Internet of Things Privacy, Security and Attacks

V. Harsha Shastri, PhD
Associate Professor in Computer Science, Department of Computer Applications, Aurora Deemed to be University, Uppal, Hyderabad 500098, Telangana, India

K. Srinivas Rao
Assistant Professor in Computer Science, Department of Computer Applications, Aurora Deemed to be University, Uppal, Hyderabad 500098, Telangana, India

Raman R.K.
Assistant Professor in Computer Science, Department of Computer Applications, Aurora Deemed to be University, Uppal, Hyderabad 500098, Telangana, India

ABSTRACT

Data protection and anonymity is a major issue with the Internet of Things. Problems may arise as a result of ineffective security measures, human ignorance, or outdated device software. Smart devices are vulnerable to hacking. A billion connected devices could be used to access private data, spread malware and cause harm. Businesses, consumers, and even Government agencies use Internet of Things devices and concern is always there in terms of security for manufacturers and end users. The Internet of Things helps to improve business efficiency and simplifies employees' work. The transportation, agricultural, healthcare, and building sectors are among the many that are making more use of this technology. It is challenging to safeguard most Internet-connected "things" with traditional, resource-intensive defenses since these devices are often poor and have limited hardware capabilities; this raises serious privacy and security challenges.

Keywords

Internet of Things (IoT), privacy, security, attacks, networks

1. INTRODUCTION

The introduction of networks in 1972 allowed for the connection of computers using various topologies. To process the control system, we may employ a pair of wires that link the actuators and sensors. Connectivity protocols like Zigbee, Bluetooth, or Ethernet should allow a network of sensors to safely exchange data with one another. Improvements in both information technology and operational technology fueled the expansion of the Internet of Things (IoT). Progress in OT aimed at making field equipment "smarter" has led directly to Fieldbus technology [1]. But the real problem is figuring out how to have these variations communicate with one another; this calls for IP-based communication.

To characterize a system of networked computer devices that allow individuals to interact and work together online, Kelvin Ashton first used the term "The Internet of Things (IoT)" in 1999. According to research, there will be 50 billion connected devices by the year 2020, and that figure will rise to 14.7 billion by 2023.

A network of physical objects that can communicate with one another and share data wirelessly via an internet connection is called the Internet of Things (IoT). In order to guarantee optimal performance, the devices generate and collect data while also communicating with one another. The data collected from IoT devices could contain extremely private and sensitive information. Security and privacy are becoming increasingly important issues as the number of devices continues to grow.

The number of devices in use is projected to reach 64 billion by 2025. This growth is beneficial as it could help carry out our day-to-day activities. For example, smart lightning could help reduce electricity bills and energy consumption. While there are many advantages, there are also hazards associated with scaling up devices, such as potential security vulnerabilities and an increase in access points for hackers and cybercriminals. Unfortunately, the interconnectedness of networks in the IoT has led to the availability of untrustworthy and anonymous online sources. Businesses must improve IoT security if they want their consumers to have trust in the network.

Cybersecurity threats and the vulnerability of IoT systems' sensitive data have been exacerbated due to infrequent password changes and outdated devices. An increase in the likelihood of data breaches and other security concerns is caused by such poor security methods. Because of its lack of robust security measures, the Internet of Things is seen by most security experts as an open invitation to cybercriminals.

An Internet of Things platform integrates and analyses data from many devices by linking them to various items and gadgets that have built-in sensors. A basic example would be the sensors seen in shops. Trends, recommendations, and early problem detection might all be possible with this data.

While online, apps that rely on the Internet of Things (IoT) are susceptible to a wide range of traditional threats. These include worms, malware, spyware, Trojan horses, harmful code injections, and backdoor assaults. Authentication, authorization, and accountability are three of the most important services provided by traditional threats. The process of confirming that a person is associated with a thing is known as authentication and authorization. The three-factor authentication and authorization method is the gold standard for determining if an individual has the permissions to access a resource. An other definition of malware is a computer virus. Trojan horses, spyware, ransomware, worms, and viruses are all examples of malware. A combination of high-frequency electromagnetic waves and a more complex kind of malware poses a significant threat to IoT devices.

Here is the breakdown of the remaining sections of the paper: Issues with security and privacy are discussed after a brief literature review in the next section.

2. LITERATURE REVIEW

The security of the Internet of Things has been the subject of several studies and publications. Concerning low-end systems, Yang et al.'s study [2] details personal and safety concerns and their corresponding remedies. Internet of Things (IoT) device restrictions, such as extended battery life, lightweight computing, security attack categorization, and control access methods and architecture are the four stages that Weber, Gopi, and Rao's surveys cover when discussing security-related difficulties and concerns [3, 4]. Concerning the privacy of the Internet of Things (IoT), Aleisa and Renaud outline the problems, difficulties, principles, dangers, and solutions that surround this topic [5]. Tewari and Gupta presented yet another study on the topic of security concerns related to the Internet of Things (IoT). By dissecting the multi-layered design of IoT devices, new security holes are revealed. Problems with heterogeneous integration across layers were addressed, and resources for IoT research were made available [6]. Security protocols for the Internet of Things (IoT), such as authentication, encryption, trust management, and emerging technologies for IoT device security, were studied by Noor and Hassan in 2019 [7].

Concerning problems with the industrial Internet of Things, Sengupta et al. undertake new research. An approach based on blockchain technology may be described by categorizing security and privacy risks according to their destructibility [8]. In addition, Weber and Wang et al.[9,10] have investigated blockchain technology and its functions, including smart contracts, decentralization, asymmetric encryption, and access management. At length, Khan and Salah went over the protocols for communication, management, and tiered architecture on the network [11]. Concerning the Internet of Things (IoT), Qian et al. [12] investigated security and privacy issues related to multi-layer architecture. Internet of Things (IoT) terminal devices may be protected without the involvement of a third party according to the suggested security practices [13].

3. CHALLENGES OF PRIVACY AND SECURITY IN IOT

Threats to cyberspace privacy and security are major worries for many public and private sector organizations. The cyber security incidents have shown that the Internet of Things is susceptible to assaults. Reason being, new security measures are needed due to the fact that the Internet of Things is interconnected and therefore opens the door to the anonymous and untrustworthy Internet [14]. The users are not acknowledged of the security impacts until the breaches took place causing loss of data.

3.1 Security

There are fresh challenges that have arisen as a result of the Internet of Things (IoT) deployment that must be solved. One of the major entry points for cyberattacks and the disclosure of user data due to inadequately protected data streams occurs with poorly secured Internet of Things (IoT) devices and services. The security might be compromised if a device is not properly protected and connected.

When it comes to authentication, the Internet of Things is vulnerable, which makes it difficult to provide security in many contexts. This authentication method isn't very strong as it can only ward against certain types of attacks, such replay attacks or Denial of Service (DoS). Because of the abundance of information gathered by IoT gadgets, data security is a significant weak spot in the authentication process. Take contactless credit cards as an example. They allow for the reading of card numbers and names even without IoT authentication, which means that hackers may utilize the cardholder's monetary equilibrium information and character to buy things.

The man in the center assault is common in the Internet of Things (IoT), and it occurs when an outside entity attempts to impersonate network nodes to gain admittance to delicate data. Since the attacker doesn't need to know who the victim is, this attack successfully gets the bank server to accept the transaction as legitimate [15].

3.2 Privacy

In order to fully grasp the privacy challenges surrounding the Internet of Things (IoT), it is crucial to first identify the sources of these risks. In the Internet of Things (IoT) ecosystem, smart objects are pervasive and can distribute data and conduct sample procedures from anywhere. There is a direct correlation between the pervasive internet connection in IoT and the escalation of privacy problems. The internet of things (IoT) has the potential to make personal data accessible from anywhere in the globe, but only if there is a special way to conceal it.

4. SECURITY ISSUES IN IOT

Security risks may make it difficult, if not impossible, to implement arrangements that utilize the Internet of Things. The development of appropriate mitigation techniques, however, may benefit from a crystal-clear picture of the IoT security risks.

4. 1 Inadequate password protection

Hackers could have the option to get into the framework easily if they use the default passwords. Internet of Things (IoT) equipment including routers, video recorders, and video cameras were attacked with the Mirai virus, which is an example of this kind of assault. In order to get access, the Mirai malware used sixty-one generic, hard-coded identities and passwords.

The infection then dealt with north of 400,000 connected gadgets, prompting the very first 1Tbps appropriated refusal of administration attack.Twitter, Netflix, Airbnb, and GitHub are among the Amazon Web Services and its customers that are impacted by the Distributed Denial of Service (DDoS) assault. As of this year (2021), the most active botnet is Mozi, a Mirai-type virus.

4.2 Limited Compliance from IoT Manufacturers

The incapacity of IoT manufacturers to comply is another critical component impacting the security component of privacy and security in the IoT. After you sync your fitness tracker with your Bluetooth device, it will usually stay visible. Your Gmail credentials could be leaked via your fridge.

Any increase in worries about the security of the Internet of Things is likely to coincide with the continued development of devices by manufacturers that have inadequate security measures. Manufacturers of internet-connected gadgets have been including internet connection in their products without prioritizing the ‘security' component while they were creating them. The following are examples of manufacturer-caused security threats to the Internet of Things,

1. Hardware issues
2. Lack of security in data transfer and storage
3. Hard-coded, weak, or guessable usernames and passwords

4.3 Device Update Management

Difficulties with device update management might be a source of security problems related to privacy and security in the Internet of Things. There is a generalized danger to IoT security from insecure firmware or software. You could still run across new security holes even if a manufacturer ships an updated product.

The security of IoT devices relies heavily on updates, which should be applied as soon as new vulnerabilities are found. One way to increase the risks to the security of IoT devices is to use them without updating them as needed. More so, since devices will upload backups to the cloud, update management can be precarious. Access to sensitive information might be compromised by any hostile agent in the absence of suitable connection encryption and security for updated files.

4.4 Lack of Secure Interfaces

Internet of Things (IoT) security is crucial because of vulnerable interfaces. When it comes to data processing and transmission, every single IoT device is engaged. There are a number of Internet of Things vulnerabilities caused by unsecured interfaces, which are necessary for the gadgets to speak with applications, protocols, and services.

Internet, application programming interfaces (APIs), cloud, mobile, and application interfaces are all potential passage guides for programmers toward take delicate information or damage devices. Issues with device authentication and permission and insufficient or nonexistent encryption mechanisms are the most prevalent security concerns in IoT interfaces.

5. OS security in IoT

An operating system is a program that allows software to control hardware. At the very bottom of the software stack lies this system component. A number of things are handled by OS security, including the prevention of programming mistakes, secret storage, and the distinct allocation of execution and memory.

System type, processing power, and danger level are a few of the considerations that go into choosing an OS for Internet of Things (IoT) settings. Because of their low power and computing capabilities, IoT devices often come with a restricted selection of CPUs. That being said, OS security will be doing its best. One open-source real-time OS that is tailored for computers with limited resources is Zephyr OS [16]. It stands out because of the special care that went into its design, which prioritises safety. As a result, it allows for independent memory storage and thread execution. In addition, it specifies the client level of power and the boss level of authority. A major flaw, nevertheless, is that it does not have an adequate permission system [17].

Table 1 shows that operating systems account for eighty percent of the top ten items in terms of the largest number of reported different vulnerabilities over the last 20 years [18]. Given that operating systems provide attackers elevated access to almost every system component, these numbers should come as no surprise. The operating system may be compromised in several ways by attackers. Figure 1 displays a few of these ways. Malware such as rootkits may infiltrate the working framework and seize control of certain operations by using these approaches.

Table 1: The ten most vulnerable goods over the last two decades, ordered by total number of vulnerabilities

#	Product Name	Vendor Name	Product Type	# of vulnerabilities
1	Debian Linux	Debian	OS	3067
2	Android	Google	OS	2563
3	Linux Kernel	Linux	OS	2357
4	Mac OS X	Apple	OS	2212
5	Ubuntu Linux	Canonical	OS	2007
6	Firefox	Mozilla	Application	1873
7	Chrome	Google	Application	1858
8	IOS	Apple	OS	1655
9	Windows Server 2008	Microsoft	OS	1421
10	Windows 7	Microsoft	OS	1283

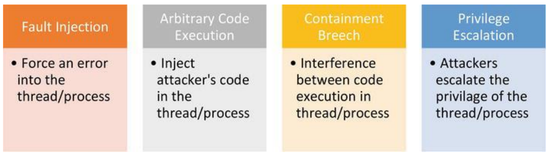
Fault Injection
• Force an error into the thread/process
Arbitrary Code Execution
• Inject attacker's code in the thread/process
Containment Breech
• Interference between code execution in thread/process
Privilege Escalation
• Attackers escalate the privilege of the thread/process

Figure 1: Attack vectors targeting IoT device operating systems

5. NETWORK SECURITY IN IOT

Wireless connections will power the majority of the IoT devices. While some of these technologies are part of Personal Area Networks (PANs), others are part of Wireless Local Area Networks (WLANs), or both. These technologies allow for the wireless connection of various products in today's market. Encryption techniques must be used to protect data while it is in transit. Since air is a common medium, anybody may obtain the data if this is not addressed. The safety of the individual wireless devices; if hackers get their hands on routers and access points, they might potentially change the settings of the network or send traffic to malicious addresses.

One cutting-edge industrial IoT technology that has the potential to connect IT and OT is Ethernet Time-Sensitive Networking (TSN) [19]. One of TSN's best features is that it provides for a high degree of interoperability without being tied to any one manufacturer. Also, it could plug and play with devices that weren't part of the TSN network since it was built on top of Ethernet. Additionally, tight-time synchronisation techniques allow non-critical and important traffic to coexist without increasing latency concerns. The ability to schedule traffic based on its priority is another crucial characteristic that empowers the concurrence of high-and low-need streams in a similar organization. Actually, TSN stores packets with varying priority using the concept of multiple queues. By sending two identical packets over two separate paths in the network, TSN creates redundancy at the packet level. One will be handled if it comes sooner, while the other will just be rejected. This is a fantastic method for guaranteeing the dependability of networks used in industrial settings. Lastly, keep in mind that any framework may make use of TCN as a link-layer protocol. OPC-UA exemplifies this kind of situation. In [20].

6. CLASSIFICATION OF SECURITY ATTACKS IN IOT

Internet of Things (IoT) security risks may be categorized into many forms, such as physical, network, software, online, side-channel, cryptanalysis, and access-level attacks.

6.1 Physical attack

In physical assaults to take place, the targets must be physically present with the equipment. The hardware components of Internet of Things devices are targeted by physical assaults [21, 22]. There are three types of assaults based on how they interact with the systems they target: intrusive, noninvasive, and semi-invasive [23, 24].

6.1.1 Invasive attacks- The term "invasive attack" describes situations when the hacker physically approaches the chips or disconnects the relevant equipment. Based on the target IoT device and the kind of attack to be launched, highly skilled individuals with specialized equipment are needed to conduct intrusive physical assaults. [23].

6.1.2 Noninvasive attacks- By using the input interface of the targeted devices, the attacker approaches them. The targeted IoT devices are damaged by these assaults, but no physical harm is done.

6.1.3 Semi-invasive attacks- While approaching the targeted IoT devices, the assailant avoids touching any of the interior wiring or components.

6.1.3.1 Jamming attacks - Their purpose is to obstruct wireless communication channels in IoT networks via the use of malevolent nodes that emit noise signals [25].

6.1.3.2 Sleep denial attack - They have an effect on the device's sleep mode, keeping it up to raise battery usage and impact Internet of Things devices. Unfortunately, these attacks may also send unauthenticated packets, which can lead to battery waste while decoding.

6.1.3.3 Fake node injection - These attacks are the most detrimental to IoT devices because they allow hackers to inject a malicious node into the network or create a misleading personality with the help of a fake hub. The result is that all the nodes in the network get inaccurate information [27]. By draining the resources of the whole IoT system, these attacks also cause subpar performance. At its worst, bogus node injection attacks may prompt the absolute obliteration of an IoT organization or even give the aggressor full control of the organization [28].

6.1.3.4 - Tag cloning - They get access to sensitive personal information by scanning the RFID tags of the targeted device with their own predetermined RFID tag. They pose a threat to the manufacturer's bottom line and public perception of the brand [29]. The goal of tag cloning attacks is to get access to sensitive information, including bank account details. [30].

6.1.3.5 Radiofrequency interference attacks - To prevent RFID from communicating with other Internet of Things devices, powerful radio frequency signals are used. Radio jamming assaults occur when an adversary uses radio frequency transmissions to create solid-state interfering signals. [26, 31].

6.1.4 Network Attacks - The following categories are used to categorize network attacks.

6.1.4.1 Wormhole attack - By taking control of the nodes in the network or introducing malicious code, attackers may create private channels that allow them to modify the transmission route of data in an IoT network. Once the attackers obtain the data, they can send just the packets they want to the destination. In order to disrupt network traffic and harm network topologies, wormhole attacks are undertaken [32-34].

6.1.4.2 Sybil attack - Intrusion of a malicious node masquerading as several normal users allows attackers to create numerous false identities. They are a lone user or hacker who uses a single platform to start several identities. Social media accounts that are not real on platforms like Instagram, Facebook, or Twitter are similarly vulnerable to Sybil assaults [35]. Attacks on routing algorithms are another possible use for them [36].

6.1.4.3 Selective forwarding - By launching a malicious node on the way between the source and objective hubs, the aggressor makes a dark opening that takes in every one of the information bundles going through the IoT organization. However, with selective forwarding, the node drops all but the specific data packets destined for their intended recipients. Any kind of data transmission may be filtered using a selective forwarding attack [37, 38].

6.1.4.4 Traffic analysis attack - As part of traffic analysis assaults, bad actors introduce a rogue node onto the network that alerts the regular traffic routines and gathers routing data. Internet of Things (IoT) networks are vulnerable to traffic analysis attacks, even when message packets are encrypted. Less data is retrieved as the distance from the root node increases [39].

6.1.4.5 Routing information attack - Information packets may be dropped, redirected, spoofed, or redirected as a result of routing malicious attempts. The predicted impact of these assaults is to change the flow of messages [27]. Similarly, this class includes the modifying attacks that aim to change the route data. Various subcategories of routing information attacks include network segmentation, routing loops, rushing, and replay routing information [37].

6.1.4.6 RFID spoofing - In RFID unauthorized access, individuals get access to user data by reading RFID tags without their knowledge or consent. Because RFID tags are legible to everyone, there are no strong safeguards in RFID systems to secure Internet of Things devices. [40].

6.1.4.7 RFID unauthorized access - Criminals steal data from RFID tags without the owners' knowledge or consent. RFID systems lack strong security measures to safeguard Internet of Things devices due to the fact that RFID tags may be read by anybody [40].

6.1.5 Software Attacks -.

Software attacks refer to harmful programmes or codes that are intentionally installed with the intent to injure, damage, or get unauthorized access to a person's equipment.

6.1.5.1 Operating system attacks - Operating systems rely on a multitude of services and open ports. Unfortunately, these same ports may be exploited by malicious actors who install harmful programmes, allowing them to modify system functionality and perhaps steal data or information.

6.1.5.2 Viruses: It's software that can replicate itself and spread to other machines via shared files sent over wireless or wired networks, USB drives, or other portable media. It is difficult to protect Internet of Things (IoT) devices from viruses as a result of their low memory and capacity limit and the absence of update systems. As a result, these devices are easily compromised. Internet of Things (IoT) devices have been targeted by viruses such as Mirai, SILEX, Stuxnet, and Bricker Bot [31]. Internet of Things devices become unbootable when infected with the CIH virus, which targets BIOS [41].

6.1.5.3 Trojan horse - Trojan horses are harmful programmes that impersonate legitimate ones in order to mislead users into downloading and installing them onto their devices. Upon triggered, it causes damage to user devices by data theft, file deletion, or the distribution of harmful software such as viruses or worms. Trojan attacks allow hackers to take control of IoT devices or steal sensitive information such as bank credentials, account numbers, screenshots, and passwords [42]. In order to get access to bank account credentials, hackers target Internet of Things devices using the Zeus Game over Trojan [43].

6.1.5.4 Phishing attacks - Typically, a fraudulent message that seems to have originated from reputable sources may infiltrate the harmful program. The goal of a phishing assault on an Internet of Things (IoT) device is to get sensitive information, such as the password or login, or to install a malicious program. [22, 44].

6.1.6 Web Attacks -.

There are a lot of issues with IoT web apps because of bad coding. The databases and servers of these IoT web apps include sensitive personal or financial information, and hackers exploit these vulnerabilities to get access to this data. Here are some common web application attacks.

6.1.6.1 DDoS attacks - Circulated disavowal of administration assaults happen when programmers endeavor to overpower a framework or organization by blocking its resources. One typical kind of distributed denial of service (DDoS) attack in the Internet of Things involves overwhelming a resource with requests causing it to become unavailable. referenced in [45,46].

6.1.6.2 Explication of a misconfiguration - If data, rights, and passwords are misused due to incorrect configuration settings or configuration errors, this is known as security misconfiguration. Security and privacy concerns arise as a result of improperly set up Internet of Things applications. Many security concerns with IoT devices emerge from default settings, improper setup, or technical flaws with databases and operating systems.

6.1.6.3 SQL injection attacks - Among injection attacks, SQL injection attacks are a subset. Attackers use SQL injection attacks to access database servers and steal sensitive information by inserting malicious SQL queries [47].

6.1.6.4 Spyware - The goal of spyware is not to physically harm Internet of Things devices, but rather to secretly gather information about users' behaviors. Duqu is one example of an Internet of Things (IoT) spyware that tracks users' online behavior [48]. Malware on the Internet of Things has the ability to capture video and transmit it to unauthorized parties via email.

6.1.6.5 Reprogram attack - Hackers get access to IoT devices using poorly secured programming codes; they alter or rewrite the code to command IoT devices, or even take over the code to control the whole IoT network. Modifying network programming methods makes reprogramming IoT devices remotely easy [49].

6.1.7 Firmware Attacks -

It is crucial to install new security fixes and update the firmware in IoT gadgets since new vulnerabilities are being developed daily to attack the Internet. Regular system updates aren't feasible for the wide range of IoT devices.

6.1.7.1 Control hijacking - Hackers altered the code in order to take control of the IoT frameworks and modify the control stream. A few instances of these assaults include integer overflows, buffer overflows, and format string vulnerabilities [50].

6.1.7.2 Eavesdropping - Criminals steal data sent by Internet of Things devices by taking advantage of insecure network communication. We may claim that the victim's discussion is covertly overheard or read by the invaders. Since eavesdropping attacks do not disrupt the regular operation of the IoT network, they are difficult to detect [21, 51].

6.1.8 Side-Channel Attacks -.

The most serious Internet of Things (IoT) threats that rely on hardware are side-channel attacks. The restricted resources of IoT devices, such as battery life, storage space, and computing power, as well as the opportunities for side-channel assaults and the difficulty in detecting these harmful programmes, make them more susceptible to these types of attacks [52, 53].

6.1.8.1 Timing attacks - The use of timing irregularities, such as overclocking, to launch them is common practice for injecting malicious nodes or exploiting the flaws of other IoT devices to leak important information [55]. In order to acquire sensitive information such as bank account numbers, PIN codes, passwords, and cryptographic keys, these attacks may monitor how long it takes a program to complete specified activities. Attacks that use side-channel timing aim to deduce an algorithm's key [24, 54].

6.1.8.2 Power analysis attacks - The power consumption of different cryptographic hardware components of IoT devices is continuously monitored by attackers, who then analyse changes in electric current to extract secret information contained in the devices.

6.1.8.3 Electromagnetic attacks - Intruders collect and analyze electromagnetic radiations in order to get sensitive personal data from the hardware components, such as display displays, of Internet of Things devices. In order to intercept electromagnetic signals, hackers have been known to bring a micro antenna closer to the IC. Defense operations make advantage of these electromagnetic assaults [24, 55, 56].

6.1.8.4 Cryptanalysis attacks - The attacker can only obtain encrypted data, often known as ciphertext, using these techniques; they cannot access the accompanying plaintext. Success or failure of these attacks in IoT systems is dependent on the difficulty of deciphering the ciphertext [57].

6.1.8.5 Known-plaintext attacks - The essential trouble for the aggressor is to decipher the encrypted text using the known plaintext, which is just a tiny amount of the encrypted information. An attacker could use tactics like discovering the encryption key or diverging shortcuts to try to guess the rest of the crypto text [57].

6.1.8.6 Chosen-plaintext - By breaking into the encryption equipment, hackers may decipher the encryption algorithm and get the plaintext. In order to get the encryption key for an Internet of Things (IoT) cryptosystem, an attacker would use this algorithm to transform different chosen plaintexts into crypto text, compare and analyse the resulting crypto text, and so on [57, 58].

6.1.8.7 Chosen-ciphertext attacks - By first decrypting the selected ciphertext into plaintext and afterward utilizing this plaintext to depict the following ciphertext, attackers hope to get temporary access to the decryption processes. There is a connection between the decryption processes in IoT systems and chosen-ciphertext attacks [58].

6.1.9 Access-Level Attacks -. The Internet of Things (IoT) system is more susceptible to several types of assaults due to its limited resources and architecture. There are two main kinds of security assaults in IoT systems that are determined by the user's degree of access.

6.1.9.1 Active attacks - The attackers try to alter the hardware or communication packets of the IoT-based system by reading them. They have the ability to change route information, which may disrupt routing protocols [59]. Injecting mistakes or noise signals into message transmission is the main goal [113, 60].

6.1.9.2 Masquerade attacks - The criminal poses as a genuine client to gain admittance to the IoT network and send data there [59].

6.1.9.3 Modification of message - Modifications to data, manipulation of message packet sequence, or delays in the transmission of the intended message packets are all examples of packet tampering [59].

6.1.9.4 Repudiation - Once the attacker has sent or received the message, he or she will likely deny that any such communication was transmitted or received. [59].

6.1.9.5 Replay - Hackers secretly read it, make changes, then resend it to the intended recipient [62].

6.1.10 Denial of service attacks - The efficiency of IoT networks was diminished because attackers made an excessive number of requests for resources [27].

6.1.11 Passive Attacks.- When an attacker gains access to a message or data stored in an IoT system, they may use this data for their own purposes without changing the original content. Although the targeted IoT systems are unharmed, confidentiality is compromised in these attacks.

6.1.11.1 Traffic analysis attacks - The hacker covertly monitors the IoT network and records data about it. The attacker may be able to deduce the nature of the discussion from the recorded information, which includes the length, size, and sequencing of the message packets [39].

6.1.11.2 Privacy attacks - An intruder watches and records critical information, which they will then release to the public. A "release of message content" [63] assault describes these kinds of cyberattacks.

6.1.12 Location-Based Attacks - Internet of Things (IoT) attacks can be set up into two essential sorts, considering the region of the adversary: internal attacks, which involve insiders with knowledge of the designated framework or who live inside the targeted network's perimeter, and external attacks, which involve outsiders without knowledge of the framework or who can send off the assault from anyplace.

6.1.12.1 Internal attacks - The IoT network is compromised when unauthorized individuals with access to the device introduce harmful code or nodes. Intruders are familiar with the whole IoT infrastructure, including software, hardware, and devices, and they are all members of the same IoT network [64]. In their effects, these assaults ripple across the physical and network layers [65].

6.1.12.2 External attacks - An external aggressor acquires remote admittance to the IoT network and inserts a flaw or fault as part of an external assault. The attackers may use any public network or even start the assaults from anywhere. The attackers' understanding of the targeted IoT system's architecture and applied technologies is little, if any, at all [66, 67].

6.1.13 Host-Based Attacks - Cybercriminals aim their attacks targeting the operating systems of Internet of Things devices in order to steal sensitive data, including cryptographic keys. For their debut, they target the host systems of Internet of Things devices. We may broadly categorize these assaults as either software- or hardware-compromised, or as user-compromised.

6.1.13.1 User-compromised attacks - They are released with the intention of retrieving sensitive information from Internet of Things devices, including keys, passwords, and financial data.

6.1.13.2 Software-compromised attacks - Their purpose is to drain IoT frameworks by making their asset supports flood. One side effect of programming split the difference assaults is when the power abruptly goes out in devices that use batteries for the Internet of Things [66].

6.1.13.3 Hardware-compromised attacks - In hardware-compromised attacks, hackers compromise hardware devices in IoT systems in order to steal data or insert bugs and harmful nodes. The attackers should have the option to physically access the IoT devices in order to carry out these assaults [35].

7. CONCLUSION

The Internet of Things (IoT) emphasizes the need of privacy and security. As more and more industries use IoT devices, the need to ensure the network's security is growing. Maintaining the authenticity of data is also crucial, particularly when Internet of Things (IoT) sensors are used in healthcare settings. We explained different types of attacks on IoT devices. There is an emphasis on the privacy and security concerns. Since IoT devices are connected wirelessly, there can be breach when data is transmitted in the network. Even the operating system security is of prime importance. Security and privacy issues with Internet of Things devices, as well as potential assaults on these devices, are the main topics of this article.

8. REFERENCES

[1] Foundation Fieldbus [Internet]. Available from: http://www.foundationfieldbus.com/ [Accessed: 2021-01-11]

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in Internet-of-Things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[3] R. H. Weber, “Internet of things: privacy issues revisited,” Computer Law and Security Review, vol. 31, no. 5, pp. 618–627, 2015.

[4] A. Gopi and M. K. Rao, “Survey of privacy and security issues in IoT,” International Journal of Engineering & Technology, vol. 7, no. 2.7, p. 293, 2018.

[5] N. Aleisa and K. Renaud, “Privacy of the Internet of Things: a systematic literature review,” in Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 1–10, Hilton Waikoloa Village, Hawaii, 2017.

[6] A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.

[7] M. B. M. Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: a survey,” Computer Networks, vol. 148, pp. 283–294, 2019.

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

[9] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, “Blockchain for the IoT and industrial IoT: a review,” Internet of Things, vol. 10, article 100081, 2019.

[10] R. H. Weber, “Internet of Things – new security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.

[11] M. A. Khan and K. Salah, “IoT security: review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[12] Y. Qian, Y. Jiang, J. Chen et al., “Towards decentralized IoT security enhancement: a blockchain approach,” Computers and Electrical Engineering, vol. 72, pp. 266–273, 2018.

[13] A. Sultan, M. A. Mushtaq, and M. Abubakar, “IOT security issues via blockchain: a review paper,” in Proceedings of the 2019 International Conference on Blockchain Technology, pp. 60–65, Espoo, Finland, 2019.

[14] Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications; Wiley: West Sussex, UK, 2017; pp. 243–261

[15] Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051. Available online: https://ieeexplore.ieee.org/abstract/document/7442758 (accessed on 10 April 2020)

[16] The Zephyr Project [Internet]. Available from: https://zephyrproject.org/ [Accessed: 2021-02-05].

[17] Cheruvu, S., Kumar, A., Smith, N., & Wheeler, D. M. (2020). Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment (p. 488). Springer Nature.

[18] Top 50 Products By Total Number Of "Distinct" Vulnerabilities [Internet]. Available from: https://www.cvedetails.com/top-50-products.php [Accessed: 2021-01-12].

[19] Finn, N. (2018). Introduction to time-sensitive networking. IEEE Communications Standards Magazine, 2(2), 22-28.

[20] Schwarz, M. H., & Börcsök, J. (2013, October). A survey on OPC and OPC-UA: About the standard, developments and investigations. In 2013 XXIV International Conference on Information, Communication and Automation Technologies (ICAT) (pp. 1-6). IEEE.

[21] M. Abomhara and G. M. K. Ien, “Cyber security and the Internet of Things: vulnerabilities, threats, intruders and attacks,” Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[22] J. Deogirikar and A. Vidhate, “Security attacks in IoT: a survey,” in 2017 International Conference on I-SMAC, pp. 32–37, Palladam, India, 2017.

[23] S. Bhunia and M. Tehranipoor, Eds.“Physical Attacks and Countermeasures,” in Hardware Security, pp. 245–290, Morgan Kaufmann, 2019.

[24] M. Hutle and M. Kammerstetter, “Resilience against physical attacks,” in Smart Grid Security, pp. 79–112, Syngress, Boston, USA, 2015.

[25] A. Fadele, M. Othman, I. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, “A novel countermeasure technique for

reactive jamming attack in Internet of Things," Multimedia Tools and Applications, vol. 78, 2019.

[26] H. Li, Y. Chen, and Z. He, "The survey of RFID attacks and defenses," in 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4, Shanghai, China, 2012.

[27] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," Sensors, vol. 19, no. 5, 2019.

[28] P. Ganapathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4, 2009.

[29] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," in Lecture Notes in Computer Science, vol. 5538, pp. 291–308, Springer, Berlin, Heidelberg, 2009.

[30] M. Obaidat, S. Obeidat, J. Holst, A. al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the Internet of Things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," Computers, vol. 9, p. 44, 2020.

[31] H. Akram, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018.

[32] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1976–1986, San Francisco, CA, USA, 2003.

[33] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, 2017.

[34] [34] B. Mustafa, M. W. Iqbal, M. Saeed, A. R. Shafqat, H. Sajjad, and M. R. Naqvi, "IOT based low-cost smart home automation system," in 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, pp. 1–6, Ankara, Turkey, 2021.

[35] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): taxonomy of security attacks," in 2016 3rd international conference on electronic design, pp. 321–326, Phuket, Thailand, 2016.

[36] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372–383, 2014.

[37] D. Sisodia, On the State of Internet of Things Security: Vulnerabilities, Attacks, and Recent Countermeasures, University of Oregon, 2020.

[38] L. Bysani and A. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in 2011 International Conference on Devices and Communications, pp. 1–5, Mesra, India, 2011.

[39] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things," International Journal Of Network Security, vol. 18, no. 3, pp. 459–473, 2016.

[40] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: a layered approach for attacks defenses," in 2017 International Conference on Communication Technologies, pp. 104–110, Rawalpindi, Pakistan, 2017.

[41] E. Ronen, A. Shamir, A. O. Weingarten, and C. O'Flynn, "IoT goes nuclear: creating a zig bee chain reaction," in 2017 IEEE symposium on security and privacy, pp. 195–212, San Jose, CA, USA, 2017.

[42] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," Computer Science Review, vol. 38, article 100312, 2020.

[43] C. Dong, G. He, X. Liu, Y. Yang, and W. Guo, "A multi-layer hardware trojan protection framework for IoT chips," IEEE Access, vol. 7, pp. 23628–23639, 2019.

[44] A. Tsow, "Phishing with consumer electronics-malicious home routers," MTW, vol. 190, 2006.

[45] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," IEEE Access, vol. 6, pp. 24694–24705, 2018.

[46] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, 2004.

[47] L. Qian, Z. Zhu, J. Hu, and S. Liu, "Research of SQL injection attack and prevention technology," in 2015 International Conference on Estimation, Detection and Information Fusion, pp. 303–306, Harbin, China, 2015.

[48] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, Duqu: analysis, detection, and lessons learned, ACM European Workshop on System Security, Bern, Switzerland, 2012.

[49] U. Sabeel and S. Maqbool, "Categorized security threats in the wireless sensor networks: countermeasures and security management schemes," International Journal of Computers and Applications, vol. 64, no. 16, pp. 19–28, 2013.

[50] A. Mohanty, I. Obaidat, F. Yilmaz, and M. Sridhar, "Control-hijacking vulnerabilities in IoT firmware: a brief survey," in Proceedings of the 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), and attack taxonomy, New York, USA, 2015.

[51] I. Naumann and G. Hogben, "Privacy features of European eID card specifications," Network Security, vol. 2008, no. 8, pp. 9–13, 2008.

[52] H. D. Tsague and B. Twala, "Practical techniques for securing the Internet of Things (IoT) against side channel attacks," in Internet of things and big data analytics toward next-generation intelligence, pp. 439–481, Springer, 2018.

[53] H. Y. Ghafoor, A. Jaffar, R. Jahangir, M. W. Iqbal, and M. Z. Abbas, "Fake news identification on social media using machine learning techniques," in Lecture Notes in Networks and Systems, pp. 87–98, Springer, Singapore, 2022.

[54] A. A. Pammu, K.-S. Chong, W.-G. Ho, and B.-H. Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications," in 2016 IEEE Asia Pacific Conference on Circuits and Systems, pp. 650–653, Jeju, Korea, 2016.

[55] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware security in IoT devices with emphasis on hardware trojans," Journal of Sensor and Actuator Networks, vol. 8, no. 3, 2019.

[56] A. Sayakkara, N. A. Le-Khac, and M. Scanlon, "Leveraging electromagnetic side-channel analysis for the investigation of IoT devices," Digital Investigation, vol. 29, pp. S94–S103, 2019.

[57] D. Shree and S. Ahlawat, "A review on cryptography, attacks and cyber security," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, 2017.

[58] S. S. Kulkarni, H. M. Rai, and S. Singla, "Design of an effective substitution cipher algorithm for information security using fuzzy logic," International Journal of Innovations in Engineering and Technology, vol. 1, no. 2, 2012.

[59] R. Datta and N. Marchang, "Chapter 7-security for mobile ad hoc networks," in Handbook on Securing Cyber-Physical Critical Infrastructure, pp. 147–190, Morgan Kaufmann, Boston, USA, 2012.

[60] C. Li, "Security of wireless sensor networks: current status and key issues," Smart Wireless Sensor Networks, vol. 14, pp. 299–313, 2010.

[61] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: vulnerabilities, attacks, and countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2020.

[62] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things supported by mobile edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 56–61, 2018.

[63] K. Somasundaram and K. Selvam, "IOT – attacks and challenges," International Journal of Engineering and Technical Research, vol. 8, no. 9, 2018.

[64] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," Journal of Electrical and Computer Engineering, vol. 2019, Article ID 4568368, 13 pages, 2019.

[65] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, "A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4831–4843, 2019.

[66] M. D. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in 2015 IEEE World Congress on Services, pp. 21–28, New York, NY, USA, 2015.

[67] S. Alanazi, J. Al-Muhtadi, A. Derhab et al., "On resilience of wireless mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in 2015 17th International Conference on E-health Networking, Application Services, pp. 205–210, Boston, MA, USA, 2015.