Internet of Things (IoT) Vulnerabilities: A Comprehensive Review

A.D.N. Kumarasiri, K.K. Bawantha, M.H.A. Hafas, P.L.A.J. Liyanage, S.F. Asra, M.R.M. Hanan, and A.M.A. Sujah

Abstract The fast integration of Internet of Things (IoT) gadgets into our critical infrastructure and daily lives has created an unprecedented attack surface, turning the security concerns that were once viewed as technical weaknesses into critical disruption threats to operational security and safety of the people. We conduct a critical overview of the present situation in the field of IoT security, synthesizing the results and methodological framework of a collection of 60 peer-reviewed publications released 2017-2025. Our discussion suggests that, although the underlying weaknesses of the old firmware, weak authentication, and insecure protocols are a continuing threat at the endpoint, and to the communication and application layer of devices, advanced attackers are broadening their use of the run-of-the-mill vulnerabilities to more advanced and industrialized attacks on operational technology (OT) and other systems of cyber-physical nature. The main threat has been transferred to targeted disruption. Furthermore, the review also critically analyzes the current methods of vulnerability detection and compares the traditional methods of vulnerability detection such as static and dynamic analysis with more modern methods of vulnerability detection such as resilience measures and Zero Trust Architecture (ZTA). The remaining part of the review states that to be able to protect the IoT ecosystem, we will have to become more careful in how we transition through reactive and device-based patching strategies, to more proactive architectural strategies, which emphasize resiliency across the ecosystem. We also critically review research gaps, such as defining and bridging the theory-practice gap and scalable and cost-effective solutions to security vulnerabilities and the special situation of insecure resource-constrained environments.

***Index Terms*— IoT Security, Cybersecurity, Vulnerability Analysis, Public Key Infrastructure (PKI), Threat Detection**

I. Introduction

INTERNET of Things (IoT) is changing the daily life and work by integrating daily devices into the internet so that they can gather and exchange information, improving efficiency and smartness in any industry [1],[2] Wearable devices that track the health of patients are constantly used in healthcare, whereas smart systems in factories can optimize the production process in real-time [3]. Farmers in agriculture can use IoT devices to check soil quality and automatically irrigate the soil, enhancing crop production and saving resources [4]. These are some of the examples of how IoT streamlines the business and facilitates a smart decision-making process in different fields [5].

Nevertheless, the intensive development of IoT creates severe security issues. IoT devices are vulnerable to cyberattacks due to their usual lack of computational power and the range of their types [6],[7]. Outdated software, poor encryption, improper network configuration, and inefficient access controls are the vulnerabilities that open an opportunity to the hackers [8]. The essential systems, such as hospitals, transportation, and energy grids, are still at risk due to the lack of security standards that should address the device proliferation [9]. One breached device has the potential to start bigger attacks, endangering confidential information and business continuity [10].

The review takes sixty research papers to offer an insight into the vulnerabilities of IoT and the methods through which researchers are planning to detect and address them. The articles include methods of attacks, new types of threats, and devices, communication, and application security [11]. The offered solutions that have a chance to be effective to the machine learning to detect threats, blockchain to protect the systems, and multi-layered defense solutions to enhance the security of the IoT [12]. The obstacles also include insufficient device computing capabilities, the absence of quality data, and the constantly developing cyber threats, thus causing issues when it comes to the universal security strategies [13].

The review highlights the necessity of security measures at several levels and provides recommendations on how the researchers, industry members, and policymakers need to eliminate

A.D.N. Kumarasiri is an undergraduate from the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka.

K.K. Bawantha is an undergraduate from the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka.

M.H.A. Hafas is an undergraduate from the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka.

P.L.A.J. Liyanage is an undergraduate from the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka.

S.F. Asra is an undergraduate from the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka.

M.R.M. Hanan is a demonstrator at the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka. (Email: mrm.hanan.official@gmail.com)

A.M.A. Sujah is a Lecturer (Prob) at the Department of ICT, South Eastern University of Sri Lanka, Sri Lanka. (Email: ameersujah@seu.ac.lk)

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

the current barriers [14]. The need to keep up with new threats, cross-industry cooperation, and the creation of multi-purpose and smart security measures to safeguard privacy, trust, and consistent functionality of an ever-changing, interconnected world is necessary to secure IoT systems [15].

II. METHODOLOGY

In this literature review, 60 peer-reviewed articles in various fields of IoT were scrutinized with a closer look to the manifestations of security flaws. The articles have been selected with care to ensure that they are relevant and exhaust the topic. This paper trusted credible sources including IEEE Xplore, Springer, and Science Direct to search using the terms including IoT vulnerabilities, static analysis, dynamic analysis and hybrid methodologies. To ensure that the review is current, the chosen studies were published in the period between 2017 and 2025. The review grouped the studies based on the kind of vulnerability they covered at device, communication or application level as well as the analysis techniques applied, including static, dynamic or hybrid techniques. It also discussed other application fields such as healthcare, industrial internet of things and smart homes. The individual studies have been thoroughly analyzed to identify shared trends, patterns, and gaps in the study, and consideration has been given to issues such as the role of machine learning, use of blockchain, and novel lightweight encryption methods. Other areas of weakness of the research that were highlighted in the review included excessive use of theoretical reviews or proposing solutions, which may not be as effective on a large scale. The review allowed obtaining a clear and in-depth picture of the field by clustering studies together according to their methods and main contributions, as well as to indicate which areas require additional exploration. It harmonized theoretical knowledge and practical issues in the security of IoT.

III. LITERATURE REVIEW

Combining the method of both static and dynamic evaluation of the vulnerabilities of Docker containers has enhanced IoT security with the help of AWS resources [16]. Clair is a static analysis tool, and Falco is a dynamic analysis tool, which is used to identify an existing vulnerability in code and unusual behavior at runtime, respectively. These are complementary approaches and AWS IoT Core guarantees the security of connections between devices. AWS CloudWatch has around the clock monitoring and Guard Duty detects threats, which forms a resilient security architecture. Nevertheless, static analysis may yield a high number of false positives and dynamic analysis cannot detect concealed vulnerabilities. Also, there is a challenge of scaling and third-party dependency in the implementation of AWS. Nevertheless, the combination of static and dynamic approaches is a beneficial factor to improve vulnerability identification and to build the multi-layered security plan despite all these problems [17]-[18].

IoT devices are investigated by means of firmware vulnerabilities that are analyzed using a combination of static, dynamic, and hybrid approaches [19]. Without running firmware, the insecure patterns of code are detected by the tools such as Binwalk and Ghidra, through the process referred to as the static analysis [20]. Dynamic Analysis is a real-time monitor of firmware activity and makes anomaly and threat observations. In order to cover all the ground, hybrid methods are used. There are more complex methods, like symbolic execution and fuzz testing, which are only restricted by device memory and proprietary code and testing infrastructure limitations. Therefore, there is no way of achieving complete protection of the IoT firmware and a layered approach is the best [21]-[22].

The application of machine learning (ML) techniques to the security threat in IoT is gaining popularity. The known threats are detected by supervised learning on the use of labelled data; anomalies are detected by unsupervised learning on unlabeled data and reinforcing learning enhances the intrusion detection process over time. Machine learning models, e.g. CNNs, RNNs, etc., are successful at analyzing complex data of the IoT in real-time [23]-[24]. The obstacles are lack of computing power of devices, the lack of high-quality data, and vulnerability to adversarial attacks. The presented Vulnerability and Threat Assessment Framework implement the standard techniques of threat modeling, the analysis of the network, the testing of the network and the use of honeypots in order to enhance the resilience of the IoT. Nevertheless, a combination of these strategies can offer to ensure the safety of the IoT systems a well-organized and multi-layered methodology [25].

In some of the studies, weaknesses in the physical layer of the IoT solutions, specifically LoRaWAN networks, have been identified, and risks like jamming, eavesdropping, as well as signal spoofing are pointed out [26]. Based on Software Defined Radio (SDR) testbeds, LoRaWAN networks are vulnerable to packet loss, communication breakdowns, and data breaches. Frequency hopping, adaptive data rates, and encryption are mitigation techniques that assist in enhancing security but complicate and consume power, especially when configuring low-energy IoT devices. Security testing is also limited by real world simulation constraints [27].

Other articles discuss security vulnerabilities at device, communication, and application levels with unauthorized access, data breaches, and denial-of-service (DoS) attacks being the most common types of threats [28]. It has been suggested to use a multi-layered methodology consisting of both static and dynamic testing of hardware ideals, software network protocol testing, intrusion and penetration testing, and end-user application testing [29],[30]. Strong encryption, authentication protocols, and intrusion detection systems are efficient countermeasures that are faced with the challenge of heterogeneity, resource constraints, and use of third-party services. The principles of security-by-design, real-time monitoring, and constant updates are required to ensure resilience [31].

Another research direction focuses on the dangers of third-party components (TPCs) in IoT firmware. A threat scan of more than 34,000 images of the firmware showed that there are rampant vulnerabilities in the older components, such as software bugs and CVEs. The problems with detection may be connected with obfuscation and runtime [32]. Timely updates, lifecycle management and security requirement are important to minimize systemic risks. Also, recent research on Wi-Fi-based IoT networks, with the help of such tools as ESP8266 NodeMCU, demonstrates that weak encryption and authentication leave devices exposed to malware, botnets, and even deauthentication attacks. Although

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

hardware-specific outcomes can restrict generalization, the study highlights the significance of formal defense mechanisms, real-time monitoring, and solid security implementations as the means of securing the IoT infrastructures [10].

Research on IoT-based home automation has put much emphasis on security and privacy issues such as unauthorized access, weak encryption, and insecure communication methods. Embedded sensor prototypes, attack vectors detection, and defensive mechanisms propose that smarter encryption and authentication can help to enhance system security, but all of the results are largely hypothetical and only available in the field of home automation, which must be exposed to dynamic security policies in smart homes [33]. Wireless sensor networks (WSNs) can be used in industrial IoT to enable smart manufacturing and Industry 4.0, but they are vulnerable to attacks like hardware, data interception, and malware attacks. The current countermeasures usually cannot keep pace with the changing threats, which suggests the significance of resilience-oriented, process-conserving security controls [34]. The use of machine learning algorithms, including Decision Tree, Random Forest, and Artificial Neural Networks have been used to identify threats in smart home with the Random forest achieving an accuracy of 99.4% ones. Although this is yielding results, there are issues such as scalability and real-time implementation [35]. Introducing more user awareness and additional technical defenses are necessary because corporate and user practices usually fail to capitalize on vulnerabilities [36]. Other cryptographic weaknesses of IoT systems are buffer over-read and inappropriate encryption in the firmware that require safe and proven cryptographic functions to secure multi-agent systems [37].

Industrial IoT and heterogeneous devices in general use legacy communication protocols, which add to the security risk, such as unauthorized access and information modification, as well as DoS attacks. Encryption, secure communications protocols, intrusion detectors, and blockchain-based decentralized authentication are some of the most exemplary countermeasures, but the problems of scalability, resource constraints, and dynamic threats remain a few [38],[39]. IoTSeer and vulnerability scanners such as Shodan allow finding and categorizing defects in smart homes and agriculture and enhancing risks recognition and mitigation strategies, but in practice, they are often not empirically justified in the field. The fast growth of the Internet of things (IoT) has revolutionized industries, healthcare, agriculture, smart homes, and manufacturing and provided superior efficiency, automation, and connection [15]. Yet such expansion has put IoT systems at risk of many security risks, jeopardizing the functionality of devices, data integrity, and user privacy [40]. IoT has facilitated better patient care in healthcare, although it has posed essential dangers because of unprotected medical equipment and software [41]. The article based on the results of the research by the National Vulnerability Database (2001-2022) exposed the vulnerability of electronic health records, wireless infusion pumps, and other medical systems, as well as hard-coded credentials and insufficient credentials management. One of the advice researchers give to mitigate the risk factors in healthcare IoT settings is secure software design, regulatory compliance, and real-time monitoring, and it is necessary to incorporate proactive solutions to guarantee safety in healthcare IoT settings beyond the analysis of historical data [42].

Poor encryption, weak authentication and user ignorance are also threats to smart homes [43],[44]. Although possible remedies, such as strong encryption, improved development methods and user training are meant to improve security, it has not been empirically validated [45]. Machine learning models such as Decision Trees, Random Forests, and Artificial Neural Networks (ANNs) are potential in identifying threats related to the IoT, and the accuracy of the latter is 99.4%. Nonetheless, the issues of scalability and real-time implementation within dynamic environments have not been resolved, which suggests the disparity between the theoretical frameworks and real-life implementation. The attacks on industrial IoT are hardware attacks, malware attacks and data intercepting, especially in smart manufacturing, and Industry 4.0 [46]. The analysis of vulnerability with the help of such tools as Shodan and Nmap identified important vulnerabilities, and the mitigation plans were not tested in real field conditions. It has been suggested to use hybrid deep learning models that combine CLSTM, CBiLSTM, and CNN-BiLSTM to identify vulnerabilities in IoT code, which provides better detection with synthetic data augmentation, but there are still the issues of bias and applicability in the real world [47]. The IoT devices were identified to be weak both in software and hardware with hybrid analysis techniques proposed as potential solutions. However, their practical implementation with non-Linux systems has not been exercised much [48].

The most common attacks in consumer IoT devices, such as webcams, routers, and wearable devices, are botnet attacks, malware and weak authentication protocols [49]. Research indicates that the use of old firmware, bad cryptography habits, and insecure codes are some of the contributing factors to the exploitation of the devices. Some of those suggested measures are effective encryption, multi-factor authentication, software regularly updated, and continuous monitoring [50]. High-tech options such as AI-based solutions, blockchain adoption, and post-quantum security are on the list of promising enhanced solutions, though the majority of them have not been tested under real-life circumstances [51]. Studies highlight the vulnerabilities on various levels, such as device, network, application, and peopleware. Possible threats are unauthorized access, data breach, denial of service (DoS) attack, and insecure communication protocols [52],[53]. Spinal tools like IoTSeer enable dynamic modeling of smart home devices and can precisely identify faults and policy violations with lower false positives but requires a lot of resources to initialize and pre-programmed policies [54]. RF-based attacks, including jamming and packet manipulations, were demonstrated to impact the functionality of the IoT devices until the next reboot, which indicates the necessity to protect the systems against radiophonic attacks more thoroughly [55].

Other vulnerabilities of IoT firmware and software include vulnerabilities in third-party code and improperly written code. Memory-related problems, denial-of-service threat, and poor authentication were shown in systematic reviews of C/C++ codebases of a variety of platforms such as Arduino and Raspberry Pi. Such findings highlight the significance of secure coding

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

TABLE I
COMPARATIVE ANALYSIS OF VULNERABILITY DETECTION METHODS

Method	Strengths	Limitations	Examples
Static	Efficient in detecting known flaws; resource light	Cannot detect runtime or emerging vulnerabilities.	Ghidra, Binwalk
Dynamic	Captures runtime threats and complex interactions.	Resource intensive; limited scalability	Falco, Penetration Testing
Hybrid	Comprehensive; combines static and dynamic benefits.	High computational demand; complex implementation	IoTSeer, Symbolic Execution

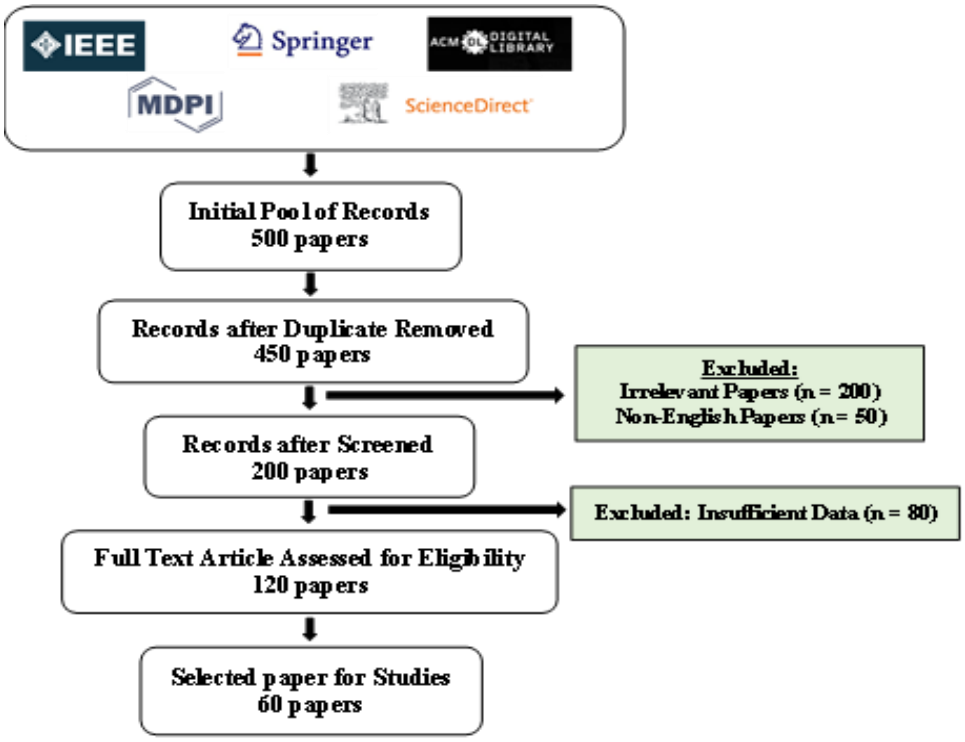

Fig. 1: PRISMA Diagram

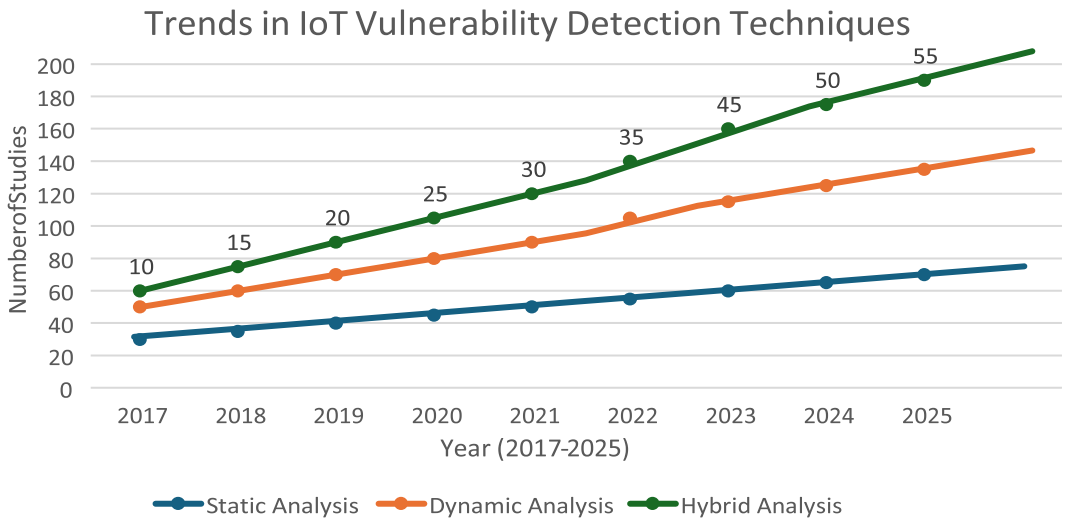

Fig. 2: Trends in IoT Vulnerability Detection Techniques

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

principles, identifiers of vulnerabilities, and auditing of the firmware to avoid exploitation. The fact that IoT devices can be a heterogeneous group and rely on a centralized system, only contributes to the complexity of security issues [56]. Resilience has been proposed to be improved with decentralized authentication, blockchain-based solutions as well as trust mechanisms. In addition, the interplay of the physical and digital threats, which are the out-of-band vulnerabilities necessitate active classification, characterization, and mitigation strategies beyond the conventional security model. Graph-based analysis and depth-first search have been used to determine vulnerabilities and rank high-risk attack paths in smart homes as efficient and yet controlled-condition solutions. Even with extensive research, a good number of solutions that have been proposed are either theoretical or in small scale. The agreement focuses on multi-layered security frameworks that combine encryption, authentication, intrusion detection, software updates, as well as user education [57]-[59]. New methods such as AI vulnerability detection, blockchain as a means of safe authentication, and deep learning as a vulnerability predictor have potential, but need more empirical confirmation and scalability testing [60]. Resilience and trustworthiness in similar IoT ecosystems can be improved by collaborated work between manufacturers, regulators, and users and universal security standards [15].

IV. Synthesis of Findings

The review's synthesis is essentially able presentation of the key conclusions regarding the 60 papers that were reviewed, together with their many categories of insights into IoT security trends, detection methods, and vulnerabilities. The most common and well-known aspect of vulnerability with regard to IoT devices is the ongoing expansion of devices without the timely adoption of comprehensive security measures. Device level, communication level, and application-level vulnerabilities were the three most important vulnerabilities found during the investigation. Weak authentication mechanisms, hard-coded passwords, and obsolete firmware were the most common concerns found on the device layer. These devices were also among the most frequently identified to have the potential to pose serious problems with system integrity and user privacy. Higher encryption and secure communication infrastructure are required because communication layer vulnerabilities are characterized by data interception and protocol exploitation. Application layer threats like weak access control and unsafe APIs highlight the pervasive flaws in software implementation and design. The most often used approaches in vulnerability detection research are static, dynamic, and hybrid. Static approaches do not monitor runtime behavior or potential threats, despite being remarkably effective at detecting known flaws, particularly in firmware and code structures. Runtime monitoring and penetration testing are used in dynamic techniques, which can provide a more accurate image of realistic vulnerabilities but are limited in terms of scalability and computational resources. The most comprehensive but resource-intensive approaches are hybrid ones, which combine static and dynamic techniques. Blockchain enables decentralization in device authentication and data integrity, while complementary technologies like machine learning help anomaly detection and threat prediction. Despite their potential, these cutting-edge solutions have encountered significant challenges in practical deployments, particularly in IoT situations with limited resources.

The most prominent developments reimagine the idea as a multi-layered security structure with integrated adaptive defense systems, proactive vulnerability management, and cooperative solutions with other industries, regulatory, and academic partners. Another trend under consideration is the increased importance placed on IoT domains in terms of attack prevention. Health, smart cities, and industrial automation are among the fields that have extremely different requirements from the varied risk profiles. It also draws attention to certain significant flaws, such as insufficient real-world testing, a lack of uniformity in the security standards, and the inability of the suggested solutions to scale. In order to handle the new complexities that IoT ecosystems are facing, the findings also support directing efforts toward scalable, affordable, and interoperable frameworks.

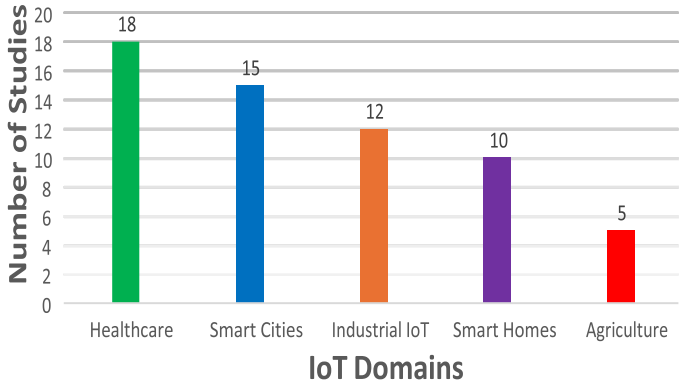

Fig. 3: Focus on IoT Vulnerability Research across the Domain

V. Discussion

The review's conclusions unequivocally highlight the wide range of IoT vulnerabilities dispersed throughout the device, communication, and application layers, which pose serious challenges to the security of diverse and resource-constrained IoT systems. The absence of current security solutions to handle the accelerating rate of change that IoT technologies and their threat environments have come to accept is a recurring theme. While static analysis techniques have proven to be quite effective in detecting known vulnerabilities, they typically fall short in capturing dynamic, runtime threats. On the other hand, dynamic analysis provides real-time information but is resource-hungry and does not scale effectively when big IoT networks are involved. Combining both of the methodology's advantages, hybrid techniques appear to have a lot of potential. Their implementation is fraught with difficulties, especially in contexts with limited resources. When combined with cutting-edge technology like blockchain and machine learning, there is a chance to alleviate some of these speculative shortcomings. Despite its disadvantage, the use of machine learning in prediction analytics and anomaly detection is proven to be

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

rather effective. Using machine learning in real-world IoT systems is limited by applications that demand large amounts of data and a lot of processing power. Blockchain's decentralized and unchangeable features also make it a powerful tool for establishing safe data sharing and device authenticity. However, lightweight blockchain protocols are necessary for the IoT scenarios' greatest resource consumption and scalability. The existing complex security landscape is made even more so by new threats including emerging vulnerabilities from 5G-enabled IoT systems and disruptions in encryption brought about by quantum computing. The response underlines the significance of performing proactive actions, such as the implementation of multi layered protection mechanisms, standardized protocols, and an emphasis on security by design principles. It also suggests that in order to overcome any potential vulnerabilities in IoT security frameworks, manufacturers, regulators, and researchers should continue to work together. The discrepancy between theoretical and applied models is another crucial realization. Practical IoT installations have not yet tested the majority of the suggested solutions. These results suggest that future research should focus on creating flexible, scalable, and reasonably priced security solutions tailored to IoT devices. Supporting zero-day vulnerabilities, immediate threat detection, and new regulatory compliance should be their main priorities. The development of those responses has become a top goal for global cybersecurity initiatives due to the growing integration of IoT in smart cities, critical infrastructures, and health systems.

The IoT networks form the basis of linking devices in various settings. Nevertheless, vulnerabilities of network technologies, including LoRaWAN, Wi-Fi-based IoT system, and industrial IoT protocols have become a significant concern. In the example of LoRaWAN networks, some of the physical layer threats include jamming, eavesdropping, and signal spoofing, where mitigation measures such as frequency hopping and adaptive data rate provide such protection at the cost of lowering the energy efficiency. Equally, owing to the use of Wi-Fi, IoT devices are vulnerable to malware, botnets, and de-authentication attacks due to the poor encryption and authentication engines. Outdated systems, which can be easily attacked by unauthorized people, manipulated information, and denial-of-service (DoS) attacks, are a particular challenge faced by industrial IoT protocols. In all IoT networks there is a frequent challenge of maintaining a balance between enhanced security and the lack of resources, such as processing power and power consumption, which means that future-scalable, real-time defense needs to be developed in heterogeneous network environments.

IoT is being extensively used in the areas of agriculture, healthcare, smart homes, education, and manufacturing, in terms of application. In farming, the sensor networks of IoT are used to monitor the quality of soil, automated irrigation, and the optimal use of resources. Nevertheless, agricultural IoT systems tend to have insecure communication protocols that pose a high risk of data breach, which can pose a threat to crop productivity. IoT devices like a wearable monitor and wireless infusion pumps are in a critical situation in the healthcare sector as they are confronted with weak encryption, hard-coded credentials, and weak credential management, which compromises patient safety and confidentiality. Although regulatory frameworks and secure development processes give some protection, lack of live threat detection is one of the weak links. Poor encryption and lack of communication security are also susceptible to smart homes, particularly focusing on convenience, and this would most likely result in unauthorized access. Random Forest algorithms, which are machine learning models, have demonstrated a very high level of accuracy in identifying these threats, but scalability in practice is still not an easy task. The education sphere is a developing stage where the use of IoT can improve research, yet the existing security measures are rather abstract and do not have practical support. IoT reinforces Industry 4.0 with smart systems in the sphere of manufacturing and industrial applications, but hardware attacks, malware, and data interception are also serious threats. Such tools as Shodan help to define vulnerabilities, and mitigation measures are not tested empirically in most cases. The combination of deep learning models can be promising in the area of vulnerability recognition, but the presence of bias and the lack of practical use is holding it back.

IoTs are also characterized by unresolved security vulnerabilities at several levels. Poor infrastructure also arises due to the old firmware, poor authentication and poor network configurations. There are also many devices that are dependent on third-party components that are known to be vulnerable, which increase systemic risks because of inadequate lifecycle management and infrequent updates. Vulnerabilities may be defined as device, communication and application layers. Hard-coded passwords and the use of outdated firmware's are device-level threats whilst the possibility of data interception and leveraging weak protocols are communication-level threats. Unsafe API and inappropriate access controls represent another vulnerability at the application level. Combined, all these layers of weaknesses compound general security risks of IoT systems.

There are a few particular types of attacks that are commonly aimed at IoT settings. Brute force attacks use the weak authentication systems, which result in unauthorized access. Attacks like buffer overflow attacks take advantage of insecure firmware and usually result in denial-of-service attack or execution of malicious codes. The botnet attacks are prevalent in the consumer specific devices like routers and webcams where lack of security enables attackers to form massive networks to coordinate attacks. Despite their advantageous functions in monitoring patients, wearable health devices are especially vulnerable to breaches of privacy and unauthorized access of third parties as there are no sufficient security controls.

Cryptographic tools and artificial intelligence (AI) applications are essential toward fixing these issues to provide security to IoT. Cryptography is still a foundation stone, and strong encryption algorithms, multi-factor authentication, and firmware updates they can be achieved were found to be critical protection measures. However, there are still issues of buffer overflow and broken cryptographic implementations, particularly in the IoT that has limited resources. Decentralized authentication and data integrity have been discussed in blockchain technology, but the challenge of scalability and energy efficiency prevents its usage. Simultaneously, AI and

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

TABLE II
EMERGING TECHNOLOGIES FOR IOT SECURITY

Technology	Applications	Challenges
Machine Learning	Anomaly detection, predictive analytics	Requires large datasets; high computation
Blockchain	Decentralized authentication, data integrity	High energy consumption; scalability issues
Quantum Cryptography	Future proof encryption techniques	Experimental; hardware dependent
Lightweight Protocols	Secure communication for constrained devices	Limited by processing and storage capacity

Machine Learning (ML) systems are also used in the context of anomaly detection, intrusion prevention, and predictive threat analysis. Architectures like the convolutional neural networks (CNNs), recurrent neural networks (RNNs), decision trees, and random forests have demonstrated remarkable performances with some registering a high accuracy of up to 99.4 percent in the detection of smart home threats. Nevertheless, these methods require large amounts of data and require large amounts of computing resources, and they are susceptible to adversarial attacks. The hybrid methods of implementing static, dynamic, and ML-based detection methods are becoming a potential solution, but additional real-world validation is required to achieve the potential fully.

Summary and Research Gaps: This synthesis grouping indicates redundant themes and issues like restricted devices, resource limitations, the existence of legacy elements, and the lack of practical testing of suggested security resolutions. The new technologies such as blockchain, quantum cryptography and lightweight protocols are promising but require additional testing and standardization. Some of the recommendations involve the development of multi-layered, scaled and adaptive security architectures, collaboration between manufacturers, regulators and researchers and also prioritizing on the aspects of security-by-design, which incorporates resilience as a proactive element of the IoT ecosystems.

VI. CONCLUSION

Thorough overview of the IoT security weaknesses and protection systems shows the urgent issues that are involved in the protection of the fast-growing sphere of interconnected gadgets. The device, communication, and application layers have vulnerabilities which are widespread, such as poor authentication, poor firmware, exploitation of protocols, and inadequate encryption. Heterogeneous IoTs have a complex nature, which is aggravated by the resource endowments of most devices, restricting the efficacy of the conventional security strategies. The literature synthesis shows that new solutions, including machine learning to identify threats, blockchain to decentralize the authentication process, and hybrid vulnerability assessment methods, have a potentially great future. Nevertheless, there are implementation limitations in practice such as scalability, computational overhead, real-time applicability and absence of standardized security. Research to practice the discrepancy between theoretical studies and practical deployment is the plausibility of scalable, resistant, and cost-effective architectural solutions with a focus on security through design and proactive ecosystem protection solutions. Future studies should focus on filling these gaps by coming up with light but strong security measures, improving interoperability between various systems in the IoT and encouraging multi-disciplinary approaches between industry, academia and regulatory agencies. Ability to integrate dynamically respondent adaptive security frameworks, which are able to respond to changing threat landscapes, will be critical to the protection of critical infrastructure and guarantee user privacy and trust. To sum up, the Internet of Things security needs a combined effort to overcome the theory-practice gap, unify security standards, and develop practical solutions to the specifics of the IoT environment. The complete potential of IoT can only be achieved with the help of joint dedication and continuous innovation without any harm to safety and reliability. This conclusion combines the results of the clustered sets, gives the summary of the main findings, omits gaps and offers research directions in the future, according to the expectations of the reviewer.

REFERENCES

[1] A. Aditya, D. Vidyarthi, and M. J. Nene, "A study of common vulnerabilities in IoT devices," in Proc. 11th Int. Conf. Reliability, Infocom Technologies and Optimization (ICRITO), 2024, pp. 1–6, doi: 10.1109/ICRITO61523.2024.10522155.

[2] L. Cambosuela, M. Kaur, and R. Astya, "The vulnerabilities and risks of implementing Internet of Things (IoT) in cyber security," in Proc. 11th Int. Conf. Reliability, Infocom Technologies and Optimization (ICRITO), 2024, pp. 1–5, doi: 10.1109/ICRITO61523.2024.10522460.

[3] C. M. Mejía Granda et al., "Security vulnerabilities in healthcare: An analysis of medical devices and software," Med. Biol. Eng. Comput., vol. 62, no. 1, pp. 257–273, 2023, doi: 10.1007/S11517-023-02912-0.

[4] K. E. Muwanga and E. Muwanguzi, "End user security using smart devices with ability to access IoT services," Int. J. Innov. Sci. Res. Technol., pp. 2805–2810, 2024, doi: 10.38124/ijisrt/IJISRT24SEP1430.

[5] J. Singh et al., "IoT vulnerabilities and countermeasures: A review," Int. J. Comput. Appl. Technol. Res., vol. 12, no. 3, pp. 75–81, 2023, doi: 10.7753/IJCATR1203.1005.

[6] T. Bakhshi, B. Ghita, and I. Kuzminykh, "A review of IoT firmware vulnerabilities and auditing techniques," Sensors, vol. 24, no. 2, 2024, doi: 10.3390/s24020708.

[7] S. Barrett, B. Boswell, and G. Dorai, "Exploring the vulnerabilities of IoT devices: A comprehensive analysis of Mirai and Bashlite attack vectors," in Proc. 10th Int. Conf. IoT: Systems, Management and Security (IOTSMS), 2023, pp. 125–132, doi: 10.1109/IOTSMS59855.2023.10325725.

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

[8] X. Feng et al., "Detecting vulnerability on IoT device firmware: A survey," IEEE/CAA J. Automatica Sinica, vol. 10, no. 1, pp. 25–41, 2023, doi: 10.1109/JAS.2022.105860.

[9] P. K. D. Pramanik et al., "A comprehensive review on IoT vulnerabilities, attacks and countermeasures," J. Netw. Comput. Appl., vol. 235, 2024, doi: 10.1016/j.jnca.2023.103768.

[10] M. Rizwan et al., "IoT vulnerabilities and their mitigation using blockchain," Cluster Comput., vol. 26, pp. 1325–1338, 2023, doi: 10.1007/s10586-022-03634-5.

[11] M. Bhole, W. Kastner, and T. Sauter, "Towards unveiling vulnerabilities and securing IoT devices: An ontology-based approach," in Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA), 2024, pp. 1–8, doi: 10.1109/ETFA61755.2024.10710882.

[12] P. Ma, L. Zhu, and C. Zhang, "Research on vulnerability mining method based on artificial intelligence in Internet of Things," in Proc. IEEE ICIPCA, 2024, pp. 1470–1473, doi: 10.1109/ICIPCA61593.2024.10709035.

[13] C. Mittal, "Obstacles and countermeasures for protecting Internet of Things devices from emerging security risks," Cyber Security: A Peer Reviewed Journal, vol. 8, no. 1, p. 48, 2024.

[14] D. Tran et al., "IoT security: Attacks, vulnerabilities and defense mechanisms," J. Commun. Inf. Netw., vol. 8, no. 2, pp. 75–88, 2023, doi: 10.23919/JCIN.2023.000022.

[15] A. Sharma et al., "IoT: Threats, vulnerabilities and challenges," Int. J. Eng. Trends Technol., vol. 71, no. 5, pp. 210–217, 2023, doi: 10.14445/22315381/IJETT-V71I5P223.

[16] V. Ajith et al., "Analyzing Docker vulnerabilities through static and dynamic methods and enhancing IoT security with AWS IoT Core, CloudWatch, and GuardDuty," Preprints, Jun. 2024, doi: 10.3390/iot5030026.

[17] F. Arat and S. Akleylek, "A new method for vulnerability and risk assessment of IoT," Comput. Netw., vol. 237, 2023, doi: 10.1016/j.comnet.2023.110046.

[18] H. Patel and D. Patel, "Security challenges in IoT: A review on vulnerabilities, attacks and countermeasures," Int. J. Comput. Appl., vol. 184, no. 31, pp. 1–6, 2022, doi: 10.5120/ijca2022922490.

[19] X. Li et al., "A comprehensive survey of vulnerability detection method towards Linux-based IoT devices," in Proc. ACM Int. Conf., 2023, pp. 35–41, doi: 10.1145/3605801.3605808.

[20] I. Delgado et al., "Exploring IoT vulnerabilities in a comprehensive remote cybersecurity laboratory," Sensors, vol. 23, no. 22, 2023, doi: 10.3390/s23229279.

[21] A. Alzahrani and M. Z. Asghar, "Cyber vulnerabilities detection system in logistics-based IoT data exchange," Egyptian Informatics Journal, vol. 25, 2024, doi: 10.1016/j.eij.2024.100448.

[22] M. Uddin, "IoT devices vulnerabilities and security challenges: A comprehensive review," Future Gener. Comput. Syst., vol. 144, pp. 375–390, 2023, doi: 10.1016/j.future.2023.03.008.

[23] X. Peng et al., "IoT security: Vulnerabilities, attack surfaces, and defense mechanisms," IEEE Access, vol. 11, pp. 28767–28783, 2023, doi: 10.1109/ACCESS.2023.3247185.

[24] K. N. Qureshi et al., "Security challenges, vulnerabilities, and attacks in Internet of Things," J. Inf. Security Appl., vol. 72, 2023, doi: 10.1016/j.jisa.2023.103407.

[25] M. Beyrouti et al., "Vulnerability and threat assessment framework for Internet of Things systems," in Proc. 6th Conf. Cloud and Internet of Things (CIoT), 2023, pp. 62–69, doi: 10.1109/CIOT57267.2023.10084894.

[26] P. H. Nguyen *et al.*, "Security vulnerabilities of IoT protocols: A survey," *Wireless Netw.*, vol. 29, pp. 1547–1565, 2023, doi: 10.1007/s11276-023-03309-0.

[27] M. Pawlicki, "Cybersecurity vulnerabilities in IoT ecosystems," *Appl. Sci.*, vol. 13, no. 4, p. 2356, 2023, doi: 10.3390/app13042356.

[28] M. Rao, "IoT and its security issues: Threats and vulnerabilities," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 12, no. 2, pp. 90–97, 2023, doi: 10.17148/IJARCCE.2023.12218.

[29] D. A. Cîmpean *et al.*, "Security assessment of an Internet of Things device," *Lect. Notes Netw. Syst.*, vol. 989, pp. 284–294, 2024, doi: 10.1007/978-3-031-60227-6_26.

[30] Z. I. Dafalla and A. Samraj, "Internet of Things security threats and attacks: Vulnerability assessment," *Lect. Notes Netw. Syst.*, vol. 711, pp. 1274–1287, 2023, doi: 10.1007/978-3-031-37717-4_85.

[31] A. Salem *et al.*, "IoT vulnerabilities and security threats: Review and future directions," *Sensors*, vol. 23, no. 17, p. 7324, 2023, doi: 10.3390/s23177324.

[32] D. Selvaraj and M. Uddin, "A large-scale study of IoT security weaknesses and vulnerabilities in the wild," *arXiv*, 2023, doi: 10.48550/arXiv.2308.13141.

[33] A. Khalid, N. A. A. Rahman, and K. S. Harun, "Secure IoT-based home automation by identifying vulnerabilities and threats," in *Digital Innovation Adoption*, 2024, pp. 40–50, doi: 10.2174/9789815079661-124010007.

[34] J. H. Kim, *A Survey of IoT Security: Risks, Requirements, Trends, and Solutions*. Singapore: World Scientific, 2017, doi: 10.1142/S2424862217500087.

[35] M. R. Joel *et al.*, "An analysis of security challenges in Internet of Things (IoT)-based smart homes," in *Proc. 2nd Int. Conf. Electronics and Renewable Systems (ICEARS)*, 2023, pp. 490–497, doi: 10.1109/ICEARS56392.2023.10085106.

[36] L. C. Goncalves *et al.*, "Study of vulnerabilities in IoT environments using Shodan and Censys tools," *Int. J. Adv. Res.*, vol. 10, no. 11, pp. 1306–1317, 2022, doi: 10.21474/IJAR01/15795.

[37] C. Mu *et al.*, "Vulnerability analysis for IoT devices of multi-agent systems," *Lect. Notes Electr. Eng.*, vol. 934, pp. 1510–1519, 2022, doi: 10.1007/978-981-19-3998-3_141.

[38] K. Manasa and L. M. I. Leo Joseph, "IoT security vulnerabilities and defensive measures in Industry 4.0," in *Advanced Technologies and Societal Change*, 2023, pp. 71–112, doi: 10.1007/978-981-99-2115-7_4.

[39] H. Wang *et al.*, "Security vulnerabilities of IoT ecosystems and solutions," *ACM Comput. Surveys*, vol. 55, no. 12, pp. 1–36, 2023, doi: 10.1145/3510433.

[40] C. M. Ogbodo *et al.*, "Internet of Things security: Threats, vulnerabilities and countermeasures," *Int. J. Inf. Security Sci.*, vol. 12, no. 1, pp. 15–26, 2023, doi: 10.5281/zenodo.7745169.

[41] A. Harkai, "Main characteristics and cybersecurity vulnerabilities of IoT mobile devices," *Smart Innov. Syst. Technol.*, vol. 367, pp. 219–230, 2024, doi: 10.1007/978-981-99-6529-8_19.

[42] M. A. Rahman *et al.*, "IoT vulnerabilities and security solutions: A systematic review," *Future Internet*, vol. 15, no. 5, 2023, doi: 10.3390/fi15050165.

[43] S. Devineni and B. Gorantla, "Security and privacy issues in Internet of Things (IoT) devices using COPRAS method," *REST J. Data Analytics Artif. Intell.*, vol. 2, no. 4, pp. 15–22, 2023, doi: 10.46632/JDAAI/2/4/3.

[44] R. Singh and S. Kumar, "IoT security vulnerabilities in smart devices: An overview," *Int. J. Eng. Res. Technol.*, vol. 12, no. 6, pp. 1025–1031, 2023, doi: 10.17577/IJERTV12IS060162.

[45] R. Rana *et al.*, "IoT vulnerabilities: An analysis of threats and security measures," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 500–509, 2023, doi: 10.14569/IJACSA.2023.0140660.

[46] D. B. Rawat *et al.*, "Cybersecurity in IoT: Threats, vulnerabilities, and mitigation," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4051–4064, 2023, doi: 10.1109/JIOT.2022.3228959.

[47] H. Mei *et al.*, "Detecting vulnerabilities in IoT software: New hybrid model and comprehensive data analysis," *J. Inf. Security Appl.*, vol. 74, 2023, doi: 10.1016/j.jisa.2023.103467.

[48] J. Mizera Pietraszko and J. Tańcula, "Vulnerability analysis of IoT devices to cyberattacks based on naïve Bayes classifier," *Lect. Notes Comput. Sci.*, vol. 13758, pp. 630–642, 2022, doi: 10.1007/978-3-031-21967-2_51.

[49] B. I. Mukhtar *et al.*, "IoT vulnerabilities and attacks: SILEX malware case study," *Symmetry*, vol. 15, no. 11, 2023, doi: 10.3390/sym15111978.

[50] K. Okoye *et al.*, "IoT vulnerabilities: Analysis and mitigation techniques," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 11, no. 6, pp. 2400–2407, 2023, doi: 10.15680/IJIRCCE.2023.1106022.

[51] A. Thakur and R. Yadav, "IoT devices: Security vulnerabilities and prevention techniques," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 11, no. 5, pp. 1800–1807, 2023, doi: 10.15680/IJIRCCE.2023.1105060.

[52] M. Lalit *et al.*, "IoT networks: Security vulnerabilities of application layer protocols," in *Proc. 14th Int. Conf. MACS*, 2022, pp. 1–5, doi: 10.1109/MACS56771.2022.10022971.

[53] A. Sheikh *et al.*, "Security vulnerabilities in IoT communication protocols," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 7, pp. 310–318, 2023, doi: 10.14569/IJACSA.2023.0140738.

[54] A. R. Yadulla, M. Yenugula, V. K. Kasula, B. Konda, and B. Y. R. Thumma, "Comprehensive analysis of IoT security: Threats, detection

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992

methods, and defense strategies," *J. Internet Things*, vol. 7, no. 1, pp. 19–48, 2025, doi: 10.32604/jiot.2025.062733.

[55] E. Anthi *et al.*, "Investigating radio frequency vulnerabilities in the Internet of Things (IoT)," *IoT*, vol. 5, no. 2, pp. 356–380, 2024, doi: 10.3390/iot5020018.

[56] R. Nagy, A. Farkas, and G. Hosszu, "Classification of the security vulnerabilities in the IoT network," *Procedia Comput. Sci.*, vol. 198, pp. 68–75, 2022, doi: 10.1016/j.procs.2021.12.218.

[57] A. A. Abomhara and G. M. Køien, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardware Syst. Security*, vol. 2, no. 2, pp. 97–110, May 2018.

[58] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Netw.*, vol. 56, pp. 122–140, Mar. 2017, doi: 10.1016/j.adhoc.2016.12.004.

[59] S. Ul Haq *et al.*, "A survey on IoT & embedded device firmware security: Architecture, extraction techniques, and vulnerability analysis frameworks," *Discover Internet Things*, vol. 3, no. 17, 2023, doi: 10.1007/s43926-023-00045-2.

[60] Y. Zhang *et al.*, "A comprehensive analysis of IoT vulnerabilities and defense mechanisms," *IEEE Access*, vol. 11, pp. 116500–116515, 2023, doi: 10.1109/ACCESS.2023.3289675.

Copyright ©2026 belongs to Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, #32360, Sri Lanka
ISSN: 2961-5992