Security and Privacy Challenges in the Internet of Things: A Qualitative Content Analysis

Arkan Pradipta[1*], Nabila Kusumawardani[2]
[12]Department of Information Technology, Mikroskil University, Medan, Indonesia
*Correspondence: arkan.pradipta01@gmail.com

ARTICLE HISTORY
Received: *[13/10/2025]* **Revised:** *[20/11/2025]* **Accepted:** *[05/01/2026]* **Published:** *[28/02/2026]*
Vol/No/Pages: *[Vol 1(No.1), 1-9]*

Abstract

The Internet of Things (IoT) allows physical devices to interconnect through networks to collect, process, and exchange data across sectors, including smart homes, industry, healthcare, and public services. While it offers benefits such as automation, operational efficiency, and data-driven decision-making, the IoT ecosystem also presents complex security and privacy challenges. The heterogeneity of devices, limited computing resources, continuous connectivity, and the management of large volumes of data expand the attack surface and increase the risk of information misuse. This study aims to analyze the main themes in the literature on IoT security and privacy and to formulate mitigation recommendations based on the categories of threat, system layers, and protection mechanisms discussed in prior research. The study uses a qualitative approach with content analysis of literature focused on IoT security, privacy, vulnerabilities, detection mechanisms, and mitigation strategies. The synthesis identifies five main themes: device vulnerabilities and authentication, communication and network security, data protection and privacy, threat detection and response, and security governance across the device lifecycle. The results show that mitigation oriented to a single technology is inadequate for the interrelated risk characteristics of the IoT. A more comprehensive approach is needed through layered security, strong authentication, access restriction, encryption, device updates, anomaly monitoring, privacy protection by design, and continuous governance. The study provides a conceptual framework to help organizations connect threat categories with mitigation mechanisms and implementation needs.

Keywords: Internet of Things; cybersecurity; data privacy; qualitative content analysis; risk mitigation; layered security

1. Introduction

The Internet of Things (IoT) is a technological paradigm that connects physical objects, sensors, actuators, computing devices, and digital platforms through communication networks to support the automatic collection and exchange of data. Its application is expanding in smart homes, manufacturing, transportation, agriculture, healthcare, and urban infrastructure. Such integration enables real-time monitoring of conditions, the automation of processes, improved efficiency, and the development of more responsive services. Yet increased connectivity also deepens dependence on the security of devices, networks, applications, and data-processing infrastructure [1], [2].

IoT security is a different matter from the security of conventional information systems because the ecosystem comprises devices with diverse computing power, memory capacity, energy consumption, and update mechanisms. Some devices are designed to operate for long periods with minimal user intervention, while others have limited ability to apply resource-intensive security mechanisms. This heterogeneity makes it difficult to standardize security configurations and manage vulnerabilities consistently. As a result, a weakness in one component can affect the security of other devices or even an entire connected network [3], [4].

A range of prior studies has identified threats, vulnerabilities, and protection mechanisms in IoT environments. Krishna et al., for example, discuss a taxonomy of threats and attacks together with the challenges of addressing them [5], while Rachit et al. review the development of IoT security trends [6]. Obaidat et al. set out the relationships among security and privacy challenges, security frameworks, enabling technologies, and countermeasures [1]. The study by Altulaihan et al. likewise positions cyber threats, preventive measures, and future research directions as important components in developing IoT security [7]. These studies show that IoT security is a multidimensional problem that cannot be explained through a single type of attack or a single protection technology.

Beyond technical security, privacy is an important dimension because IoT devices can collect data about habits, activities, location, environmental conditions, and user characteristics. Data that appear non-sensitive when collected in isolation can reveal personal information when combined and analyzed at scale. In a smart-home context, for example, patterns of device use can offer clues about occupants' activities and routines. In healthcare, data from connected devices can relate to individuals' health conditions and behavior. Privacy protection therefore needs to cover the purpose of data collection, access restriction, storage arrangements, information sharing, and data deletion, not only the confidentiality of communication [8], [9].

Security and privacy issues are also bound up with the characteristics of the application sector. The Industrial Internet of Things (IIoT) requires attention to service availability, process integrity, operational safety, and the continuity of production. Tan and Samsudin discuss the technologies, countermeasures, and ongoing challenges of IIoT [10], while research in smart-home environments emphasizes the relationship among the protection of devices, networks, and personal information [9]. In IoT-based healthcare, risk must also be considered in terms of data sensitivity and the consequences of service disruption. Mitigation strategies must therefore consider the context of use, the sensitivity of information, and the impact of system failure.

The development of detection technologies based on machine learning and deep learning has further widened the range of mitigation options. Such approaches can be used to recognize unusual traffic patterns, detect deviant device behavior, and help identify potentially malicious activity. Bharati and Podder discuss the applications, challenges, and development directions of machine learning and deep learning for IoT security and privacy [11]. Even so, the use of artificial intelligence does not automatically resolve security problems. Data quality, model generalization, computational needs, the risk of manipulation, and the explainability of detection results all still need to be considered. Detection technology is best positioned as part of a broader security strategy.

Recent literature also shows attention to authentication, access control, scalability, and privacy protection. The study by Kokila and Srinivasa Reddy highlights authentication, access control, and scalability models in IoT security [12]. Wakili and Bakkali discuss privacy-preserving methods for IoT networks [13], while Ataullah and Chauhan review security- and privacy-enhancing technologies [14]. These developments show that the main challenge is not merely the availability of security technology but also its fit with device limitations, operational needs, and organizational capacity.

Although prior research has examined a variety of threats and mitigation mechanisms, a thematic synthesis is still needed to connect risk categories with protective measures that can be applied. Literature oriented toward attack taxonomies, data protection, anomaly detection, and layer-based security can offer complementary perspectives. Yet separate discussions can make it difficult for organizations to set mitigation priorities, understand the dependencies among mechanisms, and assign security responsibilities across the device lifecycle.

In light of these problems, this study aims to analyze the content of the literature on IoT security and privacy challenges, identify the main themes emerging in discussions of threats and mitigation mechanisms, and formulate recommendations that connect risk with protective measures. The study addresses three questions: (1) what are the main categories of security and privacy challenges discussed in the IoT literature; (2) what mitigation mechanisms are relevant to reducing these risks; and (3) what implementation challenges need to be considered so that mitigation can be applied sustainably?

The contribution of this study lies in a conceptual synthesis that connects threats, system layers, protection mechanisms, and implementation priorities. This framework is intended to help researchers and practitioners understand that IoT security requires a combination of technical safeguards, data management, operational monitoring, and organizational governance.

2. Method

Research Design

This study uses a qualitative approach with the content-analysis method to identify, group, and interpret themes related to the security and privacy of the Internet of Things. Content analysis was chosen because it allows the researcher to examine the substance of publications, recognize conceptual patterns, compare the focus of discussions, and build analytical categories from relevant sources.

The focus of the analysis covers four main dimensions: threats and vulnerabilities, impacts on security and privacy, mitigation mechanisms, and implementation challenges. These four dimensions are used to build a cross-literature synthesis without assuming that all prior research uses identical terminology, threat models, or evaluation methods.

The material available for preparing this draft consists of a list of references relevant to IoT security and privacy. This manuscript must therefore be understood as a draft qualitative synthesis based on the provided references, not as a content-analysis report that has completed all stages of searching, retrieving full texts, coding, and consistency checking. Claims about the number of documents analyzed, the frequency of themes, or the level of inter-coder agreement are not made, because data from carrying out those stages are not yet available.

Data Sources and Scope

The conceptual sources of the study come from publications that discuss cybersecurity, privacy, vulnerabilities, architecture, detection mechanisms, authentication, access control, and countermeasures in the IoT. The provided references include review articles, systematic surveys, studies of security technologies, and research focused on particular application contexts, such as smart homes, IIoT, and healthcare.

The scope of the literature is not limited to a single type of threat, because IoT security problems arise across various system components. Publications that address the security of devices, communication, applications, data management, and governance are treated as complementary sources. Literature focused on particular mechanisms is also used to clarify mitigation options, especially for authentication, access control, machine learning, and privacy protection.

To make this study a replicable content analysis, the final conduct would need to record the databases used, search dates, search strings, publication-year range, inclusion and exclusion criteria, and the number of documents at each selection stage. This information cannot be determined from a reference list alone and must be completed on the basis of a search actually carried out.

Eligibility and Selection Criteria

The suggested selection criteria include direct relevance to IoT security or privacy, discussion of threats or mitigation mechanisms, clarity of bibliographic information, and the availability of adequate information for analysis. Publications that merely mention the IoT without substantively discussing security or privacy issues should not be included in the final corpus.

The selection process should be carried out in stages through examination of titles, abstracts, and full texts. Publications meeting the criteria are then recorded in a data-extraction sheet. To reduce selection bias, inclusion and exclusion decisions should be based on criteria set before the analysis rather than on the fit of findings with the researcher's expectations.

Because search and selection data have not been included in the material for this draft, the number of publications passing selection cannot yet be stated. The available reference list serves as an initial corpus that still needs to be verified and adjusted in line with the actual selection procedure.

Content Analysis Procedure

The content analysis is designed in four stages. First, familiarization and information extraction are carried out by reading the selected publications and recording the research aim, the IoT application context, the type of threat, the components affected, the impact of the risk, the mitigation mechanisms, and the limitations reported.

Second, initial coding is carried out by assigning codes to relevant information. Initial codes may include weak authentication, insecure configuration, firmware vulnerabilities, network attacks, data leakage, user tracking, anomaly detection, encryption, access control, device updates, and security governance. These codes serve as initial categories that must be checked and adjusted when full texts are analyzed.

Third, grouping codes into themes is carried out by identifying relationships among categories with similar characteristics. For example, weak authentication and credential management can be grouped as issues of identity and access, while excessive collection and uncontrolled data storage can be grouped as data-privacy risks.

Fourth, synthesis and interpretation are carried out by comparing themes across publications, identifying relationships between threats and mitigation, and formulating recommendations that take the implementation context into account. If coding is performed by more than one researcher, the final process should include a check of inter-coder agreement and documentation of how differences in interpretation were resolved.

Analytical Framework and Trustworthiness

The analytical framework connects three elements: the category of threat, the system component or layer affected, and the relevant mitigation mechanism. This framework allows a threat to be understood in terms of where it emerges and the protective measures that can be applied.

The reliability of interpretation can be strengthened through documentation of coding decisions, recording the source for each theme, comparing findings that support or limit an interpretation, and re-examining the relationship between textual evidence and conclusions. Researchers also need to distinguish recommendations explicitly discussed by a source from recommendations that are the product of synthesis across sources.

This approach is important so that the results do not equate the existence of a technology with evidence of its effectiveness. The use of encryption, for example, is a relevant protection mechanism, but the effectiveness of its implementation still depends on key management, configuration, the scope of the communication protected, and integration with other security controls.

3. Results

Overview of the Literature and Emerging Themes

The conceptual synthesis of the available references shows that IoT security and privacy can be understood through five main themes: (1) device security, identity, and authentication; (2) communication and network security; (3) data protection and privacy; (4) threat detection and response; and (5) security governance across the device lifecycle.

These five themes are interrelated. A device vulnerability can become the starting point for a network compromise, while unauthorized access to a network can open opportunities for data theft or manipulation. Conversely, security mechanisms that protect a network do not necessarily prevent the excessive use of data by applications that hold legitimate access. The analysis of IoT security therefore needs to consider the relationships among technical aspects, information management, and organizational processes.

Survey literature that discusses IoT security broadly provides a basis for understanding the relationships among threats, vulnerabilities, enabling technologies, and countermeasures [1], [4], [15]. Further reviews likewise map the field and its critical categories, from systematic reviews of IoT security to broad surveys of security and privacy concerns and security-and-solutions surveys [16], [17], [18], [19]. Studies focused on the data perspective, on system layers, or on particular application contexts help clarify that sources of risk can emerge in different components and require tailored responses [8], [20].

The following themes are the product of a conceptual organization of the topics covered in the reference list. They cannot yet be interpreted as empirical coding results counted from the full texts of all publications.

Device Security, Identity, and Authentication

The first theme concerns device security, identity management, authentication, and access control. IoT devices may have insecure default configurations, weak credentials, limited authentication mechanisms, un-updated firmware, or poorly protected administration interfaces. Such weaknesses can allow unauthorized parties to take over a device, change its configuration, or make it part of an attack on other systems.

Studies of IoT threats and key security issues position device characteristics and system vulnerabilities as an important part of the protection challenge [3], [5]. Rachit et al. also discuss IoT security trends [6], while Kokila and Srinivasa Reddy specifically review authentication, access-control, and scalability models [12].

From a mitigation perspective, device protection needs to begin at procurement and initial configuration. Each device should use a verifiable identity, unique credentials, authentication appropriate to the level of risk, and access rights restricted to need. Easily guessed default credentials need to be changed before a device is put into operation. In addition, administrative access must be restricted and logged so that configuration changes can be traced.

Firmware updating is also an important part of device security. Organizations need to know the devices in use, their software versions, the manufacturer's update support, and the procedure for handling vulnerabilities discovered after deployment. Devices that no longer receive updates require a specific risk assessment—for example, through network isolation, function restriction, or replacement if the risk is unacceptable.

Communication and Network Security

The second theme covers the security of the communication and networks that connect devices with gateways, servers, applications, or data-processing platforms. Unprotected communication can open opportunities for eavesdropping, message manipulation, identity spoofing, or disruption to service availability. Networks that are not separated by function can also allow a compromise of one device to spread to other components.

Reviews of IoT security show the importance of understanding threats at various layers and the relationship between enabling technologies and countermeasures [2], [1]. Ostovari et al. place security and privacy in a layered context [20], while Tan and Samsudin discuss the challenges associated with IIoT environments [10].

Mitigation recommendations for this theme include the use of communication protocols that support cryptographic protection, validation of endpoint identity, secure management of certificates or keys, and network segmentation by function and level of risk. Devices with different operational needs should not be placed in a single segment without adequate communication restrictions.

Monitoring network traffic is also needed to recognize activity inconsistent with normal operational patterns. However, monitoring must take into account device resource limitations, traffic volume, and the need to preserve user privacy. The collection of network data should be limited to the information needed to detect threats and support investigation.

Data Protection and Privacy Risks

The third theme concerns the protection of data and user privacy. IoT devices can collect data related to identity, location, habits, household activities, environmental conditions, and health information. Privacy risk arises not only when data are stolen by an attacker but also when an organization collects, stores, uses, or shares information beyond the necessary purpose.

Hou et al. discuss IoT security from a data perspective [8], while Ogonji et al. review security and privacy issues more broadly [4]. The study of smart homes by Magara and Zhou underscores the relevance of security and privacy in environments connected to personal activity [9]. Wakili and Bakkali make privacy-preserving methods the focus of their study [13], while Nezamdoust et al. discuss security and privacy mechanisms in IoT-enabled telehealth systems [21].

Privacy mitigation needs to include limiting data collection, reducing direct identifiers when they are not needed, setting retention periods, protecting storage, and restricting secondary use. Organizations also need to explain the purpose of data collection and who can access it. User consent, where required, should be accompanied by understandable information about the data collected and the consequences of its use.

Encryption can help protect the confidentiality of data in transit and at rest, but it is not sufficient to address all privacy risks. Data that have been decrypted by an authorized application can still be misused. Privacy protection therefore needs to be supported by access control, data minimization, the separation of identity from operational data where possible, and policies for using and deleting information.

Threat Detection and Incident Response

The fourth theme covers the identification of attacks, the detection of anomalous activity, security monitoring, and incident handling. The diversity of IoT devices and communication patterns makes threat detection a challenge, especially when a system must distinguish changing normal behavior from malicious activity. An undetected attack can cause data loss, service disruption, process manipulation, or the spread of compromise to other devices. The study by Krishna et al. positions a taxonomy of threats and solutions as an important element in IoT security research [5]. Altulaihan et al. discuss countermeasure techniques and future research directions [7], while Tariq et al. examine IoT cybersecurity and directions for further research [22]. Bharati and Podder highlight the use of machine learning and deep learning for security and privacy [11].

Machine-learning-based approaches can help detect unusual communication patterns and identify deviations in device behavior. Even so, detection models need to be evaluated by their detection-error rates, their ability to recognize new threats, their computational needs, and their resistance to manipulation. A model that produces too many false alerts can burden a security team, while a model that fails to detect threats can create a false sense of safety.

Detection systems therefore need to be combined with clear incident-response procedures. Organizations should have mechanisms to isolate compromised devices, revoke misused credentials, secure digital evidence, restore configurations, and evaluate the impact of an incident. Response should also include notifying relevant parties when a data breach meets the applicable reporting criteria.

Lifecycle Security and Organizational Governance

The fifth theme concerns security governance across the device lifecycle, from supplier selection, design, procurement, configuration, and operation to maintenance and decommissioning. IoT security cannot be assured merely by installing protection technology at the start of deployment. New vulnerabilities can be discovered after a device is in use, operational needs can change, and manufacturer update support can end.

The study by Omolara et al. discusses areas of IoT security that still require attention [15], while Altulaihan et al. emphasize research directions and mitigation [7]. Ataullah and Chauhan review security- and privacy-enhancing technologies [14], and Moucharraf et al. discuss architectures, threat models, detection methods, and countermeasures in IoT security [23].

From an organizational perspective, mitigation requires asset inventory, risk assessment, configuration policy, update procedures, supplier oversight, and the assignment of responsibility. Organizations also need to set criteria for when a device may be used, when it must be restricted, and when it must be retired because of risk that can no longer be managed.

Governance also involves a balance among security, cost, service availability, and user needs. Devices with limited resources may not be able to apply all the mechanisms available on general computing systems. Mitigation decisions therefore need to be based on the level of risk, the consequences of failure, device capability, and operational needs, rather than on applying as much technology as possible.

Synthesis of Threats and Mitigation Recommendations

Based on the five themes, the relationship between threats and mitigation measures can be summarized in the framework shown in Table 1.

Table 1. Synthesis of IoT Threat Categories and Mitigation Recommendations

Risk category	Example issues	Mitigation recommendations
Devices and identity	Weak credentials, insecure configuration, outdated firmware	Unique identity, strong authentication, least-privilege access, managed updates

Communication and network	Eavesdropping, message manipulation, lateral movement	Encryption, endpoint validation, network segmentation, traffic monitoring
Data and privacy	Excessive collection, leakage, secondary use	Data minimization, purpose limitation, access control, managed retention and deletion
Detection and response	Undetected attacks, delayed response	Anomaly monitoring, alert correlation, device isolation, incident-response procedures
Lifecycle governance	No inventory, end of update support, unclear responsibility	Asset management, supplier evaluation, periodic risk assessment, device-decommissioning plan

Note. The table is a synthesis of conceptual recommendations, not a measure of the relative effectiveness of each mechanism. The choice of measures needs to consider the application context, available resources, data sensitivity, and the potential impact of disruption.

4. Discussion

Security and Privacy as Interdependent Problems

The synthesis shows that IoT security and privacy need to be understood as two interrelated but not fully identical dimensions. Security focuses on protecting the confidentiality, integrity, and availability of systems and information. Privacy concerns the propriety of collecting, using, storing, disclosing, and deleting data that can relate to individuals. A system may have strong technical security controls yet still raise privacy problems if it collects information excessively or uses data beyond the purpose explained to users.

The data perspective discussed by Hou et al. [8] and the survey of IoT privacy and security by Ogonji et al. [4] help explain that protection is not sufficient on the communication channel alone. Protection must cover the entire data flow, from collection by sensors to storage, analysis, sharing, and deletion. This approach reduces the risk that securing one component masks a weakness in another.

The implication is that organizations need to distinguish controls aimed at preventing unauthorized access from controls that limit technically legitimate data processing that does not fit the established needs or purposes. Encryption, for example, helps protect data from parties without the key, but it does not determine whether an application is entitled to collect particular data. Purpose limitation and data minimization must complement such technical controls.

The Importance of Layered and Risk-Based Security

A layered security approach is relevant because threats can emerge at devices, networks, applications, computing services, and data-management processes. Ostovari et al. discuss security and privacy from a layered perspective [20], while Obaidat et al. comprehensively review security frameworks, enabling technologies, threats, vulnerabilities, and countermeasures [1]. Both perspectives support the understanding that no single mechanism can close every avenue of attack.

Applying layered security does not mean that all devices must use the same controls. An effective mitigation strategy needs to be risk-based. Devices that control industrial processes or support healthcare may require protection priorities different from those of consumer devices whose failure has a more limited impact. Risk assessment needs to consider the likelihood of a threat, the level of exposure, the value and sensitivity of data, the impact on operations, and the capacity for recovery.

In environments with computing constraints, controls need to be chosen with attention to resource cost and operational consequences. Cryptographic, authentication, and monitoring mechanisms must be implemented with appropriate configurations, without neglecting minimum security needs. A layered, risk-based strategy is therefore more realistic than an approach that relies on a single technology or requires all devices to apply identical controls.

The Role and Limitations of Intelligent Detection

Machine learning and deep learning can strengthen threat-detection capabilities by analyzing traffic patterns, device behavior, and deviations from normal activity. Bharati and Podder discuss the potential and challenges of such approaches in IoT security and privacy [11]. However, the synthesis also shows the need to distinguish the ability to detect anomalies from the ability to prove that an activity is an attack.

Unusual activity is not always malicious, while an attack designed to resemble normal behavior can escape detection. Changes in devices, usage patterns, and network conditions can also affect model quality. Detection models therefore need to be tested under conditions relevant to the deployment environment, including on resource-constrained devices and changing networks.

Organizations also need to attend to the governance of the data used to train and operate models. Broad collection of traffic or telemetry can create new privacy risks. The development of AI-based detection therefore needs to

follow the principles of data minimization, access restriction, periodic evaluation, and human oversight when detection decisions have a major impact on operations.

Context-Specific Implementation Challenges

The characteristics of the deployment environment shape the dominant types of threat and the priorities for mitigation. In smart homes, the main concern may include protecting personal information, securing consumer devices, and restricting third-party access [9]. In IIoT, disruption to availability, process integrity, and production continuity can have broader consequences [10]. In telehealth, the confidentiality of health information, access control, and service reliability need to be primary considerations [21].

These differences in context show that mitigation recommendations are best built around risk scenarios. Organizations need to map the devices in use, data flows, inter-system dependencies, and the consequences if a device fails or is compromised. This mapping becomes the basis for setting security requirements, the level of monitoring, update procedures, and recovery mechanisms.

Implementation challenges can also arise from dependence on suppliers, variation in technical standards, maintenance costs, limited expertise, and long device lifespans. In such conditions, security must be part of procurement and contract management, including clarity on update support, vulnerability disclosure, and responsibility for incident handling. Organizations that rely only on built-in security features without assessing long-term support risk retaining devices that become increasingly difficult to secure.

An Integrated Mitigation Framework

Based on the thematic synthesis, this study proposes a mitigation framework consisting of five layers of measures. First, device and identity protection—including asset inventory, secure configuration, authentication, access restriction, and firmware management. This layer aims to reduce the opportunity for a device to be used by unauthorized parties.

Second, communication and network protection—including encryption, endpoint validation, network segmentation, control of access among components, and traffic monitoring. The aim is to limit eavesdropping, communication manipulation, and the spread of compromise.

Third, data and privacy protection—including data minimization, limitation of processing purposes, access control over information, managed retention, and appropriate deletion. This layer ensures that technical security is complemented by control over how data are collected and used.

Fourth, detection, response, and recovery—including event logging, anomaly detection, alert handling, device isolation, configuration recovery, and post-incident evaluation. This layer is needed because prevention cannot guarantee that every attack will be blocked.

Fifth, governance and continuous improvement—including security policy, supplier evaluation, risk assessment, training, auditing, and management of a device's end of life. This layer connects technical controls with organizational responsibility.

These five layers need to be applied as a whole. Strong authentication, for example, will not be enough if a device continues to run vulnerable firmware that is not updated. Likewise, encryption will not prevent data misuse by an application with excessive access rights. An integrated framework allows organizations to examine the dependencies among controls and identify gaps that are invisible when each technology is evaluated separately.

Research Implications and Future Directions

The literature synthesis points to several relevant research directions. First, empirical evaluation is needed of the effectiveness of combinations of security mechanisms in real IoT environments. Research should not merely compare algorithms or detection methods under laboratory conditions but also consider energy consumption, latency, scalability, detection-error rates, and ease of maintenance.

Second, research needs to develop privacy-protection mechanisms applicable to resource-constrained devices. Wakili and Bakkali discuss a comparison of privacy-preserving methods [13], while the study by Nezamdoust et al. shows the importance of examining such mechanisms in IoT-based healthcare [21]. Future research can compare approaches by level of protection, computational cost, communication needs, and fit with the context of use.

Third, an approach to security management across the device lifecycle is needed. Research can examine how organizations manage devices that no longer receive updates, coordinate vulnerability disclosure, and assign responsibility when a device or service involves many suppliers.

Fourth, research on AI-based detection needs to incorporate privacy, resistance to manipulation, and the explainability of decisions. Model performance should be judged not only by accuracy but also by the operational consequences of detection errors and the need for human oversight.

Fifth, future research needs to improve the transparency and comparability of results. The threat taxonomy, the definition of metrics, test scenarios, and the characteristics of the devices used must be reported clearly so that results can be replicated and compared. This direction aligns with the need to develop IoT security research that not only produces new methods but also provides evidence of their implementation feasibility.

Limitations

This study has methodological limitations that need to be considered in interpreting its results. First, the synthesis in this draft is based on the provided references and cannot yet be treated as the result of a systematic analysis of the full texts of all publications. Second, the search procedure, the number of documents selected, and the actual coding process are not yet documented in the available material. The study therefore does not present theme frequencies or claim data saturation.

Third, the IoT security literature covers diverse application contexts and evaluation methods, so the conceptual findings cannot automatically be generalized to all devices or operational environments. Fourth, the presence of a mechanism in the literature does not, in itself, prove its effectiveness in real implementation. The recommendations in this study must therefore be understood as a conceptual synthesis framework that requires verification through full-text analysis and, where possible, empirical evaluation.

To improve academic rigour, a subsequent stage needs to carry out a documented database search, apply consistent selection criteria, code the full texts, and retain evidence connecting each theme to its source publication.

5. Conclusion

This study develops a qualitative synthesis of the security and privacy challenges of the Internet of Things through five conceptual themes: device and identity security, communication and network security, data protection and privacy, threat detection and response, and security governance across the device lifecycle. The synthesis shows that IoT risks do not stand alone but arise from the relationships among technical vulnerabilities, data flows, system configuration, and organizational management processes.

The mitigation recommendations formulated include strong authentication, need-based access control, device updates, encryption, network segmentation, data minimization, anomaly monitoring, incident response, supplier evaluation, and management of a device's end of life. The application of these mechanisms needs to be adapted to device characteristics, the sensitivity of information, the level of risk, and the consequences of disruption in each context of use.

The main contribution of this study is a conceptual framework that connects threat categories with mitigation mechanisms and governance needs. The framework underscores that IoT security and privacy are inadequate if they rely on a single protection technology. A layered, risk-based approach is needed so that the protection of devices, networks, data, and organizational processes can complement one another.

Even so, the findings in this draft remain a conceptual synthesis of the available references. Validation as a complete qualitative content-analysis study requires documented literature searching and selection, full-text examination, and traceable coding. Further research needs to test the effectiveness of combinations of mitigation mechanisms in various IoT environments, especially in light of device limitations, privacy needs, scalability, and the sustainability of security management.

Declarations

Acknowledgements. The authors would like to acknowledge the researchers whose published works on Internet of Things security and privacy provided the conceptual foundation for this study.

Author Contributions. Arkan Pradipta contributed to the conceptualization, methodology, literature synthesis, thematic analysis, and writing of the original draft. Nabila Kusumawardani contributed to the literature review, interpretation of the findings, critical revision of the manuscript, and refinement of the conceptual framework. Both authors contributed to the development of the manuscript and approved its final version.

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest. The authors declare that there is no conflict of interest regarding the publication of this article.

Data Availability. This study is a literature-based review. The references used to develop the conceptual synthesis are listed in the manuscript and include digital object identifiers (DOIs) where available. No new datasets were generated or analyzed for this study.

6. References

[1] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the Internet of Things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," Computers, vol. 9, no. 2, art. 44, 2020. https://doi.org/10.3390/computers9020044

[2] M. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Computer Networks, vol. 148, pp. 283–294, 2019. https://doi.org/10.1016/j.comnet.2018.11.025

[3] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things security: Challenges and key issues," Security and Communication Networks, vol. 2021, art. 5533843, 2021. https://doi.org/10.1155/2021/5533843
[4] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," Computer Science Review, vol. 38, art. 100312, 2020. https://doi.org/10.1016/j.cosrev.2020.100312
[5] R. R. Krishna, A. Priyadarshini, A. V. Jha, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," Sustainability, vol. 13, no. 16, art. 9463, 2021. https://doi.org/10.3390/su13169463
[6] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: A survey," SN Applied Sciences, vol. 3, art. 121, 2021. https://doi.org/10.1007/s42452-021-04156-9
[7] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," Electronics, vol. 11, no. 20, art. 3330, 2022. https://doi.org/10.3390/electronics11203330
[8] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," Computer Networks, vol. 148, pp. 295–306, 2019. https://doi.org/10.1016/j.comnet.2018.11.026
[9] T. Magara and Y. Zhou, "Internet of Things (IoT) of smart homes: Privacy and security," Journal of Electrical and Computer Engineering, vol. 2024, art. 7716956, 2024. https://doi.org/10.1155/2024/7716956
[10] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of Industrial Internet of Things (IIoT): A survey," Sensors, vol. 21, no. 19, art. 6647, 2021. https://doi.org/10.3390/s21196647
[11] S. Bharati and P. Podder, "Machine and deep learning for IoT security and privacy: Applications, challenges, and future directions," Security and Communication Networks, vol. 2022, art. 8951961, 2022. https://doi.org/10.1155/2022/8951961
[12] M. Kokila and K. Srinivasa Reddy, "Authentication, access control and scalability models in Internet of Things security—A review," Cyber Security and Applications, vol. 3, art. 100057, 2025. https://doi.org/10.1016/j.csa.2024.100057
[13] A. Wakili and S. Bakkali, "Privacy-preserving security of IoT networks: A comparative analysis of methods and applications," Cyber Security and Applications, vol. 3, art. 100084, 2025. https://doi.org/10.1016/j.csa.2025.100084
[14] M. Ataullah and N. Chauhan, "Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review," Security and Privacy, 2024. https://doi.org/10.1002/spy2.448
[15] A. E. Omolara et al., "The Internet of Things security: A survey encompassing unexplored areas and new insights," Computers & Security, vol. 112, art. 102494, 2022. https://doi.org/10.1016/j.cose.2021.102494
[16] A. Amiruddin, A. A. P. Ratna, and R. F. Sari, "Systematic review of Internet of Things security," International Journal of Communication Networks and Information Security, vol. 11, no. 2, 2019. https://doi.org/10.17762/ijcnis.v11i2.3533
[17] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A review of security and privacy concerns in the Internet of Things (IoT)," Journal of Sensors, vol. 2022, art. 5724168, 2022. https://doi.org/10.1155/2022/5724168
[18] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and solutions survey," Sensors, vol. 22, no. 19, art. 7433, 2022. https://doi.org/10.3390/s22197433
[19] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A literature review on security in the Internet of Things: Identifying and analysing critical categories," Computers, vol. 14, no. 2, art. 61, 2025. https://doi.org/10.3390/computers14020061
[20] P. Ostovari, S. Deep, A. K. Bashir, and X. Zheng, "A survey of security and privacy issues in the Internet of Things from the layered context," Transactions on Emerging Telecommunications Technologies, 2020. https://doi.org/10.1002/ett.3935
[21] M. Nezamdoust, M. Alizadeh, A. Seilsepour, and A. Asosheh, "A systematic mapping review of privacy and security mechanisms in IoT-enabled telehealth systems," Discover Internet of Things, vol. 6, art. 22, 2026. https://doi.org/10.1007/s43926-026-00290-1
[22] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," Sensors, vol. 23, no. 8, art. 4117, 2023. https://doi.org/10.3390/s23084117
[23] M. Moucharraf, M. Ridouani, F. Salahdine, and N. Kaabouch, "IoT security: A comprehensive review of architectures, threat models, detection methods, and countermeasures," Future Internet, vol. 18, no. 5, art. 266, 2026. https://doi.org/10.3390/fi18050266

© Journal of Sinar Data and Informatics (JSDI) — Sinar Asia Institute. This article is distributed under the Creative Commons Attribution (CC BY 4.0) license.