JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

IOT SECURITY: APPLICATION DOMAIN, ATTACKS, THREATS SOLUTIONS AND CONTEMPORARY CHALLENGES IN THE LIGHT OF QUALITY STANDARDS

[1]AHMED MOHAMED MAHER, [2]DR.S.SUGANYA

[1]Research Scholar, Department of Computer Science, Rathinavel Subramaniam College of Arts and Science, India.

[2]Master of Computer Application, Assistant Professor, Department of Computer Science, Rathinavel Subramaniam College of Arts and Science, India.

Abstract— the new age in connectivity is the Internet of Things (IoT). It may enable physical objects to create, receive, and share information smoothly using the IoT. Different IoT applications concentrate on automating various tasks and aim to allow inanimate physical objects to behave with no human interference. In order to improve the level of convenience, productivity and automation for consumers, current and future IoT implementations are extremely promising. It needs top security, privacy, authentication, and recovery from attacks to incorporate such a world in an ever-growing manner. To achieve end-to - end secure IoT environments, it is imperative to make the requisite improvements in the IoT's design applications In this paper, we cover the applications in various fields of the Internet of things in addition to targeted attacks, as well as potential threats and methods of solution and dealing with them in addition to some contemporary challenges in light of quality standards to reach the maximum level of Internet of things security.

Keywords: Internet of Things, security, standards, indicators, quality, indoor, outdoor.

1 Introduction

The emerging developments in embedded technology and the Internet have facilitated the interconnection of artifacts around us. It envisages a future in which IoT devices are invisibly embedded in the world and huge amounts of data will be produced. To make it clear and usable, such data will have to be saved and processed .The IoT model includes various actors including mobile carriers, app developers, suppliers of access infrastructure, and so forth. IoT applications are also very large and these networks can be used in construction, service management, etc., agriculture and healthcare. The next paradigm of interconnection that enables communication between devices and machines that enables actions to occur without human intervention is ioT. The development of the IoT environment requires a convergence of another communications technology. The concept of smart gateways has contributed to the linking of IoT devices to the regular Internet. It aims recent efforts at interconnecting IoT infrastructure and cloud computing which complements IoT's potential. Increasing complexity also magnifies the security challenges these networks face. The complexity of IoT networks is because of the enormous number of devices connected to the Internet and to the enormous amount of data produced by those devices. Attacks in IoT are possible because the devices in the IoT network are a simple intrusion target [1]. When the hackers have been penetrated, they will gain control and execute malicious activities, and target other devices close to the node. IoT devices do not have the tools to detect viruses or malware. Is an inevitable consequence of their poor memory and low power existence. The lack of virus and malware protection available on IoT devices makes them highly vulnerable to bots and conduct malicious activity on other network devices. When an IoT computer has been compromised the attacker can even hijack the device's routing and forwarding operations. Besides attacking several other machines in the network, additionally attackers, can access confidential data collected and transmitted by IoT devices. The lack of confidentiality, honesty and data protection in IoT could interfere with the widespread use of this technology [2]. It is clear from the discussion until now that protecting IoT devices is greatly compounded by their Resource-constrained design, because of which IoT networks cannot easily deploy solutions for attack prevention and privacy protection used on conventional networks.

2 Application of IoT

There are several areas of life where IoT can be implemented. The IoT reflects a perspective where the Internet is merged with every object. Here each physical entity (precisely said a thing) is connected to the computing world and can be regulated and coordinated remotely. Such objects can also be used as an entry point to connect with other objects and access different Internet resources. Therefore, because of its presence in each sphere of the physical world, IoT has been evolved as a paradigm whose implementation can cover a wide variety of application domains. Its tremendous exposure is easily foreseeable soon. The product of the ability to connect embedded devices with minimal Processor, memory and power

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

resources enables the IoT to discover applications in almost any field [3]. Many academicians and researchers have recognized an extensive range of IoT applications. In 2012, a ranking report [4] was published that described 50 remarkable application areas of IoT. Finally, these application areas were further generalized into 13 sets Smart-cities, Smart-environment, Smart-water, Smart-metering, Security & Emergencies, Retail, Logistics, Industrial control, Smart-Agriculture, Smart-Animal-farming, Demotic and Home automation, Smart-Education and e-Health. According to Perera et al. [5], the IoT application fields can be roughly put into five key categories: smart wearable, smart home, smart city, smart environment, and smart enterprise. Matta et al. [6] also proposed the classification of application areas into five broader categories. It bases this classification on the tasks. These categories are: indoor; outdoor; Environmental; Technological; and Emergency and Critical Situations. These categories can be further discussed under the name of different subcategories, as shown in Fig. 1.

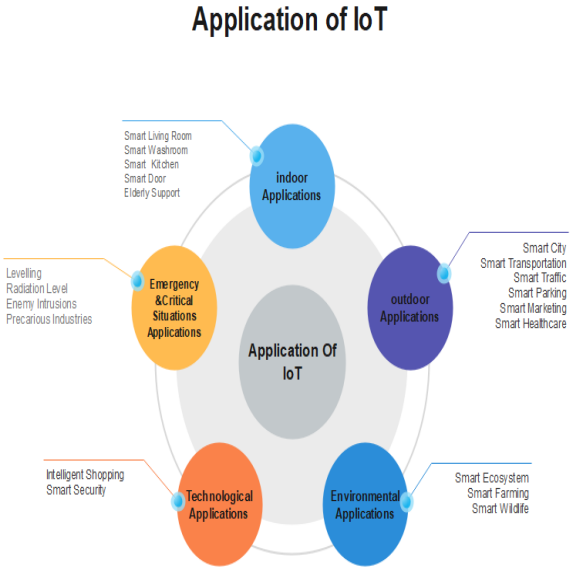


Fig. 1. Application of IoT

2.1 Indoor applications

Indoor applications may include a smart living room, smart washroom, smart kitchen, smart cooling, smart door, and smart elderly support [7, 8]. The smart living room includes the provision of playing the music of guest's choice on their arrival can be implemented. It can be implemented in a way that lights can be dimmed off or completely off based on weather and/or occupancy of the room. Smart washroom may have the provision of water temperature to be maintained based on weather and person's own likeness. It can extend its applicability to a warming of water in the tank according to the current season. It can also be designed in such a way that, in the event of any water overflow or leakage, required communication and suitable action can be accomplished. One of the biggest needs in today's busy life is a smart kitchen. This category is relevant when there is a busy life for all individuals staying in a home. In this situation, it can store raw food in a vessel or a suitable cooker which can then be remotely controlled. They can cook such that food. This type also includes the situation that there might be some unexpected occurrence, such as overheating of any food, or leaking of boiling milk or tea, and preventing the mishaps. By installing the sensors and warning equipment, gas leakage can also be detected and taken care of. Smart cooling applies, according to the consumer, to the temperature control of multiple areas of the building. The bed, kitchen or even washroom temperature may be controlled based on a person's presence or absence, or even based on the preference of a specific person. On the entry of an authenticated user, the smart door gets open and is closed accordingly. It can work in some other personalised way, as if the time is after midnight, the door can also relay a specified person's message on the smartphone. If all people living in a house are on a vacation, another clause might be that it may be customised to warn them also of an authenticated person in their absence. Smart help for the aged requires extra treatment for disabled persons. Taking care of their loved ones is the most important ritual of everybody's life. Elderly people require extra treatment and children in the home. If the house is a smart home, they will even get tracked and get help. The humans living on this planet are ageing

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

endlessly. Today, in many parts of the world, the older generation (aged 65 and over) makes up 7 percent or more of the total population. In fact, 1 billion people would be over the age of 65 by the middle of this century, and they may be counted as non-workers. From 125 million to 434 million worldwide [5], the population aged 80 and over is estimated to more than triple between 2015 and 2050. To thrive and live an enriched, healthy and stable life, this community would take special treatment. The quality of life will also be substantially increased by the effective application of the IoT. Here, you can use smart wristbands and headbands. These bands have receptors that can detect the chemical present in their sweat and are measured and then analysed by these chemicals. The resultant is passed on to another A wireless computer (may be a cell phone) may also assist in measuring and monitoring the welfare of the individual.

2.2 Outdoor applications

Smart cities, smart infrastructure, smart flow, smart parking, It can include smart marketing and smart healthcare in outdoor applications [7]. The intelligent streetlight system that can go on or off depending on the weather and the amount of natural light which involves applications focused on the smart city. It will manage the amounts of waste in garbage bins stored in the town and also plan the disposal of refuse. Monitoring the sound level created by groups or announcements close schools and hospitals and in a residential area [9] is another concern discussed in such a deployment area. Transportation forms one of the major components of the busy running community in today's life, and Smart Transportation is thus strongly emphasized [9]. Heavy-loaded, medium-loaded and under-loaded transport vehicles can be categorised in preparing routes and time slots. Introducing the IoT system can schedule and manage this. One should devise Smart Traffic in relation to smart transportation. This subcategory focuses primarily on the provision of overall traffic control surveillance in a region. It requires tracking the route of traffic within a city, both cars and pedestrians. It can also include detection and movement for the shortest route between two points in this document. Smart parking that integrates two simple provisions is another challenge. The first concerns a device that can track the allocation of urban or surrounding parking spaces. The other is to steer cars inside a certain parking area into the open space. Smart marketing comprises the development and use in the city of different goods. It includes the promotion, on a guideline basis, of goods. It also tracks the seasonal demand for a commodity, i.e. whether it is winter or summer; days, i.e. weekdays or weekends, or can also depend on the holiday seasons. One of the most relevant social technologies is Smart Healthcare [10]. It should deal with the availability of ambulances from a local hospital with in the shortest period, and it must ensure that the ambulance takes the shortest path. This involves the drug-reminder phase, i.e. the reminder of drug routines for the elderly or prescribed treatment for children or individuals with long-term illnesses [9].

2.3 Environmental applications

Smart habitats, smart forestry, smart biodiversity and smart water can be used in environmental applications. The Smart Environment tackles the problems of air and water quality enhancement. It also deals with noise pollution, especially in residential areas, near hospitals and schools. It requires the provision of environmental services that can cause environmental surveillance. Note litter that is non-biodegradable. It can also assist the authorities in limiting public use of polythene and other non-biodegradable products. In areas artificially prepared by humans for husbandry, smart farming deals with both livestock farming and Agro-business. The sensing, interpretation and tracking of a separate set of animal-related circumstances can prove very useful. This includes climatic conditions, temperature, toxic gas amounts, the ratio of the number of animals to the amount of food, the number of caretakers and even the surrounding fences. Further helpful and counter-action actions may be taken based on the analysis [11]. The gathering and study of information from natural environments and wildlife populations should be the responsibility of intelligent wildlife. This awareness will lead to the steps to enhance the environment. It may also feel the basic case of emergency in the wildlife area, either connected to an animal or a human being. It is possible to produce relevant signals; it is possible to test and take more effective life-saving measures. The aquarium, resorts and amusement parks where animals are housed for fun and exhibition can also apply to this. It is possible to record incidents of injuries or incidents, either deliberate or accidental, on time, and thus beneficial for society. The smart water subcategory mainly deals with water safety. It may verify harmful chemicals in water sources, viruses, or some kind of fungus. After careful examination and decisions, necessary medicated chemicals, insecticides and intoxicants may be inserted into the water body. It can protect both marine species and water plants. It also applies its use during the summers, and the rainy season to water levelling.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

2.4 Technological applications

Intelligent Shopping and Smart Security [12] can involve technical applications. Intelligent shopping includes multiple situations, such as proposing enticing offers based on their likings and preferred brands to individual consumers. That can be achieved by maintaining a customer's list of the most typical days or dates for shopping. By analysing this information and shopping habits, it can monitor the client on its smartphone. The device will request ads of the user's likings on the user's Google or Facebook profile on a suggestion basis. Another solution is to show the availability and recall the need for items after tracking and testing the preference, style and time gap of his shopping. Via smart protection, Security in various ways. [13]. In a highly sensitive situation, such as a nuclear power plant or military agencies, it could be the protection of information, items, and facilities. In a classified situation such as medical history, it also increases its execution, Institutions for law enforcement and the financial industry. It is also possible to provide protection in the normal market field, in modern manufacturing settings, or even in the education sector.

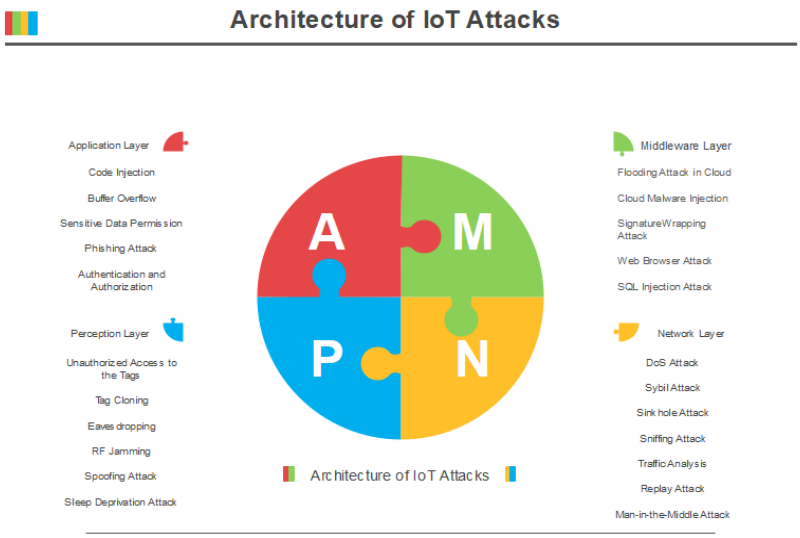
2.5 Emergency and critical situations applications

Emergency and critical situations applications may include natural calamities, water levels, radiation levels, enemy intrusions and precarious industries [14]. The first sub-category concerns the potential prediction of changes in conditions that could lead to some natural catastrophe, and proceeds accordingly. The installation of an IoT system, containing sensors and transmitters into a water source, entails water levelling. The sensors detect the information and relay the information to a processing system where it can be processed. After analysing the outcomes, it will provide more guidelines for organisations dealing with water level issues. Similarly, radiation levels can be monitored in radiation generating vicinities. These vicinities may range from the least critical microwave oven to the most critical nuclear power plant, where a threat can be triggered by minute changes in radiation levels. Intrusions from opponents are another key concern in different areas of the globe. By installing sensors and cameras on the boundaries, appropriate precautions for unintended intrusions may be stopped or taken. Under emergency and urgent condition applications, fragile businesses form the implementation field. This area includes businesses where it is important to take special measures to be safe and protected. Industrial areas such as flares, coal mines, reservoirs, and lakes are also life-threatening points, to mitigate public-level risks or individual-level mishaps, effective and comprehensive IoT deployment should be used in these areas.].

3 Architecture of IoT Attacks

Now it has switched to security and IoT attack analysis. Privacy problems depend on the architecture of the four layers.It explores the major weakness in this chapter. Sources and the way of prevention as shown in Fig. 2.

Fig. 2. Architecture of IoT Attacks



ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

3.1 Application Layer

In the application layer, the attacks primarily target (unauthorised) accessing the user's personal info. Usually Attackers Take advantage of software and device bugs (e.g. Injection of text, overflow of buffer), or unauthorised access to attack. One technique for possessing an illegal agent by counterfeiting, the same permission as legal users, is granted Identification. Apart from these threats, Viruses, worms, and Trojans also challenge the sheet. Other malicious programmes (Rootkit, spyware, Adware, etc.) also undermines user's privacy.

3.1.1 Code Injection

This attack requires injecting malicious code into the device. System by exploiting errors in the programme [15]. Injection coding it may intercept data for several reasons, e.g., Get hold of the environment and spread worms [16]. THE Shell injection and HTML scripting are typical attacks. Yeah. Injection. This form of attack will cause the failure of the machine Control and violate the security of the customer to the attacker, or even a full shutdown of the machine.

3.1.2 Buffer Overflow

This assault requires a breach of the code or code boundaries. Buffer of data by manipulating bugs in the software. Most individuals' Programs function with a pre-defined architecture of memory for containing segments of code and records. The intruder writes a long data sequence to a specified area, resulting in a long data sequence Series overflow past its pre-defined area of Dwelling. The consequence may be the alteration of other knowledge (For example, when the sequence invades the data region of another data buffer), malicious code execution (e.g., by invading a code segment), and killing the flow of programme control. Popular methods include common approaches, Overflow of stack heap-based buffers, format string attack, Error in integer, and double free [17]. Overflows in buffers One of the most prevalent attacks on software Applications and. WellinTech KingView, for example, 6.53 HistorySvr, a programme for industrial automation, was threatened by a weakness to heap buffer overflow [18]. In addition, there have been demonstrations explaining how this method of attack can cause an unauthorised agent to execute arbitrary code and get user rights [19].

3.1.3 Sensitive Data Permission/Manipulation

This form of assault refers to unauthorised entry and tampering with the Sensitive info, breaching the privacy of consumers]. This attack exploits implementation vulnerabilities in authorization the model. It has held attackers demonstrations Exploiting gaps in the authorization model to monitor apps in smart homes, creating issues Break-in and robbery, for example. Prior job studied the incidents used to interface between Smart device and Smart app. Notice that there are Smart apps and Smart devices face an especially irritating issue for Protection for records. A Smart device transfers confidential details to Events are used by Smart app; Smart app uses events to track Intelligent Device. Regardless of the lack of enough Protection of the event can cause the event to leak and even cause the user to suffer more serious harm. Due to the lack of adequate user interface security, the Users' privacy could be breached. In order to work out the structure for protecting the above issues has been proposed to protect Sensitive data by announcing trends of expected data flow.

3.1.4 Phishing Attack

An attacker pretends to be a true attacker in this kind of hack User or legal agency for the collection of classified knowledge about users, such as passwords and details of credit cards. For this attack, the popular medium is email, where Critical data are accessed by an intruder as users opens the mail.

3.1.5 Authentication and Authorization

The system of authentication plays an important role in IoT security and privacy protection. The current authentication methods will not establish fine-grained assurance. For instance, when updated, applications can download malicious payloads, and attackers may use it to manipulate a computer remotely. Meanwhile, the permission model still has bugs. Over-privilege, which allows the system to access information using nothing needed, is a common issue. In addition, it is also a root of the permission issue to use the default setup. I grant if unauthorised permission to a file and directory, an attacker can exploit this vulnerability to build attacks to varying degrees. The smart card has flaws in remote authentication in a particular application scenario considered in prior work, a great smart-home security mechanism, it may carry unauthorized operations out by an intruder, such as the door opener. Which can cause leakage and tampering with user details? In comparison, in the

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

smart house, owing to the lack of a perfect security system, unauthorized operations, such as opening a lock, may be carried out by an intruder.

3.2 Middleware Layer

Interfaces and utilities for the application layer are supported by the middleware layer. In order to affect the application layer, attackers can attack the service (e.g. the Web service). The attack on the server and database will influence the security of information Security and service of the device. Cloud attacks are largely targeted at virtualization and data, posing a massive threat to users' privacy. The goal of the attack on the middleware layer is to destroy the users' quality of service and privacy.

3.2.1 Flooding Attack in Cloud

This is one form of cloud denial-of - service attack. Here, attackers are continuously sending requests to a cloud provider that depletes cloud capacity, affecting service efficiency. The side effects of such attacks can be dramatically magnified in sophisticated cloud systems. When the cloud infrastructure finds that the existing instance of the database cannot satisfy the specifications, it will migrate the affected database to other servers. This will lead to additional demand on other staff to work for servers.

3.2.2 Cloud Malware Injection

Through inserting malicious server instances or virtual machines into the cloud, the attacker may change the details, gain access, and execute malicious code. It implies that, for instance, assailants copy and upload the victim's service instance, but the malicious instance responds to the request when some service requests the instance of the victim. As a result, the intruder can get the service's confidential data.

3.2.3 Signature Wrapping Attack

The cloud system uses an XML signature to guarantee the service's integrity. Eavesdropped messages are changed by the attacker without invalidating the signature [20]. It is well known that Amazon Elastic cloud computing provides high-quality cloud services. Furthermore, EC2 provides SOAP interfaces for controlling the machines deployed. To change eavesdropped messages, attackers exploit vulnerabilities in SOAP. An attacker will execute arbitrary commands and operations as legitimate users.

3.2.4 Web Browser Attack

In the cloud, the Web browser is used to execute commands such as authentication and permission commands on remote servers [20]. But no encrypted the browser can generate XML tokens itself. To get entry without authentication, attackers exploit this vulnerability. A cloud service based on a web service can generate some metadata containing an extensive amount of content related to implementing cloud services and services. Once such metadata is obtained by the attackers, they may pose a threat to the cloud [20].

3.2.5 SQL Injection Attack

By embedding SQL statements into the input data, a poorly designed programme may be vulnerable to such attacks. For reading, writing, and removing processes, attackers use these SQL statements. This kind of attack cannot just accessing the private data of the user but still endangering the whole storage structure. As SQL injection attacks Web applications, the current page displays distinct effects compared to the facts.

3.3 Network Layer

IoT has many types of networks, including the Internet and WSN. Various networks use various protocols and equipment, so it often varies the attacks on the network. The DoS attack, which is the most widespread attack, it can drain network capacity and affect network service availability. Through eavesdropping and analysing the traffic through the network, it can collect communication patterns. An obvious attack a malicious agent can execute is the so-called attack after receiving the contact pattern. Assault Replay. In addition, there are specific network node attacks. The attackers can get the transmitted information and take control of the network, such as Sybil attack, replay attack, and man-in-the-middle attack, by breaching the network node. The network layer intrusion can also be used to intrusion using the vulnerabilities of network protocols and network nodes to destroy network communication.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

3.3.1 DoS Attack

A denial-of - service attacks (DoS attack) is carried out on the network by flooding the victim with requests, generating an extensive amount of network traffic [15, 16]. This attack can exhaust all available resources, making network resources unavailable to users. In comparison, a lot of unencrypted user data could even be leaked [15]. In addition, as an attack platform, a distributed denial-of - service attack (DDoS attack) can combine several computers and start DDoS attacks on one or more targets.

3.3.2 Sybil Attack

A node in the scheme provides the victim node with multiple identities, allowing the victim node to perform an operation multiple times, defeating redundancy [15]. Ever after the Wireless Sensor Network (WSN) The attacker has several identities, the victim node may transfer information to a longer routing distance via the compromised node.

3.3.3 Sinkhole Attack

Using an included node by attackers attracts data flow from nearby nodes [15]. It tricks the machine in [15] and believes the data to have already reached its destination. The attacker can use malicious nodes in a WSN to attract network traffic and then arbitrarily operate the sensor data.

3.3.4 Sniffing Attack

In order to access network information, attackers use sniffer devices and applications and then collect useful data for further attacks [15].

3.3.5 Traffic Analysis

Attackers deduce communication patterns and loads by analysing the number and size of data packets transmitted. The greater the number of packets that can be analysed, the greater the availability of useful information. You can apply this attack to encrypted packets; you can also analyse their pattern of communication. Via traffic analysis from WSN, it can get three types of data.. Next, an intruder in the network can identify the operation. Second, an intruder can access the spatial location of wireless access points (APs. Finally, an attacker may learn the specifics of the protocol used in the transmission process.

3.3.6 Replay Attack

Attackers collect data by eavesdropping between the two parties. The messages received are exchanged repeatedly between communication pairs, thus wasting the tools of communication [17]. RFID in This assault also occurs in the correspondence between the reader and RFID tag technologies. Not only does this form of attack consume computational resources between reader and tag, but it also consumes back-end database resources]. Besides the above effects, it is possible for attackers to get readers Grant access via radio signal broadcasting [17].

3.3.7 Man-in-the-Middle Attack

A real-time attack, occurring between two interacting victim nodes, is this attack. A node is disguised by the attacker as a valid node that interacts with two nodes of the victim [15]. The attacker wins the confidence of two nodes and gets data regarding two nodes of the victim.

3.4 Perception Layer

It uses a significant range of sensor and recognition technologies in the perception layer. To dynamically change the network topology, sensor nodes typically use ad hoc network technologies. For the diversity of the deployment environment, sensor nodes also use wireless communication. In this one, In this case, attackers can eavesdrop on contact between nodes. In addition, through physical attacks, the attacker can access the relevant attributes of the computer directly, and then start further attacks, such as tag cloning and spoofing attacks. In the perception layer, RFID technology is commonly used, and attackers will destroy contact between the reader and the RFID tag, such as by RF jamming. The perception layer's ecosystem is comparatively constrained by capital and electricity, the environment of perception layer is relatively restricted by resource and power, so the node uses sleep to prolong. In order to speed up the battery consumption, such as a sleep deprivation attack, attackers can keep the node in working condition. The assault on the awareness layer typically attempts to destroy the processing of data and communication.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

3.4.1 Unauthorized Access to the Tags

RFID systems lack efficient authentication techniques, meaning that unauthorised attackers can quickly enter tags [15]. Attackers can abuse data. Once an intruder can reach the network on wireless sensor networks, he can start attack or free use of the network.

3.4.2 Tag Cloning

Successful attack requires RFID tags being cloned. To do this, by reverse engineering or directly from its implementation environment [15], the attacker may access the information. Previous work [15], for instance, revealed compromises where RFID readers could not say the difference between the initial tag and the compromised tag.

3.4.3 Eavesdropping

Attackers can easily hear the system and the node of the perception layer, especially in wireless communications [15, 17]. An intruder may use an antenna inside an RFID device to record communications between legal tags and readers. Unauthorised entities may use the antenna to record data exchanged between the reader and the tag [17].

3.4.4 RF Jamming

In order to interfere with communication between the legitimate tag and the readers [15, 17], the attack device sends RF signals. To interact with all the signals within its radius, an intruder may use the RFID tag, avoiding Communicating with all tags with the reader [17]. This form of attack may destroy the mechanism of data collection at the awareness layer.

3.4.5 Spoofing Attack

The intruder disguises a tag here as a legitimate tag that gains the same authorization and operation as the legitimate tag [17]. As a result, they can trick the reader to gain the same authorization as the legitimate stamp. In previous work [17], it was seen that the attacker requires access to the contact channel that is the same as the original tag to gain the same authorization as the legitimate tag, and must have an in-depth knowledge of the protocols and authentication. Notice that in the transmission process, spoofing attacks can lead to packet loss. In addition, this method of attack will force nodes to resend the data, potentially dramatically raising network traffic. It also speeds up node power consumption, thus reducing the lifespan of the node.

3.4.6 Sleep Deprivation Attack

The perception layer's unit and node are constrained by the battery's capacity. It is important for the system to sleep while not operating in order to extend its lifespan. By continuously sending control information to the system and holding the node in a functioning state, this method of attack tries to subvert this process [15].

4 Threats solutions

A threat is an operation in a system that takes advantage of safety vulnerabilities and it has a negative effect [21]. Threats may come from two major threats: Sources: nature and humans [22, 23]. Threats of natural origin, such as earthquakes, Hurricanes, earthquakes, and fires, may cause computer systems to suffer significant harm. Few protections against natural hazards can be enforced, and no one can it will discourage them from occurring. The best solutions for safe systems against natural threats are disaster recovery plans such as backup and contingency plans. Human threats are those that are created by people trying to damage and interrupt a device, such as malicious threats comprising internal[24] (someone has allowed access) or external threats[25] (individuals or organizations operating outside the network). It divides human risks into the following categories:

• Unstructured threats that comprise mainly novice people who are using hacker tools that are readily available.

• Structured threats as individuals identify and should understand device flaws, Codes and scripts create and manipulate them. An example of a formal framework Advanced Persistent Threats (APT) [26].

Are a threat. APT is a sophisticated commodity, Network attack targeting high-value market and government data Organizations such as manufacturing, economic divisions and National security, data theft [27]. An increasing number of pervasive gadgets have expanded the number of security risks with consequences for the general population, as IoT becomes

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

a reality. Sadly, the IoT has a new range of security risks. There is a rising understanding that ransom it could exploit where and vulnerable to attack by the latest generation of mobile phones, computers and other electronics.

5 Challenges

In order to satisfy the trillions of IoT devices, the section addresses the remaining challenges to be solved. The aim of the section is to provide the research instructions in the domain for the new researcher.

Interoperability: IoT has three key categories of challenges related to interoperability, namely technical, semantic and pragmatic. In the same computing model, the technical challenges concern device capabilities, protocols, and related standards to coexist and communicate, while semantic concerns the capabilities of different IoT components responsible for processing and analysis the data exchanged. Pragmatic, however, is concerned with the capacities of the elements of the structure to observe the intentions of the parties. It is possible to achieve technological interoperability by providing agent-based mediation between IoT equipment and standards. Semantic interoperability is a prerequisite for machine-computable logic, the exploration of knowledge, and the federation of information systems with data. Pragmatic Interoperability can be accomplished by creatively designing.

Scalability: The IoT is expected to face many challenges relating to the possibly endless number of interacting entities and major variations in terms of interaction patterns and actions. In order to support trillions of smart devices, current IoT architectures need to be scaled up. It can distil the IoT systems' scalability control into two sections. First, the rapid growth of IoT devices has been noted. Present management, however, because of their limited capacities, protocols do not scale well to meet IoT interface requirements. Second, social interactions between where some IoT system entities are human portable devices, the owners of the devices need to be considered. Scalability control In order to allow ad hoc based computing services by providing some rewards, protocols are supposed to track social relationships between devices.

Flexibility: Because there are several IoT applications, the provision of services to the various IoT applications has become very difficult according to their requirements. IoT users typically need on-the-move services that are dynamically optimised, personalised, value-added, and autonomous. In addition, the flexible, context-aware, and reconfigurable multiple service network architecture can support customised, autonomous, and dynamic networks by building and using them. For the construction of future network infrastructure architectures, it requires models of service declarative specifications.

Energy Efficiency: The cornerstone of the IoT is small devices. These devices, however, have restricted processing capacities, memory, and battery capacity. Since these devices are very lightweight, compute-intensive software and routing processes will not run on IoT devices. Consider ship Knowledge of energy in routing protocols is still lacking. Although some protocols support communication with low power, these protocols are in an early stage of growth. Energy harvesting techniques could promise solutions to meet IoT energy requirements.

Mobility Management: In terms of IoT network and protocol performance, node mobility can generate diverse challenges. Because of severe energy and processing constraints, the existing mobility protocols of vehicular ad hoc networks (VANETs), mobile ad hoc networks (MANETs), and sensor networks do not cope well with traditional IoT devices. Management of mobility is a critical role, and it has two phases. First, it requires motion detection in order to be aware of the movement of the system, which requires Linking to a network's new zone. Second, it is important to integrate the signalling and control signals in such a way that it can help to know the positions of nodes in a network. Repeated scans can accomplish detection of movement, and by passive messages from participating protocols. Or a beacon from a protocol on mobility. One of the fundamental problems in the IoT model is mobility management the architecture of the IoT must also take that into account.

Security: The variety of IoT applications and the heterogeneity of IoT communication infrastructures contribute to a range of security problems that are equally complex. In IoT bottom-up mode, it can provide protections. A secure booting procedure should be followed by the machine in a bottom-up manner, accessing control laws, system authentication procedures, and firewalling, and must be able to accept security software updates and patches in a non-disruptive manner. Way. Since IoT protection is a key concern, effective security measures (physically and non-physically) must be implemented at both the system and network levels. To identify and counteract threats, IoT devices must have intelligence. Fortunately, a revolutionary would not need this, Instead, in the IoT paradigm, the evolution of interventions that have proved effective in other networks must be adapted by considering the IoT paradigm. Smart devices' computing capabilities.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

6 Conclusion

IoT faces several attacks and threats that must be recognized for protective action to be taken. In this paper, applications, security attacks and security threats it introduced to IoT. The overall goal was to identify threats, attacks and vulnerabilities faced by the IoT. In the light of quality standards and indicators, it performs a critical assessment study based on previous issues, besides recent unexpected variables such as epidemics (COVID-19 pandemic), and because of these variables, the importance of security and protection for the Internet of Things will increase. Therefore, the importance of quality standards and indicators for the security of the Internet of things considering modern variables, the process of diagnosis, treatment and prevention is carried out.

References

[1] X. Xiaohui, "Study on security problems and key technologies of the internet of things," in Proceedings of IEEE Fifth International Conference Computational and Information Sciences (ICCIS), Hubei, China, June 2013.

[2] A. Kanuparthi, K. Ramesh, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, pp. 61–64, Berlin, Germany, November 2013.

[3]. Vongsingthong, S.; and Smanchat, S. (2014). Internet of Things: A review of applications and technologies. Suranaree Journal of Science and Technology, 21(4), 359-374.

[4]. INFSO D.4 Networked Enterprise, RFID INFSO G.2 Micro and Nanosystems; and Working Group RFID ETP EPoSS. (2008). Internet of Things in 2020: Roadmap for the future. Version 1.1. Brussels, Belgium: European Commission.

[5]. Perera, C.; Liu, C.H.; and Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. IEEE Transactions on Emerging Topics in Computing, 3(4), 585-598.

[6]. Matta, P.; Pant, B.; and Arora, M. (2017). All you want to know about internet of things (IoT). Proceedings of 4th IEEE International Conference on Computing, Communication and Automation (ICCCA).Greater Noida, India, 1306-1311.

[7]. Kraijak, S.; and Tuwanut, P. (2015). A survey on Internet Of Things Architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. Proceedings of 11th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM). Shanghai, China, 26-31.

[8]. Perumal, T.; Sulaiman, M.N.; Mustapha, N.; Shahi, A.; and Thinaharan, R. (2014). Proactive architecture for Internet of Things (IoTs) management in smart homes. Proceedings of the IEEE 3rd Global Conference on Consumer Electronics (GCCE). Tokyo, Japan, 16-17.

[9]. Jalali, R.; El-khatib, K.; and McGregor, C. (2015). Smart city architecture for community level services through the Internet of Things. Proceedings of 18th International Conference on Intelligence in Next Generation Networks. Paris, France, 108-113.

[10]. Hassanalieragh, M.; Page, A.; Soyata, T.; Sharma, G.; Aktas, M.; Mateos, G.; Kantarci, B.; and Andreescu, S. (2015). Health monitoring and management Using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. Proceedings of IEEE International Conference on Services Computing. New York, United States of America, 285-292.

[11]. Lin, Z.; Hu, H.; Zhang, Y.; Qiao, J.; and Xue, J. (2011). The application of the internet of things in agriculture. Applied Mechanics and Materials, 687-691, 2395-2398.

[12]. Bing, K.; Fu, L.; Zhuo, Y.; and Yanlei, L. (2011). Design of an internet of things-based smart home system. Proceedings of 2nd International Conference on Intelligent Control and Information Processing. Harbin, China, 921-924.

[13]. Matta, P.; and Pant, B. (2018). TCpC: A graphical password scheme ensuring authentication for IoT resources. International Journal of Information Technology, 1-11.

[14]. Balampanis, S.; Sotiriadis, S.; and Petrakis, E.G.M. (2016). Internet of Things architecture for enhanced living environments. IEEE Cloud Computing, 3(6), 28-34.

[15]. Farooq MU, Waseem M, Khairi A, Mazhar S (2015) A critical

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

Analysis on the security concerns of Internet of Things (IoT). Int J

Comput Appl 111:7.

[16]. Zhang W, Qu B (2013) Security architecture of the Internet of Things oriented to perceptual layer. Int J Comput, Consum Control (IJ3C) 2(2):37–45.

[17]. Mitrokotsa A, Rieback MR, Tanenbaum AS (2010) Classification

Of RFID attacks. Gen 15693:14443

[18]. Zhu B, Joseph A, Sastry S (2011) a taxonomy of cyber-attacks on SCADA systems. In: Internet of Things (Ithings/CPSCom), 2011 international conference on and 4th international conference on Cyber, Physical and Social Computing. IEEE, pp 380–388.

[19]. Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q (2009) AVOIDIT: a cyber attack taxonomy.

[20]. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. In: 2009 IEEE International Conference on Cloud Computing. CLOUD'09. IEEE, pp 109–116.

[21] H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in Coping with Global Environmental Change, Disasters and Security. Springer, 2011, pp. 61–106.

[22] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in Proceedings of the

2011 International conference on intelligent semantic Web-services and

Applications. ACM, 2011, p. 12.

[23] R. K. Rainer and C. G. Cegielski, Introduction to information systems: Enabling and transforming business. JohnWiley & Sons, 2010.

[24] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 857–862.

[25] P. Baybutt, "Assessing risks from threats to process plants: Threat and vulnerability analysis," Process Safety Progress, vol. 21, no. 4, pp. 269–275, 2002.

[26] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network security, vol. 2011, no. 8, pp. 16–19, 2011.

[27] F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat:Acase study of malware for political espionage," in Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. IEEE, 2011, pp. 102–109.