samra
Computer Engineering Dep.
Islamic Univeristy of Gaza
Gaza, Palestine
aasamra@iugaza.edu.ps

Abstract*— The emergence of the IoT technology has garnered significant interest in recent years, with its ability to integrate multiple sensors and nodes for seamless interconnectivity without human intervention. The three layers of the IoT system, namely the physical perception layer, network layer and application layer, require secure mechanisms to guarantee the end-to-end integrity of the data and interactions across these levels. However, IoT applications face several security challenges, which this paper aims to address. By conducting an extensive review of existing works on IoT security and blockchain technology, this paper shows a comprehensive analysis of the security matters in each layer of the IoT architecture. In addition, it highlights the potential of blockchain technology as a promising solution to address these security issues. Furthermore, this paper delves into the different aspects of IoT security, such as scalability, interoperability, distributiveness, resource scarcity and security concerns. As of yet, there is no particular reference architecture for the IoT, and creating a new one is a complex process, despite various standardization efforts. Nonetheless, this paper presents the three common IoT architectures that are currently in use. Overall, the goal of this survey is to deliver a comprehensive overview of the security challenges faced by the IoT and the potential of blockchain technology to make a secure and reliable solution.*

Keywords—IoT, Blockchain, security, network, transportation, smart home, computing

I. INTRODUCTION

The Internet of Things (IoT) has become a developmental technology that has earned a vast scope in research and engineering applications. This is largely due to the fast development of smart devices and the rapid growth of high-speed networks. The IoT enables the interconnection of various devices and sensors without requiring human intervention, which solves many problems and challenges [1]. An extensive range of IoT applications and services have emerged in various markets including healthcare, surveillance, security, transportation, and food safety [2]. In the context of the Internet of Things (IoT), the term "things" refers to physical and embedded devices that are interconnected, including sensors and semiconductors, to monitor and collect several forms of data related to both machines and human social life. These data can then be combined, fused, analyzed, processed, and mined to extract valuable data that can be used to enable intelligent and global services [3]. A wide range of embedded devices, from small wearables to large machines, are interconnected with sensor chips and can be remotely controlled to perform specific functions. These devices communicate with each other via public networks or private networks utilizing standard communication protocols to share data [4]. In general, the IoT system usually contained three layers: the application layer, the physical perception layer, and the network layer. These layers are interconnected through cyber-physical social features. However, the IoT environment cause various security challenges like access control, verification, authorization, and privacy [5]. IoT applications require secure mechanisms that get through these levels to guarantee the end-to-end integrity of the aggregated data and the related interactions. The transparency of data collection processes and interactions is the key to satisfying these requirements, in addition to the ability to examine these interactions and processes. Both the auditability and transparency requirements inspire the consideration of blockchain to support integrity and security in IoT [6].

This paper mainly focus on the IoT security issues and blockchain technology as a promised solution that solve these security issues, by conducting an extensive review of current researches in the subject of IoT security and blockchain technology.

Section II will overview the IoT Architecture. Section III will describe the IoT factors impacting security. Section IV will overview the Block Chain Technology. Blockchain Solutions for IoT Security will be discussed in Section V, while Section VI will be the conclusion.

II. IOT SYSTEM ARCHITECTURE

To ensure efficient functioning of the Internet of Things (IoT), there are several key factors that essential to be handled. These factors include scalability, interoperability, distributivity, resource scarcity, and security. [7]:

Scalability: Is necessary to accommodate the increasing number of services and devices without any negative impact on performance.

Interoperability: Is important for devices from different vendors to work together towards common objectives.

Distributive: Is crucial to enable the collection and processing of data from various sources in a distributed manner.

Resources scarcity: Both computational resources and power must be considered.

Security: Not allow unauthorized external control could seriously delay the deployment of IoT.

At this time, there is no particular reference architecture for IoT, and creating new one is showing very complicated regardless of various standardization determinations. In general, there are three common IoT Architectures as shown in Fig. 1.

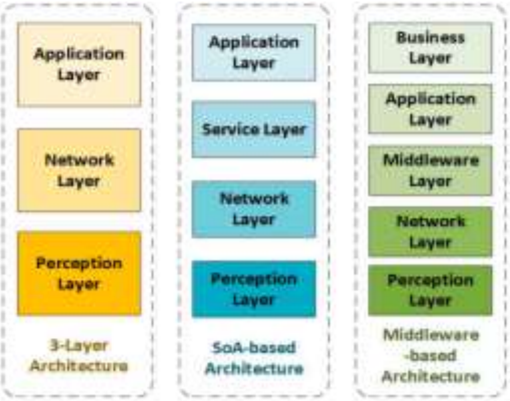

Fig. 1. The IoT system archicture [7]

In this section the main anticipated characteristics of the IoT Three-Level Architecture will be highlighted.

In [3] it is presented that the IoT system including three layers, as shown in Fig. 1:

The physical perception layer comprises of a vast amount of sensors, actuators, and mobile devices that utilize sensing technologies to gather data about physical objects and social environments. This layer collects a massive amount of data which is then translated into entities in the cyber world. On the other hand, the network layer consists of all network elements with different configurations such as wireless sensor networks, ad hoc networks, cellular mobile networks, and the Internet.

The network layer is responsible for tasks such as data coding, broadcast, fusion, mining, and analysis at data processors. It plays a crucial role in delivering essential information to the application layer. coding, broadcast, fusion, mining and examining at data processors in order to deliver important information to an application layer.

Aapplication layer includes a range of distributed networks (such as P2P, Cloud Computing, and Grid), application interfaces, and systems that intelligently offer the necessary services or applications to end-users in the IoT ecosystem [8].

Recently, the cyber-physical social relationships established across these three layers have been explored and analyzed to provide advanced services for end-users.

While in [5] it shows that the IoT system is depicted as consisting of three layers, as shown in Fig. 2.

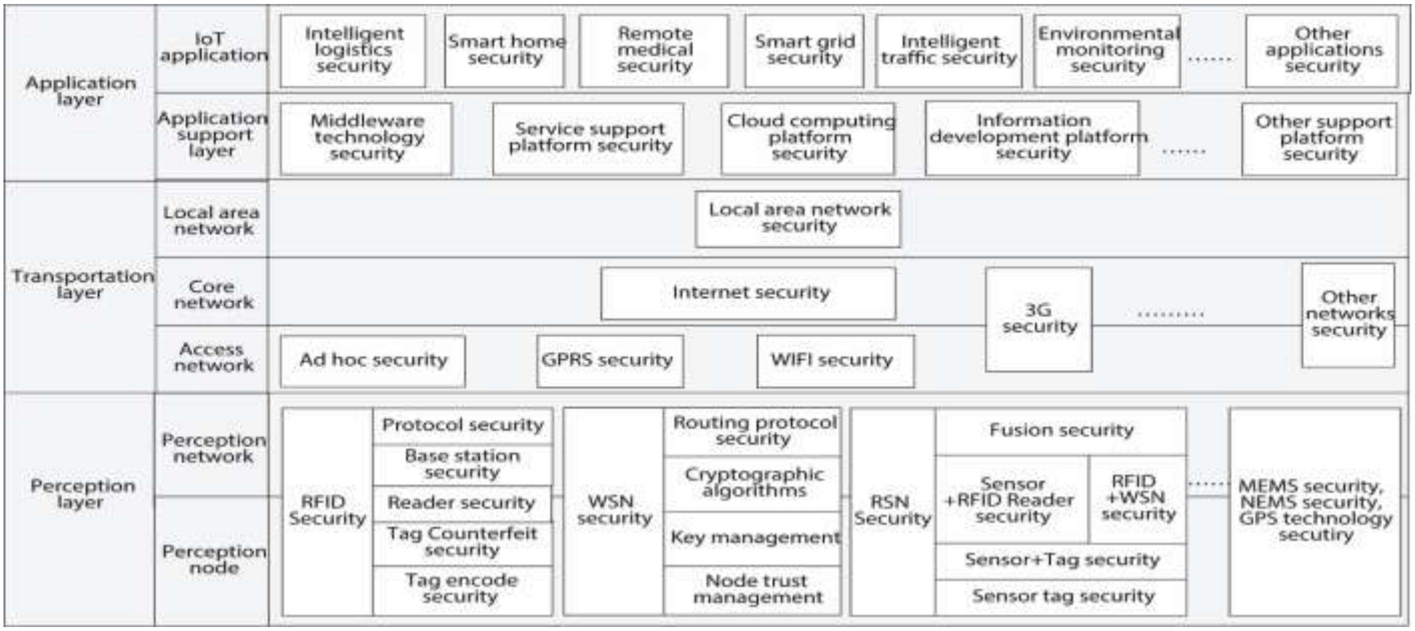

Fig. 2. The IoT system architecture [5]

Perception layer plays a crucial role in collecting data, controlling objects, and enabling object perception in the Internet of Things (IoT). This layer can be separated into two components: the perception node, consisting of controllers or sensors, and the perception network, which connects to the transportation network. The perception node primarily focuses on controlling and collecting data, whereas the perception network transmits aggregated data to the gateway or provides control instructions to the controller. Various technologies, such as WSNs, RFID, GPS, and RSN, are utilized in this layer to achieve these objectives.

Transportation layer offers a global access environment for the perception layer, information perception, storage, and transmission, as well as the application layer. It can be categorized into three layers based on its functions: the core network, the access network, and the local area network. The transportation layer comprises a diverse range of heterogeneous networks.

The application layer supports various business services and enables intelligent computation and resource allocation. Throughout the entire process, the application support layer identifies and filters valid data, malicious data, and spam data. The application layer typically includes middleware such as M2M, service support platforms, and cloud computing platforms.

To provide a more detailed analysis of IoT security issues, the perception layer has been categorized into perception nodes and perception networks, while the transportation layer has been divided into LAN, access network, and core network based on data transmission within the IoT phase. The application layer has been further classified into IoT applications and the application support layer, as illustrated in Figure 2. It is crucial for IoT to guarantee the security of the whole system, including all layers such as the perception layer, transportation layer, and application layer. The perception layer encompasses RFID security, WSNs security, and RSN security. Similarly, the application layer involves securing the application support layer as well as other IoT applications. Finally, the transportation layer's security includes core network security, access network security, and local network security.

A. *Perception layer Security issues*

The perception layer is connected to the application layer over the network layer. The Perception layer technologies contain several kinds of sensors, such as ZigBee, sensor nodes, RFID and sensor gateways. In [5], the author summarized several security issues related to perception layer as shown in Table 1.

TABLE I. PERCEPTION LAYER SECURITY ISSUES

Technology	Security issue	Description
RFID technology	Uniform coding	The lack of a consistent global encoding standard for RFID tags can result in the reader being unable to access tag information or errors occurring during the reading process.
	Conflict collision	Simultaneous data transfer from multiple RFID tags may cause the reader to be unable to retrieve data accurately. However, utlizing the anti-collision technique can avoid several tags from sending information to the reader at the same time.
	RFID privacy protection	RFID tags with low cost are inadequate in resources, such as small storage size and weak computational abilities. Therefore, lightweight solutions are required to achieve privacy protection, including data privacy and location privacy.
	Trust management	In IoT RFID systems, trust management, such as digital signature technology, should be considered. Trust management typically exists between readers and RFID tags, as well as among readers and base stations.
WSNs	Cryptographic algorithms in WSNs	Wireless sensor networks have diverse application areas that require high data security, and includes data confidentiality and data integrity, that could be addressed via data encryption.
	Key management in WSNs Network	The Key management remains a significant problem to be resolved for WSN security and is a crucial element for resolving other security matters. Key management contains secret key generation, updating, distribution, storage, and destruction processes. Key distribution is the most significant concern in key management.
	Secure routing protocols for WSNs	The WSN routing protocol is susceptible to attacks, which can cause a network outage. Therefore, developing a secure and efficient routing protocol has been the consideration of many WSN studies.
	Trust management of	WSNs have unique features like delimited resources of sensor nodes, easy node capture, and

	nodes in WSNs	specialized communication methods, which make them vulnerable to various attacks. Therefore, relying solely on passwords and cryptographic algorithms is insufficient for ensuring WSN security. A trust management mechanism is necessary to ensure WSN security.
RSN	Problems of heterogeneous integration	Integrating data from heterogeneous sources is a significant challenge, as WSNs and RFID may use varied protocols, causing compatibility problems among communication protocols and data formats. To address this issue, unified data encoding standards and item information exchange protocols must be used for RFID and WSNs within the context of IoT. Software-level cooperation between RFID and WSNs is required for system-level integration.

B. *Transportation layer Security issues*

Table 2 outlines the security challenges that the transportation layer encounters due to its functional structure. The transportation layer is comprised of three layers: the core network, access network, and local area network, which are all composed of a diverse set of heterogeneous networks.

TABLE II. TRANSPORTATION LAYER SECURITY ISSUES

Functional architecture	Security issue	Description
Access network	WiFi security issues	The security risks of WiFi can be separated into two groups: those resulting from network traps and those resulting from network attacks. These risks include access attacks, DDoS/DDoS attacks, and malicious phishing AP.
	3G network security issues	Security issues in 3G networks include user information leak, incomplete data, illegitimate attacks, and other related security problems.
	Ad hoc security issues	Ad hoc networks are vulnerable to security issues such as illegal node access, data security, and network routing security (such as DDoS/DDoS attacks).
Local area network	Data leakage and server's independent protection security matters	Failure to implement network access control measures can result in the illegitimate use of network resources, such as the use of malicious code, manipulation of unnecessary system services, and failure to frequently update the operating system patches.

C. *Security issues of the Application layer*

The application layer resides above the transportation layer and is responsible for managing various business services and leveraging intelligent computation and resources. The application support layer filters out valid, spam, and malicious data during the entire process. Middleware, such as M2M, service support platforms, and cloud computing platforms, are commonly found in the application layer. Security issues in the application layer depend on the types of supported services, as outlined in Table 3.

TABLE III. APPLICATION LAYER SECURITY ISSUES

Services and middleware	Security issue	Description
Cloud Computing	Security threats	Cloud computing services are a worthwhile target for hackers due to the sensitive data of enterprises being stored on them.
	Service interruption and attack issue	Cloud computing services have experienced familiar service interruptions such as data backup, system shutdown, and data center offline events. Additionally, DDoS attacks and service interruptions are frequent.
	Investigate audit issues	The global accessibility of computation, storage, and network bandwidth services in cloud computing is counterbalanced by the risk of fraudulent access to user account information. Additionally, the diverse legal requirements for obtaining evidence of illegal activities in different countries and regions pose a challenge in tracing network crimes that are based on cloud computing platforms.

Integrated or individual specific application business	Intelligent transportation	An intelligent logistics system involves several subsystems, such as receiving, transferring, sorting, sending, and transportation. Real-time and accurate features are essential for efficient operations, and RFID technology is a suitable solution. To track objects during transportation, RFID readers utilize GPS systems via GSM/CDMA networks to transmit the object's recent position to the data center. However, similar to the internet, RFID systems are vulnerable to viruses and hacking attempts. Information leakage is considered the most severe data security risk for RFID systems used in intelligent logistics.
	Smart home	The primary technologies applied in an intelligent home system include network control, communication, and mobile terminal technologies. These technologies face security issues such as building damages, privacy-aware theft, and illegal eavesdropping.

Typically, application layer security is specific to each application and cannot be resolved at other layers.

III. BLOCKCHAIN TECHNOLOGY

Blockchain technology has arose as a security technology that is mainly used as a distributed network [9] and decentralized structure for crypto digital currencies [10]. In general, the blockchain is designed as a public database that keeps the data in a non- tampering ledger. It links secured hashed blocks by using cryptography [11]. The blockchain recorded each transaction by trust-proved nodes.

The blockchain is suitable for the IoT field and can aid in addressing security concerns. With the growth of IoT technology and the growth in the number of linked devices, security obstacles have emerged. In this section, we will summarize the studies that have suggested Blockchain as a viable solution to IoT security issues.[12].

The blockchain serves as a secure and continuously maintained database with a growing set of features and data models. Its primary features include enabling users to create transactions and record them on its blocks. Each block verifies if the transaction details are in the correct sequence, preventing data tampering. The transactions saved on the blockchain are distributed globally among the nodes in the network, supporting the decentralized concept [13]. It is evident that certain characteristics of the blockchain technology are well-suited for the IoT domain and can help mitigate security concerns.

IV. BLOCKCHAIN SOLUTIONS FOR IOT SECURITY

Given the rapid development of IoT technology, there are numerous challenges and security problems accompanying with the growing number of linked devices. However, blockchain technology offers a promising solution to address these problems. In this section, we will provide a summary of previous studies and research that highlights blockchain as the most effective approach to resolving security issues in the IoT, as discussed in section III.

*A. **Blockchain for solving Perception layer Security issues***

The perception layer of IoT includes RFID, WSNs, and RSN security, utilizing various technologies such as ZigBee, sensor nodes, and sensor gateways. The security of RFID and WSN technologies is crucial due to their use in sensitive applications in fields such as technology and medicine [14]. RFID technology is considered revolutionary in the embedded communication model as it simplifies the configuration of microprocessors for wireless communication. There are two categories of RFID tags: active and passive[15]. Active tags have a power source while passive tags do not and rely on the reader's inquiry signal to start communication. They are commonly used in applications such as road toll tags and bank cards and have virtually unlimited lifespans. Potential threats to RFID include tracking, repudiation, DoS, spoofing, data freshness, self-organization, time management, secure localization, accessibility, survivability, robustness, and counterfeiting [5]. Blockchain technology has emerged as a promising solution to address some of the security problems in RFID. In [16] the authors propose a secure lightweight blockchain-enabled RFID-based validation protocol for supply chains in 5G MEC environments. This protocol utilizes AI approaches for better forecasts, analysis, and delivery of data authenticity and reliability via blockchain. While, in [17] the authors propose a novel blockchain-based mutual validation security protocol for distributed RFID systems. The proposed protocol leverages the distributed, authenticated, and synchronized ledger of blockchain to accomplish secure authentication and maintain confidentiality without third-party intervention.

In [18], the authors identified weaknesses in the ordinary approaches of authentication in IoT and recommended a system based on WSN identity authentication and blockchain technology. They combined blockchain decentralization with the nodes in the IoT structure, creating a hybrid blockchain-based identity authentication scheme for the entire network. In this scheme, public blockchains interconnect with many private blockchains, each of which exists among the cluster heads of a WSN, addressing authentication security issues in WSN.

B. Blockchain for solving Transportation layer Security issues

The transportation layer has three sub-layers: the core network, the access network, and the local area network, each with distinct functions. It comprises a mix of heterogeneous networks. WiFi networks present security risks such as network traps and network attacks. A solution proposed in. In [19], involves using blockchain to address access control issues in wireless networks. This method eliminates the need for users to disclose their identity while ensuring that they are trustworthy and enabling decentralized anonymous access control to network resources.

C. Blockchain for solving application layer Security issues

The authors proposed a blockchain-based design for IoT cloud computing that utilizes distributed access control and data management. Unlike traditional trust models that delegate data access control to a central, reliable authority, the proposed design enables users with data ownership and is tailored for IoT data flows, ensuring secure data sharing. Another proposal is a framework that combines the Internet of Things (IoT) and fog computing, as presented in. In [6], the authors proposed a blockchain-based design for IoT cloud computing that utilizes distributed access control and data management. Unlike traditional trust models that delegate data access control to a central, reliable authority, the proposed design enables users with data ownership and is tailored for IoT data flows, ensuring secure data sharing. Another proposal is a framework that combines the Internet of Things (IoT) and fog computing, as presented in [20]. This framework utilizes blockchain technology to facilitate communication, transfer, and exchange of data between IoT devices at the edge of the network. The communications in the proposed framework follow a point-to-point network architecture, with certain IoT devices called Miners, which authenticate the communications in the network. If the communications are verified, they are added to the blockchain and sent to the network. A smart home is a type of residence that utilizes Internet of Things (IoT) technology to provide its inhabitants with luxurious amenities, enhanced security, improved accessibility, and an overall better quality of life. The IoT serves as the foundation of a smart home network, connecting various smart devices such as smartphones and wearables. However, smart home systems are not without their challenges, and several studies have suggested that blockchain technology could be a hopeful solution to address these security threats. Authors in [21] proposed a novel blockchain instantiation that eliminates Proof of Work (POW) and instead relies on a classified structure and distributed trust to enhance security and confidentiality while being more suitable for IoT. Their proposal was demonstrated in the context of a smart home. Furthermore, in [22] the authors highlighted the potential of blockchain in revolutionizing traditional smart home applications, leveraging its key features of decentralization, immutability, security, and anonymity. A healthcare collaboration platform facilitates communication among healthcare units such as doctors, patients, labs, suppliers, nurses, and authorities. However, ensuring secure interconnections between various entities can be challenging. In [23], The Pseudonym Based Encryption with different Authorities (PBE-DA) protocol, introduced by the authors, employs blockchain technology to achieve complete privacy for Electronic Health Records (EHRs) of patients and anonymous access to data from cloud providers in e-health platforms. PBE-DA offloads the logic for key creation and verification from IoT devices to the associated gateway, relieving the IoT node from the computational burden of generating cryptographic data

In [6], authors proposed a blockchain-based layered trust architecture for IoT, recognizing that blockchain mechanisms alone cannot guarantee data reliability at the source. The architecture comprises three main layers: the data layer, the application layer, and the blockchain layer.

V. Conclusion

In conclusion, the IoT has revolutionized the way we interact with our environment, but with its increased utilization, security and privacy have become critical concerns. This paper has shed light on some of the major security challenges in IoT, including those related to the application layer, perception layer, and network layer. However, blockchain technology has shown great potential for addressing these challenges by providing secure and decentralized communication and data management. With the ability to guarantee the integrity and the data confidentiality, blockchain has emerged as a promising solution for securing IoT. As such, further research in this area is necessary to develop more robust and secure IoT systems that can be trusted to handle sensitive information.

References

[1] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” in Procedia Computer Science, 2018, vol. 132, pp. 1815–1823, doi: 10.1016/j.procs.2018.05.140.

[2] G. Aggarwal, N. Mishra, and B. Pinkas, “Secure computation of the median (and other elements of specified ranks),” J. Cryptol., vol. 23, no. 3, pp. 373–401, 2010, doi: 10.1007/s00145-010-9059-9.

[3] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014, doi: 10.1016/j.jnca.2014.01.014.

[4] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[5] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and

challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[6] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in CCSW 2017 - Proceedings of the 2017 Cloud Computing Security Workshop, co-located with CCS 2017, Nov. 2017, pp. 45–50, doi: 10.1145/3140649.3140656.

[7] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: State of the art," Stud. Syst. Decis. Control, vol. 36, pp. 55–75, 2016, doi: 10.1007/978-3-319-22168-7_3.

[8] J. Wang, S. Bin, Y. Yu, and N. Xinxin, "Distributed Trust Management Mechanism for the Internet of Things," vol. 350, pp. 2463–2467, 2013, doi: 10.4028/www.scientific.net/AMM.347-350.2463.

[9] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78–85, 2017, doi: 10.1109/MCOM.2017.1700041.

[10] S. Www, "S ato shi N a k a m oto A Peer-to-Peer Electronic Cash System," 2020.

[11] G. Zyskind and A. S. Pentland, "Decentralizing Privacy : Using Blockchain to Protect Personal Data," 2015, doi: 10.1109/SPW.2015.27.

[12] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Jun. 2019, doi: 10.6028/NIST.IR.8202.

[13] K. Fan et al., "Blockchain-based secure time protection scheme in IoT," IEEE Internet Things J., vol. 6, no. 3, pp. 4671–4679, Jun. 2019, doi: 10.1109/JIOT.2018.2874222.

[14] G. H. Alzeer, G. S. Aljumaie, and W. Alhakami, "Security and Threats of RFID and WSNs: Comparative Study," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 5, pp. 276–285, 2021, doi: 10.14569/IJACSA.2021.0120534.

[15] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[16] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," IEEE Trans. Ind. Informatics, vol. 16, no. 11, pp. 7081–7093, 2020, doi: 10.1109/TII.2019.2942389.

[17] S. Wang, S. Zhu, and Y. Zhang, "Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems," Proc. - IEEE Symp. Comput. Commun., vol. 2018-June, pp. 74–77, 2018, doi: 10.1109/ISCC.2018.8538567.

[18] Z. Cui et al., "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," IEEE Trans. Serv. Comput., vol. 13, no. 2, pp. 241–251, 2020, doi: 10.1109/TSC.2020.2964537.

[19] A. A. Brincat, A. Lombardo, G. Morabito, and S. Quattropani, "On the use of Blockchain technologies in WiFi networks," Comput. Networks, vol. 162, 2019, doi: 10.1016/j.comnet.2019.07.011.

[20] T. Alam, "IoT-Fog: A Blockchain-based Middleware Framework for Communication Security in the Internet of Things Tanweer Alam. " IoT-Fog: A Blockchain-based Middleware Framework for Communication Security in the Internet of Things," 2019.

[21] Ali Dorri∗ and and P. Gauravaram, Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 2017.

[22] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," Comput. Electr. Eng., vol. 83, no. 2020, p. 106585, 2020, doi: 10.1016/j.compeleceng.2020.106585.

[23] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," Procedia Comput. Sci., vol. 141, pp. 159–166, 2018, doi: 10.1016/j.procs.2018.10.162.