Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Identifying Network Security Issues in the Applications of Internet of Things (IoT)

Assist. Prof. Dr. Hiyam Hatem Jabbar[1]
Assist. Prof. Dr. Satar Habib Mnaathr[2]
Assist. Prof. Dr. Muatamed Abed Hajer[3]
[1] Department of computer science
Collage of computer science and Information Technology
University of Sumer
[2]Department of Biomedical Engineering
Collage of Engineering, University of Thi-Qar
[3]Department of computer science
Collage of computer science and Information Technology
University of Sumer
Thi-Qar 64001, Iraq
[1]Email: hiamhatim2005@gmail.com
[2]Email: satar.hab@utq.edu.iq
[3]Email:m.hajer@uos.edu.iq

ARTICLE INFO

Received:19 Dec 2024

Revised: 17 Feb 2025

Accepted:26 Feb 2025

ABSTRACT

Current network security solutions face challenges in effectively mitigating issues due to the resource constraints, heterogeneity, and dynamic behavior of IoT networks .There is a growing need to enhance measures to counteract cyber threats, as cybercrime becomes more widespread. The importance of network security is highlighted by the constant connectivity of individuals and organizations, leading to the need for robust security methods against evolving threats . In spite of the presence of various security measures, the failure to implement solutions remains a major challenge in addressing cyber threats in wireless networks. Utilizing machine learning and deep learning techniques is essential to fill these gaps and improve security measures in distributed systems. Integration of these advanced technologies can offer built-in intelligence and more efficient strategies to counter constantly evolving cyber threats. This study aims to recognize potential attacks on Internet of Things networks and suggest solutions to tackle them. Security concerns are categorized based on the layers of the Internet of Things architecture. In spite of this classification, the security of the whole system is threatened by problems in these layers. Also, solutions are presented to them. Therefore, in order to carry out future studies we have stressed the need for this type of security solution.

Keywords: Network Security, IoT Architecture, Survey on IoT, Attacks, IoT Layers.

INTRODUCTION

The Internet of Things (IoT) originated in 1999 when Kevin Ashton, a brand manager at Proctor and Gamble, utilized RFID technology to enhance supply chain efficiency. Since then, IoT has expanded to encompass various industries through the use of Internet-connected sensors and tracking devices [1].

Current network security solutions face challenges in effectively mitigating issues due to the resource constraints, heterogeneity, and dynamic behavior of IoT networks. There is a growing need to enhance measures to counteract cyber threats, as cybercrime becomes more widespread [2]. The importance of network security is highlighted by the constant connectivity of individuals and organizations, leading to the need for robust security methods against evolving threats [3]. Despite various security mechanisms, the lack of implementation of solutions remains a significant issue in combating cyber threats in wireless networks [4].

The Internet of Things (IoT) is made up of physical devices that are interconnected via the internet, allowing users to interact with and control them remotely. Its fast expansion in recent times has impacted different industries such as healthcare, residential settings, and infrastructure, establishing IoT as a pivotal technology for the coming years. IoT devices are typically equipped with sensors that collect real-time data for monitoring and decision-making. It is necessary to convert the raw data into a readable format so that users can monitor the status of their devices. This technology can be utilized in various practical applications, including everyday life, by utilizing different devices and physical objects, such as sensors and controls. By connecting devices to a common network, smart homes, cities, and other healthcare systems can be developed and managed. The transmission of data in these circumstances must be secure. The main concern here is how to protect the information from hacking. IoT technology is expected to grow rapidly by 2025, with the number of devices expected to reach 75 billion. Figure 1. Figure 1. Distribution of connected devices worldwide for access technology in 2016-2021. [6].

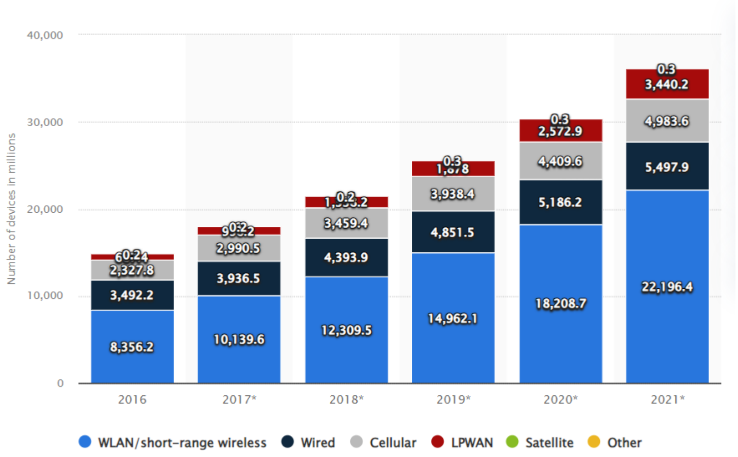


Figure 1. Connected devices worldwide by access technology 2016-2021 [6]

The main goal of IoT is to connect all devices together.This connection will facilitate the exchange of information and lead to the development of intelligent systems. New technologies have made our lives easier and replaced old ones, as evidenced by recent human history. The horse has been replaced by the automobile, kerosene lamps have been substituted by electric lighting, and typewriters are now replaced with word processors. In addition, the intelligent environments created by IoT will provide people with many conveniences, such as washing machines that save time. Therefore, IoT technology will bring about a lasting transformation. The development of IoT may be hampered by obstacles such as IPv6 implementation, sensor power issues, and standards establishment. However, security remains a major concern.

SECURITY FEATURES OF INTERNET OF THINGS

The term "security features" pertains to distinct qualities or features of a system, protocol, or information that play a vital role in safeguarding its security. These properties are essential when creating systems that safeguard data, uphold integrity, and restrict unauthorized access [7]. Security must be addressed in every aspect of our activities, wherever and whenever they occur. As a result, security plays a vital role in IoT development. Without it, it would be challenging to integrate IoT if reliability is not ensured. Digital data relating to people's actions, conversations, movements, and plans is already abundant, and the advent of IoT will only increase this data, potentially exposing sensitive user habits and behaviors. Consequently, inadequate protection of this data could lead to undesirable outcomes.

Compliance Forge released the CIAS framework in 2017 as a replacement for the traditional CIA Triad, which has been the cornerstone of cyber security. With advancements in embedded technologies such as IoT and OT, coupled with the emergence of AI and AAT, the absence of a safety element renders the CIA Triad inadequate for defining the full scope of cyber security [8]. The fundamental security objectives for information, data, and computing services are summarized by these three principles. Along with authenticity, non-repudiation, and privacy, other significant security needs should be considered (refer to Figure 2).

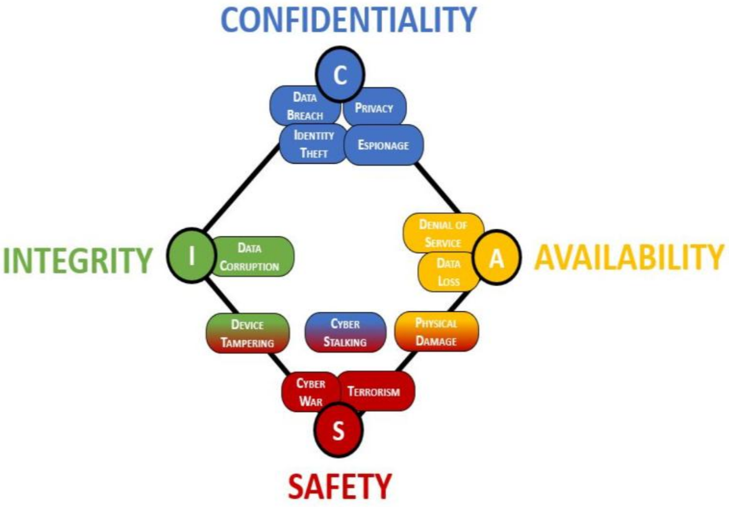


Figure 2. Confidentiality, Integrity, Availability and Safety (CIAS) Model Common security properties include [9]:

Confidentiality guarantees that only authorized individuals can access information, with the goal of safeguarding data from unauthorized access and disclosure.

Integrity guarantees that data remains unaltered and free from tampering by unauthorized parties, and involves maintaining data accuracy and completeness throughout its entire lifecycle.

Availability: Ensures that authorized users have reliable access to information and resources when needed. This property is crucial for maintaining the functionality of systems.

Authorization: Determines what an authenticated user or system is allowed to do. It controls access to resources and ensures that only authorized actions are performed.

Authentication: Verifies the identity of users, devices, or systems before granting access to resources. It ensures that entities are who they claim to be.

Non-repudiation: Requires that a party must admit the authenticity of their signature or acknowledgement in delivering e-mails. Provides substantiation for the legitimacy and provenance of information, frequently employed in legal proceedings.

Auditability: Allows for the monitoring and logging of system activities, enabling the detection of security breaches and the reconstruction of events after an incident.

Accountability: Ensures that actions can be traced to an individual or entity. This property is vital for auditing and monitoring purposes, ensuring that users are held responsible for their actions.

Privacy: Protects personal or sensitive information from unauthorized access or disclosure, ensuring that data is handled according to legal and ethical standards.

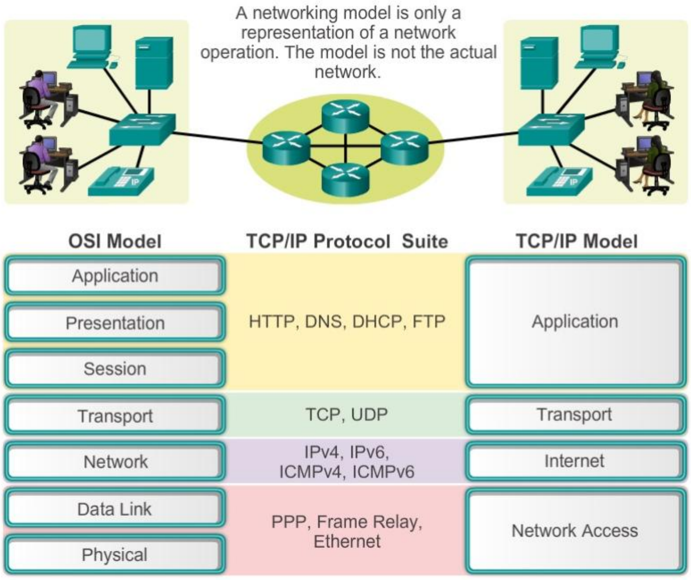
These properties are fundamental in designing secure systems, whether for software, networks, or organizational processes.

INTERNET OF THINGS (IOT) ARCHITECTURE

The TCP/IP model is a layered framework that illustrates how different protocols interact. This model provides several advantages, such as simplifying protocol design by clarifying the information handled at each layer and establishing clear interfaces. It enhances compatibility among products from different vendors, ensuring that changes in one layer do not impact others. Additionally, the layered model offers a standardized way to describe networking functions and capabilities.

THE MAIN BASIC TYPES OF NETWORKING MODELS

A protocol model is a close approximation of essentially the same protocol suite, which comprises an interrelated set of hierarchical protocols that cover all the necessary functions to link the human network to the data network. For example, the activities occurring at each of the different protocol layers in the TCP/IP stack are represented by a model at the top of every layer. In contrast, a reference model establishes consistency between different protocols and network services by defining the actions required at a specific level without prescribing a particular implementation approach. It is important to note that a reference model is not intended to be an implementation specification or to provide a detailed definition of network architecture services.By using a reference model, one can gain an in-depth comprehension of the functioning's and processes that are involved.Most reference models for the Internet are based on the OSI model. It serves as a guide for the design, troubleshooting, and operational specifications of data networks' and TCP/IP network architectures are illustrated in Figure 3.



A networking model is only a representation of a network operation. The model is not the actual network.

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Figure 3. Architectural diagrams of OSI and TCP/IP networks.

IoT technology uses a similar architecture with some differences. The IoT network architecture has four layers, including the application layer (equivalent to analog and virtual reality), the middleware layer (2x optical fiber), the network layer (3x porous optical fiber), and the physical layer. As shown in Figure 4, each of these layers enables the utilization of distinct technologies.

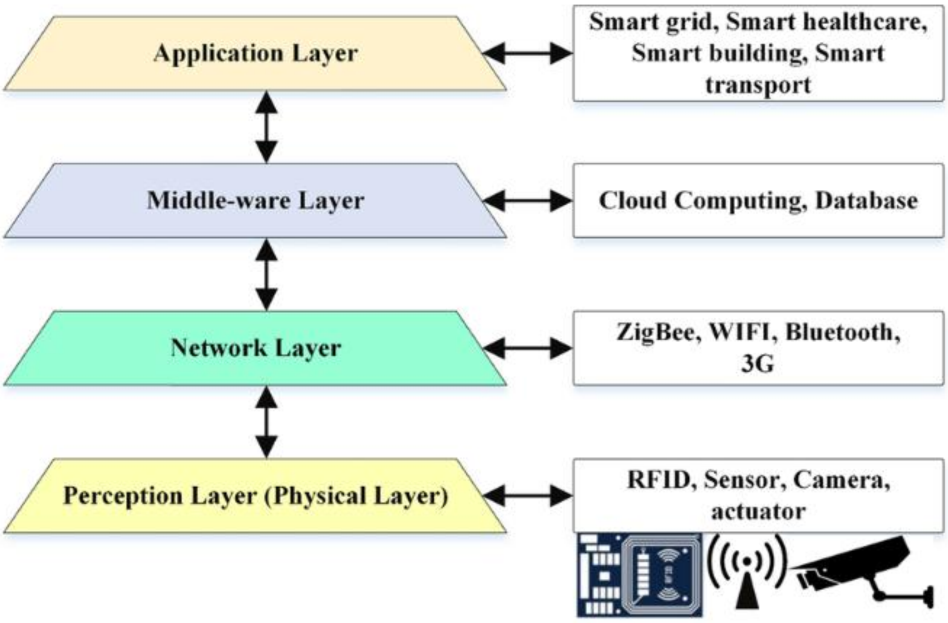

Application Layer
Smart grid, Smart healthcare, Smart building, Smart transport
Middle-ware Layer
Cloud Computing, Database
Network Layer
ZigBee, WIFI, Bluetooth, 3G
Perception Layer (Physical Layer)
RFID, Sensor, Camera, actuator

Figure 4. Four-layer model of IoT Architecture

The architecture of IoT lacks a single universally agreed-upon structure, with various proposed architectures by different researchers. While some advocate for a three-layer architecture, others support a four-layer approach, as in this work, citing the increasingly complex nature of IoT applications. Each layer faces potential threats and security issues, potentially disrupting task execution and leading to undesirable circumstances. It's important to identify possible threats to these layers to ensure the seamless operation of services in smart environments.

MALWARE ATTACKS FOR IOT/CONNECTED DEVICES

In the first six months of 2022, there was a 77% increase in malware attacks targeting IoT/connected devices, according to Sonic Wall. The report also stated that ransomware attacks went down by 23%, while incidents of cryptojacking went up by 30% and intrusion attempts rose by 19%. Cryptojacking involves using the processing power of unauthorized devices to mine cryptocurrency, potentially impacting IoT devices as well [18, 19]. These findings are from the Sonic Wall Cyber Threat Report for the first half of 2022.
%132increase in Encrypted Attacks
%77increase in Malware Attacks on IoT / Connected Devices
%30increase in Cryptojacking Attacks
%19increase in Intrusion Attempts
%11increase in Malware Attacks
%23decrease in Ransomware Attacks

IoT devices have lower processing power than typical IT equipment such as servers or PCs, and they do not run on widely used operating systems like Windows or Linux. Therefore, traditional IT cybersecurity tools are not effective for IoT devices, which leaves them more susceptible to different cyber-attacks, including malware attacks. The graph in Figure 5 of the Sonic Wall report [11] illustrates the monthly increase in global IoT malware volume.

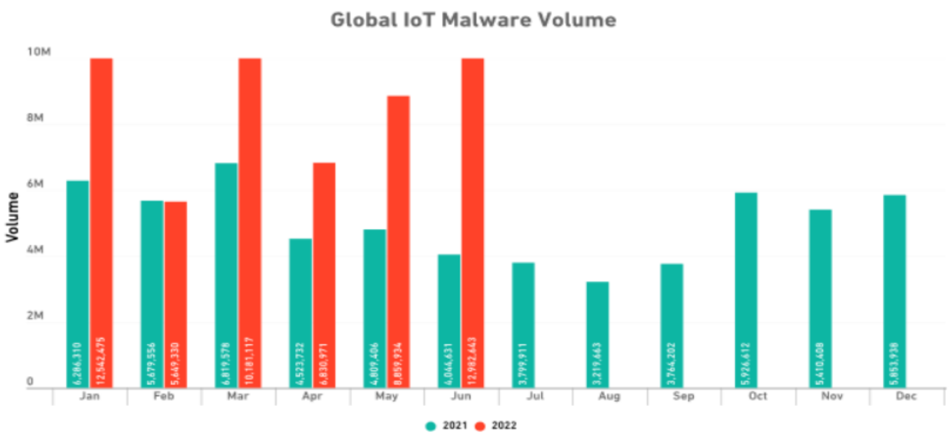


Figure 5. Sonic Wall report shows the global IoT malware volume increase month-by-month [11]

SECURITY ISSUES IOT NETWORK

The varied makeup of IoT, limitations on energy consumption, and varied communication approaches (such as machine-to-machine, human-to-machine, and human-to-human) introduce extra intricacies and raise different security issues. It is crucial, therefore, to evaluate the possible security risks linked with each of these components. In this section, we will explore the security implications of network characteristics, providing an overview of every layer within the IoT framework.

1. *Physical Layer*

This layer contains physical components such as smart objects and power supplies, which are used to collect data at the physical layer. To prevent any unauthorized access or damage, such components must be secured and protected from interference or physical force. Possible scenarios, such as computer theft and server login tampering, as well as the hacking of financial centers at homes and surveillance devices, have been identified by multiple authors. [11,12].IoT sensors involve a vast amount and must be made to endure the elements, as well as other important weather conditions; otherwise, they could pose numerous security threats.

2. *Network Layer*

The network layer contains elements that manage communication and data transmission. At this layer, security and privacy measures are put in place to safeguard data, as outlined in Section II. A significant threat to the network layer is a DoS attack, which is a type of assault that makes services unavailable to legitimate users [13]. This type of attack is typically executed by inundating the server with a high volume of requests, leading to slowdowns or unresponsiveness to subsequent requests, thus disrupting data transfer within the existing infrastructure, which comprises client and server devices. When multiple machines target the same machine, it is referred to as a Distributed Denial of Service (DDoS) attack [14]. The IoT presents an environment highly conducive to DDoS attacks, posing potential disruptions to most smart systems. As mentioned in the previous section (Section III), the Network layer employs various communication technologies such as, WiFi, cellular networks, Bluetooth and Zigbee. Wireless sensor networks are part of these communication technologies and possess the capability to operate without being bound to a specific network topology, making them susceptible to the types of attacks [15]. The network layer faces other common threats, such as the injection of false information, which can trigger inappropriate reactions in a system. Additionally, storage attacks can lead to the alteration of crucial data within a device's memory. Furthermore, gateway attacks involve unauthorized access to nodes [16].

3. *Middle-Ware Layer*

The middleware layer carries data from the sensors collected by each sensor onto an application level and sends control signals to actuators that are connected to IoT devices in the sensing layer. Therefore, security risks such as sniffing attacks, eavesdropping, and data manipulation are often present in the middleware layer [17].

Eavesdropping. Communication between two locations is monitored through eavesdropping. When compromised sensors in healthcare systems or smart homes collect user-generated information, this type of attack is a potential consequence of IoT.

Sniffing attacks. Involve the placement of malicious sensors alongside normal sensors to collect information from them purposefully. The extensive use of smart environment and devices in these systems allows for individuals to be easily recognized, tracked, and profiled. Data transmitted between different communication technologies for example (Wi-Fi, WSN, ZigBee, etc.) may contain **noise**, potentially causing incomplete data transmission. Intruders may exploit this opportunity to modify the data [18].

4. *Application Layer*

The application layer serves as an abstraction layer, defining standard communication protocols and interface methods for hosts in a network, and is integral to the TCP/IP suite and OSI model. It supports advanced systems like smart cities and healthcare, where most user activities occur, making it susceptible to exploitation. Attacks on this layer can lead to application failures and service interruptions, highlighting its vulnerabilities.

A- Modifying node-based applications:- When manipulating node-based applications, situations can occur such as sensors for temperature or humidity displaying constant values when tampered with. Additionally, tampered cameras may show outdated images. In this scenario, the environment could be heated instead of being freezing, and vice versa, all due to the exploitation of malicious codes through the installation of root kits in susceptible applications [20].

B- Security patches cannot be received: The Internet of Things includes a wide range of devices, including sensors, mobile phones, tablets, personal computers, washing machines, refrigerators, microwaves, cars, among others. Developing a patch to fix a harmful code or any other bug that could impact the functionalities of different devices and be compatible with all software would be highly difficult, if not unfeasible [21].

C- Malicious attacks:- The Internet of Things (IoT) is expanding rapidly, with a rising number of devices. Consequently, the spread of a "worm" within the IoT ecosystem could lead to disastrous outcomes. In this situation, devices tainted by worms might disrupt the proper functioning of a system or even cause a complete system crash. By altering DNS settings on IoT devices such as routers, attackers can reroute traffic without authorized users' knowledge or consent. This allows them to steal sensitive information, distribute malware, or conduct phishing attacks. In addition, IoT devices include smartphones and mobile applications. Consequently, it is crucial to consider the various risks associated with mobile devices and not neglect them [21, 22].

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

SUGGESTED SOLUTIONS

Addressing security issues and devising remedies for them, numerous researchers are concentrating on various challenges. Developers are striving to create more secure code, and more and more security testing is needed to detect vulnerabilities in IoT devices and identify potential attacks. Various types of attacks on wireless sensor networks (WSNs) are also under investigation. This section outlines possible measures for enhancing IoT security.

The six primary categories are physical attacks, side channel attacks, environmental attacks, cryptanalysis attacks, software attacks, and network attacks. Among these, network attacks are the most damaging as they can lead to numerous issues in IoT systems and disrupt information exchange between IoT devices and the server. Furthermore, Table.1 [23] provides a comparison of various existing solutions and their effectiveness in optimizing basic security functions and countering the previously mentioned attack types. According to the table, all the solutions are able to prevent software attacks, but none of them can defend against side channel attacks. Additionally, all solutions are optimized for basic security functions except for the last one, which is a data-driven approach for embedded security. The conclusion drawn from the table is that there is a need for improved security solutions in IoT, as most current solutions focus on software attacks and overlook the hardware aspect of the system.

Table 1. Presents A Comparison of Current IoT Security Solutions and Their Impact.

Existing Solutions - Comparison Parameters	**Counter Measures Against Attack**			**Optimization Of The Basic Security Functions**			
	Side-channel	HW-attack	SW-attack	Energy efficiency	Flexible	Computation time	cost
An FPGA implementation of a flexible secure ECC processor			✓		✓	✓	
HW-SW implementation of public-Key Cryptography for wireless sensor networks			✓		✓		✓
Implementation embedded security on dual-virtual-CPU system			✓	✓			✓
A security approach for off-chip memory in embedded microprocessor system			✓				✓
A compiler-hardware approach to software protection system		✓	✓		✓		
Embedded security: new trends in personal recognition system		✓	✓				✓
A data- driven approach for embedded security			✓				

So, we can see Figure 6, which illustrates the classification of IoT security. This scheme is specific to organizing different types of security risks and weaknesses in various IoT application areas. Its purpose is to assist in establishing a security structure for the diverse IoT environment. It will also aid in crafting security models for limited-capacity devices. All security aspects are discussed in preceding sections.

Kumar et al. and Kamalov et al. described current approaches and their limitations to ensure IoT security and trust in [24, 25]. These approaches are classified below, despite their limitations.

Application Layer

In their publication [26], Ksibi and colleagues focus on enhancing security metrics for systems of e-Health information. They suggest five components aimed at improving security assessments and protocols. Riaz and Choi examined attacks on complex systems and recommended a strategy of attacking systems to develop more robust security methods as a solution [27].

In their study titled “Preference-Based Privacy Protection Method”, Salayma and Choi addressed data privacy issues [28].According to their proposal, a third-party entity would assess the user's privacy needs and provide information to the service provider, which would then modify the level of personalization provided before linking the device to an IoT. Bhol et al. conducted a study on security measures using a probabilistic assessment approach.Intheir model, security is defined as the probability of occurrence and resource misallocation. [29].

Benlloch-Caballero et al. [30] developed a flexible security demonstration for IoT infrastructure and proposed a flexible security enhancement system based on the SMC (Self-Managed Security Cell) model for decentralized assets. Sagar [31] addressed the challenge of a framework that dynamically adapts to changing environments while anticipating unknown threats. As a solution, a flexible learning approach that modifies internal parameters and dynamically adjusts the structure of security systems was presented.

Middle-Ware Layer

In their study, Caballero-Torres et al. [32] advocate for the need for a secure and comfortable lifestyle for the elderly by advocating for smart objects and technologies such as RFID, NFC, and closed-loop hierarchy (CLH) to maintain continuous communication (KIT).

Kocher et al. [33] focus on the necessity of obtaining real-time information from physical objects and propose the use of cyber sensors to capture information from these objects for later utilization or immediate response.

Myre et al. [34] Emphasize the security of network nodes and recommend using a successor node to authenticate them as retaliatory measures against security risks. This solution involves the secure transmission of a decryption key when the center is authenticated while continuing to develop sibling centers.

During his research, Kumar explored the role of asset management and valuation in an all-encompassing computing environment [35] and proposed a self-managed cell (SMC) approach that incorporates orchestration, discovery, and role services.

Rehman et al. [36] identified security objectives and threats in data intelligence and proposed Adaptive Security Management (ASM) to address these challenges through four steps: continuous monitoring, analysis and prediction, decision-making, and utilizing adaptive security models. Sensors play a crucial role in collecting information about devices and their environments. This approach has demonstrated significant effectiveness, particularly in hospital settings.

Network Layer

In their study, Janani et al. [37] address the problem of verifying data transmission between the device and the cloud. The device could be equipped with an identity supervisor and a service supervisor to handle this task effectively, according to their suggestion.

Vadivel et al. [38] explore the risks for intelligent transportation systems (ITS) and propose the use of a public key framework commonly used in certificate authentication (CA) to manage and monitor network security credentials in ITS devices to prevent eavesdropping..

The focus of Wang et al. [39] is on addressing vulnerabilities in device security and data integrity. They achieve this by following a process: when a user requests access to a device, the device requests authorization from a Registration Authority (RA). If the RA approves, the device sends the user an address, and upon receiving a positive response, the user is granted access to the device.

Bajahzar [40] have expressed worries regarding the security of smart home systems and communication devices. Their suggestion involves the utilization of entity authentication, secure storage, security evaluation, digital signatures, and verification to guarantee secure communication between devices, as well as data encryption and decryption.

Physical Layer

In their research, Semary et al. [41] focused on addressing the issue of device connectivity by suggesting the use of RFID labels embedded in smart objects for facilitating quick communication between devices.

Another recent research approach involves Minani et al. [42], who presented a security testing station and an elaborate explanation. The main objective of his work is to evaluate IoT devices with different software and hardware configurations to detect vulnerabilities

A study conducted by A. Visalakshi et al. [43] They have examined the different types of attacks on wireless sensor networks (WSNs) and suggested possible solutions for these attacks.

In their research, Ahmed and Gandomi [44] outlined the potential risks posed by sensors to IoT devices and proposed targeted measures to safeguard these devices' sensors.

Furthermore, M. Akinsanya et al. [45] conducted a survey on malware and current security threats for the IoT space and suggested implementing an efficient system for running secure applications.

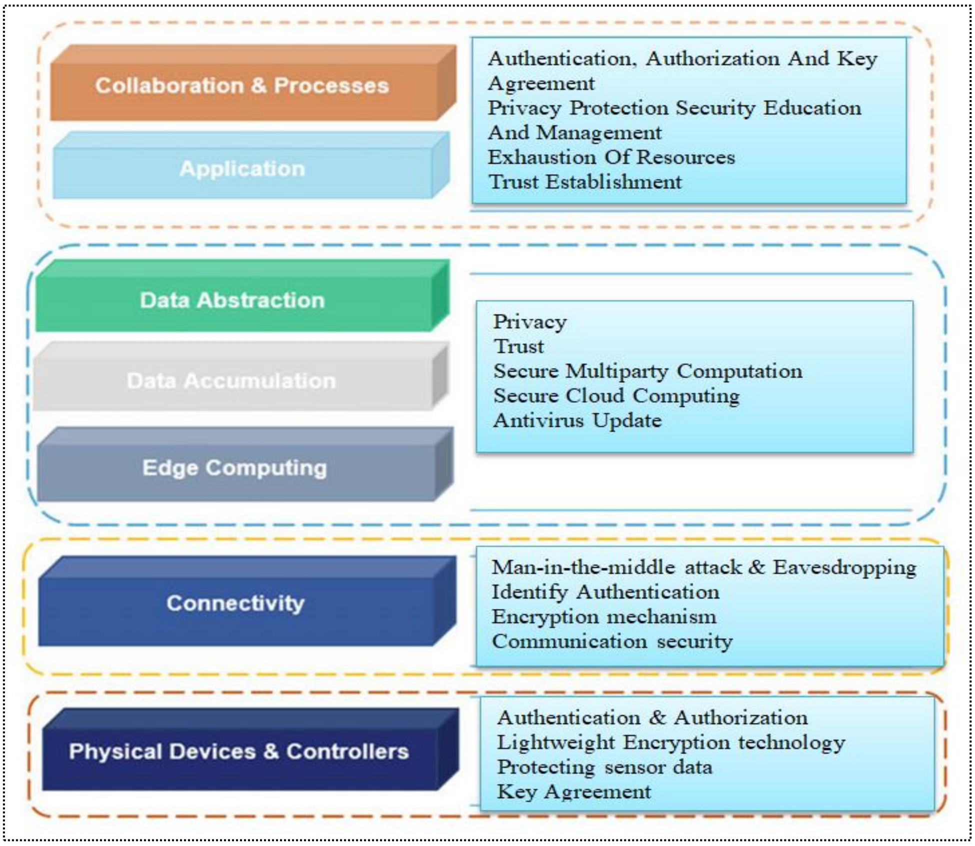

Collaboration & Processes
Application
Authentication, Authorization And Key Agreement
Privacy Protection Security Education And Management
Exhaustion Of Resources
Trust Establishment
Data Abstraction
Data Accumulation
Edge Computing
Privacy
Trust
Secure Multiparty Computation
Secure Cloud Computing
Antivirus Update
Connectivity
Man-in-the-middle attack & Eavesdropping
Identify Authentication
Encryption mechanism
Communication security
Physical Devices & Controllers
Authentication & Authorization
Lightweight Encryption technology
Protecting sensor data
Key Agreement

Figure 6. Classification of IoT security

RESULTS OF STUDY

The results show that IoT systems face significant security challenges at all levels of their architecture. Although there are many solutions, such as adaptive security models, hardware innovations and, cryptographic methods, current approaches have gaps, especially in addressing hardware vulnerabilities such as side-channel attacks. The study highlights the critical need for holistic security solutions that integrate hardware and software protection. Continuous research and development is essential to protect IoT environments against constantly evolving threats and to ensure secure interactions between devices across different application domains. Moreover, Table 2. shows the challenges addressed, proposed solutions, and expected outcomes.

Table 2. Summarizes the results of category, challenges addressed, proposed solutions, and expected outcomes.

Category	**Challenges Addressed**	**Proposed Solutions**	**Expected Outcomes**
Physical Layer	Device connectivity issues, malware, and sensor vulnerabilities	Secure execution systems, security testbeds, RFID labels, and sensor-targeted measures	Connectivity improvement and vulnerability assessment, secure execution for IoT applications
Network Layer	Smart home system risks, Data interception, and vulnerabilities in device-cloud transmission	Identity/service supervisors, RA-based authorization, encryption, digital signatures, and public-key frameworks for ITS	Enhanced data transmission integrity and communication security between IoT devices

Middleware Layer	Security metrics, real-time data capture, and Asset management	Cyber sensors, authenticated offspring nodes, Adaptive Security Management (ASM), and Self-Managed Cells (SMC)	Effective real-time monitoring, adaptive security, and asset assessment
Application Layer	Data privacy, evolving security frameworks, and robust e-Health systems	Flexible learning frameworks, Third-party privacy evaluation, probabilistic security assessment	Enhance user-oriented privacy and dynamically adapt to evolving security threats
General IoT Attacks	Side-channel attacks, Network attacks, and software vulnerabilities	Enhanced Cryptographic methods, compiler-hardware approaches, and flexible ECC processors	Network attacks mitigated, hardware protection remains underdeveloped, and software vulnerabilities addressed

CONCLUSION

An emerging area in the Internet is the Internet of Things (IoT), which allows smart devices to interact with other devices at any time and in any location. This includes sensors and embedded devices that can communicate and exchange data over the Internet. While it is optimized for rapid data exchange, security concerns have been raised such as eavesdropping, sniffing, malware, ransomware, DDoS attacks, DoS, and others. New security vulnerabilities and risks will keep advancing, leading to continuous exploration and the creation of solutions. Security problems in the IoT structure have been investigated by multiple researchers, covering the middleware layer, network layer, application layer, and physical layer. Therefore, this paper offers a comprehensive analysis of IoT security issues and security solutions at each of the above layers.

The results highlight authentication as a critical aspect of security. This study aims to determine the possible attacks on the IoT network and suggest possible solutions. The security issues are categorized based on the layers of the IoT architecture. Despite this categorization, problems in these layers can compromise the overall security of the system. The paper also presents solutions for these issues, underscoring the necessity for comprehensive security measures in future research. The study has identified and classified security issues in IoT networks based on the various layers of the IoT architecture. The study has emphasized the necessity for additional research and the development of security solutions for IoT networks.

ACKNOWLEDGMENTS

The author wishes to thank the Department of Biomedical Engineering at Engineering College, University of Thi-Qar, Al-Nasiriyah City, Iraq, for their support.

REFERENCES

[1] Chakraborty, A. (2022). Evolution of the Internet of Things and Fundamentals of Human-Machine Interaction. In *Human-Machine Interaction and IoT Applications for a Smarter World* (pp. 3-14). CRC Press.

[2] Rana, P., & Patil, B. P. (2023). Cyber security threats in IoT: A review. *Journal of High Speed Networks*, *29*(2), 105-120.

[3] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[4] Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.

[5] Dhar, S., Khare, A., & Singh, R. (2023). Advanced security model for multimedia data sharing in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4621.

[6] Vailshery, L. S. (2021). Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. *Online, https://bit. ly/2SwKVuB*.

[7] 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.

[8] Rahman, M. A., Abuludin, M. S., Yuan, L. X., Islam, M. S., & Asyhari, A. T. (2021). EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0. *IEEE Transactions on Industrial Informatics*, *18*(3), 1930-1938.

[9] Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-Physical Systems*.

[10] Kadelka, C., Butrie, T. M., Hilton, E., Kinseth, J., Schmidt, A., & Serdarevic, H. (2024). A meta-analysis of Boolean network models reveals design principles of gene regulatory networks. *Science Advances*, *10*(2), eadj0822.

[11] Sharma, Y., Sharma, S., & Arora, A. (2022, June). Feature ranking using statistical techniques for computer networks intrusion detection. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 761-765). IEEE.

[12] Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). IoT Devices in Drones: Security Issues and Future Challenges. In *Cybersecurity Issues and Challenges in the Drone Industry* (pp. 217-235). IGI Global.

[13] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Networks*, *152*, 103322.

[14] Tamayo, J., López, L. I. B., & Caraguay, Á. L. V. (2024). Detection of Distributed Denial of Service Attacks Carried Out by Botnets in Software-Defined Networks. *arXiv preprint arXiv:2401.09358*.

[15] Ali, R., Pal, A. K., Kumari, S., Sangaiah, A. K., Li, X., & Wu, F. (2024). An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *Journal of Ambient Intelligence and Humanized Computing*, 1-22.

[16] Kaur, K., Kaur, A., Gulzar, Y., & Gandhi, V. (2024). Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. *Frontiers in Computer Science*, *6*, 1420680.

[17] Maurya, S. K., Pal, O. P., & Sarvakar, K. (2024). Layered Architecture of IoT. In *Secure and Intelligent IoT-Enabled Smart Cities* (pp. 164-194). IGI Global.

[18] Wu, Huihui, Yuanyu Zhang, Yulong Shen, Xiaohong Jiang, and Tarik Taleb. "Achieving covertness and secrecy: The interplay between detection and eavesdropping attacks." *IEEE Internet of Things Journal* (2023).

[19] Shafik, W. (2024). Blockchain-based internet of things (B-IoT): Challenges, solutions, opportunities, open research questions, and future trends. *Blockchain-based internet of things*, 35-58.

[20] Zhonghua, C., Goyal, S. B., & Rajawat, A. S. (2024). Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. *The Journal of Supercomputing*, *80*(2), 1396-1425.

[21] Alhirabi, N., Beaumont, S., Rana, O., & Perera, C. (2024). Designing privacy-aware IoT applications for unregulated domains. *ACM Transactions on Internet of Things*, *5*(2), 1-32.

[22] Hamad, S. A., Sheng, Q. Z., & Zhang, W. E. (2024). *Security Framework for The Internet of Things Applications*. CRC Press.

[23] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.

[24] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

[25] Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., & Moussa, S. (2023). Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. *Sustainability*, *15*(4), 3317

[26] Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach. *Mobile Networks and Applications*, *28*(1), 107-127.

[27] Riaz, A. R., Gilani, S. M. M., Naseer, S., Alshmrany, S., Shafiq, M., & Choi, J. G. (2022). Applying adaptive security techniques for risk analysis of internet of things (IoT)-based smart agriculture. *Sustainability*, *14*(17), 10964.

[28] Salayma, M. (2024). Risk and threat mitigation techniques in internet of things (IoT) environments: a survey. *Frontiers in The Internet of Things*, *2*, 1306018.

[29] Bhol, S. G., Mohanty, J. R., & Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*, *80*, 2274-2279.

[30] Benlloch-Caballero, P., Wang, Q., & Calero, J. M. A. (2023). Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. *Computer Networks*, *222*, 109526.

[31] Sagar, S., Mahmood, A., & Sheng, Q. Z. (2024). *Towards Resilient Social IoT Sensors and Networks: A Trust Management Approach* (Vol. 48). Springer Nature.

[32] Caballero-Torres, P., Cano-Crespo, M., Ortiz, G., & Medina-Bulo, I. (2024). AALFlow: A Model-Driven Approach for the Integration of Internet of Things Heterogeneous Solutions for Ambient Assisted Living. *IEEE Internet of Things Journal*.

[33] Kocher, I. S. (2023). A Systematic Roadmap on Privacy, Security, Trust, Identity Management, and Resilience: Wireless Sensor Networks and Internet of Things Architectures. *Academic Journal of Nawroz University*, *12*(4), 398-414.

[34] Myre, E. (2021). *PKI and IoT Security: How to choose the most secure implementation?* (Master's thesis, NTNU).

[35] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

[36] Rehman, Z., Gondal, I., Ge, M., Dong, H., Gregory, M., & Tari, Z. (2024). Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. *Computers & Security*, *139*, 103685.

[37] Janani, K., & Ramamoorthy, S. (2024). A security framework to enhance IoT device identity and data access through blockchain consensus model. *Cluster Computing*, *27*(3), 2877-2900.

[38] Vadivel, G., Hussain, M. J. M., & Sangeetha, S. T. (2023). Smart transportation systems: IoT-connected wireless sensor networks for traffic congestion management. *International Journal of Advances in Signal and Image Sciences*, *9*(1), 40-49.

[39] Wang, C., Wang, D., Duan, Y., & Tao, X. (2023). Secure and lightweight user authentication scheme for cloud-assisted internet of things. *IEEE Transactions on Information Forensics and Security*, *18*, 2961-2976.

[40] Bajahzar, A. (2024). The Importance of AI-Enabled Internet of everything Services for Smart Home Management. *International Journal on Smart Sensing and Intelligent Systems*, *17*(1).

[41] Semary, H. E., Al-Karawi, K. A., Abdelwahab, M. M., & Elshabrawy, A. M. (2024). A Review on Internet of Things (IoT)-Related Disabilities and Their Implications. *Journal of Disability Research*, *3*(2), 20240012.

[42] Minani, J. B., Sabir, F., Moha, N., & Guéhéneuc, Y. G. (2024). A systematic review of IoT systems testing: Objectives, approaches, tools, and challenges. *IEEE Transactions on Software Engineering*.

[43] Visalakshi, P. (2024). Connect attack in IoT-WSN detect through cyclic analysis based on forward and backward elimination. *PeerJ Computer Science*, *10*, e2130.

[44] Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion*, *102*, 102060.

[45] Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Security paradigms for iot in telecom networks: conceptual challenges and solution pathways. *Engineering Science & Technology Journal*, *5*(4), 1431-1451.