Canadian Journal of Pure and Applied Sciences
Vol. 19, No. 1, 2, 3, pp. 5871-5879, Feb, June, Oct 2025
Online ISSN: 1920-3853; Print ISSN: 1715-9997
Available online at www.cjpas.org
doi: 10.68605/CJPAS.org/2025.19.1-3.5871-5879.1

AUGMENTED SECURITY MANAGEMENT FRAMEWORK FOR INTERNET OF THINGS (IOT) ENVIRONMENTS

Abdullah Ahmed Aljohni, Mohammed Yahya Saleh, *Abdulrehman Abdulaziz and Muhammad Asif Khan
Department of Information Systems
College of Computer Science and Engineering
Taibah University, Madina al Munawarra, Saudi Arabia

ABSTRACT

The increasing development of internet technologies has produced numerous opportunities across spectrum of applications and industries. In result of such technological development, the Internet of Things (IoT) has emerged as a standard that enables connectivity and communication among various smart devices either by wired or wireless networks. There are many benefits spawned in result of advancement in internet connected automation and IoT model is one of the top benefits. Many smart sensors, applications and devices are linked via wired or wireless network together to form an IoT. The IoT has grown during last many years and facilitated automation and resource management in various sectors including healthcare, smart cities and manufacturing. Although, there are many benefits of IoT but, cyber security threats from cyber attackers are great threat to its existence. Without necessary security measures the IoT is at perpetual risk from different threats and attacks. As a result, properly securing and managing the IoT has become a very important matter. Without comprehensive security mechanisms, IoT systems remain exposed to unauthorized access, data breaches, and other malicious activities. Therefore, implementation of effective security is significant in the deployment of IoT systems. This research proposes a security management framework for IoT systems and environments. This study adopts qualitative research methodology which focuses on review of literature to identify basic security requirements for IoT infrastructure and communication. Appropriate security mechanisms and techniques are evaluated and selected to mitigate the identified vulnerabilities. Finally, these security measures are integrated into a unified security management framework which helps to maintain privacy of IoT systems.

Keywords*:* Internet of things IoT, IoT layers, threats and attacks, security and management.

INTRODUCTION

Internet of Things (IoT) is simply a set of different devices and systems based on wired and wireless connectivity. These devices and systems comprise of hardware and software components that support various types of applications across different fields. Usually, they are used in manufacturing management, agriculture, e-commerce, energy management, logistics, aerospace, healthcare, construction, smart home automation, infrastructure management, transportation, and numerous other domains. The main objective of the IoT network is to link and connect all smart devices so that they can share and exchange data from each other. The increasing trend of latest technologies indicates that IoT is the most emerging technology throughout the world. The aim of IoT is to enable the development of user-specific applications and a wide range of industry-oriented solutions through the interconnection of smart devices and networks. IoT provides the physical connectivity that allows heterogeneous devices to communicate and collaborate seamlessly. Through reliable device-to-device (D2D) communication and interaction, IoT applications facilitate real-time data exchange and intelligent decision-making. Furthermore, IoT applications must ensure that transmitted messages are accurately received, processed, and managed within the required time constraints to support reliable and time-sensitive operations. The IoT connects embedded devices with physical objects and transform them into intelligent, internet-enabled devices. Each IoT device possesses a unique identity that enables it to be individually addressed, monitored, and managed. Through this interconnected network, smart devices can communicate and exchange data autonomously, facilitating seamless interaction and intelligent decision-making across diverse applications (Dauda *et al*., 2024). The IoT provides users great chances to achieve their aims and objectives by performing difficult and complex impractical tasks that can contribute to human well-being. The devices which provide IoT-enabled services collect relevant data, process,

*Corresponding author e-mail: a.almulhim190@gmail.com

and transmit the required information to users. These capabilities facilitate informed decision-making, improve operational efficiency, and support the development of innovative solutions across various domains (Abdalzaher *et al*., 2025). The attainment of IoT applications and services depends on the integration of existing technologies, including smart sensor networks, radio frequency identification, near field communication, and internet-based communication technologies. The integration of these technologies supports variety of devices to communicate, exchange data, and collaboratively support sensing, processing, and service delivery. IoT environments encompass a wide variety of devices with different hardware capabilities, communication technologies, processing capacities, storage resources, and energy constraints. Consequently, many IoT devices are considered resource-constrained devices, particularly at the edge of the network, where limited computational power, memory, bandwidth, and energy availability can affect system performance and scalability (Hudda and Haribabu, 2025).

Problem definition

The research problem stems from the significant security challenges that hinder the widespread development and adoption of Internet of Things (IoT) systems. As IoT networks continue to expand and connect a growing number of heterogeneous devices, they have become increasingly attractive targets for cyber attackers, who employ various techniques and strategies to exploit vulnerabilities within IoT environments. Moreover, the potential consequences of cyberattacks have become increasingly serious as IoT devices are integrated into physical environments and critical infrastructures, creating risks that extend beyond information and data security.

The research problem arises from the significant security challenges that deter the prevalent development and adoption of IoT systems. As IoT networks continue to thrive and connect increasing number of heterogeneous devices, they have become progressively attractive targets for cyber attackers. Cyber attackers employ a variety of techniques and strategies to exploit vulnerabilities within the IoT environment. Furthermore, the potential consequences of cyber-attacks have become increasingly serious as IoT devices are integrated into the physical environment and critical infrastructure, posing threats that go beyond information and data security.

Data security is therefore one of the most significant concerns in the design and deployment of IoT systems. Many legacy IoT devices were designed without sufficient security features and may therefore contain vulnerabilities that are difficult to address after deployment.

The highly interconnected nature of IoT makes these systems particularly susceptible to security threats. Consequently, the absence of comprehensive security mechanisms across IoT devices and networks represents a major challenge that must be addressed to ensure the secure, reliable, and sustainable development of IoT systems.

Motivation and research question

The security requirements of IoT systems are extensive that cover multiple features, including device security, network protection, data privacy, authentication, access control, secure communication, and system resilience. A large body of research has proposed various security mechanisms, models, and frameworks to address individual IoT security challenges. However, existing approaches often focus on specific layers, applications, or security requirements rather than providing a comprehensive, integrated, and universally applicable framework for IoT environments. Recent studies continue to highlight the fragmented nature of IoT security solutions and the need for more comprehensive approaches capable of addressing the diverse and evolving security challenges across the IoT ecosystem (Kaur *et al*., 2024; Ataullah and Chauhan, 2024; Sefati *et al*., 2025).

In substantial body of research, limited research has focused on developing integrated security approaches that provide effectiveness, adaptability, and long-term sustainability across diverse IoT applications. Therefore, further research is required to develop comprehensive and scalable security solutions capable of addressing the evolving security requirements of IoT environments (Aouedi *et al*., 2024; Javanmardi *et al*., 2025).

The above encouraged us to formulate a research question for our study as:
RQ: What are the benefits of developing a comprehensive security management framework for Internet of Things (IoT) environments?

This research aims to address the research gaps identified in previous studies concerning security and privacy in IoT environments. Specifically, the study proposes the development of a comprehensive security management framework designed to address the evolving security and privacy requirements of IoT systems. The proposed framework is intended to enhance security awareness, support effective security management, and contribute to the development of more secure, resilient, and trustworthy IoT environments.

The significance of this research lies in the development of a comprehensive security management framework and simplified security management approaches that can assist IoT systems in meeting the security requirements of both users and service providers. Effective IoT security management has the potential to protect information across all layers of IoT architecture, from devices and

communication networks to edge and cloud services. By integrating appropriate security policies, services, and mechanisms, the proposed framework can strengthen the protection of sensitive data, preserve user privacy, mitigate security risks, and enhance the overall security and trustworthiness of IoT environments.

RELATED WORK

The increasing expansion of IoT not only offers noteworthy opportunities for organizations and users but also introduces new security risks and cyberattacks. Organizations require proactive and adaptive security measures to identify vulnerabilities, and protect IoT products, services, data, and users. Therefore, widespread sprouting security management approaches are essential to maintain confidentiality, integrity, and resilience of IoT systems (Sarker, 2025). IoT systems face a wide range of security threats across their various architectural layers. At the perception or sensing layer, attackers may target sensors, actuators, RFID tags, and other connected devices. At the network layer, IoT systems are vulnerable to routing and identity-based attacks, including sinkhole, Sybil, man-in-the-middle, and denial-of-service (DoS) attacks. The middleware layer can be targeted by various attacks such as authentication violation, malware injection, SQL injection. At the application layer, attackers may exploit software vulnerabilities through malicious code injection, malware, phishing, and other application-level attacks. The interconnectivity of these layers means that a compromise at one layer can potentially affect the security and functionality throughout the IoT ecosystem (Razaque *et al*., 2025). A reliable and sustainable operation of IoT environments has become a major security challenge due to the increasing number of interconnected devices. Therefore, strengthening IoT security requires a thorough approach that considers security across the entire IoT architecture and integrates appropriate security procedures, policies, and infrastructure (Farooq *et al*., 2015).

A variety of IoT technologies enables the development of innovative solutions and services across a wide range of industries and application domains. The extensive connectivity and diversity of IoT devices also introduce significant security and privacy challenges. Protecting information within IoT environments is therefore essential for maintaining confidentiality, integrity, and availability of data and for establishing user confidence in IoT services. A comprehensive security framework that integrates these mechanisms can strengthen the protection of IoT systems and contribute to greater trust, reliability, and user acceptance of IoT-based services (Sharma *et al*., 2020; Alshahrani *et al*., 2022).

The rapid expansion and increasing heterogeneity of IoT ecosystems have also expanded the potential attack surface and introduced significant cybersecurity and privacy challenges. Recent cybersecurity guidance emphasizes that IoT security should be addressed throughout the device and system lifecycle rather than being treated as an isolated application-layer concern. Developing an effective IoT security framework requires a comprehensive analysis of the security requirements, vulnerabilities, and threats associated with each application domain. Security cannot be adequately achieved by strengthening only one layer of the IoT architecture. National Institute of Standards and Technology (NIST) IoT cybersecurity guidance therefore identifies capabilities such as device identification, secure configuration, data protection, logical access control, software updates, and cybersecurity state awareness as important components of IoT security. Therefore, effective IoT protection requires an integrated, cross-layer security approach in which security mechanisms at different layers complement one another. This approach can provide greater resilience against evolving cyber threats and help ensure the trustworthy operation of IoT systems (Fagan *et al*., 2020).

The large-scale deployment of heterogeneous IoT devices generates substantial volumes of data, creating challenges related to data processing, storage, quality, interoperability, latency, and privacy. Cloud computing provides scalable computational and storage resources; however, the physical distance between IoT devices and cloud platforms can introduce latency and communication overhead, particularly for time-sensitive applications. Consequently, edge and fog computing have increasingly been adopted to process data closer to IoT devices and improve response time and resource efficiency (Dauda *et al*., 2024).

The modern vision of IoT extends beyond simply connecting devices to a network. IoT systems are increasingly expected to incorporate intelligent and adaptive objects which can sense their surroundings and communicate with other devices in their operating environments. Recent research on smart products emphasizes that the ability of smart objects to respond to their surrounding environments is an important characteristic of intelligent systems (Carrera-Rivera *et al*., 2022).

Improperly protected IoT devices may be exploited to obtain unauthorized access, compromise sensitive information, manipulate data, disrupt services, or use compromised devices as a platform for attacks against other systems. These risks are particularly significant because IoT devices are often deployed in environments where they directly interact with physical processes and may have limited computational, storage, and security capabilities (Rani *et al*., 2021).

IoT environments continuously exchange information among sensors, devices, and organizational information systems. This extensive data exchange increases the

potential attack surface and creates additional risks to the confidentiality, integrity, availability, and privacy of sensitive information. The transmission of sensitive IoT data between devices and remote services can expose systems to various threats and exploitation of device vulnerability. The varied IoT environments and the large number of devices make it difficult to apply conventional security mechanisms across the entire ecosystem. Consequently, protecting IoT data requires security controls that address both the devices themselves and the data, systems, and services with which they interact. Organizations therefore need to establish comprehensive IoT cybersecurity frameworks capable of reducing these risks throughout the IoT lifecycle (Fagan *et al*., 2020).

The IoT remains vulnerable to a wide range of cyberattacks because of its highly distributed, heterogeneous, and interconnected architecture. Many IoT devices are deployed in physically exposed or unattended environments, while wireless communication is extensively used to exchange information between devices, gateways, edge platforms, and cloud services. These characteristics can increase the opportunities for attackers to intercept communications, compromise devices, exploit vulnerabilities, or manipulate transmitted information. Furthermore, the large-scale interconnection of IoT devices increases the potential impact of a successful attack because a compromised device may provide an entry point into other components of the IoT ecosystem (Sharma *et al*., 2021).

Among the fundamental security requirements of IoT systems are data integrity and authentication. Data integrity ensures that information collected, transmitted, and processed by IoT devices is not altered without authorization, while authentication ensures that devices, users, and other entities participating in communication can be reliably verified. Data integrity attacks can have serious consequences in IoT environments because manipulated information may lead to incorrect decisions or inappropriate physical actions. Authentication is particularly challenging in IoT environments because devices often have constrained computational, storage, and energy resources. Effective IoT security therefore requires authentication and access-control mechanisms that provide strong protection while remaining appropriate for the capabilities and operational requirements of individual devices (Sivaselvan *et al*., 2023).

A comprehensive security framework should establish strong mechanisms for authentication, authorization, access control, confidentiality, data integrity, secure communication, vulnerability management, and continuous monitoring. In addition, security mechanisms should be coordinated across device, network, edge/cloud, and application layers rather than implemented independently (Dirin *et al*., 2023).

MATERIALS AND METHODS

This study adopts a qualitative research approach using a descriptive-analytical methodology to investigate security management challenges and requirements in IoT environments and to develop an appropriate security management framework. The study begins with a comprehensive literature review to identify, examine, and synthesize existing research on IoT security threats, vulnerabilities, security requirements, and mitigation strategies. The literature review also helps identify gaps in existing research and determine areas that require further investigation.

Relevant academic literature is systematically examined and analyzed according to the objectives and research questions of the study. The findings from the reviewed literature are then used to identify recurring security issues, concepts, relationships, and requirements that can inform the development of the proposed IoT security management framework.

This research adopts a descriptive-analytical methodology and is primarily based on information gathered through a literature review. Data will be collected by systematically reviewing and analyzing relevant scientific publications. The review will focus on literature addressing IoT architecture and layers, IoT threats and vulnerabilities, IoT security requirements, security services, and security mechanisms. The collected information will subsequently be analyzed to identify key security challenges, requirements, and mechanisms relevant to the development of the proposed IoT security management framework.

The IoT architecture is commonly structured into four major layers, arranged hierarchically from the bottom to the top. These layers are the Device/Perception Layer, Network Layer, Service/Middleware Layer, and Application Layer. Each layer performs specific functions and contributes to the overall operation and communication of IoT systems. Figure 1 illustrates the four-layer IoT architecture and the relationship among these layers.

Proposed augmented security management framework for IoT

The proposed Augmented Security Management Framework for the IoT should be developed in accordance with the underlying IoT architecture. The framework is designed as a layered and coordinated security management framework for IoT environments. Its main purpose is not simply to provide individual security mechanisms, but to establish a management structure that governs, organizes, implements, monitors, and continuously improves security across the entire IoT architecture**.** Figure 2 shows the proposed framework

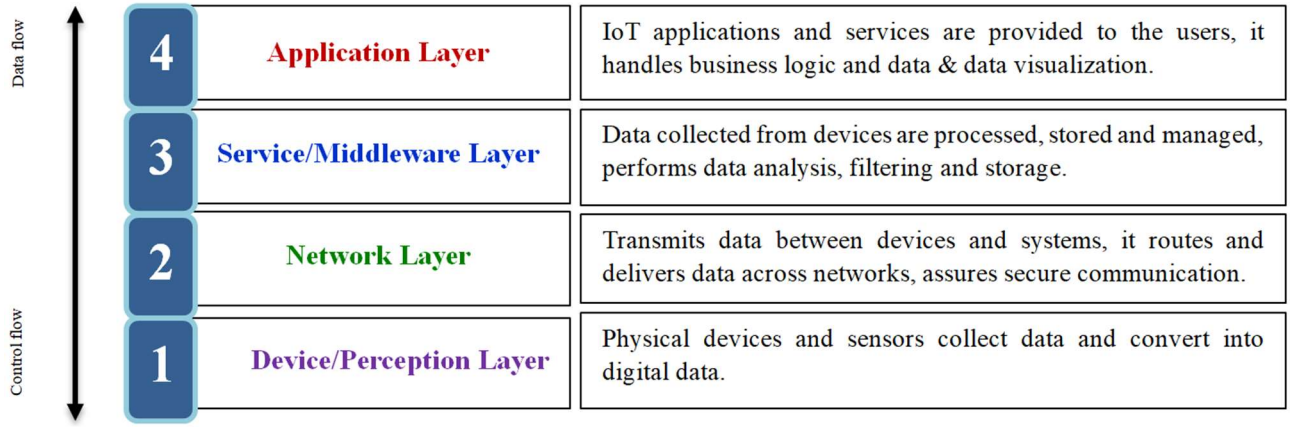


Fig. 1. Four-layered IoT Architecture.

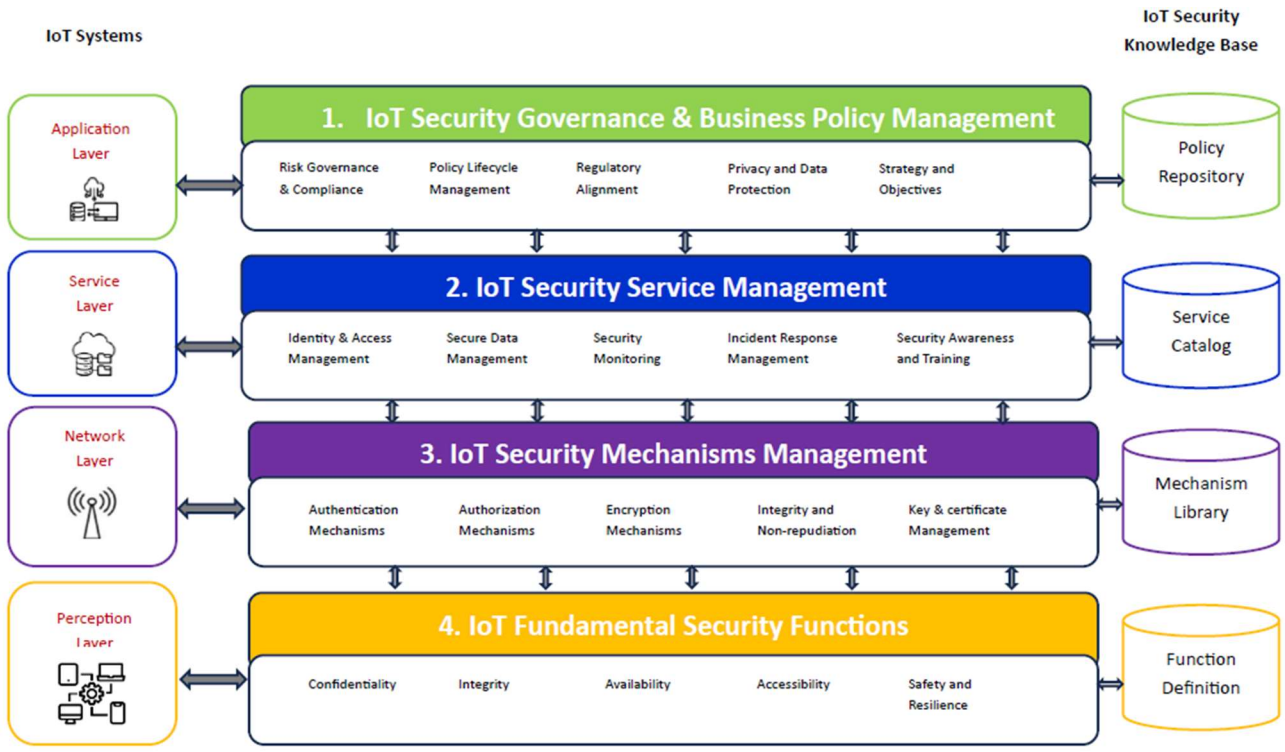


Fig. 2. Augmented Security Management Framework for IoT.

The framework can be understood through four major security-management layers supported by an IoT security knowledge base. The framework recognizes that IoT security cannot be managed effectively by protecting only individual devices. An IoT environment involves Perception devices such as sensors and actuators, Network and communication infrastructure, Service platforms including cloud and fog environments and Applications and users. Therefore, security management needs to operate across all these architectural levels.

The framework establishes four vertically aligned management layers:

- IoT Security Governance & Business Policy Management
- IoT Security Services Management
- IoT Security Mechanisms Management
- IoT Fundamental Security Functions

These four layers are connected to the four IoT architectural layers shown on the left of the figure:

Application → Service → Network → Perception/ Element

The important point is that the framework does not treat these IoT layers as isolated. The arrows indicate interaction and coordination between the IoT architecture and the corresponding security-management functions. Each layer addresses a different level of IoT security, ranging from strategic governance to fundamental security objectives.

IoT security governance and business policy management

This is the strategic and managerial layer of the framework. It establishes the overall direction for IoT security by addressing risk governance and compliance, security-policy lifecycle management, regulatory alignment, privacy and data protection, and organizational security objectives. This layer ensures that IoT security requirements are aligned with organizational strategies, legal requirements, and risk-management objectives.

IoT security services management

This layer translates governance and policies into operational security services. It manages identity and access, secure data, security monitoring and analytics, incident response, and security awareness. Its purpose is to ensure that appropriate security services are continuously available to protect IoT devices, communications, data, users, and applications.

IoT security mechanisms management

This is the technical-control layer, responsible for implementing the security services defined by the upper layers. It includes authentication, authorization, encryption, integrity and non-repudiation, and key and certificate management. These mechanisms provide practical protection against unauthorized access, data disclosure, manipulation, impersonation, and other cyber threats.

IoT fundamental security functions

This layer defines the core security outcomes that the framework seeks to achieve. It focuses on confidentiality, integrity, availability, accountability, and safety and resilience. These functions provide fundamental objectives against which the effectiveness of IoT security controls can be evaluated.

In addition to the four primary layers, the framework contains several supporting components. The IoT Security Knowledge Base provides policies, service definitions, security mechanisms, best practices, and threat intelligence to support security decisions.

RESULTS AND DISCUSSION

The findings indicate that IoT security cannot be addressed through a single security mechanism or through protection of an individual architectural layer. Instead, effective security requires coordinated management of governance, security services, technical mechanisms, fundamental security objectives, and cross-layer security requirements.

Based on the identified security requirements, the findings were organized into four major security-management categories i.e. IoT Security Governance and Business Policy Management, IoT Security Services Management, IoT Security Mechanisms Management, and IoT Fundamental Security Functions.

1. IoT security governance and business policy management

The first major category identified from the analysis was IoT Security Governance and Business Policy Management. The findings demonstrate that IoT security requires organizational-level governance before technical security controls can be effectively implemented. There are five categories including Risk governance and compliance, Security-policy lifecycle management, Regulatory alignment, Privacy and data protection, and Security strategy and objectives. These findings indicate that security management should begin with the identification of security risks, organizational requirements, regulatory obligations, and privacy requirements. Policies should subsequently be developed, implemented, monitored, and periodically updated according to changes in the IoT environment and emerging threats. Therefore, governance was positioned as the highest security-management layer in the proposed framework because it establishes the requirements and strategic direction for the remaining security layers.

2. IoT security services management

The second category emerging from the analysis was IoT Security Services Management. The findings indicate that governance requirements must be translated into operational security services capable of protecting IoT devices, users, data, networks, and applications. There are five security services including Identity and access management, Secure data management, Security monitoring and analytics, Incident response and management, and Security awareness and training. The findings demonstrate that these services provide the operational connection between organizational security policies and technical security controls. For example, a policy requiring restricted access to IoT resources must be implemented through identity, authentication, authorization, and access-management services. Accordingly, this category was positioned below the governance layer in the proposed framework.

3. IoT security mechanisms management

The third category was identified as IoT Security Mechanisms Management. This category represents the technical mechanisms required to implement the security services identified in the previous layer. The analysis identified the five mechanisms i.e. Authentication mechanisms, Authorization mechanisms, Encryption mechanisms, Integrity and non-repudiation mechanisms and Key and certificate management. The results demonstrate that these mechanisms provide the technical means through which security requirements are enforced within IoT environments. For example, identity and access management requires authentication and authorization mechanisms, while secure data management requires encryption and integrity protection. The findings therefore support the positioning of security mechanisms as the technical implementation layer of the framework.

4. IoT fundamental security functions

The fourth category identified from the analysis consists of the fundamental security functions that represent the expected security outcomes of the framework. There are five identified functions i.e. Confidentiality, Integrity, Availability, Accountability, Safety and resilience. The first three functions represent the traditional core security objectives, while accountability, safety, and resilience extend the security perspective to address the characteristics of IoT environments. The inclusion of safety and resilience is particularly important because IoT devices frequently interact with physical environments. Consequently, a cybersecurity incident may not only result in data loss but may also affect physical processes, services, equipment, or human safety. These findings resulted in the placement of fundamental security functions as the fourth layer of the framework.

The results demonstrate that effective IoT security management requires a multi-level and integrated approach rather than isolated technical controls. The qualitative analysis resulted in four principal security-management layers, supported by cross-layer security capabilities and security knowledge base. The findings further demonstrate that the proposed framework addresses IoT security at both the architectural level and the management level. At the architectural level, it addresses the Perception/Element, Network, Service, and Application layers. At the management level, it establishes governance, operational services, technical mechanisms, and fundamental security objectives.

CONCLUSION

The proposed framework provides a structured and comprehensive approach to managing security across the IoT environment. The framework recognizes that IoT security cannot be addressed through isolated technical mechanisms because IoT systems consist of heterogeneous devices, communication networks, processing platforms, services, and applications that are interconnected and exposed to different types of security threats. Accordingly, the framework aligns security management with the major IoT architectural layers while also addressing security dependencies and threats that can extend across multiple layers.

The framework is organized into four interconnected security-management layers: IoT Security Governance and Business Policy Management, IoT Security Services Management, IoT Security Mechanisms Management, and IoT Fundamental Security Functions. The governance layer establishes security policies, risk-management requirements, regulatory alignment, privacy requirements, and organizational objectives. These requirements are translated into operational security services, including identity and access management, secure data management, security monitoring, incident response, and security awareness. The security services are then supported by technical mechanisms such as authentication, authorization, encryption, integrity protection, non-repudiation, and key and certificate management. Collectively, these controls support the fundamental security objectives of confidentiality, integrity, availability, accountability, safety, and resilience.

A significant contribution to the framework is its recognition of cross-layer security requirements. Rather than assigning security responsibilities to individual IoT layers in isolation, the framework establishes interactions between the Perception/Element, Network, Service, and Application layers. This approach enables security dependencies to be considered throughout the IoT environment. For example, the compromise of a perception-layer device can affect network communications, processing services, and ultimately IoT applications. Therefore, security management must coordinate controls across the entire system rather than focus on a single architectural component.

The framework is further strengthened by the IoT Security Knowledge Base, which provides access to policies, security-service definitions, security mechanisms, best practices, threat intelligence, and vulnerability information. Cross-cutting capabilities such as AI/ML-based security analytics, Zero Trust, edge and fog security, blockchain-based trust and auditing, digital-twin simulation, and sustainability considerations provide additional support across the IoT environment. Furthermore, standards and interoperability, secure development and DevSecOps, open APIs, scalability, and lifecycle management provide the foundation required for practical implementation.

FUTURE WORK

Although the proposed framework provides a comprehensive conceptual structure for IoT security management, several areas can be investigated in future research.

A major direction for future research is to transform the conceptual framework into a working prototype. Future studies can develop a software-based security-management platform implementing the four security-management layers and evaluate its operation within a real or simulated IoT environment. The framework should be evaluated through empirical studies and real-world IoT case studies. Different IoT environments, such as smart homes, healthcare, smart cities, industrial IoT, and smart transportation, could be used to determine whether the proposed framework adequately addresses their different security requirements.

REFERENCES

Abdalzaher, MS., Krichen, M., Shaaban, MF. and Fouda, MM. 2025. Quality-focused Internet of Things data management: A survey, perspectives, open issues, and challenges. IEEE Internet of Things Journal. 12(22):46431 – 46458. DOI: https://doi.org/10.1109/JIOT.2025.3613669

Abdulkader, D., Olivier, F. and Florent, N. 2024. A Survey on IoT Application Architectures, Sensors, 24(16), 5320. DOI: https://doi.org/10.3390/s24165320.

Alshahrani, H., *et al*. 2022. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. Journal of Network and Computer Applications. 204: 103414. https://doi.org/10.1016/j.jnca.2022.103414.

Aouedi, O., Vu, T., Sacco, A., Nguyen, D., Piamrat, K., Marchetto, G. and Pham, Q. 2024. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions, Networking and Internet Architecture. DOI: https://doi.org/10.48550/arXiv.2406.03820.

Ataullah, M. and Chauhan, N. 2024. Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy. 7(6): e448. DOI: https://doi.org/10.1002/spy2.448.

Carrera-Rivera., *et al*. 2022. Context-awareness for the design of Smart-product service systems: Literature review. Computers in Industry. 142(9):103730. DOI: https://doi.org/10.1016/j.compind.2022.103730.

Dauda, A., Flauzac, O. and Nolot, F. 2024. A Survey on IoT Application Architectures. Sensors. 24(16):5320. https://doi.org/10.3390/s24165320.

Dirin, A., Oliver, I. and Laine, TH. 2023. A security framework for increasing data and device integrity in Internet of Things systems. Sensors. 23(17):7532. DOI: https://doi.org/10.3390/s23177532.

Fagan, MJ., Megas, KN., Scarfone, K. and Smith, M. 2020. IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A). National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.IR.8259A.

Farooq, MU., Waseem, M., Khairi, A. and Mazhar, S. 2015. A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications. 111(7). DOI: https://doi.org/10.5120/19547-1280.

Hudda, S. and Haribabu, K. 2025. A review on WSN based resource constrained smart IoT systems. Discover Internet of Things. 5:56. DOI: https://doi.org/10.1007/s43926-025-00152-2.

Javanmardi, S., Nascita, A., Pescape, A. and Merlino, G. 2025. An integration perspective of security, privacy, and resource efficiency in IoT-Fog networks: A comprehensive survey, Computer Networks. 270:111470. DOI: https://doi.org/10.1016/j.comnet.2025.111470.

Kaur, K., Kaur, A., Gulzar, Y. and Gandhi, V. 2024. Unveiling the core of IoT: Comprehensive review on data security challenges and mitigation strategies. Frontiers in Computer Science. 6: 1420680. DOI: https://doi.org/10.3389/fcomp.2024.1420680.

Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K. and Choi, C. 2021. Threats and corrective measures for IoT security with observance of cybercrime: A survey. Wireless Communications and Mobile Computing. 5579148. DOI: https://doi.org/10.1155/2021/5579148.

Razaque, A., Hariri, S., Alajlan, AM. and Yoo, J. 2025. A comprehensive review of cybersecurity vulnerabilities, threats, and solutions for the Internet of Things at the network-cum-application layer. Computer Science Review, 58:100789. https://doi.org/10.1016/j.cosrev.2025.100789.

Sarker, KU. 2025. A systematic review on lightweight security algorithms for a sustainable IoT infrastructure. Discover Internet of Things. 5(1):47. DOI: http://doi.org/10.1007/s43926-025-00150-4.

Sefati, SS., Arasteh, B., Halunga, S., *et al*. 2025. A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT). Cluster Computing. 28:792. DOI: https://doi.org/10.1007/s10586-025-05449-z.

Sharma, G., Vidalis, S., Anand, N., Menon, C. and Kumar, S. 2021. A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open issues. Electronics. 10(19): 2365. DOI: https://doi.org/10.3390/electronics10192365.

Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, MH. and Lim. 2020. Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE Access. 8: 167123–167163. https://doi.org/10.1109/ACCESS.2020.3022661.

Sivaselvan, N., Bhat, KV., Rajarajan, M., Das, AK., *et al*. 2023. SUACC-IoT: Secure unified authentication and access control system based on capability for IoT. Cluster Computing. 26: 2409–2428. DOI: https://doi.org/10.1007/s10586-022-03733-w.

Received: July 21, 2025; Revised: August 25, 2025;
Accepted: Sept 16, 2025.

Copyright©2025, Aljohni *et al*. This is an open access article distributed under the Creative Commons Attribution Non-Commercial License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

