IoT Attacks Countermeasures: Systematic Review and Future Research Direction

Joshua Teddy Ibibo(✉)

School of Computing, Edinburgh Napier University, Edinburgh, UK
joshua.ibibo@napier.ac.uk

Abstract. In order to connect heterogeneous nodes, objects, and smart devices of a network, such as e-transportation, e-health, e-education, e-home, and e-grip, the Internet of Things (IoT) has emerged as an efficient technology. This technology makes things easier, safer, and more productive for us all. These nodes are often resource-constrained because of their involvement in a huge network of heterogeneous devices, making them the weakest link in the chain for a cyber attacker because they generate enormous amounts of data despite a number of limitations, including memory, power, and low processor of the device. So these limitations make IoT devices vulnerable to a variety of security attacks. In this paper, we presented a survey on attacks IoT countermeasures, systematic reviews, and analyses of various IoT attacks that are occurring, classified them, discussed their defences, and identified the most significant IoT attacks countermeasures. A state-of-the-art analysis of the different attacks, including their effectiveness and degree of damage in IoT devices, has been given and contrasted. We identify the advantages and disadvantages of IoT Attack Countermeasures and proposed a Novel IoT Attack Countermeasures. Finally, we identify the open-research issue in the domain and provide directions for future research.

Keywords: IoT · Attacks · Countermeasures · privacy · security · IoT application

1 Introduction

The Internet of Things (IoT) was first used some 23 years ago by Kelvin Ashton while working on his newly developed sensor project in a presentation for Procter & Gamble in the context of RFID supply chains in 1999 [1] and David L. Brock [2] in 2001. However, Since 1832, there has been a theory of connected devices. It was possible to directly communicate between two devices by sending electrical signals when the first electromagnetic transmission was created. But the creation of the Internet in the late 1960s marked the beginning of the real Internet of Things. According to B. Ghaleb, IoT is defined as follows. "IoT is a network of connected smart objects that may exchange data over a wired network without the need for human-to-human (H2H) or human-to-computer (H2C) interaction [3]." There have been different applications that using the IoT technology have risen across all spheres of life attributed to its effectiveness and autonomy. Such applications include e-homes [4], e-offices [5], e-cities [6], e-education

Z. Tan et al. (Eds.): BDTA 2023, LNICST 555, pp. 95–111, 2024.
https://doi.org/10.1007/978-3-031-52265-9_7

[7], e-transportation systems [8], e-banking [9], and e-healthcare [10]. The implementation of this applications will be hampered by the lack of confidentiality, integrity, and data security. Majorities of the IoT attacks in the domain have received comments and discussions from [11–14]. IoT Attacks have been cited as an emerging concern to smart gadgets in a number of earlier papers [21–28]. These publications do not, however offer a taxonomy nor an analysis of the vulnerabilities and attacks implications. We provide a thorough analysis of the threats and exploits that are now being made against IoT devices in comparison to earlier works, and we offer a systematic analysis of threats to help people understand the attack methods and their effects on IoT devices. We looked at scientific publications on security, threats, and defenses in well-known databases like Google Scholar, Elsevier, the Edinburgh Napier University Library Search, the IEEE Xplore digital library, Rearchgate, and Science Direct. Out of the 500 journal and conference papers that were initially reported over the past ten years, 289 were picked for full-text examination after duplicate entries were removed and the abstract was examined. Only 85 articles were ultimately chosen for the study after 200 publications were excluded after reviewing the entire report. Below are six key contributions made by this work:

1. The research limits, unresolved issues, and potential paths for further research are mentioned.
2. The study offers knowledge about IoT architectures and infrastructure networks.
3. IoT security goals and problems are systematically clarified in the study.
4. We proposes a four-tier architecture for the Internet of Things
5. In order to secure IoT networks, it offers comprehensive and cutting-edge security novel IoT attack countermeasures.
6. Finally, it discusses the applicability of current defenses for various security attacks and offers possibilities for further research.

The rest of the paper is divided into the following sections. We look at the introduction of the domain, background and computing surveys. In Sect. 2, we go over IoT countermeasures overview, advantages and disadvantages of IoT attack countermeasures of each approach. We focus on the comparative systematic analysis of the Study in Sect. 3 and describe their overall IoT Attacks architecture and Its security challenges in Sect. 4. In Sect. 5, we provide a brief overview of the threats models on application domain and possible attacks within IoT. While in Sect. 6, we provide the countermeasures and threat models for security attacks in IoT.

1.1 Background and Statistics

Since the first theory of interconnected devices over the network was discovered in the 1980s, the concept of smart objects has been circulating. In the 1960s, the first attempts at automating smart objects that we use every day were made. Many industries tried to transfer tiny amounts of data in the 1990s transfer of packets between nodes [15]. The IoT goal has advanced significantly since then from a hypothetical idea to a top priority for many enterprises. Organizations over the world are searching for innovative methods to use and manage the data they acquire as they integrate IoT devices into their network infrastructures. Devices with IoT functionality can connect to a larger

network and perform a wide range of functions. Securing all that data, though, presents a completely new difficulty. If an IoT connection is not properly secured, it could lead to major occurrences. Most recently in the year 2022, there are statistics of industry IoT as fellow;

1. There are currently over seven (7) billion active IoT devices. However, the number of IoT devices is anticipated to more than triple by 2030 to reach 25.44 billion around the globe [17]. In 2030, there will likely be more than triple the figure 25.4 billion active Internet of Things (IoT) devices in the world
2. There will be 152,200 IoT devices connecting to the internet every minute by the year 2025 [17].
3. In the six years between 2019 and 2025, it is predicted that global IoT spending could approach 15 Dollars trillion [17].
4. By 2025, it is anticipated that IoT devices would produce 73.1 ZB (zettabytes) of data [16].
5. In the healthcare industry, where there will be a significant increase in the number of IoT-connected devices in 2020, COVID-19 stimulates further investment in the technology. As anticipated by statistics and IoT projections from years ago, the FreeStyle Libre smart CGM communicates diabetic patients' data to an app on iPhone, Android, and Apple Watch devices, and remote monitoring by caregivers [16].

However, according to IoT statistics, the CAGR decreased to 8.2% in 2020, which is a nearly twice as low increase as the predicted 14.9% at the end of 2019. With a CAGR of 11.3% from 2020 to 2024, things are anticipated to get back to normal in 2023 [18].

1.2 Computing Survey

There are many computing review survey papers on IoT attacks countermeasures, which Table 1 has summarized them.

The survey by Lin, Jie, et al. [12] improves user-friendly environments and network nodes in the event of failures, fog/edge computing has been proposed to be connected with the Internet of Things (IoT) to enable computing services devices installed at the network edge. Fog/edge computing can offer a better quality of service and quicker reaction times for IoT applications. Another author [7] purpose of this study is to describe the most recent advancements in utilizing IoT applications in education and to present opportunities and challenges for subsequent experiments. As stated researchers have neglected to offer a comprehensive review study on IoT in education, which is a component of the domain. This review study provides an overview of the potential for incorporating wearable technologies, green IoT, medical education and training, vocational education and training, and IoT in education. Since IoT adoption and applications are still in their infancy in underdeveloped countries, further research is definitely encouraged. The author [13] divided the survey into four sections, focusing on the most recent network node constraints, IoT network procedures and designs for device authentication, and an analysis of security vulnerabilities at various layers. The IoT is introduced in this paper [19] together with its well-known system design, enabling technologies, security problems, and objectives. The analysis of security flaws and the provision of modern security methods are additional features of the study [20]. A proactive network technology [21]

solution dubbed "PROSE," designed by the author of this paper, is used. It focuses on building reliable IoTs by proactively identifying critical nodes in the network so that they may be protected by deploying backups. We assume the worst-case scenario, where the attacker is able to capture/disable a section of the nodes, has comprehensive knowledge of the network architecture and traffic patterns, and is attempting to lower the maximum network throughput.

In [21], the researcher talks about several IoT attacks that are occurring, categorizes them, examines their defenses, and identifies the most notable IoT attacks in the network nodes. A cutting-edge analysis of the many attacks in the IoT has been given and compared, including their effectiveness and the degree of harm caused by the attacker. In this paper, [22], the author address the potential security threat and risks to industries using IoT devices, as well as the numerous attacks that could be made against the layered IIoT architecture's component parts and some safeguards. Finally, they proposed modern taxonomy to help reduce the risks of flaws in the IoT environment. This article [23] provided a thorough layer-by-layer analysis of IoT security vulnerabilities and the AI-based security models to mitigate such attacks within the domain. The protection of the IoT network is a big threat and future research goals are then discussed. In [24] Review the IoT's processes, goals, platforms, and methods. In order to classify IoT, we first introduce a brand-new classification system that ranks its approaches according to the relevant categories. To categorize the IoT literature, we second develop a classification strategy. In our third section, we look at the most significant IoT security breaches and the suggested defenses. Finally, we outline the unsolved problems in IoT security and privacy research and offer suggestions for future paths. However, [25] conducted a survey on IoT security in this report and examined the most pressing recent issues and Multi-layer attacks that are related to it. This study examines the IoT's security objectives and offers a taxonomy of attacks along with their remediation based on layer theory. The primary goal is to determine how, when, and why an IoT was penetrated or engaged in an attack. This [26] reviews the current defences against isolated side-channel attacks (SCA) before delving into unified defenses that help IoT devices overcome their power and footprint limitations. We also suggested using 3D integration as an IoT platform to protect the IoT system from advanced SCA. The ideal option for IoT systems is 3D integration because of its numerous benefits, including heterogeneous integration, split manufacturing, support for different IoT technologies like MEMS sensors, etc. the study [27, 28] examined machine- and deep learning-based security mechanisms for IoT and noted the drawbacks of each approach.

2 IoT Attack Countermeasures Background

The IoT uses diverse communication protocols for networks and objects, enabling M2M, T2T, H2T, and H2H interactions [29, 30]. Intelligent objects gather and transmit global data. Actuators enhance data processes and computer connections. Given IoT's scale, security is crucial, demanding attention from both business and academic experts [31].

Table 1. A Summary of Related Survey Papers

Reference	Input of Author	Attacks	Multi-layer Attacks	Threats	Privacy	Counter Measures	Threat Model
Lin, Ji et al. [12]	To research IoT centered on fog/edge technologies	1	0	2	1	0	0
Al-Emran et al. [7]	Highlight the most current developments in using IoT applications in education	0	0	0	2	0	0
Jie et al. [13]	examines how cyber-physical systems and IoT are related	1	0	2	1	0	0
Khanam et al. [19]	The author evaluates security flaws and provides modern security taxonomy	1	0	1	1	1	0
Ashraf [20]	This paper proposes PROSE-a proactive network fortifying solution in IoT	1	0	2	2	2	0
Deogirikar et al. [21]	The research analyzes several IoT threats, classifies them, and their defenses	1	0	1	0	2	0
Panchal et al. [22]	An IIoT attack taxonomy that we suggest	1	0	1	2	1	0
Zaman et al. [23]	This report provided a thorough layer-by-layer analysis of IoT security concerns	1	0	1	1	1	1

(*continued*)

Table 1. (*continued*)

Reference	Input of Author	Attacks	Multi-layer Attacks	Threats	Privacy	Counter Measures	Threat Model
Algarni [24]	Reviewing the SHS's approaches, goals, platforms, and methods	1	0	2	1	1	0
Gautam et al. [25]	We discussed a survey on IoT security and conducted an analysis	1	0	2	2	2	0
Dofe et al. [26]	We suggested using 3D integration as an IoT platform	1	0	1	0	1	0
Al-Garadi et al. [27]	examine ML/DL techniques for Internet networks	1	0	1	1	0	0
Hussain et al. [28]	Author discuss the existing ML and DL solutions for IoT network	1	0	1	1	2	1
Our	we presented a survey on attacks IoT countermeasures, systematic reviews, and analyses of various IoT network	1	1	1	1	1	1

Note: 1 = Fully Implemented, 2 = Partially Implemented, 0 = Not Implemented

2.1 Advantages of IoT Attack Countermeasures

1. Enhanced Security: The primary advantage of IoT attack countermeasures is the improved security they provide. By implementing security protocols and measures, the likelihood of successful attacks on IoT devices and systems decreases significantly.
2. Preventing Unauthorized Access: Countermeasures help prevent unauthorized access to IoT devices and networks, reducing the risk of data breaches and unauthorized control of connected devices.

3. Monitoring and Detection: Countermeasures include monitoring and detection systems that can identify potential threats and suspicious activities in real-time. Early detection allows for a quicker response and minimizes the impact of attacks.
4. Privacy Protection: IoT attack countermeasures help protect the privacy of users and organizations by ensuring that data is collected, stored, and processed in compliance with relevant regulations and policies.

2.2 Disadvantages of IoT Attack Countermeasures

1. Resource Constraints: Many IoT devices have limited processing power, memory, and battery life. Implementing strong security measures can consume additional resources, impacting the device's performance and battery life. Balancing security with resource constraints is a delicate challenge.
2. Potential Backdoors: While countermeasures are designed to improve security, if not implemented correctly, they may unintentionally create new vulnerabilities or backdoors that attackers could exploit.
3. Dependency on Third-Party Providers: Many IoT solutions rely on third-party services and cloud providers for security measures. Depending heavily on external entities raises concerns about data privacy, reliability, and vendor trustworthiness.
4. Legal and Ethical Concerns: Some IoT attack countermeasures may raise privacy and ethical concerns. For instance, data collection and monitoring practices may be viewed as invasive, leading to potential legal or public relations issues.

3 Comparative Systematic Analysis of the Study

This study examines articles on the IoT device security, privacy, and cyber-attacks. Key objectives, application domains, approaches, methodologies, and limitations in the field are all identified through the comparative systematic analysis. Many authors of original research literature were taken into consideration for the collection of the pertinent data, including Scopus, IEEE, Google Scholar, Elsevier, Springer, and ACM. The selection of papers was done using the next methodology: (1) Search each electronic database, (2) Find papers about IoT attacks countermeasures using specific keywords, (3) Compile the journal articles from steps 1 and 2, (4) Remove sources that are not from reputable peer-reviewed journals or conferences, (5) Are not pertinent to IoT attacks countermeasures, security, and privacy and (7) Classify the papers with the help of an expert panel. However, in our research with Scopus citation database more than 1,996 pieces of literature were found using databases in the English language and the starting search term "smart healthcare system security," without quotation marks. Only peer-reviewed publications released in or after 2015 were kept in this initial dataset. The dataset was reduced to about 708 results after the second pruning. ("IoT") OR ("Countermeasures") OR ("Attacks") OR ("Security") OR ("Privacy") and other IoT-related subject phrases were removed from the dataset a third time. As a consequence, a dataset with 146 items was trimmed. Reviews were disregarded because this study is primarily focused on primary sources. A final pruning process eliminated any articles that did not specifically address IoT attacks, security, and privacy along with the years of publication which is

from 2016–2022, as well as any that did not provide sufficient information on these subjects. The final dataset had 85 articles in it.

3.1 Classified by Publication Type

According to the distribution performance space, the articles chosen for review are categorised in this section. Figure 1 shows how the papers are distributed according to their broad type: 51.1% come from conferences, while 48.9% come from primary research published in reputable publications.

3.2 Classified by Publication Year

Figure 1 show how regularly articles are published in a certain field. Prior to 2015, there was little interest in the domain, and just 2% of the reviewed publications are published papers from that period. However, the number of publications that are declared in Figure 1 each year has increased significantly since 2015. In fact, 12% of the evaluated articles in 2017, the most recent complete year for which data were available, dealt with security and privacy in IoT attack defences. Given the availability of new wearable technologies and 5G networks, it is fair to anticipate that the quantity of articles discussing IoT attack defences will increase.

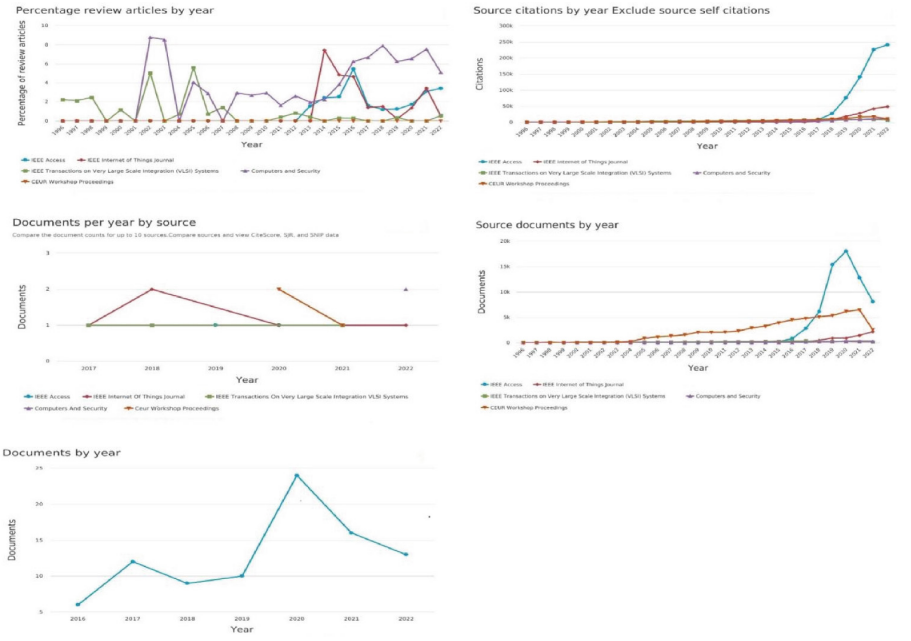

Fig. 1. Comparative Systematic Analysis of the Study

4 IoT Architecture and Its Security Challenges

Although there isn't a single accepted architecture for the IoT, there are a few unproven models with three, four, or five layers [?]. However, we will propose an acceptable model of the architecture of IoT together with their security operations as shown in Fig. 2 shows four basic layers such are, perception layer (PL), Middleware Layer (ML), Application Layer (AL), and Network Layer (NL).

4.1 Perception Layer (PL)

In IoT architecture, the PL also referred to Sensor Layer (SL), SL is a pivotal component in IoT architecture, facilitating device coordination, function control, data management, and user services [34, 35]. It employs protocols like Wireless Sensor Networks, RFID, and IDE. However, SL confronts significant security issues: weak device security, data tampering, encryption gaps, privacy risks, communication disruptions, and unauthorized access. Device impersonation and software vulnerabilities further threaten IoT [36]. Overcoming these challenges is vital for ensuring IoT ecosystem safety.

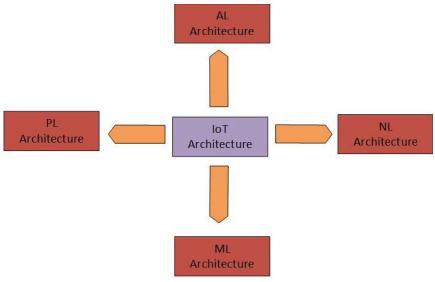

Fig. 2. An overview of IoT Architecture Within Network

4.2 Middle-Ware Layer (ML)

The ML is a subset of the IoT network architecture, related to the PL and TL [32]. The PL collects processed information from the TL, offers services using protocols, and passes data upwards. The TL handles network technologies like Wifi and Bluetooth. The ML focuses on network infrastructure, utilizing IPv6 for IoT device IP addresses. Security challenges confront the ML, which acts as a link between IoT devices and apps, attracting attackers [33]. Vulnerable middleware can lead to leaks and unauthorized access. Protocol vulnerabilities enable attacks like man-in-the-middle. Weak authentication and authorization risk data integrity. Middleware can suffer from buffer overflows and injection vulnerabilities. Securing configurations, strong encryption, and regular audits are vital for ML, ensuring overall IoT ecosystem security.

4.3 Application Layer (AL)

The AL in IoT architecture, also known as the Business Layer (BL), is the top-most layer that addresses user needs and technical standards across platforms. AL's functionality relies on key network protocols like HTTP, CoAP, and AMQP [38]. However, the AL encounters significant security challenges. Weaknesses in IoT applications can result in data breaches and unauthorized access. Insecure data handling risks sensitive information compromise. Flawed access controls may permit unauthorized manipulation of devices or data. Insufficient validation and input filtering can lead to code injection. Inadequate secure coding practices expose apps to exploitation. API vulnerabilities enable unauthorized access. Poor authentication jeopardizes identity protection. Robust security measures, secure coding, and regular assessments are vital for AL defense against threats. AL is user-oriented, managing tasks for end-users like controlling and monitoring. IoT applications span smart cars, health, home, office, banking, electricity, and environment, enhancing user experiences [37].

4.4 Network Layer (NL)

The NL within IoT architecture relies on mobile communication tools and internet technology for data transmission over long distances. It encompasses various communication networks, including a highly developed internet-based network. NL transfers data to users, processing it via intermediate network protocols originating from the Processing Layer (PL). IPV4, IPV6, RPL, and IPSec are NL tools [44]. Security challenges exist due to its critical role, facing threats like DDoS, spoofing, and traffic analysis. Inadequate segmentation allows lateral movement by attackers. Weak routing protocols risk data interception or manipulation. Absent encryption exposes data, while unauthorized network access disrupts operations. To address these concerns and ensure secure data transmission and network resilience, implementing robust access controls, intrusion detection systems, and secure routing protocols is crucial.

4.5 Security Challenges and Threat Model

For IoT applications to be safe and secure, there are certain security challenges, and threat models at each level of the IoT architecture must be addressed before the design and implementation of such layers [39]. Based on the architecture that is shown, we evaluate and analyse the current security threats that exist in the IoT architecture in Table 2 critically analysis different attacks in the architecture.

The studies carried out in [50, 53] indicate the security challenges, Multi-layer attacks, and ruthless cyber-threats enterprises have encountered recently. They detailed the security lapses and attacks that major and small firms in the UK have experienced from 2017–2022. According to statistics, there are 424 charities and 1,243 UK enterprises. 185 charities and 658 UK companies. Nearly four out of ten (42%) charities enable online donations, and just over four out of ten (44%) provide online service access for their beneficiaries [52].

5 Countermeasures and Threat Models for Security Attacks in IoT

Countermeasures and threat models play a vital role in securing the IoT ecosystem against security attacks. We propose four countermeasures and their corresponding threat models for security attacks in IoT:

1. Threat Model: Unauthorized Access Countermeasure: Implement strong authentication mechanisms, such as two-factor authentication or certificate-based authentication, to prevent unauthorized access to IoT devices and networks.
2. Threat Model: Denial-of-Service (DoS) Attacks Countermeasure: Implement traffic filtering, rate limiting, and anomaly detection to mitigate the impact of DoS attacks on IoT devices and networks.
3. Threat Model: Insecure APIs and Interfaces Countermeasure: Secure APIs and interfaces through proper authentication, access controls, and input validation to prevent API-based attacks.
4. Threat Model: Insider Threats Countermeasure: Implement role-based access controls, monitor user activities, and enforce the principle of least privilege to mitigate insider threats.

Table 2. Analytical comparisons of different attacks in IoT Network architecture

IoT Architecture					
S/N	Reference	Attack	Type	Action	Effect
1	[32–34]	Reply Attack	PL	Send signal to the network again and again	Availability of Data
2	[35, 36]	Port Scanning	ML	Obstruct the delivery and receipt of valid packages	Availability
3	[37, 38]	Poisoning Attack	AL	Maliciously injected code into network	Integrity
4	[39]	DoS	NL	Prevent legitimate to access the network	Availability

5.1 Novel IoT Attack Countermeasures

As technology advances and new IoT attack vectors are discovered, emerging IoT attack countermeasures are continuously being developed to address these evolving threats as shown in Table 3 [41–53]. We have proposed here are some of the emerging IoT attack countermeasures:

1. Hardware Security Modules (HSM) Countermeasure: Hardware Security Modules provide secure cryptographic processing and key management for IoT devices. HSMs

are tamper-resistant and protect sensitive cryptographic operations, ensuring the confidentiality and integrity of data.
2. Blockchain Technology Countermeasure: Blockchain technology is being explored to enhance IoT security by providing decentralized and tamper-resistant data storage and authentication mechanisms. It can help prevent unauthorized access and data manipulation in IoT networks.
3. Zero-Trust Architecture Countermeasure: Zero-trust architecture assumes that every device and user is untrusted until proven otherwise. This approach enforces strict access controls, continuously verifying the legitimacy of devices and users before granting access to resources.
4. Authentication and Authorization Countermeasure: Implement strong authentication mechanisms (e.g., two-factor authentication, certificate-based authentication) to ensure only authorized users and devices can access IoT systems and data.

Strengths of IoT Attack Countermeasures:

1. Diverse Defense Techniques: IoT attack countermeasures encompass a wide range of techniques, from encryption and authentication to intrusion detection systems and network segmentation. This diversity allows for a multi-layered defense approach that can effectively address various attack vectors.
2. Integration of AI and Machine Learning: AI-driven techniques, such as anomaly detection and behavior profiling, have the potential to identify new and previously unknown attack patterns. These technologies can adapt to changing attack methodologies, making them more robust against evolving threats.
3. Collaborative Solutions: Many IoT countermeasures encourage collaboration among devices and networks. Devices can share threat intelligence and collectively respond to attacks, thereby enhancing the overall security posture of the IoT ecosystem.

Weaknesses of IoT Attack Countermeasures:

1. Resource Constraints: Many IoT devices have limited computational power, memory, and energy resources. Implementing resource-intensive security mechanisms can lead to performance degradation and may not be feasible for all devices.
2. Regulatory and Compliance Challenges: Different regions and industries have varying regulations and compliance requirements for IoT security. This lack of standardization can complicate the implementation of consistent counter-measures.
3. Complexity and Usability: Some IoT security solutions can be complex to implement and manage. Complexity can lead to misconfigurations or neglect, reducing the effectiveness of countermeasures. Additionally, poor user interfaces can hinder proper configuration.

6 Future Direction, Summary and Conclusion

According to several surveys of literature studied above, the increased importance of IoT may grow over time. There are significant methods for protecting mobile mission-critical operations. A number of these could make the threat mitigation procedure more challenging and necessitate complete automation when it comes to individually or collectively safeguard the network. The following points provide a brief overview of our finding, recommendations and future direction.

Table 3. Comparative analysis of different countermeasures

Ref	Technology	Aim	Narration	Positive	Negative
[41]	Ultra-Low Power Public Key Cryptography	Reduced protocol overhead due PKC	PKC is beneficial to security services	Increased network/data security	It is a slow process
[42]	ICMetric Based Framework	Securing the IoT	Safeguard against threats	Preventing device unauthorized access	Potential for Direct Compromise
[43]	ICmetrics based security	Ensuring network integrity	Improving the security of IoT	Preventing device from cloning	Unauthenticated public keys
[44]	Anomaly-based intrusion detection systems	Proposed deep learning-based IDSs	IDSs with ML	Effective processing models	It is extremely expensive
[45]	Quality-Aware Streaming	D2D systems implementation	DASH technology	Solid network	IP spoofing
[46]	Intrusion Detection Technology in ML	Propose ML method for intrusion detection technology	Solve the safety risks of the system	Improve the detection accuracy	it is prone to DoS
[47]	Anomaly detection in IoT	Performances of ML models	IoT attack and anomaly detection	System accuracy	Incorrect Data Capture Difficulties
[48]	Symmetric and Asymmetric Key Cryptography	Proposed algorithms	Highly efficient in their respective domains	Effective network methods	High computational cost
[49]	IP-Base wireless sensor network	Propose SAKES	securing the IoT authentication model	Great inputs with security violations	May not be compactable with other IoT domain

1. More focus should be given to how to create a lightweight, reliable trust management system for both ultra-low power and powerful devices; further research must be done.
2. The security mechanisms should be updated to suit the system requirements and user needs better.
3. Resilience and Recovery Strategies: Developing strategies for IoT systems to quickly recover from attacks and restore normal operations is vital. This might involve redundancy, failover mechanisms, and rapid incident response plans.

4. Regulation and Standards: Collaborations between industry, researchers, and policymakers are essential to establish security regulations and standards for IoT devices. Research could focus on defining best practices and guidelines for IoT manufacturers to ensure security by design.
5. Human-Centric Security: Considering the human factor in IoT security is often overlooked. Future research could investigate ways to design user interfaces that help users understand and manage the security settings of their IoT devices more effectively.
6. Device Authentication and Identity Management: Enhancing authentication methods for IoT devices and establishing robust identity management mechanisms are critical. Future research could focus on developing lightweight yet secure authentication protocols and exploring the integration of blockchain technology for ensuring device identities and secure communication.

6.1 Conclusion

This article provides a thorough analysis of the Internet of Things, including its architectures, supporting technologies, and privacy and security challenges. There have been discussions about various IoT architectures, including our proposed model of the architecture of IoT along with their security operations. Figure 3 illustrates these operations with four fundamental layers: PL, ML, AL, and NL, in which our work analyzed the security issues and solutions. When employed in actual implementations, a number of applications, including the smart home, smart grid, smart health, smart transportation, and smart cities, are also vulnerable to dangers in the IoT application field. The main objectives of this study are to provide a clear, thorough, review, analysis, and deep understanding of IoT, explain the range of challenges it involves, and highlight areas that still need to be handled in order to promote the evolution of IoT. Furthermore, we have shown that little research is done in this area. We discussed security tactics while outlining unresolved issues and areas for further research.

References

1. Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S.: Vision and challenges for realising the Internet of Things. Cluster of European research projects on the internet of things, European Commision, 3(3), pp. 34–36 (2010)
2. Brock, D.L.: The Electronic Product Code (EPC) - A naming scheme for physical objects. White paper (2001)
3. Ghaleb, B.: Lecture notes in Introduction to Internet of Things (IoT). School of Computing, Edinburgh Napier University (2022). Accessed November 2022
4. Santoso, F.K. Vun, N.C.: Securing IoT for smart home system. In: 2015 International Symposium on Consumer Electronics (ISCE), pp. 1–2. IEEE, June 2015
5. Rafsanjani, H.N., Ghahramani, A.: Towards utilizing internet of things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings. J. Build. Eng. **27**, 100948 (2020)
6. Basford, P.J., Bulot, F.M., Apetroaie-Cristea, M., Cox, S.J., Ossont, S.J.: LoRaWAN for smart city IoT deployments: a long term evaluation. Sensors **20**(3), 648 (2020)

7. Al-Emran, M., Malik, S.I., Al-Kabi, M.N.: A survey of Internet of Things (IoT) in education: opportunities and challenges. In: Hassanien, A.E., Bhatnagar, R., Khalifa, N.E.M., Taha, M.H.N. (eds.) Toward social internet of things (SIoT): Enabling technologies, architectures and applications. SCI, vol. 846, pp. 197–209. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-24513-9_12
8. Kaiser, M.S., et al.: Advances in crowd analysis for urban applications through urban event detection. IEEE Trans. Intell. Transp. Syst.Intell. Transp. Syst. **19**(10), 3092–3112 (2017)
9. Ebrahimi, P., Moghaddam, D.K., Mehrabani, Y.S.S.: Challenges and Opportunities of Big data and IoT in the Electronic Banking Industry: A Systematic Literature Review (2022)
10. Selvaraj, S., Sundaravaradhan, S.: Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl. Sci. **2**(1), 139 (2020)
11. Burhanuddin, M.A., Mohammed, A.A.J., Ismail, R., Hameed, M.E., Kareem, A.N., Basiron, H.: A review on security challenges and features in wireless sensor networks: IoT perspective. J. Telecommun. Electron. Comput. Eng. (JTEC) **10**(1–7), 17–21 (2018)
12. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE IoT J. **4**(5), 1125–1142 (2017)
13. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. IEEE IoT J. **4**(5), 1250–1258 (2017)
14. Tewari, A., Gupta, B.B.: Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Futur. Gener. Comput. Syst.. Gener. Comput. Syst. **108**, 909–920 (2020)
15. Martin, J.: Osborne, Postscapes, History of Internet of Things. http://postscapes.com/internet-of-things-history. Accessed 10 Nov 2022
16. Howarth, J.: DataProt, 80+ Amazing IoT Statistics 2022–2030, 20 July 2022. https://explodingtopics.com/blog/iot-stats. Accessed 10 Nov 2022
17. Jovanovic, B.: Internet of Things statistics for 2022 - Taking Things Apart. DataProt, 13 May 2022. https://dataprot.net/statistics/iot-statistics/. Accessed 10 Nov 2022
18. Viala, S.: Reva Solution, Internet Of Things: New Challenges And Practices For Information Governance, 8 April 2015. http://www.revasolutions.com/internet-of-things-new-challenges-and-practices-for-information-governance/. Accessed 10 Nov 2022
19. Khanam, S., Ahmedy, I.B., Idris, M.Y.I., Jaward, M.H., Sabri, A.Q.B.M.: A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. IEEE Access **8**, 219709–219743 (2020)
20. Ashraf, U.: PROSE–proactive resilience in Internet of Things: targeted attacks and countermeasures. IEEE Sens. J. **18**(24), 10049–10057 (2018)
21. Deogirikar, J., Vidhate, A.: Security attacks in IoT: a survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37. IEEE, February 2017
22. Panchal, A.C., Khadse, V.M., Mahalle, P.N.: Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. In: 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). pp. 124–130. IEEE, November 2018
23. Zaman, S., et al.: Security threats and artificial intelligence based counter-measures for internet of things networks: a comprehensive survey. IEEE Access **9**, 94668–94690 (2021)
24. Algarni, A.: A survey and classification of security and privacy research in smart healthcare systems. IEEE Access **7**, 101879–101894 (2019)
25. Gautam, S., Malik, A., Singh, N., Kumar, S.: Recent advances and countermeasures against various attacks in IoT environment. In: 2019 2nd International Conference on Signal Processing and Communication (ICSPC), pp. 315–319. IEEE, March 2019
26. Dofe, J., Nguyen, A., Nguyen, A.: Unified countermeasures against physical attacks in Internet of Things - a survey. In: 2021 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 194–199. IEEE, December 2021

27. Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M.: A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tut. **22**(3), 1646–1685 (2020)
28. Hussain, F., Hussain, R., Hassan, S.A., Hossain, E.: Machine learning in IoT security: current solutions and future challenges. IEEE Commun. Surv. Tut. **22**(3), 1686–1721 (2020)
29. Horrow, S., Sardana, A.: Identity management framework for cloud based internet of things. In: Proceedings of the First International Conference on Security of Internet of Things, pp. 200–203, August 2012
30. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tut. **17**(4), 2347–2376 (2015)
31. Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the RPL-based internet of things. Int. J. Distrib. Sens. Netw.Distrib. Sens. Netw. **9**(8), 794326 (2013)
32. Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., Du, H.-Y.: Research on the architecture of internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, pp. V5-484–V5-487. IEEE (2010)
33. Yaqoob, I., Hashem, I.A.T., Mehmood, Y., Gani, A., Mokhtar, S., Guizani, S.: Enabling communication technologies for smart cities. IEEE Commun. Mag.Commun. Mag. **55**(1), 112–120 (2017)
34. Negash, B., Rahmani, A.-M., Westerlund, T., Liljeberg, P., Tenhunen, H.: LISA: lightweight internet of things service bus architecture. Procedia Comput. Sci. **52**, 436–443 (2015)
35. Chaqfeh, M.A., Mohamed, N.: Challenges in middleware solutions for the Internet of Things. In: 2012 International Conference on Collaboration Technologies and Systems (CTS), pp. 21–26. IEEE (2012)
36. Datta, S.K., Bonnet, C., Nikaein, N.: An IoT gateway centric architecture to provide novel M2M services. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 514–519. IEEE (2014)
37. Seleznev, S., Yakovlev, V.: Industrial application architecture IoT and protocols AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS. Int. J. Open Inf. Technol. **7**(5), 17–28 (2019)
38. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
39. Kharrufa, H., Al-Kashoash, H.A., Kemp, A.H.: RPL-based routing protocols in IoT applications: a review. IEEE Sens. J. **19**(15), 5952–5967 (2019)
40. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for IoT. In: 2011 International Conference on Multimedia Technology, pp. 747–751. IEEE (2011)
41. Gaubatz, G., Kaps, J.-P., Ozturk, E., Sunar, B.: State of the art in ultra-low power public key cryptography for wireless sensor networks. In: Third IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 146–150. IEEE (2005)
42. Tahir, R., Tahir, H., McDonald-Maier, K., Fernando, A.: A novel icmetric based framework for securing the Internet of Things. In: 2016 IEEE International Conference on Consumer Electronics (ICCE), pp. 469–470. IEEE (2016)
43. Hopkins, A.B., McDonald-Maier, K.D., Papoutsis, E., Howells, W.G.J.: Ensuring data integrity via ICmetrics based security infrastructure. In: Second NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2007, pp. 75–81. IEEE (2007)
44. Aldweesh, A., Derhab, A., Emam, A.Z.: Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues. Knowl. Based Syst. **189**, 105124 (2020)
45. Kim, J., Caire, G., Molisch, A.F.: Quality-aware streaming and scheduling for device-to-device video delivery. IEEE/ACM Trans. Netw. **24**(4), 2319–2331 (2015)

46. Fang, W., Tan, X., Wilbur, D.: Application of intrusion detection technology in network safety based on machine learning. Saf. Sci. **124**, 104604 (2020)
47. Hasan, M.M., Islam, M.M., Zarif, I.I., Hashem, M.M.A.: Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things **7**, 100059 (2019)
48. Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.: A deep learning approach to network intrusion detection. IEEE Trans. Emerg. Top. Comput. Intell. **2**(1), 41–50 (2018)
49. Chandra, S., Paira, S., Alam, S.S., Sanyal, G.: A comparative survey of symmetric and asymmetric key cryptography. In: 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), pp. 83–93. IEEE (2014)
50. Hussen, H.R., Tizazu, G.A., Ting, M., Lee, T., Choi, Y., Kim, K.-H.: SAKES: secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6L0WPAN). In: 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 246–251. IEEE (2013)
51. Jeba, A., Paramasivan, B., Usha, D.: Security threats and its countermeasures in wireless sensor networks: an overview. Int. J. Comput. Appl. **29**(6), 15–22 (2011)
52. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.: A survey of lightweight-cryptography implementations. IEEE Des. Test Comput. **24**(6), 522–533 (2007)
53. Baskar, C., Balasubramaniyan, C., Manivannan, D.: Establishment of light weight cryptography for resource constraint environment using FPGA. Procedia Comput. Sci. **78**, 165–171 (2016)