3rd Malikussaleh International Conference on Multidiciplinary Studies 2022 (3rd MICoMS 2022)

INTERNATIONAL CONFERENCE PROCEEDINGS
ISSN: 2963-2536

DOI: https://doi.org/10.29103/micoms.v3i.49

Towards The Secure Internet of Things: Threats and Solution

Munirul Ula[1*], Rizal Tjut Adek[2], and Muklish[3],

[1] *Department of Information Technology, Universitas Malikussaleh, Lhokseumawe, Aceh, Indonesia*
[2] *Department of Informatics, Universitas Malikussaleh, Lhokseumawe, Aceh, Indonesia*
[3] *Dept. of Civil Engineering, Universitas Malikussaleh,* Aceh, Indonesia
[*] *Corresponding author. Email: munirulula@unimal.ac.id*

ABSTRACT

The use of the Internet of Things (IoT) has recently become a worldwide trend, as this technology can connect various types of equipment such as sensors, cameras, and other devices via the internet. The broad adoption of various IoT technologies makes life easier and better for people. Internet of things applications has been widely used in Smart Building, Smart Vehicles, Construction Management, health management and many other applications. However, the IoT technology still has many flaws and weakness especially in its security and defence mechanism. This paper reviews and elaborate type of security vulnerabilities, issue and threats that IoT technology faces from academic research paper in the past 10 years. This review also aims to find the possible solutions proposed by researchers to overcome security weakness, threats and issue in IoT technology and its application. This research goal to provide guidelines for those who want to develop and improve IoT security. A systematic review was used as the methodology in this paper. The purpose of this systematic review is to survey the threats and vulnerabilities of IoT technology as reported in previous studies. This review also proposes a comprehensive countermeasure to the previously mentioned threats and weaknesses. This study's findings include the identification and classification of various threats in IoT, as well as methods for countermeasures against these attacks. It concludes with reviews of research gaps and future research directions to improve IoT security.

Keywords: *IoT Security, IoT Threat, IoT Security Challenge, IoT Security Solution, Systematic Review*

1. INTRODUCTION

Internet of Things (IoT) technology was first introduced in 1999. IoT is a system that is able to connect several smart devices to the network and allows them to communicate with other smart devices, and also be able to interact with the surrounding environment [1]. The rapid development of IoT technology has recently been greatly influenced by the development of sensor, computing and communication technology. Radio Frequency Identification (RFID) technology and Wireless Sensor Networks have played a major role in the growth of IoT in recent years [2]. RFID devices use electromagnetic waves to communicate between terminals or nodes with and other objects. The use of RFID is intended to identify and track an object using an RFID tag [3]. While the wireless sensor network (WSN) is a collection of sensor nodes connected to the network through devices such as routers and sink nodes. The use of RFID and WSN technology in IoT turns out to be a problem. RFID and WSN have very minimal protection and security systems when these devices are connected to the network [4]. To protect IoT technology from hackers or intruders, in general, there are three parts of IoT that must be protected. The first is the physical security of IoT devices, such as sensors and RFID. This physical device must be kept away from interception and interference by unauthorized parties [5]. The second is the safety of the operating system on various elements of the IoT, which must ensure that sensors, transmission systems, and other systems can function properly [6].

This paper examines various security threats in IoT technology as well as potential solutions. After the introduction, various types of IoT applications and the IoT architecture. The following section discusses the different types of IoT security threats, as well as security solutions. The discussion and conclusions are described in the final section.

2. IoT APPLICATIONS

Various IoT applications have been prototyped and implemented, such as smart-building [7], smart-home, smart-vehicle [8], smart-farming [5], and smart-industry applications [9]. This section discusses the characteristics of several IoT systems that have been widely implemented in everyday life.

2.1 Smart Vehicle Application

The smart-vehicle application is a development of the traditional transportation system by adding intelligent features to vehicle components. With IoT applications, vehicle owners can lock or unlock remotely, download road maps, access navigation services, and access traffic information. In addition, internet-connected cars can be equipped with security features to protect them from vehicle theft [10][6].

2.2 Smart Building Application

Smart homes and buildings enable efficient energy management systems. For example, a temperature control system equipped with temperature sensors and data analysis algorithms can adjust the room air temperature based on user preferences and habits [11][8][12].

2.3 Construction Management

One of the applications of the IoT system is the monitoring and management of modern infrastructure, such as bridges, traffic lights, railroads, and buildings [13]. At the project site, IoT has been used to monitor the condition of the building and structure. Furthermore, by utilizing IoT systems, construction companies can control all of their equipment on the side via the internet. These smart devices will make users' lives easier. This remotely controlled device will receive a user command to perform a setting action that will affect the surrounding environment [14] [15][16].

2.4 Health Monitoring

Recent advancements in biomedical, signal processing, energy-efficient devices, and wireless communications have transformed healthcare technology. Personal health monitoring, drug delivery systems, remote patient data retrieval, and other IoT technology adaptations in the health sector are examples of IoT technology adaptations. Data from sensors worn by patients is collected, processed, and stored in the long term so that it can be used for continuous medical records [8]. Various types of intelligent sensors have been used in fitness equipment, diets, and health monitoring systems [17]. The future of IoT systems in the health sector leads to the development of personal health monitors that enable early disease detection[18][19][20][21].

2.5 Energy Management

In the IoT-based energy industry, the utilization of intelligent systems with embedded sensors and actuators allows for a proactive approach to energy consumption optimization. [10][22]. Smart systems in electrical outlets, lights, refrigerators, and smart televisions, for example, are expected to share data with electrical energy supply companies [23][24]. A construction company, for example, may share road repair information with a navigation company that uses the Global Positioning System (GPS).Based on this information, the GPS device can determine alternative routes to avoid roads that are under repair[6] [14].

2.6 Environmental Monitoring

The use of a smart system equipped with sensors allows for environmental monitoring, including the detection of emergency situations such as floods, which necessitate emergency response operations. Furthermore, air and water quality can be studied using IoT-based devices and sensors. An IoT system can also easily monitor air humidity and temperature [13][11].

3. IoT ARCHITECTURE

In 2014, World Forum proposed an IoT architectural model consisting of seven layers [25], as shown in Fig. 3. The description of each layer in the architectural model is as follows.

1. *Layer 1-Edge Nodes:* This bottom layer is usually composed of devices such as sensors, smart-controllers, RFID readers, actuators, and the like. Confidentiality and integrity of data must be considered starting from this layer and also passed on to the layer above [10].

2. *Layer 2-Communication:* This layer consists of all components related to sending data (information) and also commands (command). This communication medium is responsible for providing a means of communication between devices at the node layer, between components at the second layer, and data transmission between the second and third layers (edge computing layer) [21].

3. *Layer 3-Edge Computing:* This third level is often also known as fog computing. At this level simple data processing is initiated. This step is intended to reduce the computational load at a higher level and also to speed up response. Most realtime applications need to compute as close to the IoT device as possible. The size of the processing at this level depends on the computing power of the service provider, server, and compute node. At this layer, signal processing methods and simple learning algorithms are usually used [26].

4. *Layer 4-Data Accumulation:* Many IoT applications do not require direct data processing. This layer allows changing the data format for data analysis purposes or sharing with computing servers at a higher level. The main task of this layer is to convert the IoT sensor output format into a format suitable for storage in the database, including filtering and reducing data and determining whether data needs to be forwarded for processing at a higher level or not.
5. *Layer 5-Data Abstraction:* This layer facilitates data processing and storage so that the next stage of processing becomes simpler and more efficient. Data processing includes the normalization or denormalization process, index determination, data consolidation, and providing access to multiple data stores [20].
6. *Layer 6-Application:* The application layer provides the information interpretation process. IoT applications at this level will require a lot of coordination with the data abstraction layer and data accumulation. IoT applications vary widely, depending on the application domain and the organization's business processes [18].
7. *Layer 7-User and Center:* In this layer, the user will take advantage of the application and also information on the results of the data processing performed on the layers below. The application of IoT at this layer can also be a data center for an enterprise [10].

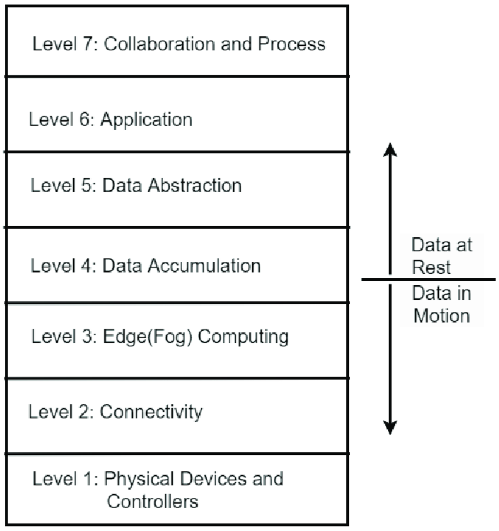
Level 7: Collaboration and Process
Level 6: Application
Level 5: Data Abstraction
Level 4: Data Accumulation
Level 3: Edge(Fog) Computing
Level 2: Connectivity
Level 1: Physical Devices and Controllers
Data at Rest
Data in Motion

Figure. 1. IoT World Forum Reference Model [27].

4. RESEARCH METHOD

The research methodology for systematic literature review mapping used in this study is based on the model proposed by Petersen et al. [28] as shown in Figure 1. The research questions aim to be answered in this study as follows:

- What are the challenges implementing IoT Security?
- What are the main threats to IoT Security?
- What are the solution for strengthen IoT security?

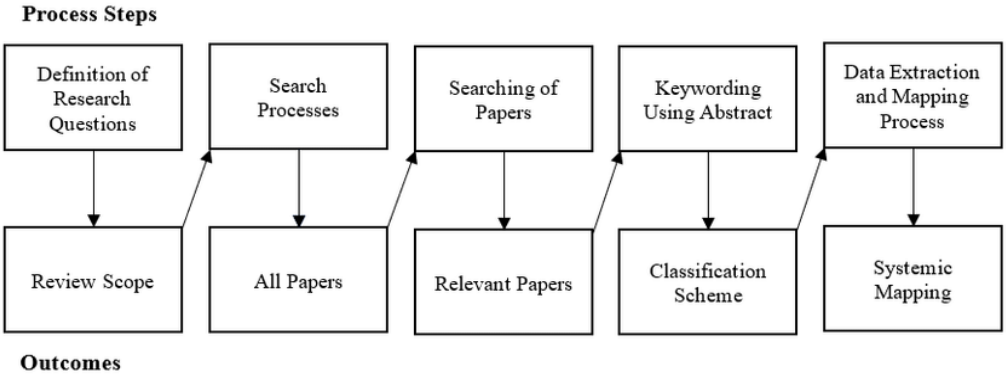

Figure. 2. Systematic Mapping Process.

The final result of this methodology is the generation of a systematic map about the study topic, which is illustrated, showing the frequencies of publications of each category.

In this systematic mapping phase, the search protocol of the research is guided and organized. The essential steps of the process are defined, such as research questions, document screening, abstraction keywords, and data extraction and mapping [28]. Two major databases chosen are Google Scholar and the Institute of Electrical and Electronics Engineers (IEEE) Xplore. The keywords used as filter as follows: ("security" OR "penetration" OR "hacking" OR "Threat OR "intrusion") AND ("Internet of Things" OR "IoT" OR "Arduino" OR "Raspberry Pi").

The Data collection process is divided into four stages: search in the databases, elimination of redundancies, final selection, and quality assessment. From the search strings generated based on terms and synonyms, a total of 526 articles is returned. After tabulating the articles, the redundancies are eliminated. Altogether, 243 redundancies were found. The title and abstract of the articles are read to select articles related to this study. In all, 32 studies were selected.

5. DISCUSSION

5.1 Security Threats on the Internet of Things

Fixing security issues in the system is an important factor in encouraging the widespread use of IoT technology. The Internet of Things is made up of many different components that work together to form a complex system. Data, devices, communication lines, sensors, and other elements make up the Internet of Things. As a result of the large number of entities and data involved in this system, the IoT security system is not properly standardized. The misuse of personal data information by outside parties, which can be used by criminals, is one of the security threats to IoT system users. [5].

Conventional security systems cannot be directly applied to IoT systems [29]. This is because objects in IoT are dynamic, in the sense that objects (devices) can freely join or separate from the IoT community where these objects join. Another very influential characteristic is the limited resources of IoT objects, both related to resources (power), processing speed (CPU), memory, channel capacity (bandwidth), and so on [9]. These characteristics make the characteristics of the security model in IoT different from conventional network security systems

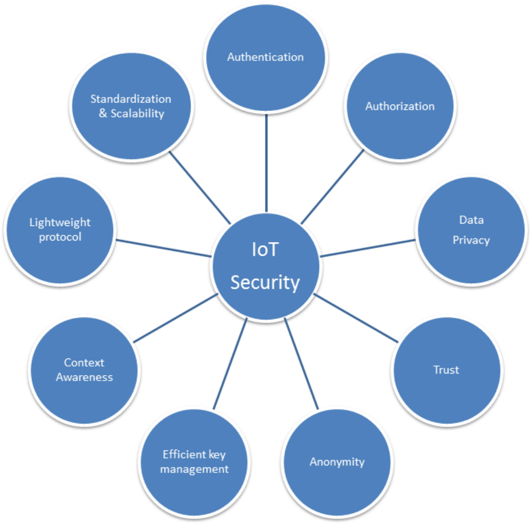

***Figure. 3**. IoT Security Requirements.*

In general, security aspects of information technology systems can be classified into three categories known as CIA-Triad, namely: (i) confidentiality, (ii) integrity, and (iii) availability. The CIA-Triad concept is not enough to define security aspects in systems that involve collaboration between many parties as is the case with IoT. A more comprehensive list of security characteristics has been developed by analyzing various sources of information and security-related literature [30]. Table I displays a list of security parameter requirements in IoT as well as their explanations and definitions.

5.1.1 IoT Security Threats at Layer Nodes

IoT systems and applications are starting to be implemented in a variety of applications from industrial management to personal health monitoring. This makes IoT systems and applications attractive for attackers to target, regardless of motivation.

One of the motivations of attackers in IoT systems is the theft of sensitive data and information, such as credit card numbers, location information, bank account passwords, and health-related data, by exploiting vulnerabilities in IoT systems.

1) Edge Node: IoT devices that are often found on edge nodes include RFID readers, sensors, and actuator nodes. The main attacks on this edge node are as follows [31].

2) Hardware Trojans. Trojan hardware attacks attack by modifying the Integrated Circuit (IC) which allows attackers to gain access to data or software running on the IC [10]. To be able to enter the Trojan, the attacker makes changes to the IC design before or at the time of fabrication and determines the trigger mechanism that will activate the Trojan. This Trojan activation mechanism can be done in two ways: i) internally, which will activate when a predefined condition is met; and ii) external, which will activate the Trojan by means of an antenna or sensor that can interact with the outside world.

3) Non-network side-channel attacks. Each node can disclose sensitive information under normal operating conditions, even when the device is not using a wireless communication medium for data transmission, such as a beacon that always transmits device status. Such vulnerabilities can be a privacy-related issue in medical systems. An example is a patient wearing a medical device that indicates a certain medical condition that has an impact on social stigma. This kind of thing can embarrass the patient if the illness is perceived negatively. In addition, medical IoT devices can also reveal personal health information, such as blood pressure, sugar levels, and so on [32].

4) Battery draining. Due to size limitations, IoT devices usually only have a small capacity battery. Therefore, this attack can have a serious impact because the device will fail to operate and fail to acquire data especially in times of emergency. For example, an attacker can find a way to drain a smoke detector battery, then an attacker can thwart the building's fire detection system alarm. In another example, the attacker could send thousands or millions of random packets requesting a response from the IoT device so that the device can drain the resources (battery) of the device [24].

5) Sleep deprivation. This DOS-type attack targets devices with limited energy capacity. In this attack, the attacker sends a number of requests that look genuine. Therefore, this type of attack is more difficult to detect. One of these attacks is a sleep deprivation attack on devices with limited battery resources [24].

6) Outage attacks. This attack occurs when an IoT device (edge node) fails to operate normally. In some cases, some tools or coordinator tools stop working. This failure can be caused by an error in the manufacturing process, battery drain, sleep deprivation, code injection, or illegal physical access to the device. One well-known example is the Stuxnet code injection attack on Iran's nuclear process control program [33].

7) Physical attack (tampering). IoT devices are often located in a vulnerable physical environment (plantations, fisheries, roads, livestock, and so on) making them vulnerable to physical attacks. With direct access, attackers can extract cryptographic information, modify circuits, change program code, or change operating systems. In fact, furthermore, the attacker can permanently damage the device. One example is the attack on the Nest Thermostat, in which the attacker tries to change the default firmware with a fake one. In this way, the attacker can control the thermostat even when the attacker has no direct access [12].

8) Node replication attacks. In this attack, the attacker installs a new node on a set of existing nodes by replicating one of the identities of the other nodes [10].

9) Camouflage attacks. In this type of attack, the attacker adds fake nodes or attacks (modifies) legitimate nodes to hide the existence of the attack. After that the modified node can operate normally as usual [34].

10) RFID tags: One of the most widely used edge-node devices in IoT systems is the RFID tag. There are several types of attacks on RFID tags, including the following.

11) Tracking. RFID devices have a unique identity. As a result, attackers can use unauthorized RFID-reader devices to read the identity of the RFID tag. This reading opportunity can be used by attackers to track an object that is the target of an attack [35].

12) Inventory. There are some types of RFID tags that contain useful information about the product to which it is attached. An Electronic Product Code (EPC) tag, for example, has two parts: a manufacturing code and a product code. As a result, someone with an EPC tag usually keeps a standard inventory so that tag readers can look at their products. [36]. This threat raises concerns about privacy. For example, an attacker might recognize a specific type of medical device, such as an insulin pump worn by a patient, and deduce that the patient has diabetes [8].

13) Cloning tags. Tag cloning (spoofing) attacks can be very profitable for hackers and very dangerous for a company's reputation. Damage can be compounded through attack automation [37]. Attackers can use cloning tags to access restricted areas of the company, bank account information, or other sensitive information.

14) DoS Attacks. In a DoS attack that attacks an RFID tag, the radio frequency channel is compromised so that the tag does not readable by tag readers and as a result the service becomes unavailable. An attacker could, for example, disable all RFID-based doors in a building to lock it down [38].

5.1.2 Security Threats at the Communication Layer

1) Eavesdropping: The attacker's actions of actively listening in on the data exchange that occurs on the communication channel are referred to as this attack. Attackers can read and collect sensitive information including usernames and passwords, as well as access control information, node configuration, share network passwords, and node identities, if the data is not encrypted. By processing and exploiting the acquired data, attackers can develop a planned attack. If an attacker can obtain the information needed to add a legal node, for example, he or she will be able to quickly add a false node to the system [39].

2) Side Channel Attack*:* This form of attack is successful against encryption, despite its difficulty in implementation. This form of attack is usually non-invasive. Typically, attackers only extract data that has been exposed by accident. The distance between packets, the frequency band, and the modulation employed, for example. One of the attacks' characteristics is that it is difficult to identify, which makes it much more difficult to avoid. Reduced information leakage or the addition of noise to information that is sensitive to leaks are two options [40].

3) Denial of Service (DoS) Attacks: Radio signal jamming is the most prevalent DoS attack against communication channels. There are two types of this attack. Continuous jamming is the first sort of attack, which is carried out indefinitely. The purpose of this attack is to shut down the communication network. Intermittent jamming is the second form of attack, which occurs on a regular basis. The purpose of this assault is to damage a time-sensitive system's performance [40].

4) Injecting Fraudulent Packet: To inject faked packets into a communication channel, an attacker can use one of three attack methods: insertion, manipulation, or replication (also known as replay attack) [9]. In the embedding scenario, the attacker inserts a new packet into the network communication. To put it another way, insertion attacks can create and send malicious packets that look to be normal. Manipulation attacks involve capturing packets and then manipulating them, such as changing headers, checksums, and data, before sending the modified packets out. The attacker acquires packets that have already been transferred between two entities in order to replay them in a replication attack.

5) Routing Attack: A routing attack is a type of attack that affects how communications are forwarded. At the communication layer, an attacker can employ a similar assault to deceive, reroute, mislead, or delete packets. The most basic type of routing assault is a modification attack, in which the attacker modifies routing information, for as by producing a routing loop or a false error message [4].

5.1.3 Security Threats on Edge Computing

Edge computing (fog computing) is an architecture that emerged along with the development of topology and infrastructure in IoT systems. In the seven-layer IoT architecture, edge-computing is a component at layer 3. Likewise, threats and security vulnerabilities have not been explored much. The following are some attack scenarios that often occur in edge computing.

1) Malicious Injection: Due to poor input validation, malicious input injection attacks are conceivable. The attacker can provide malicious data to the service provider, leading it to carry out a command (activity) on his or her behalf. To one of the tiers below this computer node, an attacker may, for example, introduce an unauthorized component capable of injecting malicious input into the server (communication level or edge node). Attackers can then steal data, endanger database integrity, or bypass authentication. Attackers can also take advantage of standard database error messages displayed by database servers. In cases where the attacker is unfamiliar with the database tables, the attacker can intentionally write a script that throws an exception, revealing more information about each table and its column names.[41].

5.2 Solutions on the IoT Security

This section discusses security solutions that need to be implemented at each layer to address security threats as discussed in the previous section.

5.2.1 Security Solution on Edge Node

This subsection discusses security solutions that can be implemented to overcome security threats to IoT systems on the edge-node side. Here are some security solutions that can be done to overcome security threats of IoT systems on the edge-node side. The security solution on Edge Node provides in Table I.

Table 1. The security solution on edge node.

Threat	**Solution**
Malicious Injection	✔ Pretesting
Inessential logging	✔ Pretesting
Inadequate Testing	✔ Pretesting
Integrity Attack	✔ Outlier Detection

1) Side-Channel Analysis: This method provides an effective approach for detecting malicious hardware-trojans and firmware installed on IoT devices. The presence of a Trojan in the firmware of IoT devices will cause a negative impact on battery usage, time delay effects, and changes in heat distribution on the IC. To detect hardware-trojans, a signal-based Trojan detection mechanism can be carried out by comparing the physical characteristics and/or heat distribution maps of the suspicious IC with the characteristics of other Trojan-free ICs [41].

2) Malicious firmware detection: Analyzing firmware signals can reveal useful information about how an IoT device operates. The malware detection in firmware method, like the Trojan detection mechanism, can process signals to detect abnormal device behavior, such as an increase in current and voltage in power consumption caused by injected malware on the device. [43].

3) Policy based Intrusion Detection System: Policy-based method (policy) is one of the promising techniques to solve security and privacy issues at this node level. Critical policy violations can be detected on an ongoing basis by introducing an Intrusion Detection System (IDS) [4].

5.2.2 Security Solution on RFID Node

Here are some security solutions that can be done to overcome security threats to IoT systems on the edge-node side for this type of RFID device. The security solution for RFID is shown in Table II.

Table 2. The Security Solution for Rfid

Threat	Solution
Tracking	✔ Blocking Method ✔ Kill Command ✔ Isolation ✔ Depatterning ✔ Information Flooding
Inventorying	✔ Blocking Method ✔ Kill Command ✔ Isolation ✔ Anonymous Tag
Tag Cloning	✔ Blocking Method ✔ Kill Command ✔ Isolation ✔ Anonymous Tag ✔ Personal Firewall
Counterfeiting	✔ Kill Command ✔ Personal Firewall ✔ Encryption
Eavesdropping	✔ Blocking Method ✔ Kill Command ✔ Isolation ✔ Anonymous Tag ✔ Personal Firewall ✔ Encryption

1) Kill-Sleep Command: This command is used during the RFID tag creation process. RFID tags have a unique PIN, such as a 32-bit PIN. If the attacker enters the correct PIN from the RFID reader, the RFID tag can be instructed to deactivate, so that the tag no longer operates after receiving this command [29]. In addition, there is a sleep command that puts the tag to sleep, for example, by making it inactive for a predetermined amount of time [19]. Safe and effective PIN management in IoT and RFID necessitates the use of highly sophisticated techniques.

2) Isolation: The most effective way to protect privacy is to isolate it from all access, which can be accomplished with the use of an isolation room. Another way is to block electromagnetic waves using an insulating container made of metal mesh called a Faraday cage [19] [30]. Another approach is to stop all nearby radio channels using an active RF jammer that is constantly interfering with a particular RF channel.

5.2.3 Security Solutions on Communication Channels

In this subsection, we discuss security solutions to overcome security threats to IoT systems on communication channels. The security solution on communication channel is provided in Table III.

Table 3. The Security Solution on Communication Channel

Threat	Solution
Infecting packet	✔ Encryption ✔ IDS
Routing Attack	✔ Reliable Routing
Unauthorized Conversation	✔ IDS ✔ Role Based Authorization

1) Reliable routing: A key feature of IoT network routing protocols is that an intermediate node or server can access the message content directly before forwarding it. As a result, some common routing attacks have been proposed in the literature. Past studies [25] [22] covered the majority of the attack scenarios that occur during the routing process.

2) Intrusion Detection System (IDS): This IDS method is crucial for monitoring network operations and communication lines at the communication layer, as well as identifying anomalies on the network, such as when a user violates a previously specified policy. SVELTE [4] was one of the first IDSs designed to meet the requirements of IPv6 connected IoT nodes. This intrusion detection system (IDS) is capable of detecting routing assaults such as false or altered information, as well as black hole attacks.

3) Cryptography: One of the most effective defenses against various assaults at the communication layer, such as eavesdropping and simple routing attacks, is the employment of cryptographic techniques to secure communication protocols. To solve communication security challenges, several encryption approaches have been developed [6] [44]. The encryption-decryption technique created for traditional wired networks does not immediately apply to most IoT components, particularly small battery-powered edge nodes. Small sensors with limited battery capacity, computing power, and memory are known as edge-nodes. Encryption consumes more memory, energy, causes delays, and causes packet loss [45]. The AES variant has demonstrated promising results for secure IoT communication.

4) De-patterning and Decentralization: De-patterning and decentralization are the two main strategies offered for providing anonymity and resistance against side-channel assaults. There is always a trade-off between anonymity and the necessity to provide information. Randomization of data transmission patterns, for example, can defend the system from side-channel assaults by adding additional packets that modify traffic patterns, making the patterns generated unidentifiable. Another technique to ensure anonymity is to disseminate sensitive data via a spanning tree, which ensures that no node gets a complete view of the original data[15].

5) Rule-based Authorization: One of the security solutions can be implemented by applying the rule-based authorization method. To prevent unnecessary responses, such as to requests by intruder or intruder nodes, a role-based authorization system verifies that components, such as edge nodes, service providers, or routers, can access, share, or modify information or not. In addition, for each communication, the authorization system must check that both parties involved in the interaction have been validated and have the necessary authority or not [40].

5.2.4 Security Solutions at the Computing Layer

In this subsection, we discuss security solutions to overcome security threats to IoT systems at the computing level. The security solution on computing layer is provided in Table IV.

Table 4. The Security Solution On Computing Layer

Threat	Solution
Hardware Trojan	✔ Side Signal Analysis ✔ Trojan Activation Detection ✔ Revise Circuit Design
Side Channel Attack	✔ Revise Circuit Design ✔ Blocking Method ✔ Kill Command ✔ Isolation
DOSs	✔ IDSs ✔ Firmware Update ✔ Personal Firewall ✔ Cryptography/Encryption
Physical Attack	✔ Revise Circuit Design
Node Replication	✔ Cryptography/Encryption
Camouflage	✔ Cryptography/Encryption ✔ Firmware Update
Corrupted node	✔ Firmware Update ✔ IDS ✔ Side channel Analysis ✔ Encryption

1) Pre-Testing: It is vital to test the process of upgrading and implementing the design before it is deployed in the IoT system. The behavior of the entire system and its components, such as routers, edge-nodes, and servers, should be carefully evaluated by inputting various inputs and monitoring outputs. The focus of pre-testing was on identifying probable attack scenarios and recreating them to determine how the system would react. It also determines which data should be kept and which should be deleted. In addition, to eliminate injection risks, the input file must be extensively verified. By adding a command into the input file, an attacker, for example, should not be able to execute it [14][46].

2) Outlier Detection: The purpose of security defense against data integrity attacks on machine methods learning is to reduce the effect of adding invalid data to the results. This invalid data is an outlier (deviation) in the dataset used. A framework for defense against poisoning type attacks has been developed based on statistics to reduce the effects of poisoning. Other studies have reported several poisoning attack countermeasures techniques in health care [19].

6. NEW CHALLENGE FOR IOT SECURITY RESEARCH

In the previous discussion, several attacks on IoT security have been described along with handling techniques. In this section, we discuss two categories of IoT security challenges that have not been discussed in the previous literature.

The majority of Internet of Things (IoT) services rely on battery-powered devices with limited storage and processing capability. Due to the particular characteristics of these devices and the cost aspects considered crucial by the manufacturers, some gadgets on the market do not enable secure cryptographic protocols. As a result, the network has a large number of communication lines that attackers can use to target attacks on entities that are thought to be secure. Several research projects have demonstrated the viability of attacking edge nodes to obtain a smart home's Wi-Fi password [47][48].

There are some fundamental flaws in IoT security implementation and implementation. The following are the IoT platform's flaws:

a) There are compatibility concerns. The various IoT platforms are not yet covered by global labeling and verification standards. Platform development organizations must follow standards in order to make IoT platforms more effective and useful.

b) One of the IoT platform's weaknesses is security. The risk of losing protection increases when all information from the used platform is transmitted.

c) Because of device interconnection, malware can easily spread to all connected devices. When a device becomes infected with malware, it infects all connected devices. In addition, the IoT protocol has the following flaws. MQTT has encryption and authentication issues. CoAP's use of DTLS has a flaw in that it is not intended to support multicast. The flaw in XMPP's Simple Authentication Security Layer (SASL) authentication is that it does not provide adequate security.

7. FUTURE RESEARCH DIRECTION

a) *Strong security protection:* Some of the most advanced malware detection and prevention methods used in IoT do not provide complete protection against new types of malware attacks. This security method cannot also be used to protect against all types of attacks at the same time. As a result, malware detection and intrusion detection methods should be more resistant to multiple malware attacks at the same time.

b) *Less computing time and lower costs:* IoT devices have limited resources, such as limited storage capacity, short battery life, and low computing power. As a result, IoT device security mechanisms should be designed to reduce computing time and communication costs.

c) *Blockchain application:* Blockchain operations can be used to secure a wide range of communication environments. This is because blockchain operations are decentralized, efficient, and transparent. In Internet of Things (IoT) environments, blockchain operations can also be used to detect malware. We can add blocks containing malware information to the blockchain using this type of detection method. More research is required in this area.

8. CONCLUSION

This paper discusses the development of IoT technology, and the security issues that afflict the technology. In the last decade, more and more IoT-based tools and systems have been used for various purposes. IoT is a technology that is always connected to the Internet, so the opportunity for attacks from external parties is very large. In this review, we classify the most common attacks on IoT systems based on layers of IoT technology. This paper also summarizes the IoT infrastructure protection methods suggested by previous studies. In addition, this paper has summarized the weaknesses of the existing protection methods in IoT systems. The final results obtained from this research are several recommendations to improve the weaknesses in the current IoT protection system. Improved security protection of IoT technology must be addressed and implemented as soon as possible so that customers can accept IoT technology and applications and realize the full potential of IoT technology and applications.

9. REFERENCES

[1] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, “Security in the internet of things – A systematic mapping study,” in Proceedings of the Annual Hawaii International Conference on System Sciences, 2018, vol. 2018-January, pp. 3750–3759, doi: 10.24251/hicss.2018.473.

[2] F. D. Garcia, G. de Koning Gans, and R. Verdult, “Wirelessly lockpicking a smart card reader,” Int. J. Inf. Secur., vol. 13, no. 5, pp. 403–420, 2014, doi: 10.1007/s10207-014-0234-0.

[3] R. Verdult, F. D. Garcia, and J. Balasch, “Gone in 360 seconds: Hijacking with hitag2,” in Proceedings of the 21st USENIX Security Symposium, 2012, pp. 237–252.

[4] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013, doi: 10.1016/j.adhoc.2013.04.014.

[5] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015, doi: 10.1007/s10796-014-9492-7.

[6] R. Verdult, D. F. Garcia, and B. Ege, “Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer,” in Supplement to the 22nd USENIX Security Symposium (USENIX Security 13), 2015, pp. 703–718, [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/verdult%5Cnhttps://www.usenix.org/system/files/conference/usenixsecurity15/sec15_supplement.pdf.

[7] L. T. Khrais, “IoT and blockchain in the development of smart cities,” Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 2, pp. 153–159, 2020, doi: 10.14569/ijacsa.2020.0110220.

[8] N. Zainuddin, M. Daud, S. Ahmad, M. Maslizan, and S. A. L. Abdullah, “A study on privacy issues in internet of things (IoT),” in 2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021, 2021, pp. 96–100, doi: 10.1109/CSP51677.2021.9357592.

[9] R. S. Mohammed, A. H. Mohammed, and F. N. Abbas, “Security and Privacy in the Internet of Things (IoT): Survey,” 2nd Int. Conf. Electr. Commun. Comput. Power Control Eng. ICECCPCE 2019, vol. 2, no. 2, pp. 204–208, 2019, doi: 10.1109/ICECCPCE46549.2019.203774.

[10] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Trans. Emerg. Top. Comput., vol. 5, no. 4, pp. 586–602, 2017, doi: 10.1109/TETC.2016.2606384.

[11] M. T. Lazarescu, “Design of a WSN platform for long-term environmental monitoring for IoT applications,” IEEE J. Emerg. Sel. Top. Circuits Syst., vol. 3, no. 1, pp. 45–54, 2013, doi: 10.1109/JETCAS.2013.2243032.

[12] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, “Emerging frontiers in embedded security,” in Proceedings of the IEEE International Conference on VLSI Design, 2013, pp. 203–208, doi: 10.1109/VLSID.2013.222.

[13] K. Su, J. Li, and H. Fu, “Smart city and the applications,” 2011 Int. Conf. Electron. Commun. Control. ICECC 2011 - Proc., pp. 1028–1031, 2011, doi: 10.1109/ICECC.2011.6066743.

[14] M. Prawira, H. T. Sukmana, V. Amrizal, and U. Rahardja, “A Prototype of Android-Based Emergency Management Application,” 2019, doi: 10.1109/CITSM47753.2019.8965337.

[15] R. Kumar and S. Rajalakshmi, “Mobile sensor cloud computing: Controlling and securing data processing over smart environment through Mobile Sensor Cloud Computing (MSCC),” in Proceedings - 2013 International Conference on Computer Sciences and Applications, CSA 2013, 2013, pp. 687–694, doi: 10.1109/CSA.2013.166.

[16] M. Bansal, M. Nanda, and M. N. Husain, “Security and privacy Aspects for Internet of Things (IoT),” Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021. pp. 199–204, 2021, doi: 10.1109/ICICT50816.2021.9358665.

[17] P. A. Sunarya, F. Andriyani, Henderi, and U. Rahardja, “Algorithm automatic full time equivalent, case study of health service,” Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1.5 Specia, pp. 387–391, 2019, doi: 10.30534/ijatcse/2019/6281.52019.

[18] P. Podder, M. R. H. Mondal, S. Bharati, and P. K. Paul, “Review on the Security Threats of Internet of Things,” International Journal of Computer Applications, vol. 176, no. 41. pp. 37–45, 2020, doi: 10.5120/ijca2020920548.

[19] M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, “Systematic poisoning attacks on and defenses for machine learning in healthcare,” IEEE J. Biomed. Heal. Informatics, vol. 19, no. 6, pp. 1893–1905, 2015, doi: 10.1109/JBHI.2014.2344095.

[20] A. M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, “Energy-Efficient Long-term Continuous Personal Health Monitoring,” IEEE Trans. Multi-Scale Comput. Syst., vol. 1, no. 2, pp. 85–98, 2015, doi: 10.1109/TMSCS.2015.2494021.

[21] E. R. Naru, H. Saini, and M. Sharma, “A recent review on lightweight cryptography in IoT,” in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 2017, pp. 887–890, doi: 10.1109/I-SMAC.2017.8058307.

[22] N. F. Rozy, R. Ramadhiansya, P. A. Sunarya, and U. Rahardja, “Performance Comparison Routing Protocol AODV, DSDV, and AOMDV with Video Streaming in Manet,” 2019, doi: 10.1109/CITSM47753.2019.8965386.

[23] E. McKenna, I. Richardson, and M. Thomson, “Smart meter data: Balancing consumer privacy concerns with legitimate applications,” Energy Policy, vol. 41, pp. 807–814, 2012, doi: 10.1016/j.enpol.2011.11.049.

[24] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, “Denial-of-service attacks on battery-powered mobile computers,” in Proceedings - Second IEEE Annual Conference on Pervasive Computing and Communications, PerCom, 2004, pp. 309–318, doi: 10.1109/PERCOM.2004.1276868.

[25] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, “Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples,” in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings, 2012, pp. 1–7, doi: 10.1109/WoWMoM.2012.6263790.

[26] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions,” Appl. Sci., vol. 10, no. 12, p. 4102 10 3390 10124102, 2020, doi: 10.3390/APP10124102.

[27] J. Sánchez, A. Mallorquí, A. Briones, A. Zaballos, and G. Corral, “An integral pedagogical strategy for teaching and learning iot cybersecurity,” Sensors (Switzerland), vol. 20, no. 14, pp. 1–35, 2020, doi: 10.3390/s20143970.

[28] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic mapping studies in software engineering,” in 12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008, 2008, pp. 68–77, doi: 10.14236/ewic/ease2008.8.

[29] R. T. Adek and M. Ula, “A Survey on the Accuracy of Machine Learning Techniques for Intrusion and Anomaly Detection on Public Data Sets,” in 2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics, DATABIA 2020 - Proceedings, 2020, pp. 19–27, doi: 10.1109/DATABIA50434.2020.9190436.

[30] Y. Cherdantseva and J. Hilton, “A reference model of information assurance & security,” in Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, 2013, pp. 546–555, doi: 10.1109/ARES.2013.72.

[31] H. Salmani and M. M. Tehranipoor, “Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1214–1225, 2016, doi: 10.1109/TIFS.2016.2520910.

[32] L. Lu et al., “KeyLiSterber: Inferring Keystrokes on QWERTY Keyboard of Touch Screen through Acoustic Signals,” in Proceedings - IEEE INFOCOM, 2019, vol. 2019-April, pp. 775–783, doi: 10.1109/INFOCOM.2019.8737591.

[33] F. Stajano and R. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2000, vol. 1796, pp. 172–182, doi: 10.1007/10720107_24.

[34] S. W. Liew, N. F. M. Sani, M. T. Abdullah, R. Yaakob, and M. Y. Sharum, “An effective security alert mechanism for real-time phishing tweet detection on Twitter,” Comput. Secur., vol. 83, pp. 201–207, 2019, doi: 10.1016/j.cose.2019.02.004.

[35] Y. Michalevsky, A. Schulman, G. A. Veerapandian, D. Boneh, and G. Nakibly, “Powerspy: Location tracking using mobile device power analysis,” in Proceedings of the 24th USENIX Security Symposium, 2015, pp. 785–800.

[35] A. Juels, “RFID security and privacy: A research survey,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 381–394, 2006, doi: 10.1109/JSAC.2005.861395.

[37] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, “Securing RFID systems by detecting tag cloning,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, vol. 5538 LNCS, pp. 291–308, doi: 10.1007/978-3-642-01516-8_20.

[38] D. N. Duc and K. Kim, “Defending RFID authentication protocols against DoS attacks,” Comput. Commun., vol. 34, no. 3, pp. 384–390, 2011, doi: 10.1016/j.comcom.2010.06.014.

[39] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, “Lock it and still lose it – on the (in)security of automotive remote keyless entry systems,” in Proceedings of the 25th USENIX Security Symposium, 2016, pp. 929–944.

[40] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, “On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them,” in ACM International Conference Proceeding Series, 2016, vol. 5-9-Decemb, pp. 226–236, doi: 10.1145/2991079.2991094.

[41] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, “Novel techniques for high-sensitivity hardware trojan detection using thermal and power maps,” IEEE Trans. Comput. Des. Integr. Circuits Syst., vol. 33, no. 12, pp. 1792–1805, 2014, doi: 10.1109/TCAD.2014.2354293.

[42] B. Biggio, B. Nelson, and P. Laskov, “Poisoning attacks against support vector machines,” in Proceedings of the 29th International Conference on Machine Learning, ICML 2012, 2012, vol. 2, pp. 1807–1814.

[43] J. Van den Herrewegen and F. D. Garcia, “Beneath the bonnet: A breakdown of diagnostic security,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 11098 LNCS, pp. 305–324, doi: 10.1007/978-3-319-99073-6_15.

[44] C. M. M. Stone, T. Chothia, and F. D. Garcia, “Spinner: Semi-Automatic detection of pinning without hostname verification,” in ACM International Conference Proceeding Series, 2017, vol. Part F1325, pp. 176–188, doi: 10.1145/3134600.3134628.

[45] C. Hicks, F. D. Garcia, and D. Oswald, “Dismantling the AUT64 Automotive Cipher,” IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 2, pp. 46–69, 2018, doi: 10.46586/tches.v2018.i2.46-69.

[46] R. Verdult, G. De Koning Gans, and F. D. Garcia, “A toolbox for RFID protocol analysis,” in Proceedings - 2012 4th International EURASIP Workshop on RFID Technology, RFID 2012, 2012, pp. 27–34, doi: 10.1109/RFID.2012.19.

[47] M. Kumar, “How to hack WiFi password from smart doorbells.” 2016, [Online]. Available: http://thehackernews.com/2016/01/ doorbell-hacking-wifi-pasword.html.

[48] A. Chapman, “Hacking into Internet Connected Light Bulbs,” 04.07. 2014, [Online]. Available: http://www.contextis.com/resources/ blog/hacking-internet-connected-light-bulbs/.