Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Layered wise Security Challenges and Solution for IoT Architecture

Menka Patel[1], Rajan Patel[2*]
[1] *PhD Scholar, Computer Engineering, Gujarat Technological University, Ahmedabad – 382424, Gujarat, India.*
[2] *Kalol Institute of Technology & Research Center, KIRC, Kalol – 382721, Gujarat, India.*
**Correspondence Author: rgpce21@gmail.com*

ARTICLE INFO

Received: 28 Feb 2025

Revised: 10 April 2025

Accepted: 05 May 2025

ABSTRACT

The Internet of Things (IoT) is transforming industries such as healthcare, smart cities, and industrial automation by enabling seamless device interconnectivity. However, its heterogeneous and resource-constrained nature introduces critical security challenges, including impersonation attacks, malicious node injection, denial-of-service attacks, and data breaches. Existing security mechanisms often fail to address these evolving threats due to IoT's dynamic environment. This paper presents a systematic review of security vulnerabilities in the layered IoT architecture (perception, network, and application layers) and explores lightweight, scalable security solutions such as blockchain authentication, AI-driven anomaly detection, and quantum-resistant cryptography. Unlike prior studies that focus on isolated threats or generic security frameworks, this research provides a structured, layer-wise security assessment and proposes practical mitigation strategies tailored to real-world IoT applications. The findings emphasize the need for energy-efficient, adaptive security frameworks to ensure confidentiality, integrity, availability, and privacy. This study serves as a foundation for future research in autonomous and scalable IoT security mechanisms, bridging the gap between theoretical security models and practical implementation.

Keywords: blockchain authentication, cyber threats, IoT security, layered security architecture, lightweight cryptography

INTRODUCTION

The Internet of Things (IoT) is a novel paradigm that has increasingly integrated into daily life. The IoT includes a collection of heterogeneous devices interconnected via the Internet, such as smartphones, smart cars, smart energy grids, and smart cities. IoT devices are extensively utilized by large organizations, homes, workplaces, and other entities to exchange data and establish network connectivity. The smart home is one of the many applications of IoT. It leverages machine learning and IoT technologies to provide accurate and affordable energy management solutions (Li et al., 2019). Another significant application is sustainable transportation planning and traffic control through intelligent transportation systems (Huang et al., 2021). Additionally, IoT is widely used for digital monitoring in agriculture, healthcare, and environmental ecosystems (Gangwani et al., 2021, Das & Namasudra, 2022). IoT devices facilitate the sharing of sensor data collected through IoT gateways or edge devices. The collected data is either sent to the cloud or analyzed locally. The IoT ecosystem consists of three core components: devices, communication networks, and computing systems that manage data flow.

With advancements in smartphone technology and various sensors, numerous devices can now be connected to the IoT. However, the growing demand for large-scale IoT deployment has led to significant security concerns (Xiang et al., 2012). Attacks and faults in IoT-based critical infrastructures could negate the benefits of IoT without adequate protection (Roman et al., 2011). Moreover, privacy is a crucial aspect of IoT. Many "things" individuals use daily at home and work are now online, implying that private and sensitive information could be exposed (Porambage et al., 2016). Unlike traditional security challenges, privacy concerns in IoT are equally critical. The system's inherent vulnerabilities stem from diverse networking technologies and resource-constrained devices that often rely on basic security and privacy solutions (Porambage et al., 2016). Additionally, IoT solution providers may overlook security

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and privacy due to complexity, time-to-market pressures, or ignorance (Richa, 2020). Security patterns, which are beneficial for non-security specialists, could address this issue effectively (Schumacher et al., 2013, Fernandez-Buglioni, 2013).

Implementing security measures in an IoT system is more complex than in traditional networks due to the large number of nodes and the heterogeneity of devices and protocols. To safeguard data and services in IoT environments, features such as confidentiality, integrity, authentication, access control, availability, and privacy must be ensured (Rekleitis et al., 2010). Although security has become a primary concern, traditional solutions are often incompatible with IoT devices. Consequently, new security solutions tailored to IoT-based applications must be developed. Recent research highlights the importance of security auditing tools and patterns for addressing vulnerabilities in IoT systems, particularly for non-security specialists. Additionally, the absence of timely updates, intrinsic vulnerabilities, and limited computing power in edge devices exacerbate these issues (Canavese et al., 2024).

Existing literature has extensively addressed specific security threats and solutions for IoT; however, there is a need to synthesize these findings into a comprehensive framework. For instance, while (Li et al., 2019) explores security measures for resource-constrained IoT devices, it falls short in addressing emerging threats in rapidly evolving IoT ecosystems. Similarly, the layered security approach proposed in (Rajmohan et al., 2022) identifies attacks but lacks practical, lightweight mitigation strategies. This paper builds upon these works by offering a systematic review of IoT security challenges and identifying specific gaps within layered architectures.

The present study provides a comprehensive analysis of IoT security, with a focus on the application, network, edge, and perception layers. By synthesizing findings from recent advancements, this research identifies vulnerabilities and proposes lightweight, scalable solutions that ensure confidentiality, integrity, authentication, access control, availability, and privacy. In doing so, it addresses critical research gaps and offers actionable insights for securing IoT systems. The study also lays the foundation for future research aimed at developing robust security mechanisms for IoT's rapidly evolving ecosystem. This paper discusses the scope and motivation for IoT security, IoT architecture, security threats in IoT, a comprehensive review of layered architecture security issues, and concludes with future directions.

SCOPE AND MOTIVATION

The Internet and the digital era are pushing the current world, affecting notions of digital life. This is where information and communication technologies have emerged as a trend, offering ideas like wireless control, remote monitoring, and other things that ease the burden on workers and people. Thanks to advancements in network connections, cognitive computing, and wireless communications, the IoT was introduced as a novel and revolutionary technology. With the help of the IoT, billions of electronic devices and things are connected, creating a digital environment that enables people to employ modern cyber technology to sense, analyze, regulate, and enhance antiquated physical manual processes. It has drawn interest from academics and commercial audiences over the past 20 years, broadening the technology's range of scientific applications across numerous industries. The significant advancement in the development of the IoT is shown in **Figure 1.** The IoT market in India is predicted to expand significantly globally in the future year. The United States, Australia, Canada, and China are the primary growing regions for IoT. Furthermore, India's Internet of Things market is expanding, with a surge in smart city efforts and rising adoption of IoT in agriculture and healthcare. The IoT has revolutionized the way we live, work, and communicates. It has made life easier. **Figure 2** shows the past to the future of the number of IoT devices connected worldwide increases. However, it has opened up new avenues for crime, as IoT devices are among the most vulnerable equipment in the world.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

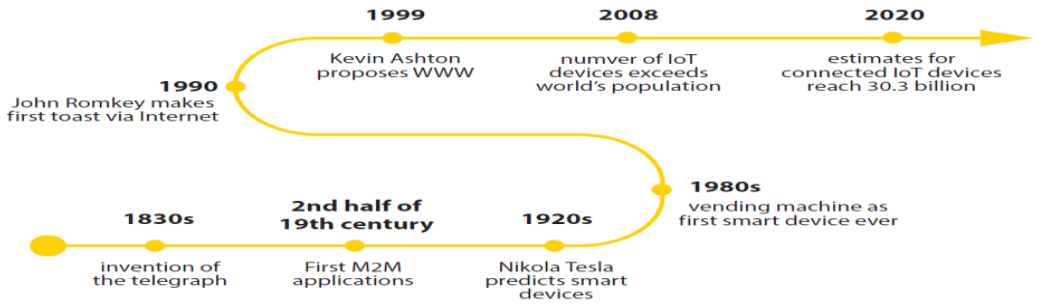

Figure 1: Significant advancement in IoT's development (Vadivelu et al., 2023)

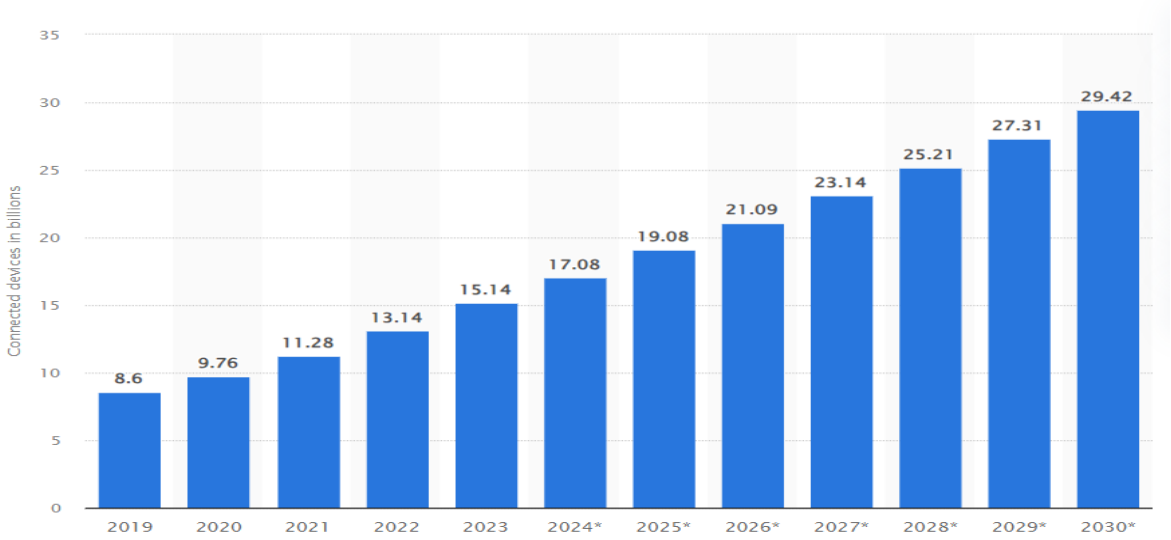

Figure: 2: Number of devices connected with IoT worldwide (Statista, 2024)

With the increases adaption of the IoT in the various sectors such as smart healthcare, smart cities, agriculture, transportation etc. concerns about the security and privacy of IoT data are growing as a result of IoT systems' increased adaptability (Agrawal et al., 2018). Due to their limited resources, the smart devices employed in the Internet of Things architecture are susceptible to many kinds of security threats (Al-Garadi et al., 2020). A single point of failure is major risk when IoT devices connect via a centralized server (Khan & Salah, 2018). It is challenging to create a security model that takes into account the heterogeneity of the Internet of Things architecture since every layer of the architecture has various security problems. Furthermore, security breaches are growing more complex every day.

Common threats of IoT architecture include impersonation, malicious node injection, phishing, physical attacks, jamming, and data leakage (Mohanta et al., 2020). Strong technology is needed to withstand these security breaches. The security system intended to detect these types of assaults needs to meet basic requirements including availability, confidentiality, and integrity. Conventional cryptography algorithms cannot provide sufficient security (Patel and Patel, 2021) for IoT devices due to their high energy consumption and low storage capacity (Roy et al., 2018). Given the continuous advancement of security threats in IoT, developing an effective security model presents a significant challenge.

IOT ARCHITECTURE

After the Internet, IoT is the most significant technology of this generation. In 2010, the number of physically linked devices overtook the number of people, and this trend continues. Due to the diverse nature of IoT devices, there is no single "construction path" for IoT deployment that applies universally across all use cases.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Nonetheless, the literature presents several architectures. One approach categorizes an IoT architecture into three layers according to their distinct characteristics (Gou et al., 2013, Li, 2017, Sethi & Sarangi, 2017 , Hassan, 2019, Burhan et al., 2018). Some methods break down the architecture into four distinct layers (Burhan et al., 2018, Bujari et al., 2018, Zhang et al., 2019) and the five-layer architecture (Burhan et al., 2018). An alternative method for describing and constructing IoT networks follows the Fog computing paradigm, which also uses three layers but categorizes devices differently as edge, fog, and cloud computing (Zhang et al., 2018). For the rest of this work, the most widely adopted three-layer architecture has been selected for its intuitive structure. The layers are as following **Table 1**:

Table 1: Components of three-layered IoT architecture

Layer	**Description**	**Components(**HaddadPajouh et al., 2021)
Application Layer	• Provide a range of services to different application • It outlines the various applications where IoT can be implemented.	• Middleware, Communication Protocols, REST APIs, Cloud services, IoT applications such as smart cities & homes, smart grid, smart healthcare etc.
Network Layer	• Connecting smart things, network devices and sensors • Used to transmit and process sensor data	• RFID, ZigBee, Bluetooth, GPRS, Wi-Fi, internet security protocols, Cloud back-end
Perception layer	• Sensors detect and collect environment information • Sensors detect physical parameters or identify other objects within the environment.	• Sensors, Mobile devices, IoT gateway, IoT nodes

Application layer:

This is topmost layer which is consists of middleware and applications. Depending on the use case, this layer may include cloud computing components, application integrations, resolution services, or web services. Its primary function is to deliver application-specific services to the user (Li, 2017, Sethi & Sarangi, 2017, Hassan, 2019).

Network Layer:

The middle layer is the network needed to transfer data between servers, other network devices, and Internet of Things devices. Different network types, such as computer networks, wireless networks, and mobile communication networks, use various protocols (E.g., ZigBee or CoAP) depending on the use case (Li, 2017, Sethi & Sarangi, 2017 , Hassan, 2019, Stiller et al., 2020). This layer is also known as the Communication Layer since it is in the process of facilitating communication between the many devices and services involved.

Sensing (or Perception) Layer:

The physical layer, includes all IoT devices (such as sensors, RFID readers or tags, and gateways), and it is the lowest layer. It frequently involves actuators and sensors that are integrated into the environment (Li, 2017, Sethi & Sarangi, 2017, Hassan, 2019). This layer is also known as the Hardware Layer because it primarily involves the integration of hardware components.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SECURITY THREATS IN IOT

One of the key considerations in the creation of IoT devices is security. All of the sensors and actuators connected to an IoT device will become vulnerable to attack. It is recommended to replace all of the hardware components and sensors in such circumstances (Mohanta et al., 2019). It is not practical to replace the compromised devices in real-time applications due to the high cost and work involved. Creating a security architecture that can get around this restriction with conventional techniques like encryption, user authentication, and access control is difficult. Figure 3 shows the classification of IoT security threats. IoT security concerns can be roughly classified as follows: impersonation attacks, access control (Jiang et al., 2023), eavesdropping attacks (Fan et al., 2021), Denial of Service (DoS) attacks, and routing attacks (Almeghlef et al., 2023). The main objectives of IoT security are to safeguard privacy, ensure confidentiality, maintain integrity, authenticate users and devices, and guarantee availability. Despite these goals, IoT devices and systems frequently face vulnerabilities to security threats.

According to a Hewlett-Packard study, a deficiency in security objectives inside the system results in "some" security vulnerabilities in about 70% of generic IoT technologies, such as unencrypted data transmissions or relatively simple passwords (Kolias et al., 2015, OWASP, 2018).

Confidentiality: Secret data must be protected from unauthorized exposure while being transported or stored (Lu & Da Xu, 2018).

Integrity: Throughout its exchange, transmission, storage, and processing, it must guarantee that the data or message remains intact, without being altered, modified, or destroyed.

Availability: The system and its services must be accessible when required. Availability, therefore, denotes the probability that a system (or component) is functional at a specific time. According to (Pokorni, 2019), this encompasses both reliability—meeting specific performance criteria in a given context—and maintainability— the capability to detach, repair, and modify components without disrupting service or exceeding established limits.

Authentication and Authorization: Before granting access to restricted resources like sensitive information, sensing devices, users, and gateway nodes must be authenticated, ensuring their identities are validated. It must be confirmed that they are who they claim to be (El-Hajj et al., 2019). Once identification is verified, it is essential to determine whether the entity has the appropriate permissions to access the system's data, resources, or applications. In the IoT context, access to a resource may depend on additional factors, such as the identity of the device's owner, which provides more details about individuals with specific responsibilities, or the location, which identifies whether a user is accessing the device locally or remotely (Kim & Lee, 2017).

Non-Repudiation: No entity should be able to conceal its actions, even if they are harmful yet initially invisible (Das et al., 2018). Nonrepudiation thereby makes sure that no party can argue that a transaction never happened when it actually occurred or vice versa.

Privacy: It is crucial to ensure that individuals' rights regarding the use of personal information are properly addressed throughout the management, processing, storage, and deletion of data. This typically involves complying with contracts, policies, and relevant regulations or laws.

SECURITY ISSUES IN LAYERES IOT ARCHITECTURE

Numerous studies and advancements have been made in the field of the Internet of Things (IoT). However, IoT systems remain vulnerable due to their heterogeneous and resource-constrained nature, leading to various security challenges. These systems are susceptible to multiple attacks and security flaws, necessitating the adaptation of security mechanisms to address threats at each layer of the IoT architecture. This section explores the security vulnerabilities present at different tiers of the IoT protocol stack, identifies associated risks and attacks, and discusses solutions such as device authentication, data integrity, secure communication, network intrusion detection, and API security. **Figure 3** classifies a few security threats on each layer of IoT architecture (Rana et al., 2022) along with the impacted security parameters.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

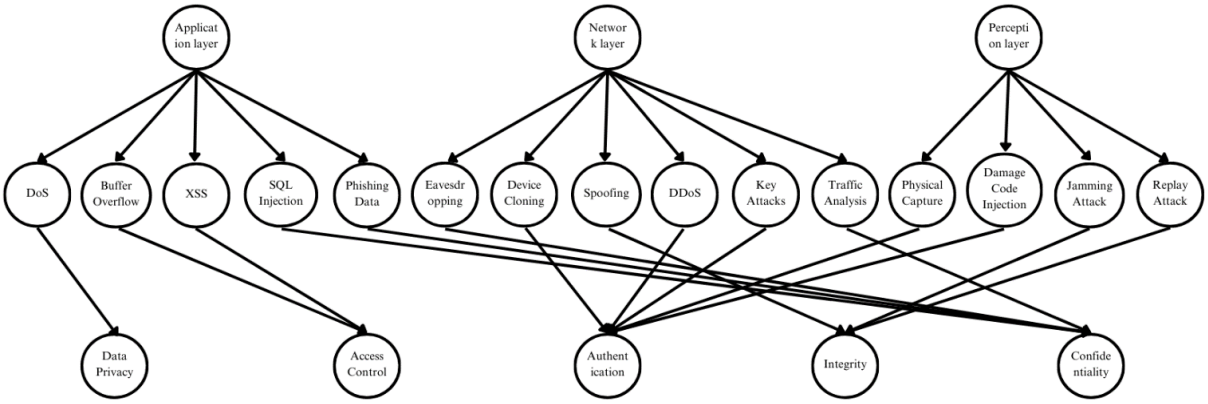

Figure 3: Security attacks and affected security parameters on IoT layer architecture

Perception layer security issues for IoT environment:

The purpose of the Perception Layer is to gather data from the outside world. The perception layer consists of sensors, RFID tags, and IoT nodes that collect and transmit environmental data. It includes a variety of modules for collecting and controlling data, including pressure vibration, sound, and temperature sensors, etc. The processing power limitations and the perception layer's storage capacity lead to security problems and attack risks such as physical tampering, spoofing, and data manipulation attacks. **Table 2** covers the common security issues and their solution of perception layer.

Table 2: Perception layer security issues and solutions

Reference	Issues	Affected layer	Solution
(Rao & Haq, 2018)	Hardware Tempering	Perception layer	For a physically secure design, construct wireless communication antennas that are capable of transmitting over long distances to enhance communication coverage and security
(Yeh et al., 2011)	Fake Node Injection	Perception layer	Authentication: Devices must undergo authentication before establishing a connection with the network.
(Deogirikar & Vidhate, 2017)	Malicious Code Injection	Perception layer	Secure booting and hashing algorithm
(Ahmed et al., 2017)	WSN Node Jamming	Perception layer	IPsec security channel: Encoding data helps ensure data privacy
(Alizadeh et al., 2012)	Sleep Denial Attack	Perception layer	Integrity of Data: Implement an error warning system, utilize detection mechanisms such as parity bits and checksums, and apply cryptographic hash functions
(Gupta &	Device	Perception	Device authentication & authorization: Implement Physical

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Varshney, 2023)	impersonation attacks	layer	Unclonable Function (PUF) based authentication for lightweight security. A recent study proposes a PUF-based protocol that ensures secure authentication and key exchange without requiring continuous internet connectivity.
(Dirin et al., 2023)	Manipulate sensor data	Perception layer	Sensor Data Integrity: Employ a security framework that enhances data and device integrity. Researchers have developed a framework that ensures the trustworthiness of IoT systems by extending trust to data, control, and management planes.

Network layer security issues for IoT environment:

The network layer, also known as the transmission layer, serves as a bridge between the perception and application layers, facilitating data transmission between IoT devices, gateways, and cloud servers using both wired and wireless connections. It plays a crucial role in ensuring seamless communication between networks, smart devices, and network equipment. However, this layer is highly vulnerable to various security threats, including Man-in-the-Middle (MITM), Distributed Denial-of-Service (DDoS), and replay attacks. These threats raise significant concerns regarding the authenticity and integrity of data being transmitted over the network, making robust security measures essential. **Table 3** lists common security problems and fixes for the network layer.

Table 3: Network layer security issues and solutions

Reference	Issues	Affected layer	Solution
(Hummen et al., 2013, Brun et al., 2018, Gope et al., 2018, Pacheco & Hariri, 2018)	Replay Attack	Network layer	To verify packets, define a timestamp and authentication parameter, and use a checksum generated by a hash value
(Malik et al., 2018, Doshi et al., 2018)	Insecure nearest node discovery	Network layer	Authentication through signatures based on encrypted ECC
(Le et al., 2013)	RPL routing attack	Network layer	Authentication can be achieved using a lightweight encryption system, and continuous monitoring of connected devices
(Ahmed & Ko, 2016, Pajouh et al., 2016, Weekly & Pister, 2012)	Sinkhole and Wormhole attack	Network layer	Verification can be performed using trust level management, hash systems, device communication analysis, anomaly detection through Intrusion Detection Systems, management of encoded key and strength of signal monitoring contribute to comprehensive security measures

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(Zhang et al., 2014, Maheshwari & Dagale, 2018)	Sybil attacks	Network layer	Analysis of graph, analysis of user interaction, Applying access control list
(Ahmed & Ko, 2016, Weekly & Pister, 2012, Alvisi et al., 2013, Mohaisen et al., 2011, Wazid et al., 2016)	Authentication and secure communication	Network layer	Lightweight ticket granting system, Using symmetric and asymmetric encryption systems for encrypting packet payload dispatch type values and gathering logs.
(Raza et al., 2014)	End-to-End security	Network layer	Applying an advanced authentication system for authentication and authorization
(Barreto et al., 2015, Ibrahim, 2016, Granjal et al., 2013)	Session Hijacking	Network layer	Light-weight encryption system, Use a secret key for long-term sessions.

Application layer security issue:

The application layer of the IoT architecture defines various domains where IoT technology is implemented, including smart cities, smart homes, smart healthcare, and animal tracking. It is responsible for delivering application-specific services, which depend on the data collected by sensors and may vary based on the application. However, security remains a critical concern in this layer, as it is vulnerable to API vulnerabilities, insecure firmware, and data privacy breaches. Specifically, IoT introduces numerous internal and external hazards and vulnerabilities when it comes to creating a smart home. Devices like ZigBee, commonly used in IoT-based smart homes to implement strong security, often have limited computational power and storage capacity (Kim & Lee, 2017). The common security issues and their solutions at the application layer are presented in **Table 4**:

Table 4: Application layer security issues and solutions

Reference	Issues	Affected layer	Solution
(Granjal et al., 2013, Arvind & Narayanan, 2019, Randhawa et al., 2019)	CoAP security with internet	Application layer, Network layer	Using DTLS, a secure application proxy, and a resource directory

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(Neshenko et al., 2019, Xie et al., 2018, Wang et al., 2018)	Vulnerable Interfaces	Application layer	Verification of password strength and secure coding practices, install application gateway firewall
(Zhou et al., 2018)	Insecure software/ firmware and OS	Application layer, Network layer	Periodic firmware/software updates, use of file signatures, and encryption with validation.
(Venkateswara Reddy et al., 2019, Liu et al., 2014)	Middleware security	Application layer, Transport layer, Network layer	Secure channels for communication with authentication, Defining a security policy, Managing and Distributing keys, Installing secure gateways and M2M (Machine-to-Machine) components, and Implementing lightweight encryption systems
(Zhao et al., 2020)	Data Integrity	Application layer	Implementation of Hashing algorithms, Blockchain technology
(AlJanah et al., 2023)	Data Privacy & Compliance:	Application layer	Implement Homomorphic Encryption for privacy-preserving data processing. Researchers have proposed a multi-factor homomorphic encryption method that facilitates authenticated access to IoT devices while ensuring data privacy.

Table 5 provides a comparative analysis of security threats across different IoT layers, highlighting their impact and corresponding mitigation strategies. The perception layer remains vulnerable to hardware tampering and malicious node injection, while the network layer is often targeted by routing attacks and replay attacks. The application layer faces risks related to API vulnerabilities and firmware exploits, requiring strong security measures.

Table 5: Comparative Analysis of IoT Security Threats and Proposed Solutions

IoT Layer	Security Threats	Impact	Proposed Security Measures	Key Technologies Used
Perception Layer	Malicious Node Injection	Unauthorized device access, data manipulation	Device authentication & authorization	Block chain, Physical Unclonable Function (PUF)
	Hardware Tempering	Sensor data corruption, identify spoofing	Secure hardware design, Temper- resistant chips	Secure Boot, Trusted Platform Module (TPM)
	Data Manipulation Attack	Altered sensor reading, false data injection	Sensor integrity verification, anomaly detection	AI- driven anomaly detection, Hashing
Network Layer	Man-in-the-Middle(MITM)	Data interception, unauthorized access	End-to-end encryption, mutual authentication	TLS, DTLS, Lightweight cryptography

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	Sinkhole & Wormhole attacks	Network traffic redirection, denial of service	Trust management, anomaly based IDS	Machine Learning, Intrusion Detection Systems
	Replay Attacks	Duplicate message injection, session hijacking	Timestamp validation, hashed message authentication	ECC-based authentication, Blockchain
Application Layer	API vulnerabilities	Unauthorized access, data leakage	Secure coding practices, API security policies	OAuth, API Gateway Security
	Data Privacy Violations	Exposure of sensitive information	Homomorphic encryption, access control	Blockchain, Attribute Based Encryption (ABE)
	Firmware Exploits	Code Injection, system takeover	Regular updates, code signing, secure firmware	Secure Boot, Digital Signatures

As shown in **Table 5**, each layer of IoT architecture presents unique security challenges that require tailored mitigation techniques. For example, blockchain-based authentication and lightweight cryptographic methods effectively counter perception-layer threats, while network-layer attacks can be mitigated using anomaly-based intrusion detection systems. The application layer necessitates secure coding practices and API security policies to protect against unauthorized access and data breaches. Implementing these security solutions enhances the resilience of IoT systems, ensuring robust protection against evolving cyber threats.

CONCLUSION

The rapid proliferation of IoT across diverse domains necessitates robust security mechanisms to counter emerging threats. This study provides a layer-wise security analysis of IoT, identifying critical vulnerabilities at the perception, network, and application layers. The research highlights major threats such as device impersonation, routing attacks, data leakage, and denial-of-service attacks, proposing effective countermeasures including lightweight cryptographic techniques, blockchain-based authentication, and AI-driven security frameworks. Unlike traditional security models that fail to accommodate resource-constrained IoT environments; this study presents scalable and energy-efficient security strategies to enhance IoT resilience. However, real-world validation and implementation of the proposed techniques remain a key challenge. Future research should focus on developing adaptive security frameworks that integrate zero-trust architectures, quantum-resistant cryptography, and real-time anomaly detection. With the increasing adoption of IoT in critical sectors such as healthcare, smart cities, and industrial automation, implementing scalable and energy-efficient security solutions is more crucial than ever. Future advancements in AI-driven anomaly detection, quantum-resistant cryptography, and decentralized security models will play a pivotal role in ensuring the long-term security and sustainability of IoT ecosystems.

CONFLICTS OF INTEREST

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

REFRENCES

[1] Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018). Continuous security in IoT using Blockchain. *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. https://doi.org/10.1109/icassp.2018.8462513

[2] Ahmed, F., & Ko, Y. (2016). Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. *Security and Communication Networks*, *9*(18), 5143–5154. https://doi.org/10.1002/sec.1684

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[3] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/comst.2020.2988293

[4] ALIZADEH, M., SALLEH, M., ZAMANI, M., SHAYAN, J., & KARAMIZADEH, S. (2012). Security and performance evaluation of lightweight cryptographic algorithms in RFID. In *Recent Researches in Communications and Computers*. WSEAS Press.

[5] AlJanah, S., Zhang, N., & Tay, S. W. (2023). A Multi-Factor Homomorphic Encryption based Method for Authenticated Access to IoT Devices. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2307.03291

[6] Almeghlef, S. M., Al-Ghamdi, A. A., Ramzan, M. S., & Ragab, M. (2023). Application Layer-Based Denial-of-Service Attacks Detection against IoT-CoAP. *Electronics*, *12*(12), 2563. https://doi.org/10.3390/electronics12122563

[7] Alvisi, L., Clement, A., Epasto, A., Lattanzi, S., & Panconesi, A. (2013). SOK: The evolution of SyBil Defense via social networks. *IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/sp.2013.33

[8] Arvind, S., & Narayanan, V. A. (2019). An Overview of security in COAP: Attack and analysis. *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)* (pp. 655–660). IEEE. https://doi.org/10.1109/icaccs.2019.8728533

[9] Aziz, T., & Haq, E. (2018). Security Challenges Facing IoT Layers and its Protective Measures. *International Journal of Computer Applications*, *179*(27), 31–35. https://doi.org/10.5120/ijca2018916607

[10] Barreto, L., Celesti, A., Villari, M., Fazio, M., & Puliafito, A. (2015). An authentication model for IoT clouds. *ASONAM '15: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015* (pp. 1032–1035). ACM Digital Library. https://doi.org/10.1145/2808797.2809361

[11] Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y. M., Augusto-Gonzalez, J., & Ramos, M. (2018). Deep Learning with Dense Random Neural Networks for Detecting Attacks Against IoT-Connected Home Environments. In *Communications in computer and information science* (pp. 79–89). https://doi.org/10.1007/978-3-319-95189-8_8

[12] Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D. (2017). Standards, security and business models: key challenges for the IoT scenario. *Mobile Networks and Applications*, *23*(1), 147–154. https://doi.org/10.1007/s11036-017-0835-8

[13] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. (2018). IoT elements, Layered architectures and Security Issues: A Comprehensive survey. *Sensors*, *18*(9), 2796. https://doi.org/10.3390/s18092796

[14] Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the edge for Resource-Limited IoT devices. *Sensors*, *24*(2), 590. https://doi.org/10.3390/s24020590

[15] Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*, *89*, 110–125. https://doi.org/10.1016/j.future.2018.06.027

[16] Das, S., & Namasudra, S. (2022). Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. *IEEE Transactions on Industrial Informatics*, *19*(1), 821–829. https://doi.org/10.1109/tii.2022.3167842

[17] Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 32–37. https://doi.org/10.1109/i-smac.2017.8058363

[18] Dirin, A., Oliver, I., & Laine, T. H. (2023). A security framework for increasing data and device integrity in internet of things systems. *Sensors*, *23*(17), 7532. https://doi.org/10.3390/s23177532

[19] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDOS detection for consumer internet of things devices. *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29–35). IEEE. https://doi.org/10.1109/spw.2018.00013

[20] El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of Internet of Things (IoT) authentication schemes. *Sensors*, *19*(5), 1141. https://doi.org/10.3390/s19051141

[21] Fan, Q., Chen, J., Deborah, L. J., & Luo, M. (2021). A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. *Journal of Systems Architecture*, *117*, 102112. https://doi.org/10.1016/j.sysarc.2021.102112

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[22] Fernandez-Buglioni, E. (2013). *Security patterns in practice: Designing secure architectures using software patterns*. Retrieved from http://ci.nii.ac.jp/ncid/BB13156499

[23] Gangwani, P., Perez-Pons, A., Bhardwaj, T., Upadhyay, H., Joshi, S., & Lagos, L. (2021). Securing environmental IoT data using masked authentication messaging protocol in a DAG-Based blockchain: IOTA tangle. *Future Internet*, *13*(12), 312. https://doi.org/10.3390/fi13120312

[24] Gope, P., Amin, R., Islam, S. H., Kumar, N., & Bhalla, V. K. (2017). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems*, *83*, 629–637. https://doi.org/10.1016/j.future.2017.06.023

[25] Gou, Q., Yan, L., Liu, Y., & Li, Y. (2013). Construction and strategies in IoT security system. *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing* (pp. 1129–1132). IEEE. https://doi.org/10.1109/greencom-ithings-cpscom.2013.195

[26] Granjal, J., Monteiro, E., & Silva, J. S. (2013). Application-Layer Security for the WOT: Extending COAP to support End-to-End message Security for Internet-Integrated Sensing applications. In *Lecture notes in computer science* (pp. 140–153). https://doi.org/10.1007/978-3-642-38401-1_11

[27] Gupta, C., & Varshney, G. (2023). A lightweight and secure PUF-Based authentication and key-exchange protocol for IoT devices. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2311.04078

[28] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. https://doi.org/10.1016/j.iot.2019.100129

[29] Huang, Z., Qiao, S., Han, N., Yuan, C., Song, X., & Xiao, Y. (2021). Survey on vehicle map matching techniques. *CAAI Transactions on Intelligence Technology*, *6*(1), 55–71. https://doi.org/10.1049/cit2.12030

[30] Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013). 6LOWPAN Fragmentation Attacks and Mitigation Mechanisms. *WiSec '13: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks* (pp. 55–66). ACM Digital Library. https://doi.org/10.1145/2462096.2462107

[31] Ibrahim, M. H. (2016). Octopus: an Edge-FOg Mutual Authentication Scheme. *International Journal of Network Security*, *18*(6), 1089–1101. https://doi.org/10.6633/ijns.201611.18(6).10

[32] Jiang, W., Li, E., Zhou, W., Yang, Y., & Luo, T. (2023). IoT access control model based on blockchain and trusted execution environment. *Processes*, *11*(3), 723. https://doi.org/10.3390/pr11030723

[33] Khan, M. A., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[34] Kim, H., & Lee, E. A. (2017). Authentication and authorization for the internet of things. *IT Professional*, *19*(5), 27–33. https://doi.org/10.1109/mitp.2017.3680960

[35] Kolias, C., Stavrou, A., & Voas, J. (2015). Securely making "Things" right. *Computer*, *48*(9), 84–88. https://doi.org/10.1109/mc.2015.258

[36] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for Low-Power and lossy networks. *IEEE Sensors Journal*, *13*(10), 3685–3692. https://doi.org/10.1109/jsen.2013.2266399

[37] Li., S. (2017). Chapter 2 - Security Architecture in the Internet of Things. In *Securing the Internet of Things* (pp. 27–48). Syngress.

[38] Li, S., Song, H., & Iqbal, M. (2019). Privacy and Security for Resource-Constrained IoT Devices and Networks: Research Challenges and Opportunities. *Sensors*, *19*(8), 1935. https://doi.org/10.3390/s19081935

[39] Li, W., Logenthiran, T., Phan, V., & Woo, W. L. (2019). A novel Smart Energy Theft System (SETS) for IoT-Based smart home. *IEEE Internet of Things Journal*, *6*(3), 5531–5539. https://doi.org/10.1109/jiot.2019.2903281

[40] Liu, C. H., Yang, B., & Liu, T. (2013). Efficient naming, addressing and profile services in Internet-of-Things sensory environments. *Ad Hoc Networks*, *18*, 85–101. https://doi.org/10.1016/j.adhoc.2013.02.008

[41] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) Cybersecurity Research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/jiot.2018.2869847

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[42] Maheshwari, N., & Dagale, H. (2018). Secure communication and firewall architecture for IoT applications. *2018 10th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 328–335). IEEE. https://doi.org/10.1109/comsnets.2018.8328215

[43] Malik, M., Kamaldeep, N., & Dutta, M. (2018). Defending DDOS in the insecure internet of Things: a survey. In *Advances in intelligent systems and computing* (pp. 223–233). https://doi.org/10.1007/978-981-10-7868-2_22

[44] Mohaisen, A., Hopper, N., & Kim, Y. (2011). Keep your friends close: Incorporating trust into social network-based SyBIL defenses. *2011 Proceedings IEEE INFOCOM* (pp. 1943–1951). IEEE. https://doi.org/10.1109/infcom.2011.5934998

[45] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881–888. https://doi.org/10.1109/jiot.2020.3008906

[46] Mohanta, B. K., Satapathy, U., Panda, S. S., & Jena, D. (2019). A novel approach to solve security and privacy issues for IoT applications using blockchain. *2019 International Conference on Information Technology (ICIT)* (pp. 394–399). IEEE. https://doi.org/10.1109/icit48102.2019.00076

[47] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-Scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702–2733. https://doi.org/10.1109/comst.2019.2910750

[48] Noor, M. B. M., & Hassan, W. H. (2018). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

[49] OWASP Internet of Things Project - OWASP. (2018). Retrieved December 16, 2020, from https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

[50] Pacheco, J., & Hariri, S. (2017). Anomaly behavior analysis for IoT sensors. *Transactions on Emerging Telecommunications Technologies*, *29*(4). https://doi.org/10.1002/ett.3188

[51] Pajouh, H. H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K. R. (2016). A Two-Layer dimension reduction and Two-Tier classification model for Anomaly-Based intrusion detection in IoT backbone networks. *IEEE Transactions on Emerging Topics in Computing*, *7*(2), 314–323. https://doi.org/10.1109/tetc.2016.2633228

[52] Patel, M., & Patel, R. (2021). Improved Identity Based Encryption System (IIBES): a mechanism for eliminating the Key-Escrow problem. Emerging Science Journal, 5(1), 77–84. https://doi.org/10.28991/esj-2021-01259

[53] Pokorni, S. (2019). Reliability and availability of the Internet of things. *Vojnotehnicki Glasnik*, *67*(3), 588–600. https://doi.org/10.5937/vojtehg67-21363

[54] Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, *3*(2), 36–45. https://doi.org/10.1109/mcc.2016.28

[55] Rajmohan, T., Nguyen, P. H., & Ferry, N. (2022). A decade of research on patterns and architectures for IoT security. *Cybersecurity*, *5*(1). https://doi.org/10.1186/s42400-021-00104-7

[56] Rana, M., Mamun, Q., & Islam, R. (2021). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77–89. https://doi.org/10.1016/j.future.2021.11.011

[57] Randhawa, R. H., Hameed, A., & Mian, A. N. (2018). Energy efficient cross-layer approach for object security of CoAP for IoT devices. *Ad Hoc Networks*, *92*, 101761. https://doi.org/10.1016/j.adhoc.2018.09.006

[58] Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2012). Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks*, *7*(12), 2654–2668. https://doi.org/10.1002/sec.406

[59] Reddy, R. V., Murali, D., & Rajeshwar, J. (2019). Context-Aware middleware architecture for IoT-Based smart healthcare applications. In *Lecture notes in networks and systems* (pp. 557–567). https://doi.org/10.1007/978-981-13-7082-3_64

[60] Rekleitis, E., RizomilIoTis, P., & Gritzalis, S. (2010). A holistic approach to RFID security and privacy. *Proceedings of the 1st International Workshop Security of the Internet of Things (SecIoT 2010), Network Information and Computer Security Laboratory*. Retrieved from https://www.nics.uma.es/pub/seciot10/files/pdf/rekleitis_seciot10_paper.pdf

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[61] Richa, E. (2020). IoT: security issues and challenges. In *Smart innovation, systems and technologies* (pp. 87–96). https://doi.org/10.1007/978-981-15-7062-9_9

[62] Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, *44*(9), 51–58. https://doi.org/10.1109/mc.2011.291

[63] Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018). BlockChain for IoT Security and Management: Current prospects, challenges and future directions. *2018 5th International Conference on Networking, Systems and Security (NSysS)* (pp. 1–9). IEEE. https://doi.org/10.1109/nsyss.2018.8631365

[64] Schumacher, M., Fernandez, E., Hybertson, D., & Buschmann, F. (2006). *Security patterns: Integrating security and systems engineering*. Retrieved from http://ci.nii.ac.jp/ncid/BA7615669X

[65] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*, 1–25. https://doi.org/10.1155/2017/9324035

[66] Statista. (2024, September 11). Number of IoT connections worldwide 2022-2033. Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[67] Stiller, B., Schiller, E., & Schmitt, C. (2021). Chapter-12 An Overview of Network Communication Technologies for IoT. In *Handbook of Internet-of-Things*. Cham, Switzerland: Springer.

[68] Vadivelu, V., Chinnasamy, M., Rajendran, M., Chandrasekaran, H., & Rathanasamy, R. (2023). Evolution of Internet of Things (IoT). In *Integration of Mechanical and Manufacturing Engineering with IoT: A Digital Transformation* (pp. 1–39). United States of America: Scrivener Publishing LLC. https://doi.org/10.1002/9781119865391.ch1

[69] Wahab, A., Ahmad, O., Muhammad, M., & Ali, M. (2017). A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, *8*(7). https://doi.org/10.14569/ijacsa.2017.080768

[70] Wang, D., Ming, J., Chen, T., Zhang, X., & Wang, C. (2018). Cracking IoT device user account via brute-force attack to SMS authentication code. *RESEC '18: Proceedings of the First Workshop on Radical and Experiential Security* (pp. 57–60). https://doi.org/10.1145/3203422.3203426

[71] Wazid, M., Das, A. K., Kumari, S., & Khan, M. K. (2016). Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. *Security and Communication Networks*, *9*(17), 4596–4614. https://doi.org/10.1002/sec.1652

[72] Weekly, K., & Pister, K. (2012). Evaluating sinkhole defense techniques in RPL networks. *2012 20th IEEE International Conference on Network Protocols (ICNP)* (pp. 1–6). IEEE. https://doi.org/10.1109/icnp.2012.6459948

[73] Xiang, G., Jianlin, Q., & Jin, W. (2012). Research on trust model of sensor nodes in WSNs. *Procedia Engineering*, *29*, 909–913. https://doi.org/10.1016/j.proeng.2012.01.063

[74] Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data Collection for Security Measurement in Wireless Sensor Networks: A survey. *IEEE Internet of Things Journal*, *6*(2), 2205–2224. https://doi.org/10.1109/jiot.2018.2883403

[75] Yeh, H., Chen, T., Liu, P., Kim, T., & Wei, H. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, *11*(5), 4767–4779. https://doi.org/10.3390/s110504767

[76] Zhang, J., Chen, H., Gong, L., Cao, J., & Gu, Z. (2019). The current research of IoT Security. *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)* (pp. 346–353). IEEE. https://doi.org/10.1109/dsc.2019.00059

[77] Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, *1*(5), 372–383. https://doi.org/10.1109/jiot.2014.2344013

[78] Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. *Future Generation Computer Systems*, *88*, 16–27. https://doi.org/10.1016/j.future.2018.05.008

[79] Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management*, *57*(6), 102355. https://doi.org/10.1016/j.ipm.2020.102355

[80] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616. https://doi.org/10.1109/jiot.2018.2847733

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.