International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (11)

IJCI

November 2025

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (11)

IoT Security and Privacy Issues: A Taxonomy

Mohamad Ibrahim Ladan
Software Engineering Department, College of Computer Science and Information System, Prince Sultan University, Riyadh, 11586, Saudi Arabia
malladan@psu.edu.sa

Abstract

The Internet of Things, IoT, is affecting almost every part of our life and it is connecting us in unprecedented ways. Every device we carry, own, or have at home or in office could be connected to the internet. It could be our air-conditioning, alarm system, smoke detector, doorbell, refrigerator, TV, water/energy meters, parking meters, pollution detectors, car navigation systems, and public or private transportation vehicles. This will lead us to be more in touch with our surroundings and eventually turn our communities and cities into fully integrated, smart, sustainable intelligent entities. All IoT-based transformations are now occurring to increase productivity and create a coordinated world across business and technologies, and to make our lives smarter and easier, however, this, as with any new technology, often comes with a cost in terms of new security and privacy challenges and risks. We, as users of this new technology are often too preoccupied by its wonderful benefits that we don’t even think about any possible privacy risks or security issues that this new technology might introduce. Moreover, the exchange, storage, processing and transfer of tremendous amounts of sensitive information has also given rise to severe security and privacy concerns that compromise the efficiency and usability of IoT. It has become a challenge for users to depend on such a vulnerable technology, where the IoT security risks outweigh its benefits. Hence, security and privacy requirement is one of the key challenges to the IoT’s growth and success, and different IoT applications and devices may require different levels of security. In this paper we review and classify the different security and privacy issues pertaining to IoT and their different uses and applications, and we discuss the different measures that can be put in place to alleviate and address these issues.

https://doi.org/10.59992/IJCI.2025.v4n11p2 E-ISSN 2976-9361

Keywords: Internet of Things, Internet of Things Security Issues, Internet of Things Privacy Issues.

1. Introduction

The IoT technology emerged at the beginning of the 21st century and has grown exponentially. It is changing our cities, world, and life by connecting us with our surrounding and everything around us in unprecedented ways. Every device we carry, own, or have at home or in office is and will be connected to the internet. It could be our alarm system, doorbell, refrigerator, TV, water/energy meters, parking meters, pollution detectors, car navigation systems, traffic lights, and transportation vehicles. Changes started to appear in our cities with so many things connected and controlled over the internet for many purposes in general but for better management of transportation, safety, health, businesses, efficient use of resources, and to get to fully integrated, smart, sustainable cities. The number of IoT devices worldwide is forecast to almost double from 15.9 billion in 2023 to more than 32.1 billion IoT devices in 2030 [1].

The IoT could be defined as a net of connected, to each other and to the internet through a wire/cable or wireless (Bluetooth, Wi-Fi, or cellular networks), devices, objects, equipment, or any other things. Some or all of them could be smart and have some sort of sensing capabilities, can communicate with each other and may be with some control/server centers via the Internet with or without any human intervention, with the ability to collect, store, process, and transfer data. The term IoT has been considered as an expanding technique applied in various applications and functions as shown in Figure 1 [2]. The key features required for employing a large-scale IoT are low-cost sensors, highspeed and error-tolerant data communications, smart computations, and numerous applications.

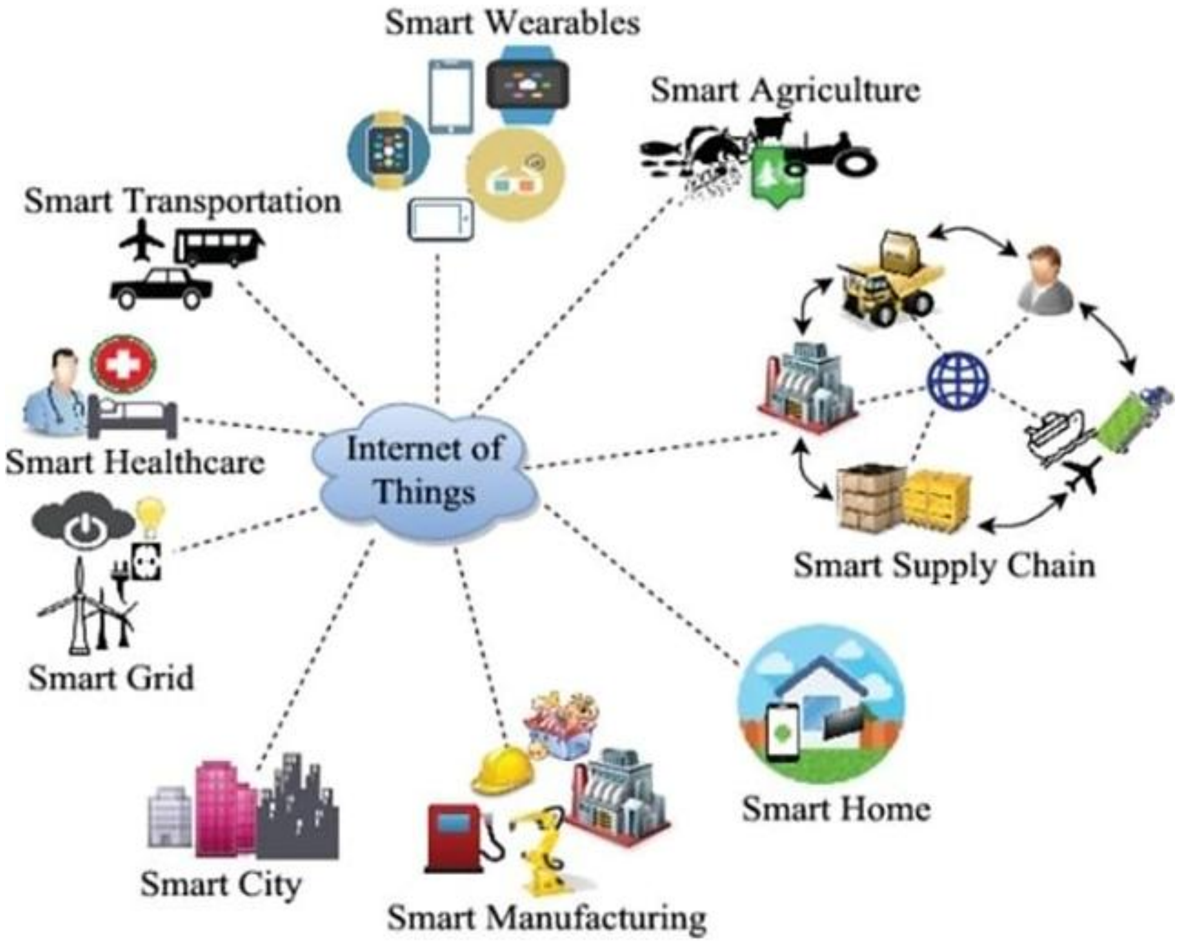

Figure 1: The IoT Application Areas

IoT devices comprises of potentially numerous types of devices and networks that are usually deployed in hostile, dynamic and heterogeneous environments. They are typically embedded with technology such as processors, memory, sensors and software and can include mechanical and digital machines and consumer objects. Moreover, with IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices. The connectivity, networking and communication protocols used with these devices largely depend on the specific IoT applications deployed. IoT technology and applications has had tremendous impact on people's lives as it helps people to live and work smarter, as well as gain complete control over their lives by offering smart devices to automate homes, businesses, public services, and other aspects of daily life.

However, the rapid and large-scale deployment of IoT devices poses a significant security concern. The authentication, authorization, system configuration, verification, access control, information storage and management verification, to name a few, are the main security challenges in the IoT realm. Vital information may leak or be tampered at any time. The security of IoT devices, the information they contain and users' privacy are not guaranteed. Moreover, with the increase in the number of hacking instances on IoT applications/devices, security concerns have been ranked number one challenge to the IoT's success [3]. In addition, the large-scale adoption of IoT technology and the rapid growth of intelligent heterogeneous devices have introduced new security and privacy issues and challenges especially that IoT devices are connected mostly over wireless networks and are typically utilized in an unattended fashion. In this type of environment, an attacker may easily gain both physical or logical access to these devices illegally especially that most of these devices have resource constraints that make deploying sophisticated or classical security measures and solutions not applicable to many of them.

This paper reviews and classify the various security and privacy issues pertaining to the IoT systems, applications, and devices. In addition, it presents some recommendations of the countermeasures and precautions that can be used to alleviate these issues. The remaining of the paper is organized as follows: In Section 2, an overview of IoT security and privacy issues and challenges is presented. In Section 3, a taxonomy of IoT security and privacy issues is given with details for the different types of attacks and issues. In Section 4, a detailed discussion of the different IoT security and privacy issues and their current countermeasures are presented. Finally, in section 5 a conclusion is given.

2. Overview of IoT Security and Privacy Issues and Challenges

Although IoT continue to improve our daily work and quality of life and most users are often very captivated with the benefits and the great features that this technology is offering, there are some security and privacy challenges associated with the pervasive connectivity platform provided by IoT that users do not even think about their implications on the privacy of their data and the security of their devices. Many IoT devices include household items, office equipment, and sensors. For a mother, a baby monitor that is connected to the internet and accessible from her smartphones at any time and from anywhere will give her freedom, convenience, and peace of mind by letting her keep a close eye on her baby while she is away from home or the baby's room doing some other tasks. But, if this baby monitor is not well designed with well-proven security measures, it may cause inadvertently negative and sometimes serious consequences to the baby or his/her parents. Another example is the voice-activated camera equipped smart TV, most customers may not be aware that in order for the TV to recognize the right voice command from the user, the TV will have to communicate the verbal command and exchange other information, some of them may be private and personal, over, most probably, an unencrypted communication channel over the internet. If these new devices are not well equipped with security measures and are not well protected, they may be unintentionally exposing their users and the users' private data and info to possible harmful people. If the baby monitor device or the smart TV is hacked, a criminal can gain access to your network and most likely to other devices on it and can monitor your house and waiting for the right time to do some criminal act that may differ in their serious and danger level. The more devices you connect to the internet the more risks you will be subject to. The variety of digital technologies that are now evolving and being integrated into our lives is overwhelming, and vulnerable unsecured devices can be used to attack other devices. Large systems can be hacked into through their IoT enabled subsystems, e.g. hacking cars through their IoT enabled entertainment systems. In 2013, hackers stole millions of credit card numbers from a big US merchant by gaining access to their systems through their IoT enabled heating subsystem [4]. The susceptibility of certain large systems to attacks through IoT devices was demonstrated by the massive Distributed Denial of Service (DDoS) attack that brought down the Domain Name System services offered by the New Hampshire Company, Dyn, affecting its 14000 internet domains [5]. In this attack, the criminals managed to deny access to key users like Twitter, Netflix and Facebook for some hours. It was made possible through attacking not well-protected home devices such as baby monitors, and security cameras, which either has no built-in security or still has the default password. It could be more serious when it involves systems or objects like self-driving cars that are part of a network of sensors and computer processes aiming at reducing accidents caused by human errors and eventually making the roads a much safer place. Though this type of cars is designed with high security measures, they will not be exempt from hacking like any other IoT device. If a self-driving car is hijacked through the software it operates with, then the hacker can change its destination, speed, direction, or simply lock the passengers in the car. So, security and privacy risks and challenges are found wherever there are sensors, software, and hardware connected to the internet. The systems that could be affected may range from home appliances, implanted and wearable medical devices, to smart cities where public services utilize technology with the aim of improving efficiency and quality, and to critical national infrastructure, such as power grids and transportation systems.

The IoT security and privacy issues center around resource-constrained IoT devices, devices with limited processing power and storage capabilities. Most of the IoT devices do not have intricate physical security and are not equipped with the appropriate hardware or software to implement strong security measures. In addition to limited processing power, the sources of energy also pose serious restrictions on the operational abilities of IoT devices. In other words, because of lack in power, storage capacity, bandwidth and microprocessor, security countermeasures like public key encryption algorithm and frequency leaping communication cannot be applied to IoT devices. These factors increase the security risks and privacy challenges of IoT devices. In addition, the security and privacy issues become even more complicated and challenging due to many factors like variation in technologies and standards used by different IoT devices, and that the standardization of IoT architecture and communication technologies are the basis for the IoT development [6].

On the other hand, IoT devices produce giga-, tera-, exa- and even zettabytes of data which causes a huge privacy challenge of storing and protecting this huge amount of data. Whether the data originated with a consumer using a product or with sensors on a machine at a factory, the questions remain: Whose data is it? Who owns the data? Does the extremely personal data collected by your fitness equipment belong to you or to the company who produced the equipment? Some sensors can be lifesaving when worn by patients in hospitals. Recent advances in electronic devices and communication infrastructure have revolutionized the traditional healthcare system into a smart healthcare system by employing IoT in medical devices called internet of medical things (IoMT) devices that have raised privacy issues concerning the information communicated between hospitals and end-users. The information conveyed by the IoMT devices is highly confidential and can be exposed to adversaries [7]. There is no standard, agreed-upon IoT data ownership model in place to clarify, and the IoT data ownership is still a controversial topic. We need a fundamental rethinking about who produces and owns the data, and give the party who owns it the right to control it [8]. Moreover, the servers for IoT are organized with cloud computing, and cloud computing has risks such as data security and privacy, data integrity, management, bandwidth, and data transfer [9].

Although many research efforts are being done to address the security and privacy issues of the IoT and despite remarkable developments in these areas, IoT is prone to significant challenges in protecting and securing IoT devices and the data they collect. It is essential to identify vulnerabilities of IoT devices, recognize security risks, detect cyber-attacks, and implement effective security measures to ensure the security of IoT devices and data they gather. Many devices are already on the market and in people's households and even when some IoT devices are outmoded and rarely used, such devices may still be a source for vulnerabilities that hackers can take advantage of for hacking other systems on the internet. When dealing with IoT security, we should keep in mind that using any not well-protected IoT device may risk any other device on the internet. The more our IoT devices are protected with strong security measures, the healthier and better for everyone else. Continuous efforts on developing and enforcing stronger security and privacy standards is still needed to keep and increase the public trust in this growing economy [10].

3. Taxonomy of IoT Security and Privacy Issues

Various approaches have been proposed in the literature to classify the IoT security and privacy issues. Most of the classification approaches mainly revolves around two general categories, namely the architectural aspects of the IoT and the protocols and standards employed within the IoT domain. In [11], they classified the IoT attacks based on different factors such as attack domains, attack threat type, attack executions, attacks based on software, attacks related to IoT protocols, attacks based on device property, attacks based on adversary location and attacks based on information damage level. In [12], they presented and reviewed IoT security threats from several perspectives and classified the threats into three main groups which are hardware threats, software threats, and threats to data in transit. In [13], they classify the different vulnerabilities based on insufficient authentication and authorization, insecure web interface, insecure network services, lack of transport encryption/integrity verification, insecure cloud interface, insufficient security configurability, insecure software/firmware, insecure mobile interface, and poor physical security. In [14], they grouped the security issues based on different factors like insufficient authentication/authorization mechanisms, lack of suitable cryptographic techniques, cyber-attacks, privacy, software/firmware related issues, and human-related factor. In [15], they classify them based on the following classes: Confidentiality, Integrity, Authentication, and Availability. In [16], they classify them based on the different layers of the IoT structure which are the physical layer, the network layer, the software layer, and the IoT protocol and data encryption layer. In our case, we classify the various IoT security and privacy issues at the highest level into two main classes: IoT Network-related issues and IoT Device-related issues. Furthermore, we discuss the different types of security and privacy issues under these two categories.

3.1 IoT Network Security and Privacy Issues:

IoT devices connect to the internet using a range of network connectivity technologies, including WiFi, Bluetooth, cellular, Zigbee and LoRaWAN (Open standard Long-Range WAN). These connection technologies use radio signals that travel through the air where they can be intercepted by location-less hacker that are difficult to track down, and hence they have their own security and privacy issues and challenges. In addition, most wireless connections are dependent on other private networks, owned and managed by others, and sometimes on a public-shared infrastructure where you have much less control of, and knowledge about, the implemented security measures. Although encryption aid to some extend in securing information moving across wireless networks, the moment the data leaves an IoT device and heads onto a communication network, it is vulnerable for different types of attacks. In what follow, we will review and categorize the different security and privacy issues that are related to connectivity and networks.

Jamming attacks: Jamming attacks are among the most effective techniques to attack and compromise the availability of wireless technologies. Jamming is an interfering signal that limits the intended receiver from correctly receiving the messages. Once the attacker deploys a jammer in a wireless network, jammer detection becomes difficult, if not impossible, due to the inaccessibility of the affected devices in the network [17]. In other words, these attacks are designed to block IoT network wireless communication channels by employing malicious nodes that generate noise signals. Other sun categories known as reactive jamming, constant jamming, and random jamming that depends on the timing and duration of jamming. Just on a separate note, GPS systems can also be the target of jamming attacks like what has been done nowadays by Israel on most GPS devices in some parts of Lebanon [18].

Eavesdropping. This is a well-known security issue in wireless networks. If the network is not secure enough and the transmitted information is not encrypted then an attacker can log on to the network and get access to sensitive data, as long as he or she is within range of the access point. Recent research has shown that eavesdropper can obtain much information regarding the types, user identities, and activities of IoT devices in the network, thus imposes a real threat to user privacy [19]. Even if the information is encrypted, by eavesdropping attackers can infer private information such as the types and working status of IoT devices in a business or residential home.

Man in the middle attack (MitM): MitM is defined as an attack in which the attacker is located in the middle of the communication as a relay/ proxy between a sender and a receiver. In this position, the attacker can intercept and alter the communications between the sender and receiver. In other words, MitM attacker intercepts and interrupts communications between devices and exploits the data between two parties.

Then, the attacker impersonates either party, stealing data and gathering sensitive information to operate scams or frauds. These types of attacks on IoT devices in general and on devices that use Long Range Wide Area Networks (LoRaWAN) has increased exponentially due to the high user demand and increased access to the internet. As a result, there is a high probability of user data being exploited by penetrating the network devices leading to cyberattacks such as remote access, extortion, sabotage, and loss of internet access [MiTM]. There are two types of MitM attacks: A passive attack and an active attack. A passive attack occurs when an attacker does not change the communication actively. Instead, the attacker secretly listens to the communication to gain access to sensitive information like usernames, passwords, and other confidential data, as most traffic is not encrypted properly. On the other hand, an active attack occurs when an attacker intentionally intercepts and modifies the communication between two entities. Once the attacker is in the communication channel, they can manipulate the communication by intercepting, changing, or inserting new messages. Impersonation, spoofing attacks, and data tampering are the most common types of active MitM attacks [20].

Denial of service (DoS) and *Distributed Denial of Service (DDoS) attacks*: DoS and DDoS attacks are reported as the most frequent attacks in IoT networks. The traditional security solutions like firewalls, intrusion detection systems, etc., are unable to detect the complex DoS and DDoS attacks since most of them filter the normal and attack traffic based upon the static predefined rules [21]. The main aim of these attacks is to make victim systems down and inaccessible for legitimate users by malicious malware. The original DoS attack is an operation-oriented attack that sends many open connections request to the destination node and keeps transmitting until the destination node becomes exhausted. The DDoS attack turns original or authorized nodes into malicious nodes to participate in the attack, so the attack will come from multiple malicious nodes. Because of some specific characteristics of the IoT devices and their environments, IoT DoS and DDoS attacks can be more harmful [22]. For example, most of the IoT devices have limited processing power, memory, and bandwidth, which makes them easy targets for DoS and DDoS attacks. Moreover, IoT devices are often interconnected and can share data with each other. Hence, when an IoT device is taken down by a DoS or DDoS attack, it can take down other connected devices as well, leading to more substantial damage.

Object replication: This type of attack takes place by duplicating an object's identification number in any IoT network leading to a huge drop in network performance since it might corrupt the packets and misdirect them. In addition, the replicated malicious node can steal the information and authentication credentials and use them for malicious acts [23].

Sinkhole attack: The Sinkhole is a networking attack that destroys the topology of the RPL protocol as the attacker node changes the route of all the traffic in the IoT network. The RPL protocol is an IP-V6 standard routing protocol for efficient and low-energy networks like sensor and IoT networks. Sinkhole attacks disrupt the intended routing paths, leading to data interception, unauthorized access, and potential data manipulation. Attackers inject a malicious node that broadcasts illusive information regarding the routings to impose itself as a route towards specific nodes for the neighboring nodes. In other words, this malicious node presents itself to other IoT network nodes as the best shortest channel for communication and thus, attracts data traffic and collects and “sinks” all of the information packets which flow on the targeted IoT network. These attacks reduce the performance of targeted networks because the whole traffic of the IoT network flows towards the sinkhole. Still, this malicious node does not drop even a single message packet; they also harm the other performance-related attributes like efficiency and reliability of communication and disrupt the network protocols [24].

Wormhole attack: Wormhole attack is a serious type of attack which listens to the network activities without changing it, consequently making it extremely hard to observe and identify. The wormhole attack inserts information on incorrect routes in the network; it also alters the network information by causing a failure of location-dependent protocols thus defeating the purpose of routing algorithms. There are different types of wormhole attacks in IoT they are Wormhole using Encapsulation, Wormhole using Out of Band Channel, Wormhole using High transmission power, Wormhole using Packet delay, and Wormhole using Protocol Deviation [25].

Sybil attack: IoT are vulnerable to Sybil attacks where attackers can manipulate fake identities or abuse pseudoidentities to compromise the effectiveness of the IoT and even disseminate spam [26]. A Sybil attack uses a single node to operate many active fake identities simultaneously, within a peer-to-peer network. It aims to undermine the authority in a trustworthy system by gaining the majority of influence in the network. A successful Sybil attacker may be able to perform unauthorized actions in the system like enabling a single entity, such as a computer, to create and operate fake several identities, such as user accounts and IP address-based accounts, fooling systems and users into perceiving them as real. The name of this attack was inspired by a 1973 book called Sybil; a woman diagnosed with a dissociative identity disorder. In the context of attacks, the term was originally coined by Brian Zill, and initially discussed in a paper by John R. Douceur, both at Microsoft Research [27].

Traffic analysis attack: Traffic analysis attacks allow an attacker to gather sensitive information about users by analyzing network traffic of user devices. These attacks are passive in nature and are difficult to detect. The attackers launch a malicious node to notify the daily traffic routines to collect the routing information. The encryption of message packets is not enough to protect the IoT network from traffic analysis attacks. There are two kinds of traffic analysis attacks: Link-load analysis attack and flow-connectivity attack. The first one discovers the traffic rate on a network communication link and the second one discovers the flow connectivity between a sender and a receiver.

Replay attack: A replay attack involves the attacker intercepting, seizing, storing message packets and then resending them as its own packets back and forth between IoT devices. The attacker can use this method to obtain unauthorized access or carry out malicious activity if the data in the packets is not sufficiently secured. Attackers utilize replay attacks when they want to delay information delivery to machines and decrease the network performance, and they also have the power to alter the instructions and trick the system into carrying out the wrong operations [28].

3.2 IoT Device Security and Privacy Issues:

The wide variety of IoT devices with their different components can pose many security and privacy threats. IoT device's component may include memory, firmware, web interface, physical interface, and networking service. Attackers can use any vulnerabilities in these components to initiate an IoT attack. IoT devices are installed almost everywhere and may include household items, office equipment, security and monitoring web cameras, traffic controllers, and so many types of sensors. If these devices are not well designed with well-proven security and privacy measures, they may be subject for hacking and may cause inadvertently negative and sometimes serious consequences to their users and their environment. One large class of IoT devices that has mushroomed recently is the security and web cameras class. These cameras are found everywhere: traffic intersections, street corners, malls, parking lots, hotels, airports and even our homes (security cameras, baby monitors, and smart door buzzers just to name few). In addition, in order to make full use of these devices, they should be connected to the internet to be able to broadcast a live feed that we can access via our phones or desktops. These feature not only opened the door for individual hackers to tap into them, but it entices the founding of some IT technical companies to do such acts and claim that they can be only used by law enforcement, security, and intelligence agencies. One example of such a company is an Israeli cyber firm called Toka. This company develops tools that allow their clients to "discover and access security and smart cameras," survey a "targeted area" and "stream and control cameras", and target cars, to "wirelessly" provide "access" and extract what Toka terms "car forensics and intelligence" [29]. These tools were used by the Israeli military to track, kill, and assassin different people during their current war against Lebanon [30] [31]. In what follow, we will review and categorize the different security and privacy issues that are related to IoT devices.

Revelation of a misconfiguration: IoT devices include everything from smart watches, smart TVs, baby monitors, alarms to medical equipment, food sensors, traffic routing, to air-conditioning just to name a few. In many of these devices, the poor configuration, security misconfiguration, improper configuration settings, mistakes in the configuration, default settings, or technical issues of databases, operating systems, and other such components are the sources of many security and privacy problems. One of the main causes of many security and privacy issues in IoT devices is the weak authentication and the use of default credentials in these devices that have usually embedded systems with no configuration required. A lot of the IoT devices are configured to use the factory-set default usernames/passwords and not only many users will never change these default passwords, but also many device manufacturers share their default credentials online. The threat of default credentials is significant and is beginning to be recognized as such.

Malicious code injection Attack: The main goal of this type of attacks is to undermine the security of IoT devices by injecting malicious code or commands into a system to gain unauthorized access, steal data, disrupt operations, or achieve other malicious objectives. These attacks are classically executed through vulnerabilities in the software or firmware of the IoT devices. Common types of malicious code injection attacks include: *SQL Injection* and *Command Injection*. The first one exploits vulnerabilities in web applications to insert malicious SQL statements into the database, potentially leading to data theft or unauthorized access. And the second one involves injecting malicious commands into the system's command-line interface, allowing attackers to execute arbitrary code [28].

Spyware: Spywares are malicious software applications that attack IoT devices and collect information about users' activities without their knowledge and without damaging the IoT devices. These spywares can record microphone signals or communication and send them to intruders through a Bluetooth connection [32].

Viruses: A virus is a computer program that can make copies by replicating itself and can infect other devices by transmitting via transferring infected files through wire or wireless networks, USBs, or different such types of portable devices. IoT viruses behave similarly to other viruses, except they infect IoT devices in a complicated way via self-replicating malicious code that is difficult to remove. Silex, for example, is an IoT virus that enters the device and bricks it, commonly known as a permanent DoS attack [33]. In addition, due to limited memory and storage space and lack of update mechanisms, it is challenging to secure IoT devices from viruses, so they quickly become victims of attackers. Mirai, SILEX, and Stuxnet are some types of viruses created to attack IoT devices [34].

Worms: a worm is a virus that can replicate itself, spreads, and propagates automatically in IoT devices, but cannot alter the device's files or functions. Worms continuously repeat themselves to create copies and fill the entire disk and memory space, so worms slow down or crash IoT devices. BrickerBot is a type of worm that destroys. Silex is another worm that overwrites IoT devices' storage disks [34].

Backdoor attacks: A backdoor is a malicious and complex malware type that negates normal authentication procedures to bypass authentication processes to remotely access system resources. Once remote access is granted, the attackers will have the ability to remotely issue system commands and do malicious acts. Some operating systems for some IoT devices have back doors that can be used to gain unauthorized access.

Trojan horse: Trojan is another type of IoT malware that seems harmless to the user despite having hidden malicious functionality. The Trojan cannot replicate itself, however, once downloaded and installed into the device, the attacker will gain control of the device and will be able to steal user data, delete user files, or spread viruses, worms, or other malicious applications [32].

Phishing attacks: Phishing is the act of sending deceitful communications like emails and text messages that appear to come from a legitimate and reputable source with the aim to gain access to sensitive data and login information, and/or to install and activate a malicious application into the victim's IoT device. Phishing is a dangerous, damaging, and an increasingly common type of cyberattack [23].

Radio Frequency Identification (*RFID) spoofing*: RFID systems do not have robust mechanisms to protect IoT devices because RFID tags are readable to everyone which make them very vulnerable. RFID spoofing, also known as RFID cloning, is a technique used to deceive RFID systems by imitating or replicating the signals of legitimate RFID tags or devices enabling attackers to impersonate a valid RFID tag or device. This allows the attacker to gain unauthorized access, bypass security measures, or perform deceitful activities. RFID spoofing aims to trick the RFID reader into recognizing the attacker's spoofed signal as a genuine RFID tag, enabling them to exploit the system for malicious purposes [11].

Permanent denial of service (PDoS): A PDoS attack is a denial of service via hardware sabotage also known as plashing. It is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. During such an attack, an attacker bricks a device or destroys firmware, rendering the device or an entire system useless. This is one method to exploit vulnerabilities and replace a device's basic software with a corrupt firmware image. In this scenario, the victim has no other choice than to repair the device or buy a new one to restore operations. It is an opposite DDoS attacks which overloads systems with requests meant to saturate resources through unintended usage without destroying them [21].

Brute-force password attacks: A brute force attack is a hacking technique that uses trial and error to break encryption keys, passwords, and login credentials. It is a straightforward but effective strategy for getting unauthorized access to user accounts, company systems, and networks. Attackers can attempt different combinations of common words to crack the password of an IoT device. Since many IoT devices prioritize convenience over security, they often have simple passwords that are easy to crack [34].

Outage attack: Outage attacks prevent remote IoT devices from finishing their routine task. In worse cases, these attacks turn off IoT devices. Outage attacks may launch a sleep denial attack and drain the battery to shut down the remote IoT device.

Side-Channel Attacks. Side-Channel attacks are non-invasive hardware-based attacks that exploit the leakage of physical information from a system during the execution of an application. They are the most hardware-based severe IoT attacks and IoT devices are more vulnerable to these types of attacks due to limited resources like battery power, storage, and processing power. The attack starts by monitoring and measuring power usage, electromagnetic radiations, timing information, and some other info and then the attacker analyzes the collected information to extract private information such as cryptographic keys [12].

Tampering attacks: Many IoT devices are placed in an environment without any physical protections to protect against an attacker gaining physical access to the device or wirelessly tampering with the software on the firmware of the device. The attacker can install malicious hardware or software to modify the behavior of the device.

Cloud-related Security and Privacy Challenges: IoT creates smart objects through the integration of sensors and objects that communicate directly with one another without the need for human involvement. Organizations can outsource their processes and other IT obligations using cloud computing. Cloud computing enables companies to focus on their core competencies, boosting productivity, better leveraging hardware resources, and lowering storage costs associated with IT infrastructure [9].

4. Discussion

The IoT security and privacy issues are more problematical by the fact that many of the users have unwillingly been ready to oversee the privacy and security issues in exchange for what the IoT technology is offering them in terms of benefits that become needed in their daily life. On the other hand, many of the IoT devices have resource constraints that prevents them from using classical security solutions. Users should be aware of the security and privacy implications of their use of IoT devices and online behavior. They should understand the implications of what they are doing and think about whether they can control what data is collected from them. The other problem is that most of the users expect companies and policymakers to have already addressed and done something about the IoT security and privacy issues. However, if users do not understand or show interest in data privacy, companies will not because they know users will not make their purchasing decisions based on privacy and security features. Users are more likely to buy an IoT device based on its usability, connectivity, compatibility, price, or even looks and ease of installation. If we take portable and wearable mobile technology which tracks and monitors users' activities and knows exactly where to find them, and we combine this with all the personal data they deliver, pictures they post and acquaintances and actions they make, then we should really be worried if this amount of data end up in the hands of an attacker. Just because users do not always understand the implications of low security does not mean they should not be protected. Consumer awareness and values to security and privacy needs are an important part of the problem that needs to be addressed. Another important part of the problem that needs to be addressed is the heterogeneity and diversity of the IoT devices with their different proprietary hardware and processing and communication software which is very hard to control, manage, and secure them. To make this second part of the problem even harder, organizations that are managing IoT environment today approach the issues from various standpoints, ranging from a stress on authentication standards to a policy of total lockdown to the use of third-party devices or applications [35]. Though it is not easy to develop an integrated solution to the IoT security and privacy issues, ISO standards have a big role in this regard and can help making the IoT more secure and safe to use. Standards like ISO/IEC 27001 and ISO/IEC 27002 provide a common language to address governance, risk and compliance issues related to information security. ISO/IEC 27031 and ISO/IEC 27035 help organizations to effectively respond, diffuse and recover from cyber-attacks [36]. There are also ISO/IEC standards that define encryption and signature mechanisms that can be incorporated into goods and applications to protect online transactions, credit card usage and stored data. There is also a need to work on privacy standards that protect data and information collected during online activities in general and while using IoT devices in particular. Privacy standards could make it easier to trace and protect our data and ensure its confidentiality. Standards should satisfactorily protect user's personal data and provides real-time control over its use and storage. In addition, they should minimize the amount of data collected by devices, inform users about any third-party processing, and enable traceability and accountability. We hope these types of standards will continue to be developed to be offered as solutions to the various and latest IoT privacy and security issues and challenges [37]. Microsoft's latest push takes an end-to-end approach to IoT security concerns in a bid to encourage customers to build applications that integrate IoT devices. The Microsoft Azure Sphere, currently in preview, provides layered security for applications that rely on IoT devices at three levels: hardware, software and cloud [38].

In summary, with the continuous growth of applications and usage of the IoT devices and networks, the IoT security and privacy issues are still open and challenging. In addition, the majority of traditional security and privacy mechanisms designed so far for Internet doesn't satisfy IoT security and privacy requirements and hence the need to develop IoT specific standards as mentioned above. While there are many research efforts being done to address this issue, many devices are already on the marketplace and in people's hands, cars, and homes that have vulnerabilities that can be abused by hackers to gain access to personal data or to other devices or things on the internet. Security and privacy standards need not only to be developed but need to be enforced. Keeping track of all the IoT devices on a network, ensuring they are secure and operating correctly are challenging activities. IoT monitoring tools simplify keeping devices updated with the latest software and firmware, automatically provide status information and identification, and are part of a larger cybersecurity strategy [39]. Meanwhile, different types of cryptographic solutions are available for data protection, but unfortunately, not all of them are suitable for IoT because of their resource-constrained environments. Lightweight cryptographic solutions are being researched to develop a strong cryptographic solution for IoT devices. Moreover, emerging and more advanced technologies like fog computing, artificial intelligence, machine learning, blockchain, and IoTA (an open-source distributed ledger and cryptocurrency designed for the IoT), are being integrated with IoT to solve the security and privacy issues. Blockchain improves the security of IoT systems by encrypting data at rest and stored data and digitally signing them with cryptographic keys [13]. At the end, IoT systems and devices should be structured and developed according to the latest security policies and standards. Furthermore, there is a need for more user alertness and awareness of the IoT security and privacy threats, and there should be more demands and research for more enhanced IoT specific security and privacy standards.

5. Conclusion

The Internet of Things, IoT, is a new trend of technology that has transformed people's lives in diverse aspects, such as smart health, smart homes, smart cities, and many other aspects. It is changing our cities, world, and life by connecting us with our surrounding and everything around us on the internet through various smart distributed, portable and sometimes wearable devices. To keep our lives safe from cyber attackers, we need to be fully aware of the security and privacy consequences of using and deploying these IoT devices and technology. The IoT security and privacy issues are getting more serious with the constant production of smarter IoT devices with weak or no security and privacy measures in them and with easy or automatic connection to the internet. Moreover, these devices are in most cases vulnerable due to their constrained resources and the inherent IoT environment conditions, basically, the dynamic aspect, the heterogeneity, and the open and wireless medium of communication. In this paper we have surveyed the current and emerging security and privacy issues of IoT and have classified them into two main high-level classes, one at the device level and the other is at the network and internet level. In addition, we have discussed the latest security and privacy measures that are in place or being under research to address the IoT security and privacy issues.

Acknowledgement: The author would like to acknowledge the support of Prince Sultan University, Riyadh, Saudi Arabia.

Funding Statement: This research was not funded by anyone.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: I declare that I have no conflicts of interest to report regarding the present study.

References

1. L. S. Vailshery, " https://www.statista.com/aboutus/our-research-commitment/2816/lionel-sujay-vailshery," Sep 11, 2024.
2. H.J. Felcia Bel and S. Sabeen, "A Survey on IoT Security: Attacks, Challenges and Countermeasures", Webology, pp. 3741-3763, 2022, DOI: 10.14704/WEB/V19I1/WEB19246
3. Harald Bauer, Mark Patel, and Jan Veira, "Internet of Things: Opportunities and challenges for semiconductor companies, https://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies", Oct. 2015.
4. M. Lazarte, "https://www.iso.org/news/2016/09/Ref2113.html#collapseSitemap," Sept. 5, 2016.
5. Paul Roberts, “Exclusive: Mirai Attack Was Costly for Dyn, Data Suggests”, The Security Ledger, Feb. 3, 2017.
6. Lo’ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider, "IOT privacy and security: Challenges and solutions," Applied Sciences, vol. 10, no. 4102, 2020.
7. M. Ali, F. Naeem, M. Tariq and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey", in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 778-789, Feb. 2023.
8. S. Shea, "https://internetofthingsagenda.techtarget.com/feature/The-great-IoT-data-ownership-debate," April 23, 2018.
9. M. I. Al Ladan, "A review and a classification of mobile cloud computing security issues," in International Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2016.
10. l. Columbus, "https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#51c742a8292d," Nov. 27, 2017.
11. Tinshu Sasi, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, Shahrear Iqbal, “A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges”, Journal of Information and Intelligence, Volume 2, Issue 6, 2024, Pages 455-513, ISSN 2949-7159, https://doi.org/10.1016/j.jiixd.2023.12.001.

12. Phillip Williams, Indira Kaylan Dutta, Hisham Daoud, Magdy Bayoumi, “A survey on security in internet of things with a focus on the impact of emerging technologies”, Internet of Things, Volume 19, 2022, 100564, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100564.
13. Swessi, D., Idoudi, H. A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures. Wireless Pers Commun 124, 1557–1592 (2022). https://doi.org/10.1007/s11277-021-09420-0.
14. Mark Mbock Ogonji, George Okeyo, Joseph Muliaro Wafula, “A survey on privacy and security of Internet of Things”, Computer Science Review, Volume 38, 2020, 100312, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2020.100312.
15. Chanal, P.M., Kakkasageri, M.S. Security and Privacy in IoT: A Survey. Wireless Pers Commun 115, 1667–1693 (2020). https://doi.org/10.1007/s11277-020-07649-9
16. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.
17. Hussain, N. Abughanam, J. Qadir, and A. Mohamed, "Jamming Detection in IoT Wireless Networks: An Edge-AI Based Approach," in Proceedings of the 12th International Conference on the Internet of Things, Pages 57 – 64, 2022.
18. Arabia,"Hezbollah-accuses-Israel-of-hacking-CCTV-Cameras-in-southern-Lebanon," https://english.alarabiya.net/News/middle-east/2023/12/28/Hezbollah-accuses-Israel-of-hacking-CCTV-Cameras-in-southern-Lebanon, 2023.
19. M. Alyami, I. Alharbi, C. Zou, Y. Solihin and K. Ackerman, "WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 385-392, doi: 10.1109/CCNC49033.2022.9700674.
20. R. Petrović, D. Simić, S. Stanković and M. Perić, "Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform," 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Nis, Serbia, 2021, pp. 307-310, doi: 10.1109/TELSIKS52058.2021.9606392.
21. F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.

22. Mohamed Riadh Kadri, Abdelkrim Abdelli, Jalel Ben Othman, Lynda Mokdad, “Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments”, Internet of Things, Volume 25, 2024, 101021, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.101021.
23. Muhammad Aqeel, Fahad Ali, Muhammad Waseem Iqbal, Toqir A. Rana, Muhammad Arif, Md. Rabiul Auwul, "A Review of Security and Privacy Concerns in the Internet of Things (IoT)", Journal of Sensors, no. 5724168, Sept. 29, 2022, https://doi.org/10.1155/2022/5724168.
24. M. F. R. Zaminkar, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism," Wireless Pers Communication, vol. 114, p. 1287–1312, 2020.
25. P. Krishnakumar, "Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT): A Review," International Journal of Recent Technology and Engineering, vol. 10, pp. 199-203.
26. K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," in IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372-383, Oct. 2014, doi: 10.1109/JIOT.2014.2344013.
27. Imperva, "What is a Sybil Attack?”, https://www.imperva.com/learn/application-security/sybil-attack/, 2024.
28. Tinshu Sasi, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, and Shahrear Iqbal, “A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges”, Journal of Information and Intelligence, Volume 2, Issue 6, 2024, Pages 455-513, ISSN 2949-7159, https://doi.org/10.1016/j.jiixd.2023.12.001.
29. Bashis Mcw and Charles Rollet, "Toka - A Hacking Platform for Video Surveillance Devices Examined", 2022.
30. Times of India, AFP "Lebanon's Hezbollah accused Israel on Thursday of hacking into CCTV cameras”, https://timesofindia.indiatimes.com/world/middle-east/hezbollah-accuses-israel-of-hacking-lebanon-cctv-cameras/articleshow/106363364.cms, Dec. 29, 2023.
31. Daily Sun, AFP "Lebanon says Israeli GPS jamming confounding ground, air traffic", https://www.daily-sun.com/post/755748, July 2, 2024.

32. Mark Mbock Ogonji, George Okeyo, and Joseph Muliaro Wafula, "A survey on privacy and security of Internet of Things," Computer Science Review, Volume 38, 2020, 100312, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2020.100312.
33. Victor, P., Lashkari, A.H., Lu, R. et al. IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. Peer-to-Peer Netw. Appl. 16, 1380–1431 (2023). https://doi.org/10.1007/s12083-023-01478-w.
34. Hezam Akram Abdul-Ghani, 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.
35. J. Scarpati, "Enterprise IoT security: Is the sky truly falling?" TechTarget, 2015.
36. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.
37. Z. Berkay Celik, Earlence Fernandes, Eric Pauley, Gang Tan, and Patrick McDaniel, "Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities," ACM Computing. Survey, vol. 52, no. 74, 2019.
38. T. Jones, "Microsoft takes holistic approach to IoT security concerns," TechTarget, 2018.
39. J. Borgini, "Features to look for in IoT monitoring tools," TechTarget, 2023.