A REVIEW OF THE INTERNET OF THINGS SECURITY ISSUES

Shameer M., L. Gnanaprasanambikai*

ABSTRACT

In the age of digital transformation and interconnected devices, security aspects of the Internet of Things (IoT) have been considered a critical area. IoT devices span various domains, ranging from personal assistance to Industrial IoT; therefore, ensuring the security and privacy of the IoT environment has become paramount. This paper provides a concise overview of security, emphasizing various aspects, starting with a discussion of IoT architecture and components, security implications of IoT, various challenges of IoT, a comprehensive framework for IoT, case studies of vulnerabilities in IoT, and finally, future trends and research directions with respect to IoT have been discussed.

Keywords : Internet of Things, Security, Challenges, Security Framework and Vulnerabilities

I. INTRODUCTION

The Internet of Things is a prominent transformative technology that has modernized the way people interact with and observe the world around us. It is considered one of the most influential technologies in the 21st century. Technically, it is defined as a vast network of interconnected physical devices, objects, sensors, and other IoT-enabled devices [1]. All these devices are capable of interacting with the external environment, collecting information from it, and then processing and exchanging that information with the help of the internet. It enables person-to-person, person-to-device, and device-to-device communications [2]. The term 'Things' represents both logical and physical entities, incorporating anything from everyday personal assistants and household appliances to industrial and environmental applications [3].

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
* Corresponding Author

At its core, IoT leverages the strength of the internet to ensure and enable continuous communication among things, allowing them to collaborate on information so they can make decisions automatically and perform tasks without human intervention [4][5]. The interconnected features of IoT open up various application domains, including agriculture, healthcare, transportation, automobile industries, smart cities, and manufacturing, to name just a few. The data generated from the IoT environment ranges from simple temperature readings to complex data like machine-generated and environmental data. IoT comprises various key components, including Radio Frequency Identification (RFID), sensors, middleware technologies, cloud services, and wireless sensor networks. Communication technologies like 5G, Zigbee, Wi-Fi, cellular services, and Bluetooth play a major role in IoT [6-9].

IoT has the potential to improve efficiency, enhance decision-making, reduce costs, and enrich the quality of life for individuals and societies. As IoT continues to evolve, it has the potential to reshape industries and our day-to-day lives. However, it also presents considerable challenges such as security, privacy, energy efficiency, interoperability, scalability, and more. Security concerns, in particular, are receiving more attention among researchers compared to other challenges, as IoT involves confidential and sensitive information [10].

The rest of the paper discusses the security aspects of IoT and delves into the topic accordingly."

II. IOT ARCHITECTURE AND COMPONENTS

IoT consists of a complex ecosystem consisting of numerous interconnected components that collaborate with each other. They are capable of collecting information from the external environment. After collecting it, they process and exchange the information among themselves to perform

specific tasks. These aforementioned activities are executed with the help of components involved in IoT. Moreover, the architecture of IoT assists in carrying out these activities. The architecture and components of IoT provide a better understanding of the security challenges associated with IoT [11—14]. The following section discusses IoT architecture.

A. IoT Architecture- An overview

IoT comprises a layered architecture that provides a better conceptualization. It helps in understanding the flow of data across layers and various controls among networks, devices, and cloud services. The figure.1 depicts the underlying architecture of IoT. The IoT architecture consists of the following layers:

1) Perception Layer: This layer comprises actuators, IoT devices, and sensors. It is considered the lowest layer and is primarily responsible for observing the external environment, sensing, and collecting data generated from it.

2) Network Layer: This layer consists of network devices, protocols, and network-enabled devices used for communication. It includes Routing Protocols for Low Power Lossy Networks (RPL), LoRaWAN, Cellular Networks, 5G, Wi-Fi, Zigbee, and more. The main role of this layer is to provide the communication infrastructure for sending and receiving data among IoT devices.

3) Middleware Layer: The primary purpose of this layer is to preprocess data, filter it, and route it before transmitting it to cloud platforms and other services. Essentially, it acts as a channel between the application layer and IoT devices.

4) Application Layer: This layer primarily provides a user interface and includes software services and applications that can interact with IoT devices deployed in the IoT environment. Additionally, this layer performs data analytics and data storage.

5) Business Layer: Decision-making, business logic, and user interactions occur at this top layer. It delivers valuable information to users and organizations and encompasses various services and business logic.

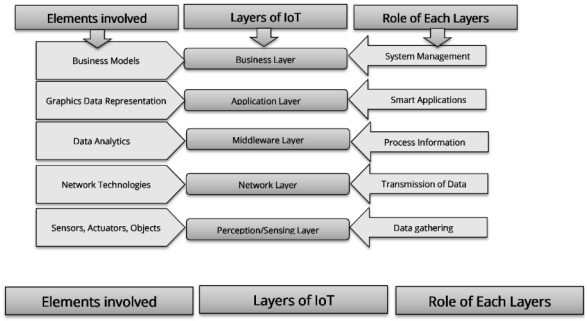

Figure 1. The underlying architecture of IoT

III. KEY COMPONENTS OF AN IOT ECOSYSTEM

The following section discusses the key components of the IoT ecosystem. Understanding the functions. and roles of these components is highly relevant and important before securing the IoT [15-17].

The following Figure 2 depicts the key components of IoT Ecosystem. The components include:

A. Key Devices (Actuators and Sensors):

Sensors are used to sense and collect data from the external environment, while actuators are employed to take appropriate actions based on commands received from the external environment. These devices are typically resource-constrained and available in various forms in the market. Without proper protection, they are vulnerable to various attacks.

B. Communication Protocols:

In IoT, each layer relies on protocols that serve as the core of communication. These protocols ensure connectivity and communication among IoT devices, cloud services, and various gateways. Examples of such protocols include Hyper Text Transfer Protocol (HTTP), AMQP, CoAP, MQTT, RPL, and more. Data transmission occurs through these protocols, and they must be protected to prevent threats, tampering, eavesdropping, and other security violations.

C. Cloud Services and Platforms:

Cloud platforms are third-party platforms that provide storage, processing, and management of the vast amount of data generated by IoT devices over time. Cloud services must

be protected from cyber-attacks due to the sensitive information they handle. Additionally, proper security measures are necessary for data stored in local clouds.

D. Data Storage and Analytics:

Effective analytics and storage solutions are crucial for gaining insights from the data generated within the IoT environment. Every piece of data stored and processed in IoT is important, necessitating the implementation of data protection regulations to ensure confidentiality, integrity, availability, and other security requirements.

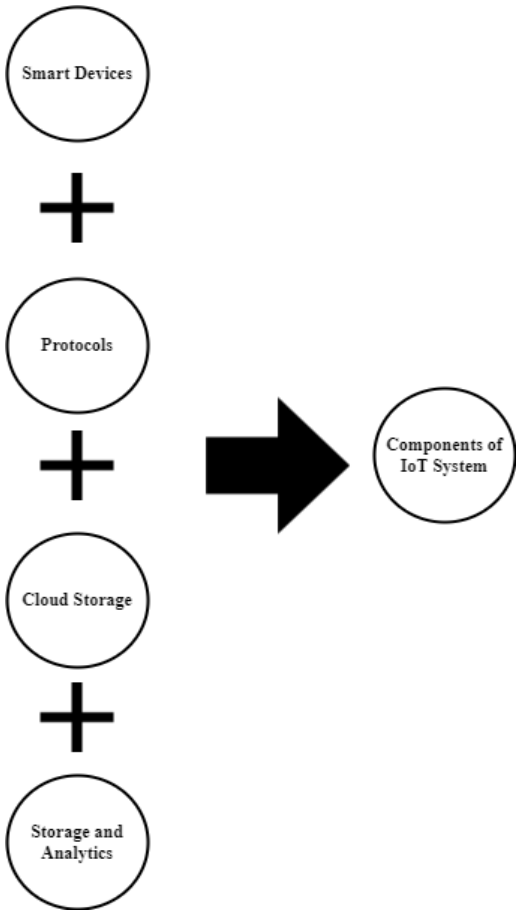

Figure 2. Key Components of IoT Ecosystem

IV. SECURITY ALLEGATIONS AT EACH COMPONENT LEVEL OF IOT

The components of IoT have their own security implications [18-21]. Herein, some of them are discussed.

A. IoT Devices: Typically, IoT devices are placed in an open and shared wireless environment; hence, these devices are vulnerable to various kinds of attacks, including firmware tampering, physical attacks, eavesdropping, unauthorized access, and more. Common security measures used here include firmware integrity checks, device authentication and authorization, and bootstrapping.

B. Communication Protocols: Protocols must be secured to prevent the opening of the gateways for various kinds of attacks, including Black hole attacks, Man-in-the Middle attacks, Replay attacks, Wormhole attacks, Sinkhole attacks, and Data interception. Effective authentication mechanisms, encrypted security mechanisms, hash functions, Intrusion detection mechanisms need to be implemented.

C. Cloud Services: Effective and robust practices must be followed to protect the cloud environment, as it holds sensitive information. Security must be ensured at all levels, including data storage, encryption, and data controls.

D. Data Storage and Analytics: Privacy of data must be ensured during storage and transmission. Techniques like pseudonymization and anonymization should be applied to protect data privacy.

Security violations can occur at every layer of the IoT architecture. Therefore, it is necessary to understand the components and architectural elements of IoT effectively so that security loopholes can be easily addressed. By implementing proper security measures, threats and vulnerabilities can be avoided in the IoT environment.

V. IOT SECURITY CHALLENGES

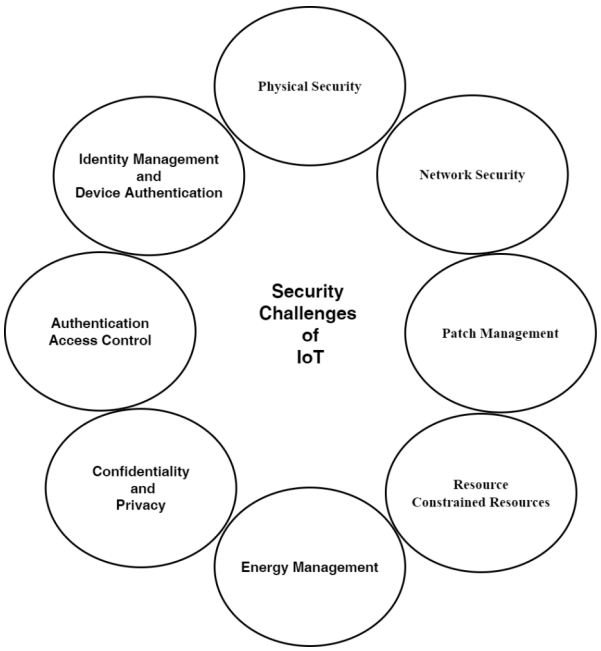

Figure 3 Security Challenges

The above Figure.3 illustrates the security challenges of IoT.

The proliferation of IoT devices and their integration into numerous facets of contemporary life has brought about extraordinary convenience and connectivity among various IoT devices. However, this rapid development also presents a multitude of security challenges that must be addressed to safeguard authentication, authorization, availability, integrity, and confidentiality in the IoT environment. The following section discusses some of the security challenges associated with the IoT ecosystem [21-24].

A. Confidentiality and Data Privacy: Data transmitted over the IoT network is highly sensitive. Ensuring the confidentiality of this data is a non-trivial task and is considered a major concern. Strong security mechanisms such as Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) need to be used when transmitting and storing data.

B. Authentication and Access Control: Authentication must be ensured in an open and shared IoT environment. Communication vulnerabilities can lead to various security breaches. Moreover, unauthorized access to IoT devices can result in security violations. Implementing robust access control and authentication mechanisms is crucial to prevent unauthorized access.

C. Identity Management and Device Authentication: The number of participating devices in the IoT environment is significant, and each device has its unique configuration, leading to the complexity of ensuring authentication. Identity management, including digital signatures, Public Key Infrastructure (PKI), and other unique identifiers, needs to be effectively implemented.

D. Physical Security: Tamper Resistance and Secure Bootstrapping: Physical tampering is possible as IoT devices are often placed in open environments. Hence, IoT devices need to be designed with built-in tamper-resistant hardware to protect against physical attacks. Additionally, secure bootstrapping mechanisms are essential to facilitate initial authentication in the IoT environment.

E. Network Security: Vulnerabilities in Communication Protocols and Intrusion Detection and Prevention: All communication activities rely on communication protocols and technologies such as RPL, Bluetooth, Wi-Fi, Zigbee, and more. Consequently, the possibility of protocol and technology vulnerabilities is high. Regular updates and patching are essential to mitigate security threats. Moreover, the introduction of Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) can help prevent unauthorized access and suspicious activities.

F. Patch Management and Over-the-Air (OTA) Updates: To address vulnerabilities and security-related issues promptly, up-to-date software patches are crucial. However, achieving this is challenging in the IoT environment, which consists of numerous devices with varying configurations deployed in different environments, leading to security concerns.

G. Resource-Constrained Devices: IoT devices are often resource-constrained, with limited energy, processing power, computation speed, and memory. Applying complex

security algorithms such as cryptography, hash functions, and key management can lead to security violations. Therefore, lightweight cryptographic algorithms and trust management-related algorithms can be applied to manage resources effectively.

H. Energy-Efficient Security Protocols: Again, due to limited energy resources in IoT devices, the application of complex algorithms involving extensive computational activities necessitates the use of efficient energy management protocols to maintain energy levels.

VI. SECURITY FRAMEWORK

Developing a unique security framework for IoT is challenging due to the vulnerabilities and challenges associated with IoT. This framework must consist of best practices, protocols, and standards, as well as security measures to ensure security requirements such as availability, confidentiality, integrity, and privacy in the IoT environment [25-31]. In this section, we discuss the security framework of IoT devices.

A. Device Security: Device security is of paramount importance in the IoT environment, given the numerous devices working together to accomplish tasks.

1. Device Authentication: Authentication ensures the initial level of security for any device in the environment. Effective and strong authentication mechanisms, such as certificates, biometrics, key management, and cryptographic techniques, are used to ensure device authentication in the IoT environment.

2. Firmware Updates and Secure Boot: Booting IoT devices securely and regularly updating firmware ensure device security and integrity. Secure storage of boot images and updates with digital signatures are essential.

3. Hardware-Based Security: To safeguard sensitive data and security-related keys, trusted platform modules (TPMs) and Hardware Security Modules (HSMs) are used in IoT.

4. Tamper Resistance: IoT devices are designed to be physically resistant to tampering, providing protection against unauthorized access.

B. Communication Security: The next level of security ensures secure communication among IoT devices, which relies on secure communication protocols.

1. Secure Protocols: Secure data transmission is achieved using authentication and encryption protocols such as MQTT, DTLS, TLS/SSL.

2. Message Integrity: Message authentication codes (MACs) prevent unauthorized modification of sensitive data during transmission, ensuring data integrity.

3. Network Segmentation: Segmenting critical IoT devices and sensitive networks from vulnerable infrastructure can prevent security breaches.

C. Identity and Access Management: Ensuring the right identity of IoT devices and granting them appropriate access prevents security violations.

1. Role-Based Access Control (RBAC): RBAC policies manage access privileges and permissions for devices and users, ensuring that only authorized parties interact with IoT and its resources.

2. Multi-Factor Authentication: Multiple Authentication Factor (MFA) mechanisms, such as passwords, biometrics, smart cards, and other authentication methods, enhance security in the IoT environment.

3. Device and User Provisioning: Secure mechanisms for onboarding and offboarding users and IoT devices are essential in the IoT ecosystem.

D. Data Security: Protecting sensitive data from theft, tampering, and unauthorized access is paramount in the IoT environment.

1. Encryption: Encryption algorithms safeguard data in IoT repositories, protecting against device theft and data breaches.

2. Data Pseudonymization and Anonymization: These techniques minimize user identity disclosure and privacy risks.

3. Secure Data Transfer: Secure APIs and encryption algorithms protect data during transmission between IoT devices and cloud platforms.

E. Incident Response and Security Monitoring: Effective management and monitoring of security violations in and around the IoT environment are essential for consistent performance.

1. Threat Detection: Prediction algorithms, such as machine learning and anomaly detection, help detect misbehaving, malicious, or suspicious devices in advance, preventing security breaches.

2. Event Management and Security Information: These systems screen, analyze, and control security violations, providing immediate responses to threats and detecting anomalies.

3. Incident Response Plan: An outlined procedure, including incident response plans and regular testing, is crucial for handling data breaches and security violations.

F. Regulatory Compliance: Third-party audits and compliance frameworks enhance the security framework's faithfulness to compliance requirements.

1. Third-party Audits: Involving third-party auditors helps assess the security framework and ensures compliance.

2. Compliance Framework: Adherence to IoT security regulations and standards such as ISO/IEC 27001, NIST, HIPAA, and GDPR is essential and should be followed.

G. Privacy Protection: Preserving user privacy is a significant challenge due to the vast amount of data handled by IoT.

1. Data Minimization: Minimizing the collection of unnecessary data from the external environment reduces privacy risks.

2. Data Ownership and User Content: Consent from IoT users regarding data access and processing is necessary, requiring proper communication.

H. Lifecycle Management: Effective management of IoT devices during their lifespan, from deployment to retirement, is crucial.

1. Patch Management: Frequent patch updates are essential to avoid unexpected vulnerabilities, ensuring security.

2. End-of-Life Consideration: Proper decommissioning and disposal are necessary to prevent data theft from retired devices.

I. Education and Awareness: While technologies can protect the IoT environment, user knowledge of these technologies is essential to prevent security violations.

1. User Training: Teaching users, developers, administrators, and all IoT users about potential risks and security best practices is vital.

2. Security Culture: Promoting a culture of security awareness and accountability among society and IoT stakeholders is crucial.

J. Vendors and Supply Chain Security: Evaluating IoT device suppliers and manufacturers for compliance with terms and conditions is essential.

1. Supply Chain Security: Ensuring the security of IoT devices during distribution and manufacturing to prevent unauthorized access and tampering is crucial.

VII. CASE STUDIES WITH VULNERABILITIES

IoT offers various benefits to the world. However, it has also brought numerous challenges. IoT devices are easily exposed to risks and vulnerabilities. In this section, some of the notable vulnerabilities will be discussed. The Mirai Botnet is one of the massive distributed denial-of-service attacks that occurred in October 2016. It targeted Domain Name Systems, resulting in internet outages. The attackers logged in with default usernames and passwords, exploiting IoT devices such as cameras, routers, etc. This happened due to a lack of security updates. From this incident, researchers observed that default usernames and passwords must be changed by both users and manufacturers. Additionally, patches need to be updated regularly [30].

In the year 2010, another malware called Stuxnet was identified. It targeted Iran's nuclear services, where it took control of Supervisory Control and Data Acquisition Systems (SCADA). This malware manipulated the program's logical controls and damaged the physical processes. This malware spread via infected USB drives. After this incident, organizations established a robust air-gapping mechanism to prevent unauthorized external device access. In the year 2015, attackers hacked the navigation and entertainment system of a Jeep Cherokee. They gained access to the braking and steering system of the vehicle. This incident raised awareness that IoT systems within a car should be isolated from other control systems, and software patches must be updated regularly [31].

IoT cameras are also often hacked by attackers. They gain unauthorized access to cameras and threaten users. Usually, this happens because of weak passwords used for camera access, and manufacturers do not provide updates for devices bought earlier. To avoid this, researchers recommend setting stronger passwords, and manufacturers of IoT devices must provide lifetime updates. At present, smart homes are also affected by threats compared to other applications. Attackers gain access to sensors, embedded devices, and smart locks. People may not configure IoT devices properly, and if one device is compromised, it affects all other devices at home. To avoid this, proper training must be given to users of the IoT ecosystem, and IoT manufacturers should provide a secure IoT ecosystem [30] [31].

VIII. CONCLUSIONS

Security in the IoT is a multidimensional and enduring challenge. As IoT continues to grow and transform individuals and industries, addressing security-related issues is becoming increasingly critical for both organizations and individuals. With a combination of best practices, the latest technologies, a dedicated framework, and a security-conscious mindset, security violations and risks can be mitigated, allowing us to enjoy the benefits of a safer and more connected future of IoT. In this paper, we discuss the security aspects of IoT. More importantly, we also discuss the challenges associated with IoT and the best practices and solutions to address those challenges. Developing security solutions for lightweight IoT devices will be considered as future work.

REFERENCES

[1] Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In 2017 international symposium on networks, computers and communications (ISNCC) (pp. 1-6). IEEE.

[2] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2021). Security aspects of Internet of Things aided smart grids: A bibliometric survey. Internet of things, 14, 100111.

[3] Bansal, M., Nanda, M., & Husain, M. N. (2021, January). Security and privacy aspects for Internet of Things (IoT). In 2021 6th international conference on inventive computation technologies (ICICT) (pp. 199-204). IEEE.

[4] Suhardi, & Ramadhan, A. (2016). A survey of security aspects for Internet of Things in healthcare. In Information Science and Applications (ICISA) 2016 (pp. 1237-1247). Springer Singapore.

[5] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. In 2014

IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.

[6] Ray, A. K., & Bagwari, A. (2020, April). IoT based Smart home: Security Aspects and security architecture. In 2020 IEEE 9th international conference on communication systems and network technologies (CSNT) (pp. 218-222). IEEE.

[7] Williams, P., Dutta, I., Daoud, H., & Bayoumi, M. (2020, June). Security aspects of internet of things–a survey. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[8] Mehnen, J., He, H., Tedeschi, S., & Tapoglou, N. (2017). Practical security aspects of the internet of things. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, 225-242.

[9] Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018, August). Securing the internet of things (IoT): A security taxonomy for IoT. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 163-168). IEEE.

[10] Cvitić, I., & Vujić, M. (2015). CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT. Annals of DAAAM & Proceedings, 26(1).

[11] Avila, K., Jabba, D., & Gomez, J. (2020). Security aspects for RPL-based protocols: A systematic review in IoT. Applied Sciences, 10(18), 6472.

[12] Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., & Xiong, L. (2019). A survey on security aspects for 3GPP 5G networks. IEEE communications surveys & tutorials, 22(1), 170-195.

[13] Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors, 23(2), 788.

[14]Mandal, N., & Uddin, G. (2022). An empirical study of IoT security aspects at sentence-level in developer textual discussions. Information and Software Technology, 150, 106970.

[15] Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2023). The survey and meta-analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT. Neurocomputing, 126533.

[16] Khare, A., Rajput, P. K., Pal, R., & Aarti. (2022, September). A Comparative Analysis on Computational and Security Aspects in IoT Domain. In International Conference on Advances in Data-driven Computing and Intelligent Systems (pp. 573-584). Singapore: Springer Nature Singapore.

[17] Alotaibi, Y., & Ilyas, M. (2022). Security risks in internet of things (IoT): a brief survey. In Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2022) (pp. 1-5).

[18] Aruna, P., Devi, S. G., Chandia, S., & Poongothai, M. (2023, January). Security Aspects in IoT: Challenges and Countermeasures. In International Conference on Smart Computing and Communication (pp. 397-403). Singapore: Springer Nature Singapore.

[19] Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 206, 108771.

[20] Liang, Wei, et al. "TBRS: A trust-based recommendation scheme for vehicular CPS network." Future Generation Computer Systems 92 (2019): 383-398.

[21] Alshehri, Mohammad Dahman, and Farookh Khadeer Hussain. "A comparative analysis of scalable and context-aware trust management approaches for internet of things." Neural Information Processing: 22nd International

Conference, ICONIP 2015, November 9-12, 2015, Proceedings, Part IV 22. Springer International Publishing, 2015.

[22] Tan, Lu, and Neng Wang. "Future internet: The internet of things." 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Vol. 5. IEEE, 2010.

[23] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82 (2018): 395-411.

[24] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[25] Giusto, Daniel, et al., eds. The internet of things: 20th Tyrrhenian workshop on digital communications. Springer Science & Business Media, 2010.

[26] Kothmayr, Thomas, et al. "DTLS based security and two-way authentication for the Internet of Things." Ad Hoc Networks 11.8 (2013): 2710-2723.

[27] Brachmann, Martina, et al. "Security considerations around end-to-end security in the IP-based Internet of things." Workshop on Smart Object Security, in conjunction with IETF83, Paris, France, March 23, 2012. 2012.

[28] Brody, Paul, and Veena Pureswaran. "Device democracy: Saving the future of the internet of things." IBM, September 1.1 (2014): 15.

[29] Kamalinejad, Pouya, et al. "Wireless energy harvesting for the Internet of Things." IEEE Communications Magazine 53.6 (2015): 102-108.

[30] Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. "The Internet of Things—A survey of topics and trends." Information systems frontiers 17 (2015): 261-274.

[31] Harbi, Yasmine, et al. "A review of security in internet of things." Wireless Personal Communications 108 (2019): 325-344.