International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Building Trust on the IoT Connected World: Addressing Security Challenges in IoT Architectures and Applications

Dr. Mahesh D. Titiya*[1], Maulik D. Trivedi[2], Dr. Sheshang Degadwala[3]

Submitted:09/03/2024 **Revised**: 23/04/2024 **Accepted**: 02/05/2024

Abstract: IoT is revolutionizing how we interact with the world, connecting everyday objects and enabling a vast array of applications. However, this interconnectedness raises critical security concerns. This paper delves into the foundation of the IoT, exploring various architectures that support its functionality. We then examine the diverse applications that leverage these architectures, highlighting the potential benefits they offer across various domains. However, the paper argues that without robust security measures, the true potential of IoT cannot be fully realized. We analyse the vulnerabilities inherent in IoT systems, exploring common security issues such as weak authentication, data breaches, and botnet attacks. To address these challenges, the paper investigates existing and emerging solutions that can fortify the security posture of the IoT ecosystem. This includes exploring secure communication protocols, encryption techniques, and leveraging advancements in technologies like blockchain and machine learning. By providing a comprehensive understanding of IoT architectures, applications, and security considerations, this paper aims to guide researchers and developers in building a more secure and trustworthy foundation for the future of the IoT.

Keywords:*IoT, IoT Architecture, IoT Security, IoT Applications, Security Challenges, Security Solutions*

1. Introduction

IoT is currently a hotspot for academic interest. Among the many diverse uses for IoT devices have been a plethora of applications, such as: Some examples include: logistics management, intelligent transportation, smart homes, smart cities, automation in buildings, smart metres, smart agriculture, automated vehicles, and smart health. [1] Smart devices in an IoT system can link to other networks to generate data, which is valuable. Unfortunately, many manufacturers of IoT devices have systems that are vulnerable to attacks because of this. Researchers are particularly worried about the safety of Internet of Things systems. One critical aspect of security is the protection of information. On this page you will find an up-to-date summary of the problems with and solutions to IoT security. To address security concerns across the board in the IoT, we also evaluate existing solutions and propose new ones.

2. IoT Architecture

The Internet of Things architecture consists of three layers: perception, network, and application layers [2-3]. The following information provides a comprehensive overview of each layer: 1) Detection layer: An Internet of Things (IoT) device refers to the physical layer or sensor layer of a network. This layer is responsible for data collection and object management. As an example of a sensor technology on the perception layer, we have RFID, WSN, GPS, etc. Second, the network layer, often called the "transmission layer" since it processes data sent from the perception layer and sent to the application layer. A various network communication technologies are used for data receipt. A wireless/wired network or a local area network(LAN) can make use of several network communication technologies [4]. Near field communication (NFC) includes WirelessHART, mobile communication, 3G/4G/5G, Wi-Fi, Bluetooth, Zigbee, Long-Term Evolution (LTE), infrared technology, fibre optic communication networks, broad television networks, and so on [5-6]. The third level is the application layer, which is also known as the service layer. It is the responsibility of this layer to manage the presentation and format of the data that is received from the network layer. On top of that, it fulfils customer requests for services. IoT has many potential uses in fields such as logistics management, healthcare, intelligent transportation, building automation, intelligent weighing, automated vehicles, intelligent homes, intelligent cities, and intelligent transportation. Computers, laptops, and smartphones are just a few examples of the smart devices that may access IoT applications. The application layer is where the message protocol travels. The acronyms AMQP, COAP, XMPP, and MQTT stand for "message queuing telemetry transport"), among others [7].

1Assistant Professor, Computer Engineering Department, Government Engineering College, Rajkot, Gujara,India
ORCID ID : 0000-0001-6181-6562,Email: mdtitiya@gmail.com
2Research Scholar, Gujarat Technological University, Ahmedabad, Gujarat, India,
ORCID ID : 0009-0004-0132-1911 Email: mauliktrivedi.ce@gmail.com
3Professor & Head Department of Computer Engineering, Sigma University, Vadodara, Gujarat, India
ORCID ID : 0000-0002-2385-7790 Email:sheshang13@gmail.com
** Corresponding Author Email: mdtitiya@gmail.com*

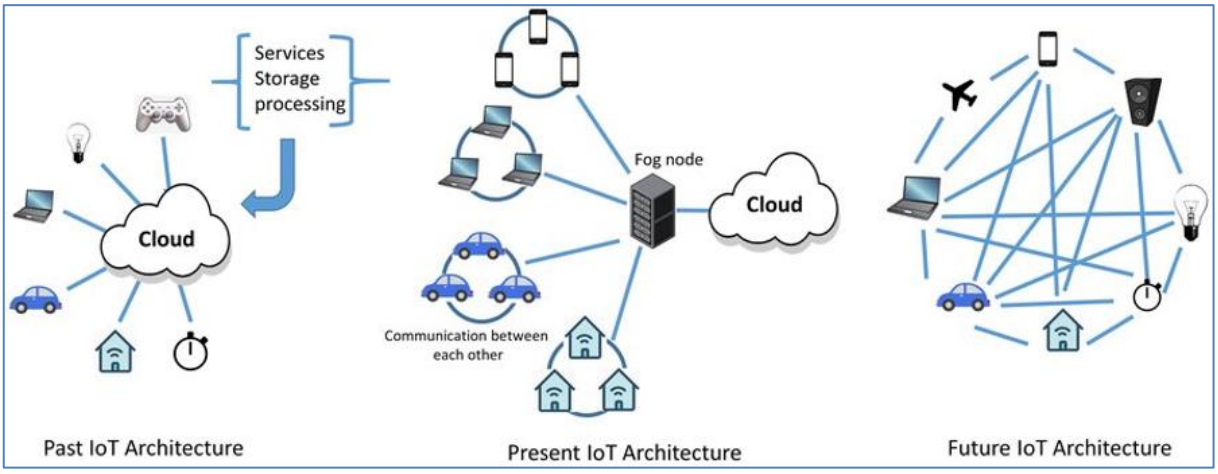


Figure 1: Past, Present, Future of IoT Architecture

3. IoT Security Architecture

An IoT security architecture is a blueprint that safeguards devices, data, and communication channels within an IoT system. It establishes strategies, policies, and measures to proactively counter cyber threats. An IoT security architecture is a blueprint that outlines strategies, policies, and tools to safeguard devices, data, and communication channels within an IoT network. It essentially builds a layered defence system to mitigate cyber threats targeting these interconnected systems.

3.1. Importance Of IoT Security Architecture

IoT devices, due to their inherent nature, can be vulnerable to attacks. They often have limited processing power and memory, making robust security implementations challenging. Additionally, the vast number of devices and the ever-growing attack surface necessitate a structured security approach. The three elements of CIA, like the other aspects we have discussed, are fundamental principles of IoT security architecture[9].

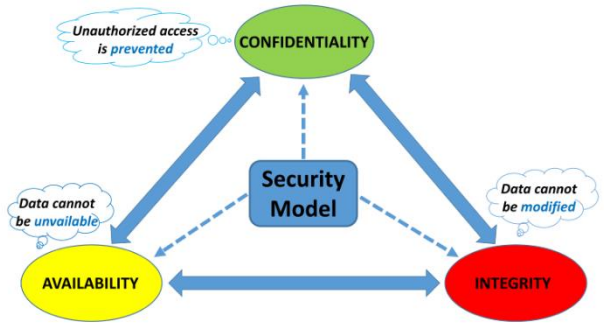


Figure 1: CIA Triad in Security Model

Here we will discuss the CIA triad in detail: The CIA triad [10] refers to three core information security objectives:

Confidentiality:

This principle ensures that only authorized users or devices Gain access to sensitive information within your IoT network Encryption plays a key role here, as it encrypts the data and makes it unreadable by unauthorized parties.

Integrity:

This principle ensures the accuracy and reliability of data. We guarantee that your data has not been tampered with in transit or at rest. Security measures such as digital signatures and tamper detection mechanisms help maintain data integrity.

Availability:

This principle emphasizes that authorized users and devices must have timely and reliable access to data and resources within his IoT network. System availability, redundancy measures, and disaster recovery planning all help ensure availability.

3.2. CIA Significance in IOT Security:

The CIA triad[10] serves as a guidance framework for securing IoT systems. By focusing on these three goals, you can develop a security architecture that protects sensitive information, prevents unauthorized modification, and ensures that authorized users have the access they need. How it Integrates with IoT Security Architecture: The various components of the IoT security architecture described previously all contribute to achieving the CIA's three goals. It is possible to improve secrecy by designing secure devices with encryption. Authentication and authorization are two methods that guarantee that only authorized individuals can access data, hence maintaining its integrity and confidentiality. Network segmentation restricts access to certain data sets (sensitivity). Data encryption protects information at rest and in transit (confidentiality). Intrusion detection helps maintain data integrity by identifying and preventing unauthorized changes. Security patch management addresses vulnerabilities that can be exploited to compromise confidentiality or integrity.

3.3. Key Components:

When designing devices, give priority to those that have integrated security features such as secure boot, encryption, and tamper detection.

Authentication and Authorization: Establish strong systems to authenticate the identity of devices and people seeking to access the network or data. Possible measures include the implementation of robust passwords, use of digital certificates, or the adoption of multi-factor authentication.Network Segmentation is the partitioning of a network into distinct zones, each with a specific security level. This practice effectively segregates essential systems from less secure devices, hence reducing the potential consequences of a possible security compromise.

Data Encryption: Employ cryptographic techniques to secure data that is stored on devices (data at rest) and data that is travelling across the network (data in transit). This ensures the confidentiality of the data and prevents unauthorised access.Establish an integrated system for the purpose of centrally managing the IDs of devices and controlling the access privileges of such devices. Through this, it is ensured that only authorized devices are able to connect and have access to the data that is being requested.Designed to monitor network traffic and identify any odd behavior, Intrusion Detection and Prevention Systems (IDS/IPS) are designed to prevent and detect intrusions. After then, these systems take preventative efforts to stave off potential

threats by inhibiting them.Security Patch Management involves the proactive identification, testing, and deployment of security patches to fix vulnerabilities in devices and software.

Implement Security by Design: Incorporate security measures at every stage of the IoT system's lifecycle, starting from the initial design and development, and continuing through deployment and operation.

Conduct regular threat modelling to evaluate potential risks and vulnerabilities that are specific to your IoT setup.

Compliance: Guarantee that your security architecture conforms to pertinent industry rules and data privacy laws. By deploying a thorough Internet of Things (IoT) security framework, you can effectively mitigate the likelihood of cyber intrusions and safeguard the authenticity of your devices, data, and entire system.

4. Security-Related Application Domains of theInternet of Things

Security is critical for the overwhelming majority of existing and upcoming Internet of Things applications. Virtually every existing sector is already employing some facet of Internet of Things (IoT). While operators are capable of managing Internet of Things apps using their existing network infrastructure, the security demands of these applications might be extremely challenging for some of them. Here we will go over some of the most important IoT applications that are safety-critic.

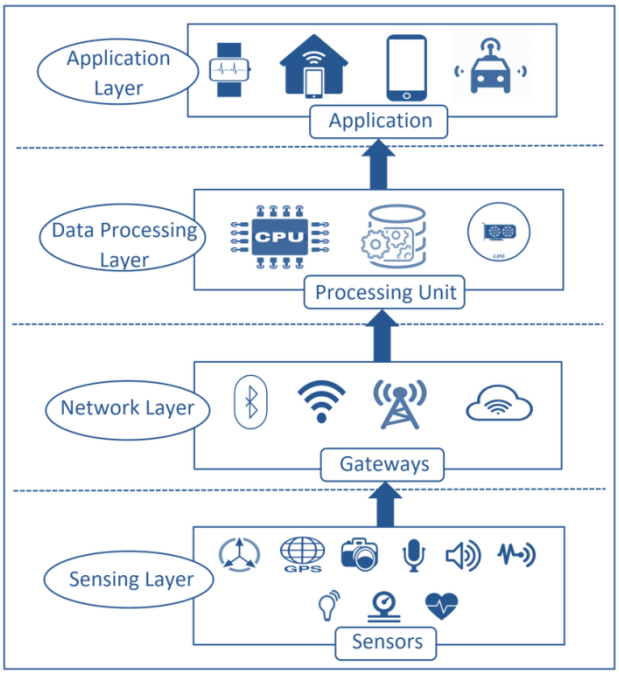


Figure 2: Application Area of IoT

4.1. Smart Cities

"Smart cities" are required to make substantial use of contemporary information and communication technology [11] in order to have a positive impact on the quality of life for all of its residents. Within this category, you can discover several types of systems such as "smart home" systems, traffic and disaster management systems, utilities, and many others. Globally, governments are actively encouraging urban development by offering various incentives, and initiatives are being implemented to enhance the intelligence of cities [12]. While the primary objective of installing intelligent applications is to improve the overall quality of life for individuals, this comes at the expense of compromising the privacy of residents. Regrettably, smart card services frequently put consumers' financial information and spending patterns at risk. Smart mobility apps possess the capability to monitor and record the geographical positions of its users. Parents might employ software applications to track the exact whereabouts of their children. However, if these apps are compromised, it might put children's safety at risk.

4.2. Smart Environment:

IoT applications in smart environments encompass various tasks such as forest fire detection, monitoring high-altitude snow cover, preventing landslips, detecting earthquakes in advance, and monitoring pollution levels, among others. There are numerous IoT applications that have a significant impact on the daily life of the local plants and animals. The data gathered by these Internet of Things applications will also prove valuable to government bodies that prioritise these industries. The consequences of security vulnerabilities and breaches in interconnected regions related to these applications are significant. IoT applications are especially susceptible to the severe consequences ofboth false positives and false negatives in this context. If, for example, an application incorrectly identifies an earthquake, both governments and enterprises face the risk of financial losses. On the other hand, if the software fails to predict an earthquake, there will be casualties and damage to both life and property. Applications designed for intelligent settings must exhibit a high level of precision and be devoid of any security vulnerabilities or data manipulation.

4.3. Smart Grids and Smart Metering:

Smart Metering refers to a broad range of applications that involve measuring, monitoring, and managing energy usage. It is a crucial component of the smart grid. Smart metres are mostly utilised for measuring and monitoring electricity consumption in the context of smart grids. Smart metres can also be utilised to combat the problem of electricity theft [13]. Intelligent techniques are also utilised to monitor the quantities of gas, oil, and water in reservoirs and storage tanks. The smart metre not only measures and optimises the operation of the solar energy system, but it also dynamically adjusts the angles of the solar panels to capture the maximum amount of solar energy. Smart metres can be employed in several Internet of Things applications to measure water pressure and the weight of things being moved through water. Unlike analogue metres, which are only vulnerable to physical attacks, smart metre systems are also

susceptible to cyber attacks. In addition, advanced metering infrastructure (AMI), which is also known as smart meters, is uniquely designed to carry out activities that go beyond the simple monitoring of energy use. Integrating all electrical equipment in a household with smart metres enables more efficient management of power use and expenses inside a smart home network (HAN). Malicious individuals or adversaries may deliberately infiltrate these communication networks, altering the collected data and perhaps resulting in financial losses for service providers or consumers [14].

4.4. Security and Emergencies:

Security and emergencies are among the prominent domains that extensively utilise IoT technologies. This encompasses a broad spectrum of applications, including the assurance that only permitted personnel are able to gain entry to restricted places. Another application for this technique is the detection of leaks in industrial or chemical plant environments. Furthermore, it has the capability to detect and convey elevated radiation levels in the vicinity of nuclear power plants and cell phone base stations. An important benefit is that this is the case. Various buildings contain systems that either store valuable products or store data that is considered confidential. Applications designed for security can be utilised to safeguard sensitive information and items. The adoption of IoT apps can safeguard these fragile structures from corrosion and even collapse by accurately identifying various fluids. Security breaches in these types of applications can lead to several serious consequences. Thieves can exploit vulnerabilities in these applications to get unauthorised access to restricted areas. In addition, erroneous radiation level notifications can have significant short- and long-term repercussions. There is significant evidence indicating that prolonged exposure of new-borns to high doses of radiation can result in serious, and perhaps fatal, problems.

4.5. Smart Retail Store:

Retailers depend on Internet of Things (IoT) applications to facilitate intelligent retail operations. Several applications exist that monitor the real-time storage status of products as they move along the supply chain. Product tracking in warehouses is now being managed using the Internet of Things to ensure accurate restocking. Several intelligent shopping applications may customise their support for each individual customer based on their preferences, habits, dietary restrictions, and so on. Furthermore, a system was implemented to allow brick-and-mortar shops to offer in-store customers a similar online buying experience as augmented reality applications. Retail organisations are facing security challenges as they adopt and use a variety of IoT applications in various MNCs [15]. The hacker may employ tactics such as disseminating false information or compromising the Internet of Things application responsible for managing product storage conditions in order to manipulate customers into making additional purchases. If Smart Retail lacks security protections, hackers can get sensitive information such as phone numbers, email addresses, debit/credit card details, and other personal data. Both the customer and the retailer face potential financial losses as a result of this situation.

4.6. Agriculture Automation and Animal Cultivation:

A sustainable agriculture automation encompasses a wide range of practices, such as soil moisture monitoring, microclimate control, selective irrigation in arid regions, and temperature and humidity regulation. Farmers can avoid financial losses and obtain great yields by utilising such technological features in agriculture. To keep fungus and other microbes from invading various grain and vegetable growing spaces, it is necessary to regulate humidity and temperature. Crop productivity and quality can both be enhanced through the manipulation of weather patterns. There are IoT apps that attach sensors to cattle to track their health and activity levels, much like crop monitoring. A breach in security for such apps could lead to the theft of farm animals or the destruction of crops.

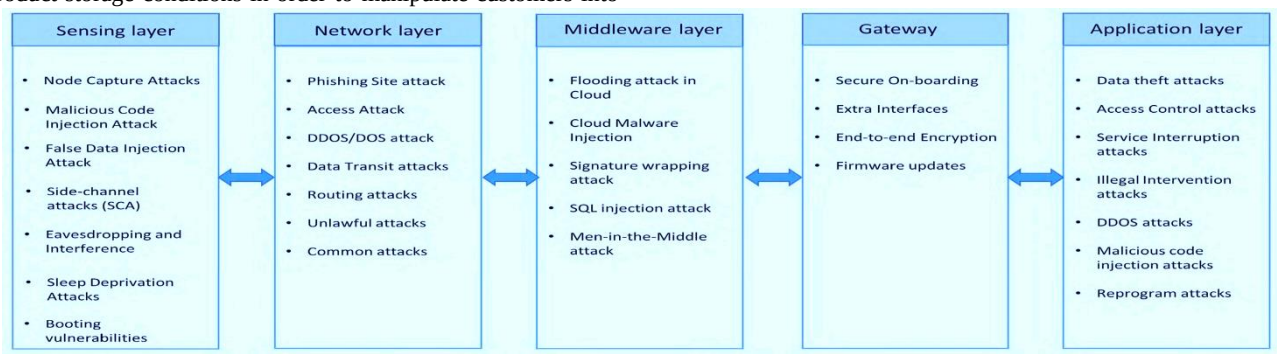
4.7. Smart Home Automation:

Home automation is a prevalent and extensively use of the Internet of Things (IoT). For instance, While there are applications that allow for the remotecontrol of household appliances for the goal of reducing energy consumption, there are also security systems that have the power to identify attempted breaches into a person's residence. The monitoring system is specifically built to track the consumption of power and water in order to maintain accurate records. Reduce costs and conserve resources. To enhance home safety, the authors of [16] propose employing logical-based security measures. The occurrence of a robbery at home can be determined by comparing the user's typical behaviours in specified places with their current activities in those same areas. However, malevolent individuals can gain unauthorised entry to residential IoT devices and attempt to inflict harm upon their users. The useof a variety of home automation systems has been associated with an increase in the number of home invasions, as demonstrated by a study [16]. There have been several instances where malicious individuals have attempted to ascertain the existence and behaviour of residents in smart homes by examining the type and amount of internet data transmitted to and from these homes.

5. IOT Architecture wise Security Threats in IOT Applications

As discussed in IOT Architecture - Part I, There are four distinct levels of IoT applications: (1) sensing, (2) networking, (3) middleware, and (4) application.

The fact that various technologies are used by each of these IoT application layers makes for a lot of problems and security risks.



At each of these four tiers, Figure 4 displays the corresponding technology, device, and application. Potential security risks in these four tiers of Internet of Things applications are detailed in this part. Figure 4 displays a variety of potential assaults on these four tiers. Additionally, this part covers the unique security concerns related to the gateways that link these layers.

5.1. Potential Threats at the Sensing Layer

The sensor layer primarily emphasises physical IoT sensors and actuators. The dynamic nature of the physical world allows for continuous changes, which can be detected by sensors [17] [19]. On the other hand, actuators utilise the collected data to execute specific tasks within the actual surroundings. Different sensors are capable of collecting different types of data. For instance, there are sensors designed to detect smoke, capture images, measure temperature and humidity, among other functions. Physical surroundings can be detected via mechanical, electrical, chemical, or electronic sensors. RFID, GPS, WSN, and RSN are all examples of sensing layer technologies commonly used in various Internet of Things applications. The sensing layer is susceptible to the subsequent significant security vulnerabilities:

Eavesdropping and Interference: Eavesdropping and interference are common concerns in IoT systems that utilise a network of nodes deployed in a public environment [20]. As a result, certain IoT applications can be susceptible to eavesdropping. Attackers have the potential to intercept and pilfer information at various points, involves the transmission of data and authentication.

Sleep Deprivation Attacks: Attacks that deprive a gadget of sleep are designed to drain the battery of an Internet of Things edge device that is not working well. Due to the fact that the battery has run out, the nodes that are part of her Internet of Things application are subjected to a denial of service. Two methods to accomplish this include deliberately either by increasing the amount of power that the edge device consumes or by utilising malicious software in order to create an infinite cycle.

Node Capturing: Sensors and actuators are examples of low-power nodes that are essential components of an application that utilises the Internet of Things. In a variety of different ways, attackers are able to take advantage of these nodes. A potential threat to an Internet of Things system is an unauthorised individual attempting to take control of a node or replace it with a malicious node.

An assailant gains control over a recently added node that appears to be a legitimate part of the system. The security of the entire IoT application could be compromised as a consequence [19].

Malicious Code Injection Attack: When an attacker inserts destructive code into the memory of a node, this is an example of a malicious code injection attack. It is possible for hackers to introduce harmful software or firmware into the software or firmware of an Internet of Things node when the node is upgraded wirelessly. A harmful piece of malware could be used by an attacker to either attempt to get access to the entire Internet of Things (IoT) system or to manipulate the node in order to carry out actions that are inappropriate.

False Data Injection Attack: An adversary who initially takes control of a node and then injects phoney data into the Internet of Things system is capable of carrying out an attack known as a fake data injection attack. An Internet of Things application can stop functioning, which might then lead to the generation of inaccurate data. This could happen if the application is not properly maintained. This is an alternative method that attackers can employ to initiate Distributed Denial of Service (DDoS) attacks on our systems.

Side-Channel Attacks (SCA): Side-Channel Attacks (SCA) encompass several forms of assaults that can result in the unauthorised disclosure of sensitive information, in addition to direct attacks on the nodes. Adversaries can get confidential data by exploiting CPU microarchitectures, electromagnetic emissions, and power consumption. Possible attacks include power consumption, timing, electromagnetic, or laser-based side channel attacks. To safeguard the cryptography modules against side-channel attacks, contemporary chips employ various defences.

Booting Attacks: At the beginning of the boot process, edge devices are susceptible to a variety of different kinds of attacks. The built-in security mechanisms are currently off, which is the reason for this situation. By restarting a node device, there is a possibility that an adversary will be able to take advantage of this vulnerability. Due to the fact that edge devices often have a low power consumption and go through periodic sleep and wake cycles, it is extremely important to ensure that the boot process offers adequate security.

5.2. Potential Threats at the Network Layer

Following the completion of the data collection procedure, the network layer sends the information to the computer so that it can be processed. When it comes to network security, the majority of problems involve:

Location-Based Phishing Attacks: There are times when these attacks zero in on particular Internet of Things devices without any effort being made by the attacker. The attackers anticipate that certain devices may fall prey to the assault. While using the internet, people face the potential danger of being targets of phishing websites. Once a hacker has gained unauthorised access to the user's account and password, the entire Internet of Things ecosystem of the client becomes vulnerable to cyberattacks. Phishing attacks targeting the IoT's organisational layer can be easily exploited, leading to compromise [21].

Access Attack: An access assault, often known as an advanced persistent threat (APT), refers to a type of cyber attack. Typically, a method of assault in which an opponent or unauthorised individual obtains entry to the IoT network. The assailant can remain concealed within the arrangement for a prolonged period of time. The objective of this style of assault is not to do damage to the system, but rather to pilfer important data or information. Due to the continuous exchange of critical information, IoT applications are very susceptible to these specific sorts of assaults [22].

DDoS/DoS Attack: A distributed denial of service (DDoS) assault occurs when the attacker inundates the targeted servers with an excessive number of unsolicited requests, causing them to become overwhelmed. By incapacitating the target server in this manner, it causes a disruption in services for genuine clients. During a denial-of-service attack, also known as a DDoS attack, the attacker uses a variety of different sources to overwhelm the server that is the target of the attack. In spite of the fact that they are not exclusive to Internet of Things applications, these attacks are more likely to concentrate on the organisational layer of the Internet of Things due to the diverse and complex nature of IoT solutions. There are a lot of Internet of Things devices that are used in Internet of Things applications that have not been setup properly, which makes them susceptible to distributed denial of service attacks. The Mirai botnet attack, mentioned in the previous part, exploited this vulnerability by continuously sending requests to poorly configured Internet of Things devices,

resulting in the disruption of multiple services [23].

Data Transit Attacks: Data transit attacks occur when Internet of Things (IoT) applications engage in the negotiation of a specific amount of data bandwidth and commercial transactions. This characteristic renders them susceptible to such assaults. Data is constantly targeted by cybercriminals and other malicious individuals due to its crucial significance. While data kept either locally or in the cloud is somewhat protected, data that is being transferred or in transit between locations is significantly more susceptible to cyber-attacks. IoT applications need extensive data development between sensors, actuators, the cloud, and other components. IoT applications are vulnerable to data breaches due to their use of many connectivity protocols.

Routing Attacks: On the other hand, routing attacks take place when rogue nodes within an Internet of Things application make an attempt to alter the routing patterns while data is being transferred. A sinkhole attack involves a malevolent individual who deceives nodes by promoting a counterfeit shortest routing path, leading them to send their traffic through it. One of the most significant dangers to the safety of computer networks is the combination of attacks, which includes wormholes and sinkholes, among other types of attacks. Through the establishment of an out-of-band link between two nodes, a wormhole makes it possible to transmit packets in an efficient manner. By creating a direct link between a compromised node and an internet-connected device, a hacker can create a vulnerability within an Internet of Things application. This weakness can then be exploited by the criminal. This allows the hacker to circumvent the primary security procedures that are used in the application.

5.3. Potential Threats at the Middleware Layer

Middleware in the Internet of Things (IoT) is responsible for establishing an intermediary layer that exists between the organisation and application layers. Middleware [24] can also offer efficient computing and capacity capabilities. The application layer depends on the APIs offered by this layer to carry out its functions. The middleware layer is comprised of a variety of components, including brokers, persistent data storage, lining frameworks, machine learning, and other functions that are otherwise comparable. Furthermore, despite the fact that the middleware layer is essential for delivering a trustworthy and strong Internet of Things programme, it is susceptible to a variety of threats. The opportunity to take control of the entire Internet of Things project is available to these attacks after they have successfully penetrated the middleware. There are a number of fundamental security concerns that need to be handled at the middleware layer. Two examples of these concerns are databases and the cloud. An analysis of the several types of attacks that could be launched against the middleware layer is presented in the following paragraphs.

MiTM Attack: A "man-in-the-middle" attack can happen when a MQTT broker, acting as an intermediary, employs the publish-subscribe protocol to enable communication between clients and endorsers. Messages can be transmitted without prior knowledge of the objective, as the distribution and subscribing customers are independent of each other. Should the attacker effectively get control of the broker and assume the role of a man-in-the-middle, they would possess full authority over all communications, unbeknownst to the customers.

SQL Injection Attack: SQL Injection Attack: Middleware is susceptible to SQL Injection (SQLi) attacks. An attacker can inject harmful SQL statements into a software during this type of attack [25], [26]. Upon successful infiltration, the perpetrators will get entry to confidential customer information and possess the capability to modify database entries [27]. OWASP's 2018 archive of their best 10 list identifies SQL injection as a prominent risk to web security [28].

Attack on Signature Wrapping: XML Marks, also known as Signature Wrapping Attacks, are utilised by web services in the middleware [29]. Signature wrapping attacks occur when an attacker takes use of a vulnerability in Cleanser (Basic Question Get to Convention) to compromise the process of computing the signature. This allows the attacker to perform operations or make changes to the observed message [30].

Cloud Malware Infusion Attack: A cloud malware infusion assault refers to a situation where an attacker successfully takes control of a cloud system and contains malicious code or a virtual computer when it is introduced into it. By attempting to construct a virtual machine event or a malicious benefit module, the attacker has the intention of making a huge profit. Through this action, the perpetrator can get confidential data about the target and customise their assault accordingly.

Flooding Attack in Cloud: It is possible to compare the effects of a flooding assault in the cloud to those of a denial-of-service (DoS) attack in the cloud regarding their impact. On account of the fact that both kinds of attacks have the same impact on the quality of service (QoS), this is the case. Attackers constantly bombard a victim with an excessive number of requests in order to do away with cloud resources. This is done with the intention of depleting cloud resources. By generating a rise in the stack size of the cloud servers, these kinds of attacks have the potential to have a significant impact on cloud frameworks.

5.4. Potential Threats at the Gateways

The connection of different devices, individuals, objects, and cloud services is facilitated by a central layer known as a gateway. IoT gateways also enable the transmission of software and hardware solutions. Gateways are responsible for managing IoT data encryption and decryption, as well as converting protocols for communication between different layers [31]. The Internet of Things (IoT) systems that are currently in use involve a number of different components. These components include TCP/IP stacks, Z-Wave, LoraWan, and ZigBee, in addition to a number of other intermediate gateways. There is a connection between access points for the Internet of Things and a number of security vulnerabilities, some of which are as follows:

Secure On-boarding: A safe and secure It is vital to take additional precautions during the on-boardingphase of the system in order to ensure the security of encryption keys during the process of integrating a new sensor or device into an Internet of Things (IoT) system. This is because the on-boarding phase is the phase in which the system is being implemented. Gateways serve as intermediaries that enable the exchange of keys between the management services and the new devices. This is done in order to simplify communication between the new devices and the management services on the other hand. Gateways are especially susceptible to man-in-the-middle attacks and eavesdroppers who are looking to steal encryption keys during the onboarding process on account of their high level of vulnerability.

Extra Interfacing: When introducing IoT devices, it is important to keep in mind the technique of minimising the assault surface. The IoT door manufacturer should implement the fundamental interfaces and protocols, so to speak. For the purpose of preventing unauthorised access or data breaches, certain administrations and functionality ought to be restricted to end-users.

End-to-End Encryption: To ensure the privacy of the information, it is necessary to have authentic end-to-end security at the application layer [33]. The programme must restrict access to decrypting the encrypted communications to only the intended recipient. Zigbee and Zwave protocols both incorporate encryption; however, this encryption does not cover the entire transmission process. The reason for this is that in order for gateways to convert data from one protocol to another, they must first decode the messages and then re-encrypt them thereafter. This is the reason why this is the case. Decoding any information at the portal level exposes it vulnerable to the threat of information privacy breaches. This applies to any and all information.

Firmware upgrades: The majority of IoT devices are limited in resources, which means they lack a user interface or the computational power to download and install firmware upgrades. Portals are mostly used to download and install firmware upgrades. For the purpose of ensuring that firmware upgrades are implemented in a secure manner, it is essential to document both the active and inactive versions of the firmware and to check the authenticity of the signatures.

5.5. Potential Threats at the Application Layer

The application layer has direct interaction with end users and offers services to them. The layer contains his IoT applications, including smart homes, smart metres, smart cities, and smart grids. There are certain security flaws that are present in the current layer, such as concerns about data theft and privacy, which are not present in any of the other layers. There are other challenges regarding security at this level that are specific to certain applications. Middleware layers and application support layers are two names that are sometimes used to refer to these sublayers, which are located between the network layer and the application layer. Apps that are connected to the Internet of Things usually include these sublayers. In addition to making it simpler to access a wide variety of business services, the support layer also makes a contribution to the intelligent allocation and utilisation of resources.

Data theft: Internet of Things (IoT) apps handle substantial volumes of highly confidential personal data. Data in transit is more susceptible to assaults compared to data at rest, and IoT applications entail substantial data transfer. If an Internet of Things (IoT) application is susceptible to data theft threats, a user will be reluctant to provide personal data while registering with the programme. Techniques and protocols such as data encryption, data isolation, user and network authentication, and privacy management are employed to safeguard IoT applications against data theft.

Access Control Attacks: Access control attacks refer to unauthorised attempts to gain access to data or accounts by bypassing or circumventing the authorization mechanisms in place. Access control assaults are a significant threat in IoT systems because if access is breached, the entire IoT application becomes susceptible to attack.

Denial of Service Attacks: Denial of Service assaults, often known as illegal disruption assaults or DDoS attacks, are described as such in current literature. Multiple instances of such hacks targeting IoT applications exist. These attacks cause genuine users of IoT application services to be unable to access them by intentionally overwhelming servers and networks with excessive traffic.

Malicious Code Injection Attacks: When it comes to infiltrating a system or network, attackers sometimes choose the way that is the least complicated or the least difficult to carry out. In the event that the system is susceptible to vulnerabilities that give rise to malicious programming or misdirection as a consequence of insufficient code review, it is highly probable that attackers will utilise these vulnerabilities as their primary point of entry. Attackers regularly use a technique known as cross-site scripting, or XSS, to install malicious scripts into websites that are considered to be trustworthy. An effective cross-site scripting attack has the potential to take control of Internet of Things accounts and to cause faults in Internet of Things systems.

Sniffing attacks: Sniffing attacks involve the use of sniffer software to eavesdrop on the network traffic of IoT applications. In the absence of adequate security mechanisms, there is a risk that an attacker could get unauthorised access to sensitive user data [34].

Reprogramming attacks: Reprogramming attacks occur when an attacker tries to remotely reprogram IoT objects if the programming process lacks properprotection. This has the potential to result in the unauthorised takeover of IoT networks [35].

6. Necessary Improvements and Enhancements for Future IoT Applications

1. IoT devices must undergo comprehensive penetration testing to assess the risks associated with their use in different situations. It is feasible to assign priority to the devices and allocate them to various applications based on the level of risk associated with each.
2. The IoT system utilises encryption methods inside its various layers and protocols. The entire system employs a multi-tiered process of encrypting, decrypting, and re-encrypting. Because of these cycles, the system is susceptible to being attacked. Implementing encryption that is complete from beginning to finish would be a preventative strategy that would protect against a variety of threats.
3. Implement protocols that mandate continuous authentication. It is necessary to implement an authentication procedure whenever one device wants to communicate with another. Digital certificates offer a potential solution to the challenge of facilitating convenient authentication through the use of linked identities in cryptographic systems.
4. Prior to implementation, it is crucial to thoroughly test and verify the scalability of any IoT security architecture. Only some users should be excluded from using the security protocols. Once the application becomes operational and experiences significant usage by the general populace, that is when the grave hazards emerge. Therefore, it is vital to utilise a suitable strategy and anticipate future events.
5. With the implementation of an encryption mechanism that is dependent on algorithms such as RSA, SHA, or hash chains, it is vital to avoid the acquisition of user and environmental data. This can be accomplished by implementing the mechanism. It is imperative that the data collected by IoT devices is securely communicated and encrypted during their development. This approach can bolster the faith of individuals, government agencies, and industries in IoT applications.
6. Given the increasing number of IoT devices and applications, it is necessary to develop a strategy to effectively handle the upcoming constraints related to cost and capacity. There is a potential requirement for a shift in the way we handle things, moving from centralised methods to decentralised methods. This would involve enabling devices to connect with each other in an

automated and secure manner. This approach can mitigate both the cost of application management and the issues arising from capacity constraints [36].

7. It is important to consider vulnerabilities connected to cloud computing, as most IoT applications depend on cloud services for storing and retrieving data. The cloud is a communal asset that numerous individuals exploit, and among those individuals, there may be adversaries who pose a threat to the data linked to IoT. Cloud storage should employ encryption to secure data prior to storage, and cloud providers should not possess the capability to decrypt any data stored within their systems. By using this approach, we may mitigate the typical risks associated with cloud computing and significantly enhance data security [37].

8. There are a number of different circumstances in which the sensors that are utilised in an Internet of Things application begin to collect or communicate incorrect data. These scenarios are in addition to problems that are caused by external sources. In a centralised architecture, these errors could be easily managed; however, in a decentralised, autonomous system, they could pose a bottleneck. Incorrectly reading or transmitting the data can lead to catastrophic outcomes. Considering this, it is crucial to establish a method for validating the movement of data, especially in a distributed framework [38].

9. The implementation of artificial intelligence algorithms or approaches to protect Internet of Things devices can be beneficial, given that the ultimate goal of all Internet of Things applications is to create a self-governing system that reduces the amount of human contact that is required. Taking this strategy has the potential to reduce the cognitive and communication burden that is present in the ecosystem of the Internet of Things [39].

7. Acknowledgement

I express my gratitude to Darshan University - Rajkot for facilitating my research work on my chosen topic and giving the necessary resources. I am also appreciative of my guide for imparting their expertise in alignment with the paper and topic.

References

[1] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving iot environments: a survey," Wireless Communications and Mobile Computing, 2018.

[2] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," Int. Conf. on IoT in Social, Mobile, Analytics and Cloud, pp. 492-496, 2017.

[3] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things security," Int. Conf on Wireless Technologies, Embedded and Intelligent Systems, pp. 1-6, 2017.

[4] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: state of the art," Int. Conf. on Robots and Sensor Clouds, pp. 55-75, 2016.

[5] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," Journal of Network and Computer Applications, vol. 128, pp. 105-140, 2019.

[6] Y. I. N. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," Journal of Industrial Information Integration, vol. 1, pp. 3-13, 2016.

[7] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Computer Networks, vol. 148, pp. 283-294, 2019.

[8] H. Suo, J. Wan, C. Zou, J. Liu," Security in the internet of things: a review ", Computer Science and Electronics Engineering (ICCSEE), 012 international conference, vol. 3, pp. 648-651, 2012.

[9] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019.

[10] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018.

[11] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, ``Smart cities: A survey on data management, security, and enabling technologies," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456 2501, 4th Quart., 2017.

[12] D. Eckhoff and I. Wagner, ``Privacy in the smart city Applications, technologies, challenges, and solutions," IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 489 516, 1st Quart., 2018.

[13] X. Xia, Y. Xiao, and W. Liang, ``ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 445 458, 2019.

[14] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, ``Toward a secure wireless-based home area network for metering in smart grids," IEEE Syst. J., vol. 8, no. 2, pp. 509 520, Jun. 2014.

[15] N. N. Dlamini and K. Johnston, ``The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review," in Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE), Nov. 2016, pp. 430 436.

[16] A. C. Jose and R. Malekian, ``Improving smart home security: Integrating logical sensing into smart home," IEEE Sensors J., vol. 17, no. 13, pp. 4269 4286, Jul. 2017.

[17] Bridgera. IoT System | Sensors and Actuators. Accessed: Feb. 9, 2019. [Online]. Available: https://bridgera.com/IoT-system-sensors-actuators/

[18] Tictecbell. Sensor d'Ultrasons. Accessed: Feb. 11, 2019. [Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons/

[19] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, ``Security enhancements to system on chip devices for IoT perception layer," in Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS), Dec. 2017, pp. 151 156.

[20] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, ``Eavesdropping prevention for heterogeneous Internet of Things systems," in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1 2.

[21] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf

[22] C. Li and C. Chen, ``A multi-stage control method application in the fight against phishing attacks," in Proc. 26th Comput. Secur. Acad. Commun. Across Country, 2011, p. 145.

[23] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ``DDoS in the IoT: Mirai and other Botnets," Computer, vol. 50, no. 7, pp. 80 84, 2017.

[24] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, ``A survey of middleware for Internet of Things," in Recent Trends in Wireless and Mobile Networks. Springer, 2011, pp. 288 296.
[25] Q. Zhang and X. Wang, ``SQL injections through back-end of RFID system," in Proc. Int. Symp. Comput. Netw. Multimedia Technol., Jan. 2009, pp. 1 4.
[26] R. Dorai and V. Kannan, ``SQL injection-database attack revolution and prevention," J. Int. Commercial Law Technol., vol. 6, no. 4, p. 224, 2011.
[27] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, ``Middleware for Internet of Things: A survey," IEEE Internet Things J., vol. 3, no. 1, pp. 70 95, Feb. 2016.
[28] Acunetix. Insecure Deserialization. Accessed: Feb. 9, 2019. [Online]. Available: https://www.acunetix.com/blog/articles/owasp-top-10-2017/
[29] J. Kumar, B. Rajendran, B. S. Bindhumadhava, and N. S. C. Babu, ``XML wrapping attack mitigation using positional token," in Proc. Int. Conf. Public Key Infrastruct. Appl. (PKIA), Nov. 2017, pp. 36 42.
[30] WS-Attacks. Attack Subtypes. Accessed: Feb. 9, 2019. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping
[31] C. Fife. Securing the IoT Gateway. Accessed: Feb. 9, 2019. [Online]. Available: https://www.citrix.com/blogs/2015/07/24/securing-the-IoTgateway/
[32] A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zam r, ``Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm," in Proc. Int. Conf. Optim. Elect. Electron. Equip. (OPTIM) Int. Aegean Conf. Elect. Mach. Power Electron. (ACEMP), May 2017, pp. 1001 1006.
[33] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, ``A blockchain connected gateway for BLE-based devices in the Internet of Things," IEEE Access, vol. 6, pp. 24639 24649, 2018.
[34] S. N. Swamy, D. Jadhav, and N. Kulkarni, ``Security threats in the application layer in IoT applications," in Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC), Feb. 2017, pp. 477 480.
[35] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, ``A comprehensive IoT attacks survey based on a building-blocked reference model," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, pp. 355 373, 2018.
[36] N. Kshetri, ``Can blockchain strengthen the Internet of Things?" IT Prof., vol. 19, no. 4, pp. 68 72, 2017.
[37] W. Wang, P. Xu, and L. T. Yang, ``Secure data collection, storage and access in cloud-assisted IoT," IEEE Cloud Comput., vol. 5, no. 4, pp. 77 88, Jul. 2018.
[38] S. Suhail, C. S. Hong, Z. U. Ahmad, F. Zafar, and A. Khan, ``Introducing secure provenance in IoT: Requirements and challenges," in Proc. Int. Workshop Secure Internet Things (SIoT), Sep. 2016, pp. 39 46.
[39] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, ``IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" IEEE Signal Process. Mag., vol. 35, no. 5, pp. 41 49, Sep. 2018.