Security Challenges and Solutions in the Internet of Things

Ahmed Y. Abdullah, Ibrahim M. Elhenawy, Ahmed Abdelmonem*

Faculty of computers and informatics, Zagazig university, Egypt

Emails: eng.ahmedyousifgmai@gmail.com; ielhenawy@zu.edu.eg; aabdelmonem@zu.edu.eg

Abstract

The Internet of Things (IoT) is pervasive in today's world and may be located almost throughout. It is employed in smart cities for things like highways and clinics, as well as in smart buildings for things like regulating doors and air conditioner units, avoiding fires, and many other things. The Internet of Things (IoT) refers to a set of interconnected computing devices that may communicate with one another by exchanging data over the internet. This provides the opportunity for the attacker to penetrate the IoT technologies and get the important data they contain. The restricted measure performance of IoT systems is the source of the issue, as they make it impossible to implement the conventional security mechanism on these devices. As a result of this constraint, it is necessary to propose lightweight algorithms that are capable of supporting IoT devices. However, Internet of Things (IoT) safety and confidentiality are important challenges that might impede the technology's long-term growth. In this study, we have addressed the security of the internet of things from two primary vantage points, namely, IoT design and protocols. We cover the many levels that make up the architecture of the Internet of Things (IoT), as well as the security problems that are connected with those layers and the possible alternatives to those concerns. We went through a variety of protocols that are used in the layered evolution of the Internet of Things, as well as the security mechanisms that were built for every protocol.

Keywords: Internet of Things; Security; Privacy; IoT; Algorithms

1. Introduction

IoT enables the integration of a wide variety of sensors and other items into a network that enables them to interact directly with each other and bypass the need for human involvement. The term "things" refers to machines, like various sensors, that are part of the Internet of Things and are used to monitor and collect various forms of data about machines as well as human social life. The development of the Internet of Things has made it possible to maintain an ongoing global link between people, things, sensors, and services. The primary goal of the Internet of Things is to establish a network infrastructure that is equipped with integrated communication protocols and software. This will interconnect and incorporate physical and virtual sensors, desktop computers, connected devices, motorcars, and items like refrigerators, dishwashers, microwave ovens, food, and medicines at any time and on any network. The advancement of technology for smartphones has made it possible for an infinite number of things to become a member of the Internet of Things by using the many sensors included inside smartphones. On the other hand, the need for the widespread implementation of the Internet of Things is fast expanding, which in turn results in a significant security problem[1-2].

The Internet of Things ecosystem presents several obstacles, the most significant of which are related to information storage and processing, as well as security, authorization, validation, password protection, and system control. IoT devices, like smartphones and pervasive computing, for example, contribute to the provision of a digital world for global connection that improves lives by being cognizant of human requirements, adaptable to those requirements, and responsive to those

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

requirements. Nevertheless, there is no assurance of safety. When a user's signal is disrupted or intercepted, there is a risk that the user's privacy will be violated, and there is also a risk that information about the user may be disclosed[3]. This problem should be solved to ensure user trust in terms of security and management of private details before widespread adoption of the internet of things (IoT) can occur. The advancement of the Internet of Things is very reliant on the resolution of security difficulties[4-5].

The Internet of Things has made people's lives easier by facilitating the delivery of automated tools. On the other hand, an unmanaged explosion presents rising difficulties regarding privacy and security[6].

The inadvertent use of IoT systems, failure to regularly change passwords, and failure to install software updates have all contributed to an increase in cyber security risks and connect directly malicious apps to sensitive data. The use of such ineffective security practices raises the likelihood of a data breach as well as other types of threats. The Internet of Things (IoT) is widely regarded among security professionals as the most susceptible target for cyber-attacks because of inadequate security protocols and policies. Even though a number of different security measures have been developed to protect internet-of-things systems from cyber-attacks, convention applies have not been adequately documented. End users were unable to utilize protective precautions to safeguard their data from being attacked as a result. Since the beginning of 2008, cybercriminals have created numerous forms of malware to infect various Internet of Things apps. They developed a variety of phishing methods to trick individuals or workers into divulging sensitive information. As a result, both personal devices and workstations in corporations are frequently subject to privacy violations as a result of high-profile attacks. If hardware makers and security experts properly estimate the cyber-attacks, it will be possible for them to create an effective defense function that will either prevent or neutralize the cyber threats[7- 8].

Devices enabled by the Internet of Things have been employed in a variety of commercial applications, including industrial ones. These firms can get a competitive advantage over their rivals with the assistance of applications. However, because of the widespread adoption of a variety of smart devices that are capable of information sharing and incorporation, the breach of privacy and data becomes a big problem for the majority of organizations. This is because it disrupts the flow of work, operations, and network services. To address these danger concerns and build comprehensive security programs and strategies to secure their corporate assets and assure the continuity and stability of their operations, it is vital to have specialists on hand[9], [10]. For instance, Internet of Things (IoT) equipped household appliances that are linked to the local network might be a source of breach for attackers, allowing them to get entry to potentially sensitive data or commercial data, or to alter and disrupt the workflow of the organization. Figure 1 shows the IoT scenario.

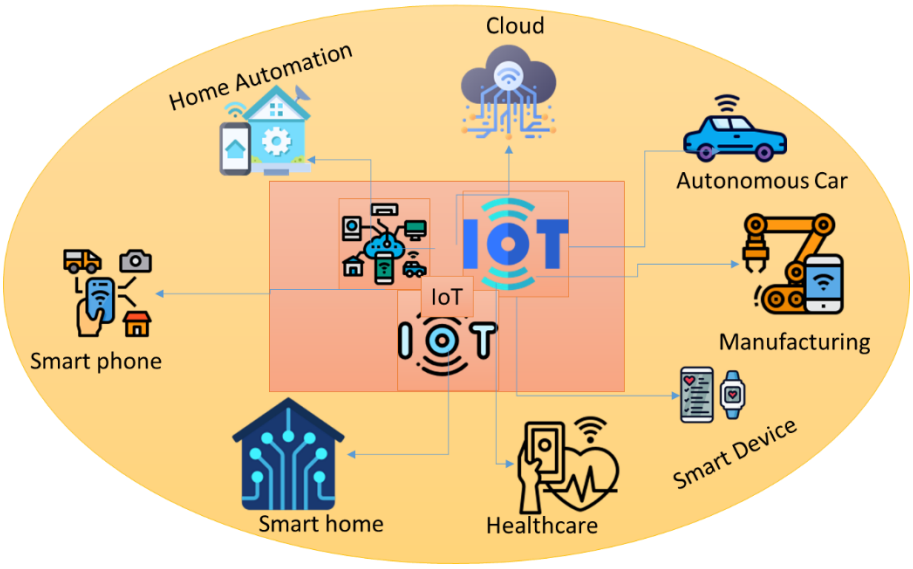

Figure 1: Internet of Things Development.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

2. Literature Review

IoT has been broken down into three levels by Qi Jing and colleagues [11], who have been concentrating on its system security and the problems associated with it. These levels are the perception layer, the transportation layer, and the application layer. They examined the characteristics of every layer, as well as the potential vulnerabilities it posed to users' data, and presented the standard remedies that are available to address these problems. In the interim, they also analysed the technologies behind each of these various solutions to compare and contrast its qualities with those of the other alternatives. They analysed the security problems of Rfid systems and their solutions to resolve such as: Uniform Coding, Conflict Collision, RFID Personal Privacy, and Authentication And authorization. Next, they analysed protection problems and technological strategies in WSNs such as: Cryptographic Algorithms in WSNs, Key Management in WSNs, Secure Routing Protocols for WSNs, and Authentication And authorization of Nodes in WSNs. For the perception layer, WSNs and RFID technology are extremely important. After doing research on RFID and WSNs, the researchers examined the new issues that the RSN faces, which are related to the combination of RFID and WSNs. They also investigated cross-layer heterogeneous integration challenges and security concerns in depth. This was done since the IoT system has to manage enormous amounts of heterogeneous data coming from a variety of sources. Access network, core network, and local area network are the three components that make up the transportation layer. In the access network, they investigated potential security flaws in WiFi, ad hoc, and 3G networks, as well as the solutions that may potentially fix such problems. They conducted research on network access control technologies in local area networks in order to address the problem of unauthorised use of network resources and provide a solution. In addition to this, they conducted an in-depth analysis of the overall function of security concerns as well as frequent security difficulties. The application layer is made up of the application substrate surface as well as the Internet of Things application layer. They have spoken about the security challenges that pertain to the application substrate surface, like security risks, service disruption and attack difficulties, and issues pertaining to investigating audits. Since problems with the security of the application layer arise from the application itself, these problems cannot be fixed at higher IoT levels. Therefore, they have presented some typical Internet of Things applications like Intelligent Transportation and Smart Home, analysed the security problems and associated systems associated with these applications, like network control technology, telecommunication technologies, and various mobile technology, and concluded that these applications pose no significant security risks. Inside the end, they especially in comparison the security concerns that were present in an IoT network to those that were present in a distributed system. Based on their findings, they came to the conclusion that an IoT system exists in a more hazardous environment, with fewer network guards and scarce funds; as a result, lightweight alternatives should always be our first decision when it comes to IoT security. They also mentioned opening security risks of IoT as an undivided entity, and they gave some various key for these issues, including an overall security architecture for the entirety of the IoT system, lightweight security products, and optimal solutions for huge large datasets.

The proliferation of Internet of Things (IoT) technology makes cybersecurity an increasingly important factor in protecting both the digital and the real worlds. First, Sha et al. [12] studied the new security problems that are provided by the characteristics of IoT systems, including the resource-constrained IoT end systems and the close connection between the cyber world and the physical world. The next step is a summary of three architectural security designs, which will serve as a guide for the construction of future security protocols and algorithms. Detailed consideration is given to both the benefits and drawbacks of each design. The presentation includes examples of how every concept might be implemented. According to their research, low competent end devices need assistance from levels that are higher up in order to establish a satisfactory degree of security across the whole Iot network.

In the realm of the Internet of Things, often known as IoT, there are an enormous variety of linked devices. These machines are communicating with one another, as well as with corporate systems and sometimes with people, in order to gather and send large amounts of data. Since there are billions of linked devices, there is a significant potential for theft of personal information and data, control of connected devices, fabrication of data, manipulation of servers and networks, and eventual damage to application platforms. As the number of these networked devices continues to expand each day, the number of security risks and vulnerabilities that are presented to these devices also continues to grow. When it comes to technical development, one of the most pressing issues that now face the Internet of

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

Things is data security. There are many different aspects to security, including the security that is built into the device itself, the security of data transfer, and the security of data storage inside the systems and the apps themselves. However, the majority of the available work does not offer a comprehensive view of the risks to data privacy and security that are posed by the Internet of Things (IoT). This is despite the fact that there is a vast amount of published material on the topic, which includes a vast number of issues and policy suggestions. Rizvi and colleagues [13] have recognised (a) the essential areas in which IoT is widely employed, (b) the security needs and issues that IoT is now experiencing, and (c) the current security options that have been presented or implemented together with their respective constraints.

Khan, Salah [14] research and examined the primary concerns about the security of the internet of things. They divided the concerns into three categories according to the different levels of the Internet of Things: high, midrange, and low. They had a concise discussion on the strategies that were recommended in the relevant literature for exploiting IoT security at various levels. In addition, a parametric study of assaults on the Internet of Things and their potential countermeasures are offered. They analysed the ramifications of the assault and mapped those implications to potential remedies that had been presented in the literature. They also explored the usage of blockchain technology to address and resolve some of the most pressing concerns around Internet of Things (IoT) security issues.

One developing use of the Internet of Things is the smart home, which enables connected gadgets to speak with one another and exchange private data. In a setting like this one, a number of different components work together to accomplish the goal of the Internet of Things. These components include smartphones, smart air conditioners and smart heaters, as well as sensors such as smoke sensors, temperature sensors, and so on, and various protocols on the backend. Although the Internet of Things (IoT) is still relatively new to the market, the companies who make the devices have not yet included any security measures. The producers of smart devices primarily concentrate on the gadgets that need less computing and have a low energy consumption, which has caused them to leave behind the security strategies for the devices. The Internet of Things (IoT) consists of a large number of devices; hence, when all of these devices are linked, several privacy and security concerns arise. Touqeer et al. [15] have conducted research about the most prevalent security dangers and privacy problems for Internet of Things smart devices. All of the problems are organised into several categories in accordance with the hierarchical structure of the smart home environment. In addition, a wide variety of written works are examined in search of safeguards and preventative measures that might be applied to the problems that have been outlined.

The Internet of Things and cloud technologies have both contributed to the vulnerability of gadgets. The many machines, as they are spread, send real-time information to open, private, or mixed clouds. This affords the opportunity to gather, store, and analyse large data streams in novel formats. In the context of healthcare, the rising proliferation of Iot systems renders patient information vulnerable to hostile assaults dependent on the security and confidentiality of the IoT devices. This is the case regardless of whether or not the IoT devices are encrypted. Despite the fact that a number of academics have investigated the open issues and security concerns in the IoT, there is, however, a lack of a comprehensive examination of the security problems in the IoT for eHealth that is hosted on clouds. Ida et al. [16] wanted to close this gap by carrying out a comprehensive examination of the vulnerabilities of the internet of things (IoT). Moreover, They discussed the current suggested solutions for the security issues that have arisen in the cloud related to the eHealth area. In addition to this, they provided the concept of an Internet of Things system hosted on the cloud.

As the network revolution continues to grow in scale and complexity, it is more important than ever to protect data from being stolen by malicious actors. Because of cybercrime, billions of dollars were stolen, which had a negative impact on the economy of the whole world. The criminals behind these crimes had the malevolent aim to compromise sensitive and important information. As a result of the fact that these crimes are done on a regular basis, increasing the security of cyberspace has become an essential need in an effort to lessen the impact of cybercrimes and potentially even prevent them altogether. Today, the revolution brought about by the internet of things (IoT) is becoming the center of research, and both security and confidentiality are recognised as the primary issues for IoT applications. This is primarily due to the implementation of IoT in crucial areas, such as healthcare systems, which raises concerns about the potential for breaches. In this article, Abdullah et al. [17] explore the current status of cybersecurity in the IoT area as well as the security issues that it faces. In

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

addition, they address various security needs and approaches that may be used to overcome these difficulties. In conclusion, the technology known as blockchain is addressed as a potential answer to the problem of ensuring the safety of IoT devices.

3. Internet of Things Safety and privacy

Consumers have reaped enormous advantages from the IoT; nevertheless, it has also brought forth certain difficulties. Cybersecurity and security threats are, according to the academics and security professionals identified, the key issues in this area. Both of these factors are creating a significant challenge for a wide variety of organizations, including public and private businesses. The weaknesses of IoT devices have been proven time and time again by high-profile and pervasive cyberattacks. This vulnerability exists for the simple reason that the interconnection of connections in the IoT carries with it available from the nameless and untrustworthy internet, which necessitates the development of innovative security solutions.

None of the identified difficulties, including security and privacy concerns, has a greater substantial impact on the adaptability of the internet of things than any of the others. It is sad, but not uncommon, for consumers not to have the necessary recognition of the security consequences until after a security breach has already happened, resulting in significant losses like the theft of essential data. This may cause large amounts of harm. As a result of the recurring security breaches that have put users' privacy at risk, customers' tolerance for inadequate safety is now on the decline. The IoT that is designed for consumers did not do very well in a new analysis concerning issues of security and privacy. There were many weak spots in today's vehicle information technology[11], [12].

A. Safety

The Internet of Things is distinct from conventional machines and other personal computers, which makes it more susceptible to a variety of security threats in a variety of ways:

Several of the tools that make up the IoT are created to be used on a large scale. Sensors are a great illustration of this principle in action.

In most cases, the implementation of IoT involves the use of a collection of devices that are the same or practically equal and share a set of features. Because of this commonality, the amplitude of any security vulnerabilities in the security that could seriously impact several more of them is substantially enhanced.

In a related manner, a great number of establishments have formulated instructions for how to carry out risk assessments. Because of this phase, there will likely be an unprecedentedly high number of links connecting the various IoT systems. It is also abundantly clear that a good number of these machines can automatically create contact and unpredictably interact with others. These factors require that one takes into account the available tools, strategies, and strategies that are connected to the safety of the IoT[13].

B. Security

Even though the problem of safety in the information and technology industry is not a new one, the adoption of the internet of things has introduced new issues that require to be handled. Customers are needed to have faith that the products and services provided by the IoT are extremely safe and free from vulnerabilities, especially as this world enables us to become more unobtrusive and integrated into our day-to-day lives. This is one of the most key avenues that are used for cyber assaults, in addition to the exposing of the information of customers by letting streams of data not secured sufficiently. With IoT frameworks and systems that have poor protection, this is one of the most significant outlets.

Because of the interconnected nature of the devices that make up the IoT, even one poorly protected or linked item can compromise the safety and resiliency of the Internet as a whole on a global scale. This behavior is brought by the simple fact that the Internet of Things presents a problem due to its widespread use of similar systems. In addition to the capacity of certain systems to be capable of mechanically linking with other things, this implies that clients of the IoT as well as the creators of IoT need to ensure that they are not introducing other users or the Internet itself to the possibility of

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

damage. The Internet of Things (IoT) is presently exhibiting a common strategy, which is essential to produce an efficient and acceptable response to difficulties[14].

C. Authentication

For example, the Internet of Things (IoT) has several weaknesses when it refers to the identification, which continues to be one of the most important challenges when it comes to the provision of safety in a variety of apps. The authentication that is being utilized is restricted in that it can only guard against a single kind of attack, like a denial of service (DoS) or active attack. Information security (IS) is one of the substantially sensitive parts in the authentication of IoT because of the widespread use of apps that are risky because of their inherent multitude of data gathering in an IoT ecosystem. This makes IS one of the considerable sensitive parts in the verification of IoT. The use of smart credit cards is a good illustration of this point, if I may provide one. These cards have the capability of allowing card numbers and addresses to be read without the verification of IoT; as a result, it is feasible for attackers to be capable of purchasing items by using the cardholder's bank account number and their identification[15], [16].

D. Attacks in IoT

The "person in the center" assault is one of the most common types of cyberattacks on the Internet of Things (IoT). This kind of attack involves a third party hijacking a communication channel to fake the identification of tangible nodes that are participating in covers approximately. Since the opponent does not need to understand the identity of the alleged victim to carry out a person-in-the-middle attack, the bank server is tricked into believing that the transaction that is taking place is a legitimate occurrence.

E. Confidentiality

The Internet of Things (IoT) potential utility is directly proportional to how effectively it can honor the privacy preferences of individual users. Worries about privacy and the possible dangers that come from the Internet of Things may play a key role in slowing down its widespread adoption. It is necessary to be aware that the rights to confidentiality and the respect for user privacy are crucial in guaranteeing that users will have faith and self-assurance in the IoT, the connected system, and the associated services that are provided. Knowing this is essential. A significant amount of effort is being put in to guarantee that the Internet of Things (IoT) is redefining privacy problems like the rise in the use of monitoring and surveillance technologies. The ubiquitous intelligence-linked artifacts are the root of the privacy problems that have arisen as a result of the Internet of Things (IoT) since they allow sample selection and information dissemination to be carried out almost everywhere. The omnipresent connectivity provided by Internet direct connections is also a vital aspect that aids in recognizing this issue because, in the absence of a specific mechanism being put into place, it will be markedly more relaxed to obtain private information from any location on the face of the planet[17], [18].

F. Interoperability

It is common knowledge that a divided ecosystem that relies on proprietary IoT technology implementation reduces the value for consumers. Although it isn't always possible to achieve complete interoperability over goods and services, customers may not like purchasing products and services in environments where there is no room for customization and there is a risk of being locked in by the vendor. Ill-planned Internet of Things devices may have a detrimental impact on the resources available via the network[19].

Cryptography is another fundamental component that has been put to use for a significant amount of time to defend a variety of applications against vulnerabilities in their security. It is not feasible to develop efficient defense mechanisms against the attacks that have been carried out using a single security app. As a result, it necessitates multiple layers of security to protect against the dangers that threaten the authentication of IoT[20].

Hacks can potentially be avoided through the creation of more sophisticated security features and the incorporation of these characteristics into goods. This evasion is possible because consumers will make purchases that already have appropriate security characteristics that help stop vulnerabilities in

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

the system. Methodologies for cybersecurity are one of the indicators that have been proposed to ensure the safety of the internet of things[21].

3. Internet of Things Challenges

A. Physical layer

At the physical layer, the nodes come together to create an ad hoc network that has a variable distribution. Within the context of the situation we are examining, the primary purpose of this layer is to facilitate communication among various connected entities via digital media. However, it is not practical to link all of the pieces properly in the vast majority of situations. For this reason, this layer of secure data transfer now incorporates nanotechnology as well as integrated forms of AI[22].

B. Network Layer

In addition to having the name "upcoming generation network," this is a merger of many other kinds of networks. For data aggregation, it addresses protocols such as MQTT 3.1 and CoAP, among others. A variety of technological approaches are used in order to modify the input at this layer.

C. Application Layer

Since it is responsible for delivering activities to end users, this layer is sometimes referred to as a service-oriented layer. The Internet of Things has a wide range of apps, such as smart homes, connected cars, smart habitats, and so on. This layer processes the data that was generated by the network layer and the physical layer below it. As a result, it incorporates several database management systems intending to satisfy the needs of the customers. It does so via the use of intelligent computing in order to deliver various services[23], [24].

4. The Solution in Security of the Internet of Things

4.1 Physical layer

Physically safe design: To address the concerns of safety, the trustworthy component was developed using an encryption approach. The physically secure architecture of machines cannot be modified and does not provide a high level of reliability.

Verification of the machine might consist of either verifying the user or disabling the tags. Deployment and usage of anti-jamming equipment to safeguard devices via the use of the Quick Response Code (QR code) technology, Randomly switching between many routes, using a built-in kill command.

Private enhancing is achieved by the use of cryptographic techniques and hash functions, the latter of which verifies the program running on the system through the use of electronic signatures.

Dynamic Risk Assessment (DRA) methodology, Encryption algorithm Mixture, Lightweight Method (HLA), and Elliptic Curve Cryptography are some examples of hazard identification algorithms (ECC).

IPSec safety channel: Node manipulation and espionage may be prevented by encrypting and authenticating data, which helps in guaranteeing the secrecy of data. Sheltering the tag or limiting the tag-reader distances are other effective ways to protect against these vulnerabilities.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

Safety of place and authenticity through K-anonymity or the Zero expertise methodology, Public Key Facilities (PKI), and Smart key Signature Facilities (KSI).

A trustworthy design, multimedia reduction, transcription, water tagging, computer vision, and cyclic redundancy test are all used for the identification of devices (CRC)

Authenticating a machine includes the following methods: Spatial-Role-Based Access Control (SRBAC), Killing or permanently deactivating a tag, and the Faraday Cage Method.

4.2 Network Layer

Encrypted communications or Digital Rights Management (DRM) systems, as well as a safe method of control, are necessary for the confidentiality of information.

Ad-hoc provision: a technology known as Safety awareness Ad-hoc Routing (SAR).

Verification: A method of controlling access using encryption, such as a non-linear implementation of this concept, the implementation of an IPSec protocol, or a cryptographic algorithms innovation arrangement that does away with data dependencies on the amount of energy consumed. Blocker tags, Blinded Tree Walking technique, Point to Point (P2P) cryptography.

The technique is known as Adhoc On-Demand Multipath Distance Vector (AOMDV) for routing; use of a private pre-shared key for authentication (PPSK).

Welcome to the flood warning and protection system: The radio range and signal strength are likened to one another.

Encryption of point-to-point communications, authentication mechanisms, hash mechanisms, and fault detection at every layer all contribute to data integrity.

The Multipath Routing Protocol is utilized as the routing protocol.

Firewall and Intrusion Detection and prevention Systems are examples of detection and prevention technologies.

The Hop-by-Hop and Reference Routing Approach to Encrypting Forwarding.

4.3 Application Layer

Safety precautions for the data include an identity protection system, the use of safe coding, and the evaluation of antivirus software.

Implementation of the Access Control Lists (ACL) methodology, Service-Oriented Architecture (SOA), and Intrusion Detection System are all aspects of access control (IDS)

Public Key Infrastructure, digital signatures, and biometric authentication are some application security measures (PKI)

Intrusion Prevention Systems, Firewalls, Anti-DoS, and Spyware are some defenses against unauthorized access and potential threats (IPS)

Security measures include protection against viruses, spyware, and adware

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

The encryption algorithm is a kind of encryption in which the ciphertext is instantaneously generated without the need for decryption, boundary inspection, encryption keys, or access control.

The mechanism for encrypting data, ensuring the integrity of identities, and managing trust in an adaptive manner

Memory cells are safeguarded against modification, making this process of data mining hyper-safe.

Anomaly detection method, Intrusion Detection System (IDS), and Statistical analysis are all types of security measures. Low-demanding on available resources firewall

Software-Defined Networking Network technology is used to improve network performance while simultaneously lowering costs and the amount of required hardware. This is done to provide room for innovation and research inside the network.

To monitor and control the flow of traffic, the SDN is communicating with the IoT. There is a connection between the SDN controller and the IoT systems. Their system comprises an IoT agent, an IoT controller, and an SDN controller. All of these gadgets are cooperating to deliver high-engagement services for IoT systems[25].

The conventional network is unable to handle many of the challenges that are being caused by the Internet of Things, thus the SDN has been merged with it. On the other hand, it offers an increasing range of services to administer, regulate, and monitor.

Protect the network from harm. SDN will give a high degree of QoS that has to be provided in the IoT structure so that it can accommodate the demands of the Internet of Things as well as the massive traffic that is generated by end users. The software-defined network (SDN) is responsible for making the network's infrastructure available. In addition to this, it monitors the communication from machine to machine and provides security for identification and trustworthiness between the machines. Flexibility in the network will also be provided by the SDN in preparation for any future expansion of the connection[26], [27]. Figure 2 shows the integration between SDN and IoT.

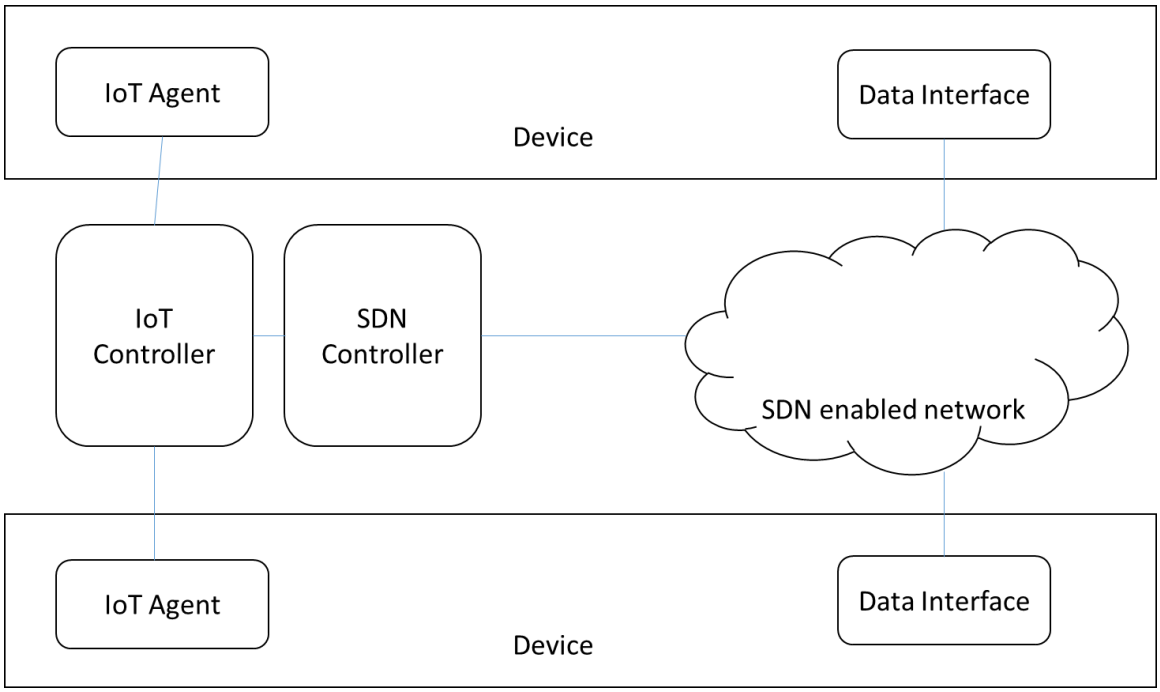

Figure 2: IoT and SDN.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

5. Factors to make an Internet of Things secure

- The occasional upgrade: Most of the time, makers of IoT devices will release security fixes quarterly. Similarly, the operating system versions and security fixes are also updated. As a result, cybercriminals have adequate time to get through the security mechanisms and steal important data.
- Integrated passwords: Because Iot systems save integrated passwords, support staff may more easily debug OS issues or remotely apply essential upgrades. Thieves, on the other hand, could use this capability to circumvent device security.
- Automated: often, businesses and end-users make advantage of the automated test characteristic of Internet of Things systems to acquire data or to make company operations more straightforward. On the other hand, if the malicious websites are not indicated, embedded AI will be able to obtain of that kind sources, which will open the door for threats to access the device.
- Access from a distance Internet of Things apps offers access from a distance using a variety of network protocols including Wi-Fi, ZigBee, and Z-Wave. In most cases, specific restrictions are not noted, which is something that cybercriminals can use to their advantage. As a result, cybercriminals could easily set up a malicious linkage thru these remote access protocols very rapidly.
- Large selection of applications developed by third parties: organizations now have access to a broad range of software applications developed by third parties, which can be downloaded from the internet and used to carry out a variety of tasks. On the other hand, there was no straightforward way to determine the genuineness of these applications. The malicious actors will instantaneously reach the system and venal the integrated dataset if the final and staff install or access applications of this kind.
- Incorrect authentication of the device The majority of applications for the Internet of Things do not make use of authentication services to prevent or restrict cyber threats. This allows the aggressors to access the door and compromise the victim's privacy.
- Weak Monitoring of things: Typically, all Internet of Things makers will establish one-of-a-kind device IDs to monitor and track phones. Nevertheless, certain firms do not have a security policy. Therefore, monitoring potentially suspicious activity on the internet may be rather difficult.

6. Conclusion

The Internet of Things (IoT) and all of its gadgets and apps are becoming more important in contemporary life. Nearly everywhere we go, from our homes and workplaces to public spaces like shopping malls, schools, and airports, there are the Internet of Things gadgets that are working hard to make our lives easier and more convenient. Devices connected to the internet of things facilitate cooperation with many stakeholders and contribute to a better knowledge of business objectives and results. In contrast, analytics and data processing that is based on the Internet of Things has the potential to improve the effectiveness and competitiveness of industrial networks. In addition, IoT systems are now integrating a variety of helpful technical advancements across a wide range of industries. To keep their networked devices from being compromised by criminal actors, several manufacturers and businesses have implemented a comprehensive set of security rules. More and more of these gadgets are connecting to our private connectivity, which has led to an increase in the number of privacy and security problems that have been documented. This paper provides a concise overview of the security risks and potential mitigation strategies applicable to the various levels of the Internet of Things (IoT). The Internet of Things (IoT) generates a tremendous number of disparate data every minute; hence, it is essential to develop effective methods for managing this data. In light of this, reliable procedures need to be devised to effectively manage and organize the huge amounts of data involved.

References

[1] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT Privacy and security: Challenges and solutions,” *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[2] A. Hameed and A. Alomary, “Security issues in IoT: a survey,” in *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, 2019, pp. 1–5.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[4] J. Mohanty, S. Mishra, S. Patra, B. Pati, and C. R. Panigrahi, "IoT security, challenges, and solutions: a review," *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2*, pp. 493–504, 2021.

[5] F. Al Shuhaimi, M. Jose, and A. V. Singh, "Software defined network as solution to overcome security challenges in IoT," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 2016, pp. 491–496.

[6] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*, 2014, pp. 230–234.

[7] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[8] R. F. Ali, A. Muneer, P. D. D. Dominic, S. M. Taib, and E. A. A. Ghaleb, "Internet of things (IoT) security challenges and solutions: a systematic literature review," in *Advances in Cyber Security: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers 3*, 2021, pp. 128–154.

[9] N. Almolhis, A. M. Alashjaee, S. Duraibi, F. Alqahtani, and A. N. Moussa, "The security issues in IoT-cloud: a review," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, 2020, pp. 191–196.

[10] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

[11] Q. Jing, A. V Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481–2501, 2014.

[12] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future generation computer systems*, vol. 83, pp. 326–337, 2018.

[13] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (IoT): A security taxonomy for IoT," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 163–168.

[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395–411, 2018.

[15] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing*, vol. 77, no. 12, pp. 14053–14089, 2021.

[16] I. Ben Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of eHealth and clouds," in *2016 11th International Design & Test Symposium (IDT)*, 2016, pp. 25–30.

[17] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.

[18] C. Toma, A. Alexandru, M. Popa, and A. Zamfiroiu, "IoT solution for smart cities' pollution monitoring and the security challenges," *Sensors*, vol. 19, no. 15, p. 3401, 2019.

[19] S. Shakya, "A perspective review of security issues in iot with cloud environment," *Journal of IoT in Social, Mobile, Analytics, and Cloud*, vol. 4, no. 2, pp. 84–93, 2022.

[20] J. Kuusijärvi, R. Savola, P. Savolainen, and A. Evesti, "Mitigating IoT security threats with a trusted Network element," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 260–265.

[21] U. Chatterjee and S. Ray, "Security Issues on IoT Communication and Evolving Solutions," *Soft Computing in Interdisciplinary Sciences*, pp. 183–204, 2022.

[22] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[23] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of things journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[24] S. Anand and A. Sharma, "Assessment of security threats on IoT based applications," *Materials today: proceedings*, 2020.

[25] C. Gonzalez-Amarillo, C. Cardenas-Garcia, M. Mendoza-Moreno, G. Ramirez-Gonzalez, and J. C. Corrales, "Blockchain-iot sensor (Biots): A solution to iot-ecosystems security issues," *Sensors*, vol. 21, no. 13, p. 4388, 2021.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022

[26] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[27] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

DOI: https://doi.org/10.54216/JISIoT.060206
Received: March 28, 2022 Accepted: July 08, 2022