SLIIT
Discover Your Future

BSc (Hons) in Information Technology

Specialized in Cyber Security

Year 2, Semester 1

CYBER SECURITY AND THE INTERNET OF THINGS

Individual Assignment

IE2022 - Introduction to Cybersecurity

Submitted by:

Student Registration Number	Student Name
IT21195402	Gunathilaka D.J.V.

Table of Contents

ABSTRACT

Our lives now cannot function without the internet. By 2020, there will likely be 34 billion Internet-connected (IoT) devices, with that number expected to rise daily. It has been noted that the security of these devices is incredibly thin and that hackers can simply infiltrate them because some manufacturers neglected to use even the most basic security measures. Modern devices support most of the communication and storage methods using standards that are simple to implement. Due to the differences in restrictions across various devices, there is no universal solution that will operate on all Internet of Things devices, leading to multiple Internet of Things categories. The Internet of Things (IoT) security challenges is the subject of this study, which will first go into the history, design, and industrial uses of the IoT. The IoT must also be made a reality, so it's important to categorize and investigate privacy issues, as well as survey and highlight the difficulties that must be solved.

INTRODUCTION

Beginning in 2000, the Internet of Things (IoT) era began. The IoT has revolutionized how everything is thought about because everything is connected to the Internet. Our way of living will become easier thanks to this idea. On the Internet of Things, everything is connected and controllable by other connected devices, so you can control your room temperature from your office. The Internet of Things will connect our homes, cars, and workplaces. Even if not, everything has an Internet of Devices connection now. As time goes on, more and more things are connected to the IoT. These gadgets that are connected will produce data. Based on the data gathered, these gadgets will not only produce data but also act accordingly.

Everything will be connected, and it will only take a few clicks to see everything in this existence. This situation highlights the significance of data and connected object security. If security is weak, bad actors in society will also be able to view, access, and abuse the same data. An example of this is a smart TV with a camera. There have been instances where people's TV cameras have been compromised. Investors are investing heavily in the Internet of Things (IoT) as a result of their growing awareness of its significance, but they are only doing so in products that can be quickly marketed and repaid. IoT security has received little or no investment at all. Concern over the security of things will grow as more things join the IoT.

IoT has been characterized in a variety of ways by different individuals and organizations. IoT is not a brand-new concept. In the past, those who had access to the internet were referred to as "the Internet of People." The government, academic institutions, and commercial sectors did not have extensive internet access until a few years ago. M2M (machine-to-machine) communication, was created to allow machines to communicate with one another using wired or wireless technologies to make decisions and perform certain tasks collectively. It is also well known for being a sensor network. These IoT items (clouds, web servers, nodes, sensors, machines, and apps) have direct internet connectivity and communicate with other IoT objects over the internet because internet access is now broadly accessible to everyone at a reasonable cost. This concept is known as "the Internet of Things" since all of these IoT objects are referred to as Things. Cisco describes its technology as the "Internet of Everything." By Bruce Schneier, the phrase "World Size Web" was first used. The Terminator movie used the term "Skynet" to describe the Internet of Things. Now let's discuss some further IoT subjects. In the world of information, things are usually categorized as virtual and physical items. Things have different identities and can communicate with one another across a communication layer. Physical items include things like the surroundings, sensors, electrical and electronic equipment, actuators, etc. IoT applications (web/mobile apps), in contrast, are virtual objects that may be saved, processed, and retrieved. Examples of these apps are Twitter, Facebook, Thingspeak, Blynk, etc. According to the definition in the following paragraph, the Internet of Things (IoT) is a network of interconnected physical and virtual things (devices, cars, buildings, and other items with electronics, software, sensors, network connectivity, etc.) that enables these objects to gather and exchange data. As shown in Figure 1, IoT is the setting that connects people, processes, and real-world and virtual objects (sensors). By using IoT online and mobile applications like CRM

systems, remote monitoring and maintenance, supply chain management location tracking, and many more, as shown in Figure 2, a lot more individuals may engage in IoT. Using a location tracking application, as an illustration, GPS sensors periodically communicate their location data to the servers that are configured to receive it. These servers then process and store the data in a database. Then, based on the requirements of the application, users are provided with a mechanism to access that data and make the right decisions or actions using mobile applications and online apps.

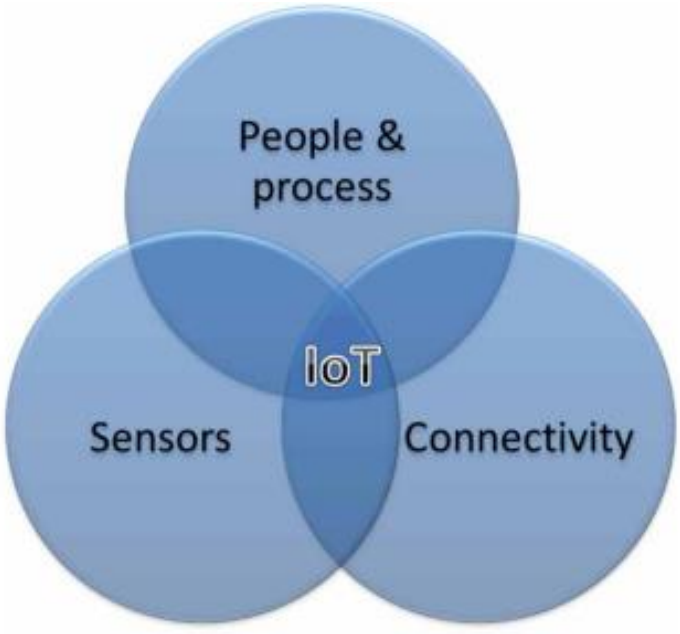

Figure 1. IoT Environment components

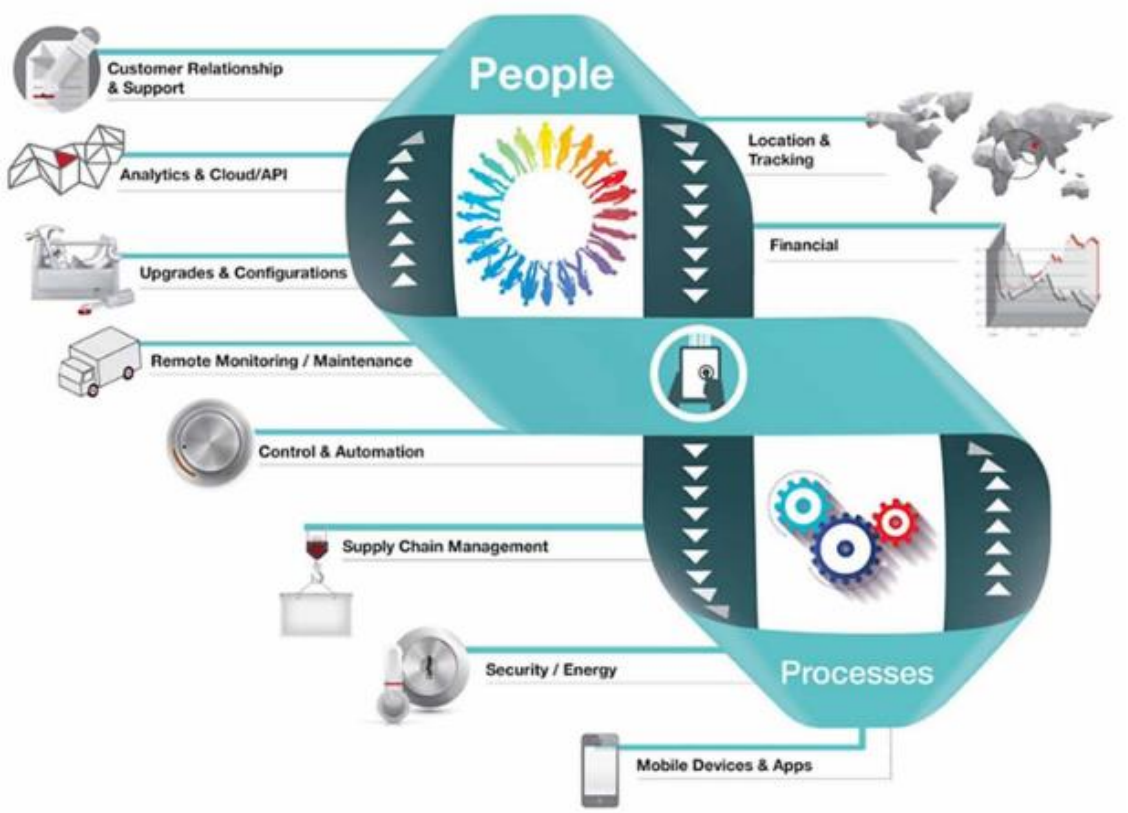

Figure 2. People & Process in IoT

Evolution

Evolution of IoT

The "Internet of Things" (IoT), a network of interconnected devices that share data online, has existed in some form for a while. The telegraph might in fact, qualify as the oldest example of this phenomenon if one accepts a broad definition of the term "internet," depending on whom you ask. A few such examples are the development of the telephone in the early 19th century and the widespread use of radar monitoring systems during World War 2. According to Forbes Media, one of the Internet of Things, the barcode was developed in 1949. Most people's first exposure to the Internet of Things (IoT) was a 1970s Carnegie Mellon experiment in which students utilized an early version of the local internet to remotely monitor a vending machine by connecting it to micro switches and other devices beyond point-to-point connectivity. They might ask if there will be a bottle of a cool soft drink before heading down the hallway to obtain their preferred beverage. John Rom key established the initial TCP/IP connection to a toaster in 1990. After a year, University of Cambridge researchers created a functioning web camera prototype to monitor the level of coffee in the coffee maker in their nearby lab. To allow viewers to see if the coffee was available, they set up a webcam to take random photographs that were then sent to neighboring computers. Technology guru Kevin Ashton originally popularized the term "Internet of Things" in a 1999 presentation on RFID technology he gave for Procter & Gamble. An RFID tag automatically identifies, and tracks tags affixed to objects using electromagnetic fields. A tiny radio transmitter and receiver, known as a transponder, make up an RFID tag. Cisco asserted that the Internet of Things had begun in 2009, when there were more things online than people, after the release of the first iPhone in 2007. An Internet of Things variant also appeared in the industrial sector, where machine-to-machine (M2M) connectivity was growing. M2M was more focused on direct communication between two or more machines than IoT, which focused on a network of internet-connected devices that progressively used big data and cloud intelligence. When M2M technology initially emerged is a subject of debate. Some people mention that the first form of telemetry was developed in 1912, or that RADAR was developed in the 1930s. But due to his early work on Caller ID, which debuted in 1968, Theodore Paraskevakos is credited as being the inventor of M2M. Additionally, Internet communication protocols would evolve. The Defense Advanced Research Projects Agency (DARPA) began work on the internet in 1962. After receiving further commercial backing, it eventually developed into the ARPANET and eventually became what it is today. A period of rapid IoT growth began in the years that followed, peaking in 2011 when IoT was included for the first time in the Gartner Hype Cycle for new technologies. In the years that followed, IoT communication capabilities were strengthened by GPS thanks to additional government and commercial investment. Unsurprisingly, IPV6 was made available to the public in the same year, enabling the transport of more traffic across the internet with improved security and dependability [Note: Oddly, IPV6 didn't become an "Internet Standard" until 2017]. M2M has more recently been incorporated into the larger industrial IoT (IIoT) / Business 4.0 ecosystem, where increased volumes of data are sent between devices through the internet to stream or automate industrial operations across numerous industry verticals. As an extension of IoT, Cisco created the concept of the Internet of Everything (IoE) in 2012. IoE is based on the four pillars of

people, data, process, and things. Several years later, the emerging Internet of Experiences (IoX) and, most recently (in 2019/20), Gartner's concept of the rising significance of the Internet of Behaviors were introduced in various marketing circles (IoB). The image below depicts an IoT development timeline.

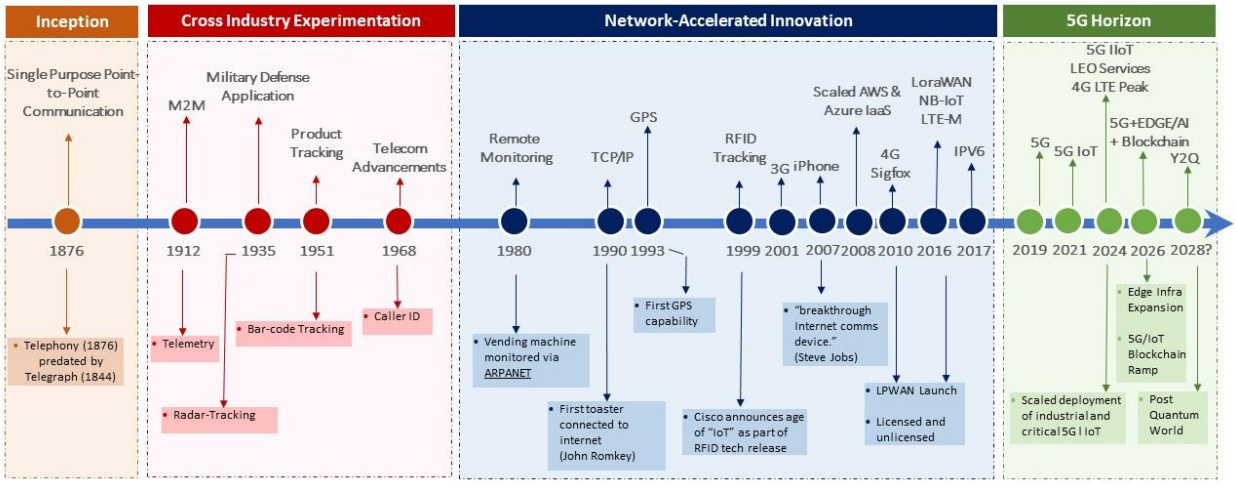

Figure 3. IoT Historical Timeline

Cybersecurity in the Internet of Things

Due to the IoT's rapid growth, new security risks and issues are emerging across all sectors. Businesses' and customers' interactions with the world will change as a result of the IoT. The number of IoT devices is expected to increase from 10 billion in 2016 to 24 billion in 2020 [1]. A major cybersecurity concern is the sharing of information with everything. The number of malicious assaults will rise as billions of IoT devices link to other networks. IoT devices can be used by online thieves as a gateway into corporate networks and cloud environments [2]. The main obstacle to IoT implementation is cybersecurity. Cyberattacks on connected devices, such as the capacity to hack a connected automobile, have already begun.

Customers nowadays are beginning to consider who has access to their data and who is accountable for keeping it secure as they recognize how their information may be used to analyze their choices. When various systems interact, competition for competitive intelligence will arise. As a result, security will become more important as a result of the increased cybersecurity issues that will be brought about. Additionally, IoT device data security is a key risk that must be treated seriously. News concerning data breaches is reported every other day [3]. Every connected object generates data, and the amount of data generated is measured in zeta bytes. This sensitive data is accessible to bad actors. Let's look at data from a thermostat as an example. This data can be utilized to determine the overall number of people and their availability. Your location and availability at a certain location can be tracked using GPS [4]. Although it doesn't seem like much, this information is sufficient for criminals to exploit against anyone. The misuse of business data is similar. Google, Yahoo, Facebook, and other firms are currently gathering social data, and hackers may access this data. Yahoo acknowledged that 1 billion of its accounts had been compromised on December 14.

The makers of IoT devices need to be aware that data privacy starts at the source. Information shouldn't be exposed once it leaves the sensor. Before processing and storing data in the cloud, encryption must be applied. The sections of this paper are arranged as follows: Section 2 will discuss IoT architecture and security breaches that occurred between 2015 and 2016. Section 3 will examine findings from the literature; Section 4 will examine findings from the survey conducted for this study, and Section 5 will cover discussion and future work.

2. IOT ARCHITECTURE

IoT standard architecture, as depicted in Figure 4 below, consists of devices, a local network, the Internet, and back-end services. The leading IT corporations in the world's intended IoT architectures are listed below.

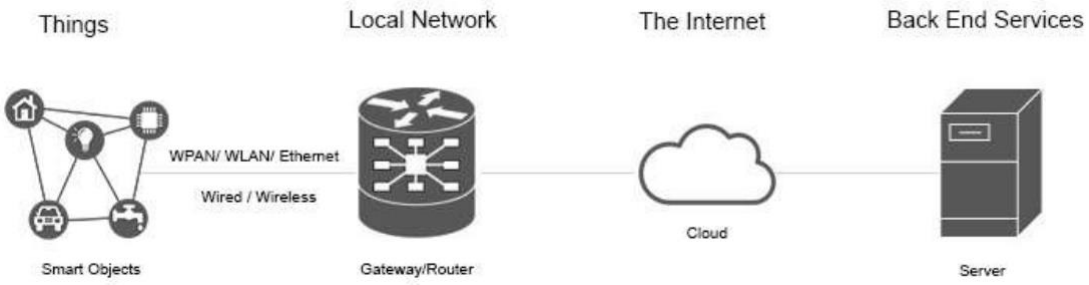

Figure 4 : IoT Standard Architecture

2.1 IoT Architecture by Microsoft

Figure 5 depicts Microsoft Azure's IoT architecture [5]. It consists of three main regions.

- Device connectivity
- Data processing, analytics, and management
- Presentation and business connectivity

Devices can communicate with one another directly or through a gateway. This architecture was created for large-scale IoT scenarios.

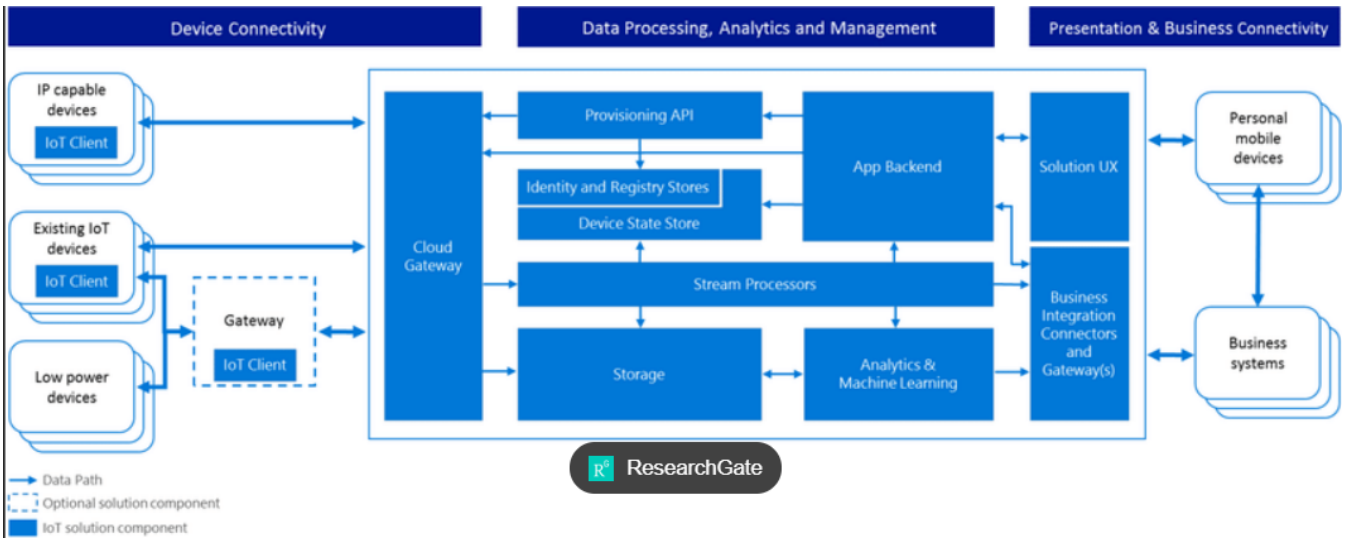

Figure 5. IoT Architecture by Microsoft

2.2 IoT Architecture by Intel

Intel and its ecosystem partners can define the IoT architecture with the System Architecture Specification (SAS) name for all things. As shown in whether they are connected to the Internet or not. Various IoT products are also released with the Intel ecosystem and this architecture provides data and device security [6].

Figure 6 below. This architecture consists of 3 components:

- Things
- Network
- Cloud

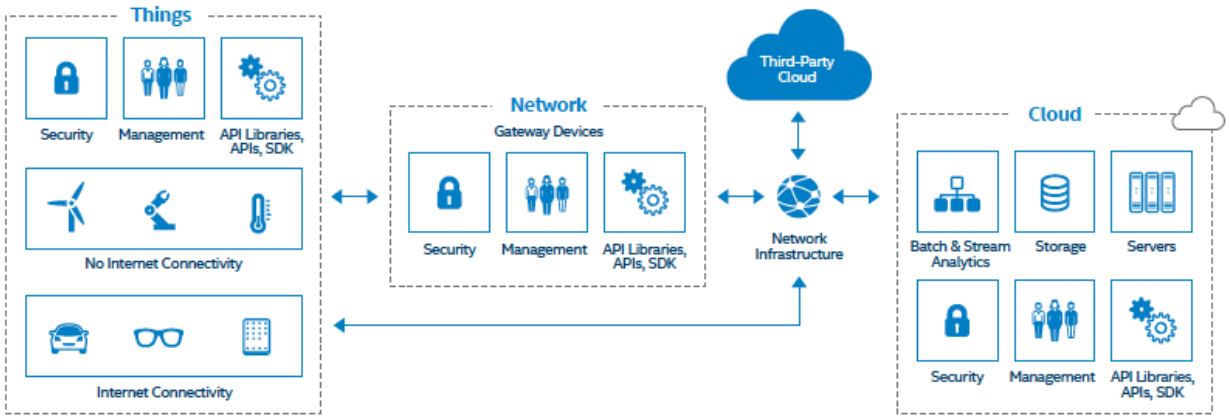

Figure 6. IoT Architecture by Intel

2.3 IoT Architecture by Google

The three primary building blocks that makeup Google's architecture.

- Device
- Gateway
- Cloud

Whether directly or indirectly connected to the Internet, gadgets can communicate with one another. Using a gateway, you can connect to devices that don't have a direct Internet connection [9]. Other network traffic using different protocols is also managed by the gateway [7]. According to Figure 7 below, data from all devices is stored, processed, and analyzed using cloud platforms.

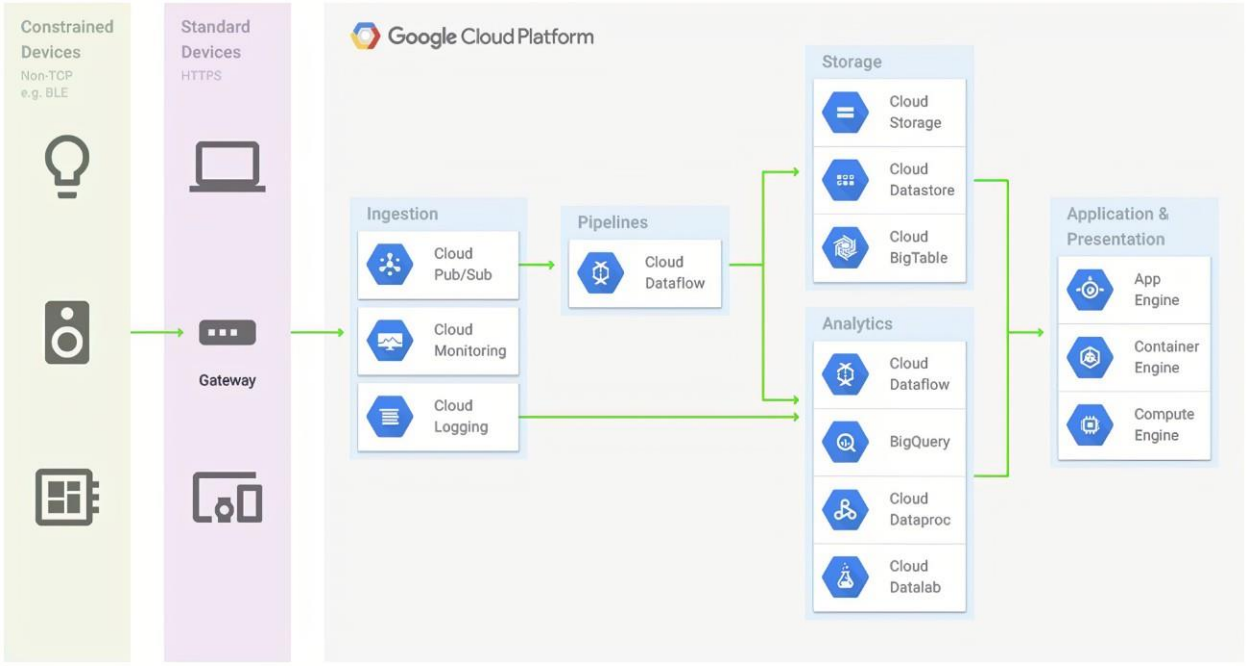

Figure 7. IoT Architecture by Google

2.4 Exploitation of an IoT Devices

A gateway for managing an IoT device can be created using the integrated circuit. The IC's security is weak, as has been noted in the past. Adding unapproved devices to the network enables access to IoT devices as well. At an American cyber security conference, this method was used to hack Google Nests [8] [9]. Infected software can access servers and devices through IoT apps. To access the network, one can make use of a gateway or router. The devices in Figure 8 below demonstrate how bogus content can be published by getting network access

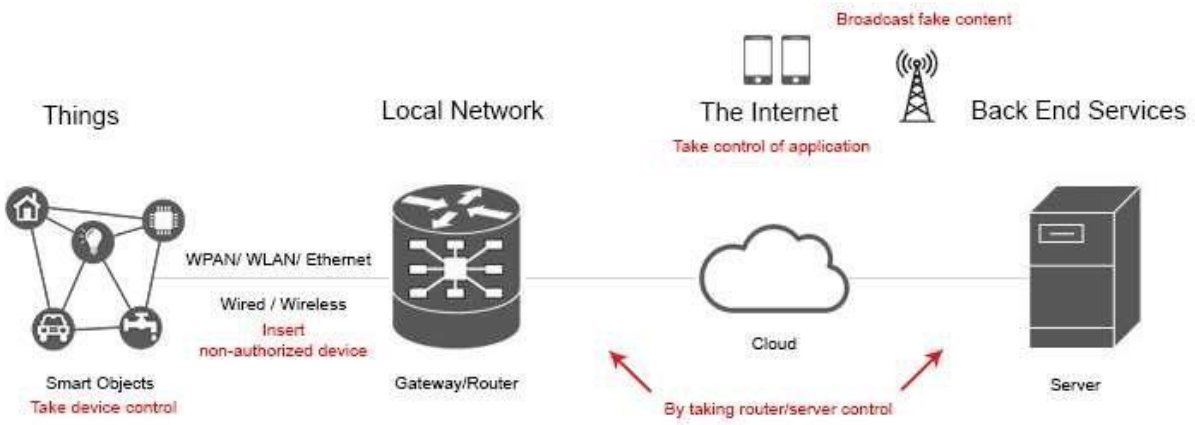

Figure 8. Exploitation of an IoT Device

2.5 IoT Industries & Breach Incidents

Everything in every industry will be covered by the IoT [10]. The following are potential main industries for the IoT: cover

- ✓ Government
- ✓ Transportation
- ✓ Defense
- ✓ Food services
- ✓ Infrastructure
- ✓ Retail
- ✓ Logistics
- ✓ Insurance
- ✓ Healthcare
- ✓ Banks
- ✓ Agriculture
- ✓ Connected Home
- ✓ Utilities
- ✓ Hospitality
- ✓ Oli, gas, and mining

In the first half of 2016, the health sector held the top spot with 263 infractions. Since 2014, there has been an increase in attacks on this industry. The next-highest amount, at 137, was attributed to breaches involving the government. Financial services came in third with 118 infractions. The number of citations for technology, retail, education, and other businesses was 102, 102, 90, and 162, respectively. Incidences of breaches in the IoT sector from 2013 to the first half of 2016 are listed in Table 1.

Table 1. Breach incidents in IoT industries

IoT Industries	1st Half 2013	2nd Half 2013	1st Half 2014	2nd Half 2014	1st Half 2015	2nd Half 2015	1st Half 2016
Healthcare	172	168	237	208	233	211	263
Finance	78	86	85	126	153	123	118
Government	127	64	109	180	161	135	137
Retail	56	41	81	113	130	108	102
Education	7	27	86	87	102	63	102
Technology	55	55	72	66	58	62	90
Other Fields	151	111	138	136	181	142	162

2.6 IoT Cyber Security Attacks from 2015-2016

As more objects are covered by the IoT, there are more breaches. Below is a list of the top cyber security infringements from 2015 and 2016.

A. San Francisco's Railway System

A ransomware attack that flashed the message "You are hacked." and infiltrated the San Francisco Municipal Transportation Agency (SFMTA) system on November 29, 2016, is known as a compromise. There is encryption throughout. The data was encrypted by cybercriminals using ransomware, as seen in Figure 9 below [11].

Figure 9. Hackers' message on San Francisco's Railway System

B. Ransomware hits Los Angeles hospital

One of the oldest private hospitals in the nation is located in Los Angeles and is called the Hollywood Presbyterian Medical Center. On February 15, 2016, a massive hack took place that fully brought the system to a halt. It was striking how much this attack resembled ransomware. The medical personnel was unable to obtain crucial patient data such as medical records, laboratory scans, and other information. The hackers demanded $3,000,000 to get this data [12]. On October 4, 2016, the medical company Johnson & Johnson advised customers that the insulin pumps used by their diabetic family members could become faulty and possibly result in an overdose [13].

C. Security Researchers killed Jeep Cherokee 2014

A 2015 demonstration of the Jeep Cherokee 2014 connected vehicle vulnerabilities was given by Chris Valasek and Charlie Miller [14]. They had full control over the radio, including the ability to change the channel, switch it on or off, and stop the car at any point. There have also been security breaches in the past involving popular vehicles like the Ford Escape and Toyota Prius. They are not the first; previously, college professors had demonstrated their access to important auto parts [15].

D. *Hacking in Aviation*

The cybercrime wave also affected the aviation sector. A flaw in the iPad software caused more than fifty American Airlines flights to be delayed on April 29, 2015. Aviation authorities have also been warned that connecting to Wi-Fi while flying could lead to a hijacking. The electronics in passenger cabins and cockpits also make use of the network shown in Figure 10 [16].

Figure 10. Tweet describing a situation from American Airlines

A German Airbus A320 was obliterated in March 2015. Aviation experts alleged that this aircraft has security flaws that hackers could take advantage of. In the past, fraudsters have also used fake boarding passes. Additionally, fraudsters can easily target air miles and reward programs [17] [18].

E. ATM Skimming Attacks

Around the world, attacks involving ATM skimming are growing more frequent. 300 million euros were recorded as the amount for 2015 [19]. Data acquired by the US-based FICO Card Alert Service, which informed customers of the issue, shows that skimming attacks increased by 546% in 2015. The majority of the time, as seen in Figure 11 below, these occur in off-site ATMs.

Figure 11. ATM Skimming Techniques

F. Leading Sources of Data Breach Incident

As in previous years, malevolent outsiders are the primary cause of data breach occurrences, with 668 data breaches in the first half of 2016. In Table 2 below, this is demonstrated. Malevolent outsiders are any unlawful employees who are present in the firm but are either known to them or not [20]. The unintentional loss trailed only the intentional loss in the first half of 2016, coming in at 178 breaches. When anyone mistakenly shares important knowledge, it results in an accidental loss. Malicious insiders, hacktivists, and state-sponsored attacks were to blame for 83, 29, and 14 of the breaches, respectively. Any sensitive information can be accessed by an employee who is malicious within the company.

Breach Sources	1st Half 2013	2nd Half 2013	1st Half 2014	2nd Half 2014	1st Half 2015	2nd Half 2015	1st Half 2016
Malicious Outsider	335	317	466	482	608	474	668
Accidental Loss	158	138	189	222	228	208	178
Malicious Insider	114	78	125	156	142	126	83
Hacktivist	20	7	4	16	18	18	29
State Sponsored	3	9	20	40	20	16	14

Table 2. Leadings Sources Of Data Breach Incident

2.7 8 Common Cyber Attacks in the IoT

There are best practices that manufacturers and developers may follow to ensure consistent security, even if the IoT industry hasn't agreed on a set of security standards. Networks are scanned by hackers in search of hardware and known weaknesses. For network connectivity, they are increasingly using unconventional ports. When they do not yet have access to the gadget, it is considerably simpler to detect. IT managers must deal with these IoT security concerns and then put preventative measures into place [21]. What is the IoT attack surface?

All security vulnerabilities that IoT devices, associated applications, and network connections may exploit are referred to as the "IoT attack surface."

IoT device security is a subject of significant concern. Threat actors can harm not just the IoT devices themselves but also the software and network that supports them. IoT device usage is rising faster than the protocols and procedures that can guarantee dependable, secure communications. The IoT attack surfaces may be protected by enterprises by a variety of means. To build these policies that can detect and respond to risks, technical knowledge and manpower are needed.

1. A botnet is a group of computers that may be used to remotely operate and spread malware.

They are used extensively by criminals for many different purposes, including stealing private information, abusing online banking data, DDoS assaults, spam, and phishing emails. Botnets are controlled by botnet operators via command-and-control services (C&C Server). Many gadgets and items run the danger of joining or already are a part of so-called thing bots, which are linked botnets made up of separate objects. Both botnets and item bots are constructed from several interconnected devices. They have two things in common: they can automatically transport data over a network, and they can connect to the Internet. While anti-spam technology may spot a single device sending thousands of identical emails, it is far more difficult to spot emails coming from a botnet, which consists of several computers. They are all attempting to send a target hundreds of emails in the hopes that the site will crash. The botnet is unable to handle the enormous volume of requests, though. Despite the difficulty of detecting botnet attacks, IT managers should take precautions to safeguard devices. Organizations should adhere to fundamental cyber security measures, such as authentication, frequent updates, patches, and verification that IoT devices adhere to security standards and protocols before being connected to the network. [21].

2. DNS threats

The decentralized DNS system, which was developed in the 1980s, is frequently used for IoT device connectivity. The deployment of thousands of IoT devices may not be supported by this. There are DNS flaws that hackers could exploit. Employing DNS tunneling and DDoS attacks to steal data or introduce malware IT managers may make sure DNS flaws do not compromise internet security by utilizing Domain Name System Security Extension. Through digital signatures, which guarantee accurate and unaltered data, these protocols safeguard DNS. To download a software update, DNSSEC confirms that an IoT device is connected to the network [21].

3. IoT ransomware

As there are more and more insecure IoT devices connected to corporate networks, ransomware attacks are becoming more common. To access a network, hackers first infect devices with malware, after which they probe access points for working login credentials. Through the use of an IoT device, a hacker can get access to the network and steal information.

Ransomware can automatically delete files if payment is not sufficient to allow the organization access to all of its data. Ransomware can be harmful to businesses and essential organizations such as government services or food suppliers [21].

4. IoT Security

IT administrators must take this risk into account when developing an IoT security policy, even if it would seem implausible that hackers will be able to physically access an IoT device. Hackers might take items and obtain access to the network's ports and internal circuits. Only authenticated devices should be deployed, and only authorized users should be given access to them [21].

5. Shadow IoT

Fitness trackers, digital assistants, and wireless printers all have IP addresses and might be valuable for business or personal convenience, but they may not always adhere to security standards. IT managers are unable to keep track of shadow IoT devices or guarantee that they are equipped with the bare minimum of security features. Privilege escalation can be used by hackers to access these devices. To prohibit employees from connecting IoT-incompatible devices to the network, IT managers can establish restrictions. To detect new connections, enforce policies, and prohibit or isolate unidentified devices, administrators can utilize IP address management tools and device discovery tools. [21].

6. Social Engineering

Phishing emails are the most common method used in social engineering attacks, and they solicit personal information or send you to trustworthy websites like banking and shopping portals [21].

7. Identity Theft

The greatest security threat to us often comes from within [21]. News reports are rife with alarming and unforeseen hackers acquiring data and money via a range of incredible hacks.

8. Denial of Service

When a service that typically operates is unavailable, there has been a denial of service (DoS) attack. Multiple devices are set up to make identical service requests through a botnet, frequently without the owner's awareness. Compared to hacking attacks like phishing and brute force, dos is less invasive. However, it might result in data loss or security breaches. How to safeguard against IoT security risks. Although there are many best practices and techniques that enterprises can employ, administrators must also be ready for various IoT dangers. IoT security includes both software to detect and respond to attacks and the enforcement of policies. Strong password guidelines and threat detection software must be in place by IoT management to guard against assaults. To stop security attacks The following fundamental tactics can be used by IT administrators: network segmentation, regular data backups, disaster recovery plans, and device vulnerability assessments. Adding an extra layer of protection is worthwhile despite the challenges posed by scattered IoT deployments. IT teams can safeguard data using technologies for data visibility, data classification, data encryption, and data privacy protection. Organizations should protect their devices by enclosing them in tamper-proof enclosures. Model numbers and passwords for the devices may also be printed on the parts by the manufacturers. IoT designers must hide conductors in multilayer circuit boards to keep hackers out of IoT devices. Attacks should have a function that is deactivated, such as short-circuiting if it is opened, to prevent hacker access.

2.8 Top 10 Cyber Security Challenges in IoT

According to [22], the following issues with IoT cyber security include:

- Crypto mining
- Rogue IoT Devices
- Data Integrity in Healthcare.
- Weak password
- Botnet Attacks
- Absence of a Robust Design
- Eavesdropping and Espionage
- Updating Issues
- Lack of Awareness
- Insufficient Testing and Compliance

1. *Crypto mining*

IoT device mining potential is yet another significant issue. GPU and CPU resources are enormously needed for cryptocurrency mining. Some hackers are infecting a lot of IoT bots to mine cryptocurrency so they can get the bandwidth they require. Although this attack is not intended to hurt any specific companies, it can have a significant negative impact on organizations that use IoT solutions. IoT botnet miners are a danger to the cryptocurrency economy. These miners can destroy an entire market with only one attack if given unrestricted access to the market.

2. *Rogue IoT Devices*

IoT device "rogue" technology risk is bigger than ever as the number of IoT devices rises. Unauthorized rogue hardware and fake Internet of Things goods are starting to circulate in several protected networks. The Raspberry Pi line of products, for instance, can be simply modified to function as fake access points, cameras, or thermostats. Even the idea that digital gadgets can behave strangely owing to malicious software and technology has served as the basis for several horror films.

3. *Data Integrity in Healthcare*

Data is continually being transferred in the IoT world. Data is continually being sent, analyzed, and stored in a corporate setting. The vast majority of Internet of Things (IoT) devices gather and extract data from their surroundings. They are connected to various gadgets, including televisions, thermostats, and even medical equipment. These gadgets also occasionally transmit data to the cloud unsecured. Unauthorized access to IoT medical devices is the result of a lack of encryption. In the IoT environment, it might be possible for controlled medical equipment to send false signals, endangering the safety of its users. As an illustration, digital pacemakers were made accessible to hackers by St Jude's implantable cardiac devices. The device's pace may be changed, the batteries could be used up, and other things, thanks to this.

4. *Weak Passwords*

When it comes to password hygiene, complacency frequently plays a bigger role than the human aspect in ignorance. We frequently use the same passwords or pick weak ones that are simple to remember. In any environment, using a weak password is like leaving yourself up to attack, but IoT-connected devices are particularly vulnerable to this. A false sense of security is implied by the default passwords that some IoT devices ship with. Users need to update their passwords as soon as possible, and then frequently go forward to something challenging to guess.

5. *Botnet Attacks*

Malware-infected IoT devices don't always pose a serious hazard. The biggest threat frequently comes from a group of infected devices. An army of malware-infected bots is assembled by hackers to carry out botnet attacks. A targeted piece of technology is then bombarded with hundreds of requests from these bots. In 2016, such an assault took place. IoT security was questioned by several businesses following the Mirai bot assault. Since many IoT devices don't receive the regular updates that a typical computer does, they are more susceptible to malware attacks and can catch infections very quickly.

6. *Absence of a Robust Design*

A substantial security risk could potentially arise from an IoT device's lack of "physical hardening." Even though some Internet of Things (IoT) devices may run without user input, they nevertheless need to be secured and shielded from external dangers. These devices are occasionally capable of remaining in isolated areas for extended periods while gradually gathering data using beacons. But if a piece of hardware can be physically broken into by a cybercriminal, then the information inside may likewise be made available. To maintain IoT devices physically secure in all contexts, both users and manufacturers must cooperate.

7. *Eavesdropping and Espionage*

The results might be quite dangerous if hackers can access your IoT software. For instance, hackers who break into IoT devices may be able to obtain private information. These criminals might then use that data as a form of ransom, holding access to the data hostage until the company pays a hefty fee. Hackers could take control of cameras and speakers to eavesdrop on people and companies even if your IoT device isn't used in a ransomware assault. Since many IoT devices can capture data, losing control over that data could quickly result in issues like corporate eavesdropping and espionage.

8. *Updating Issues*

Device update management is a further source of IoT security issues. Manufacturers can offer gadgets with the most recent software installed, but new flaws will surely surface over time. All IoT devices must receive regular updates to preserve security. Unfortunately, it's challenging for any manufacturer to make sure that customers keep updating their products once they buy them. A lot of companies may also neglect to release the necessary upgrades for their current solutions since they are focused on developing the next big piece of technology. A significant data leak could occur if there is any lag time between the discovery of a security flaw in an IoT software component and the application of a patch.

9. *Lack of Awareness*

The root of many cybersecurity problems is frequently human beings. User runs a considerably higher risk of unintentionally putting themselves in danger when they are unsure of how to utilize a technology securely. Consumers have progressively picked up skills over time,

such as how to secure Wi-Fi networks, scan their PCs for viruses, avoid phishing and spam emails, and more. IoT, on the other hand, is a relatively new technology that few people are familiar with. While manufacturing is still where the majority of IoT security issues are, improper tool usage by individuals can still pose serious security risks. Everyone must be aware of how to protect themselves before embracing IoT, whether they are a consumer or a corporation.

10. Insufficient Testing and Compliance

Determining if a piece of technology has been appropriately vetted for compliance is one of the main challenges businesses confront when using IoT. By the end of 2025, there will likely be 60 billion linked devices available. However, the majority of manufacturers are so eager to put their innovations on the market that they don't consider testing and compliance. The result is frequently items like fitness trackers that retain Bluetooth connections after usage and smart refrigerators that can display login information for email addresses. Moving forward, manufacturers must make sure that every gadget is thoroughly examined and outfitted with the appropriate privacy technology before it is released to the public.

3. FINDING FROM THE LITERATURE

The outcomes and revelations from the literature are as follows:

3.1 Healthcare Industry is Top Target in 2016

The healthcare industry has become a top target for attackers in recent years, and this trend persisted in the first half of 2016 [20]. The government had the second-highest number of violations, 137, after the private sector. Financial services came in second place with 118 data breaches. Figure 12 shows that there were 102 data breaches in the retail and education sectors, 90 breaches in the technology sector, and 102 breaches each in the retail and education sectors.

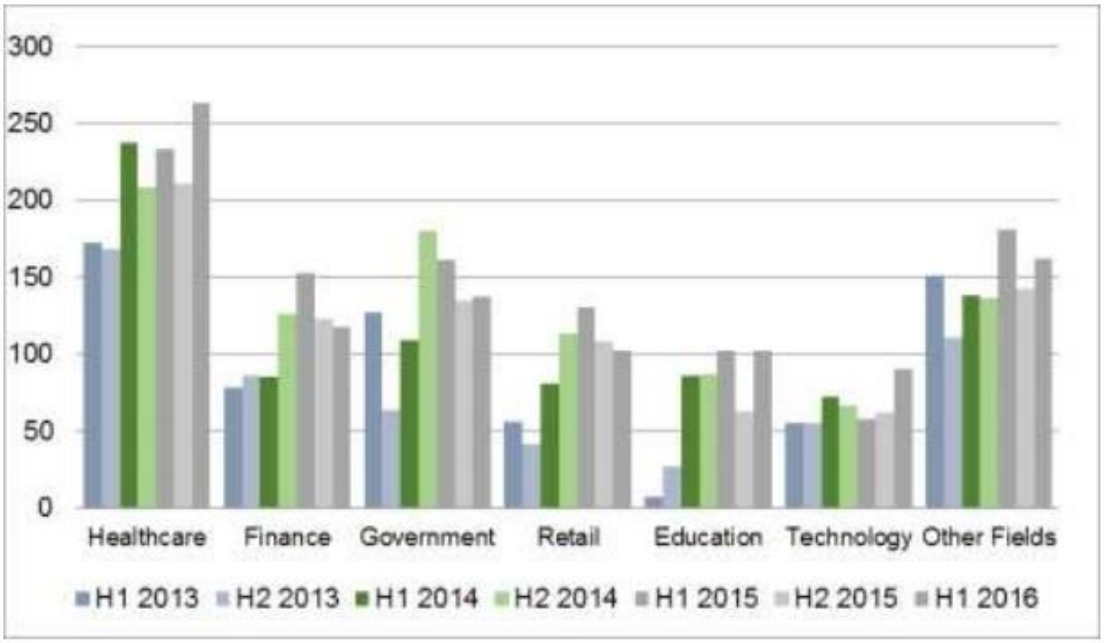

Figure 12. Cyber security incidents in different industries over time

3.2 Leading Sources of Data Breaches

Malicious outsiders were the primary cause of data breach incidents in the first half of 2016, which had 668 data breaches and was comparable to earlier periods as indicated in Figure 13 below [20].

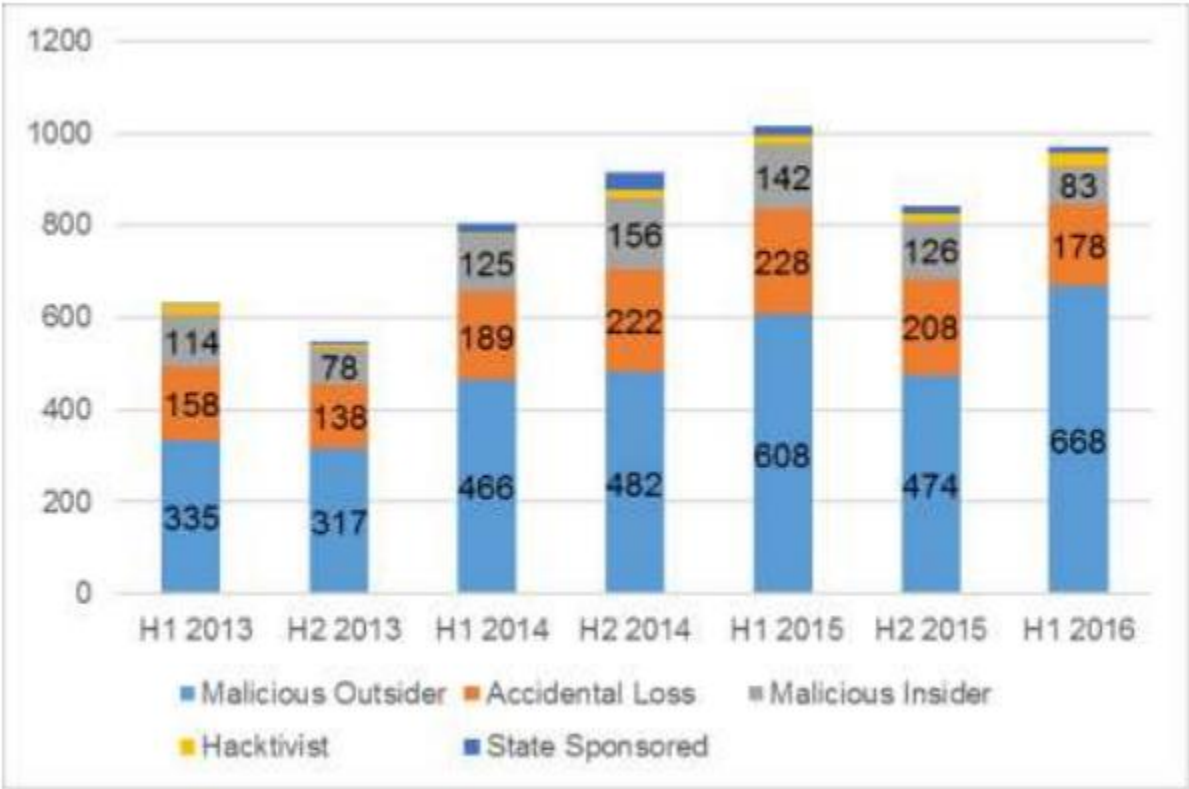

Figure 13. Leading Sources of Cybersecurity Threats from 2013 to 2016

4. FINDINGS FROM SURVEY

A random sampling procedure was utilized to select 100 responses from a web-based survey that was conducted. A survey found that users had a strong belief in the promise of the IoT. These are the primary conclusions drawn from this survey inquiry.

4.1 Familiarity with IoT

The survey respondent must have technical knowledge. In contrast to the 96.7% of respondents who were familiar with it, 3.3% of respondents had no idea what the Internet of Things was.

4.2 Adaptors of IoT

41.4% of the responses came from North America, while 31% came from Europe. Figure 14 shows that 17.2% of the population lived in Asia, 6.9% in Africa, and 3.4% in Australia.

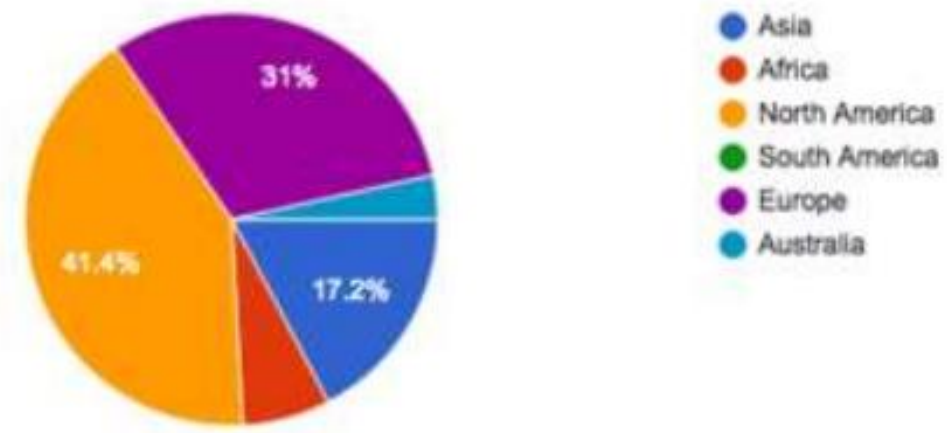

Figure 14. Survey Demographics

4.3 Survey Respondents

Participants in the survey come from a variety of industries, as seen in Figure 15. The largest vertical in terms of market share was technology, with just over 48.3%. Education, government, and financial services were the following three significant verticals, with respective shares of 20.7%, 13.8%, and 6.9%. The distribution of transportation, hotel, and other industries was equal to 3.4%.

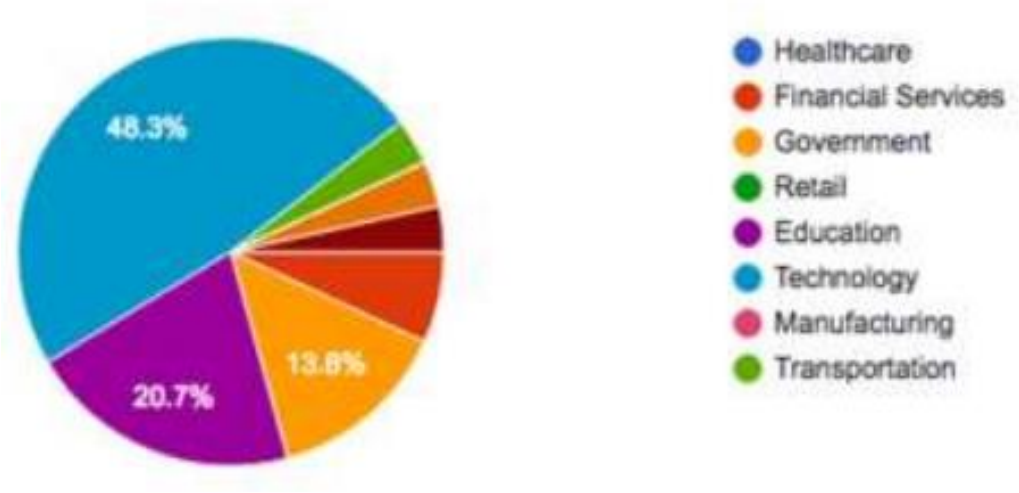

Figure 15. Survey Respondents

4.4 Lack of confidence in IoT device security

86.2% of survey respondents believe that the security of IoT devices is inadequate. Only 13.8% of respondents reported feeling slightly happier and more comfortable about the security of IoT devices. In terms of cybersecurity, the IoT poses a serious problem, but it also offers a chance for novel ideas.

4.5 Cybersecurity is important to business

Business owners were concerned about cybersecurity and understood the critical importance of their data. According to 90% of responses from large companies, cybersecurity is far more critical than cost, data analytics, functionality, and hardware integration, as shown in Figure 16

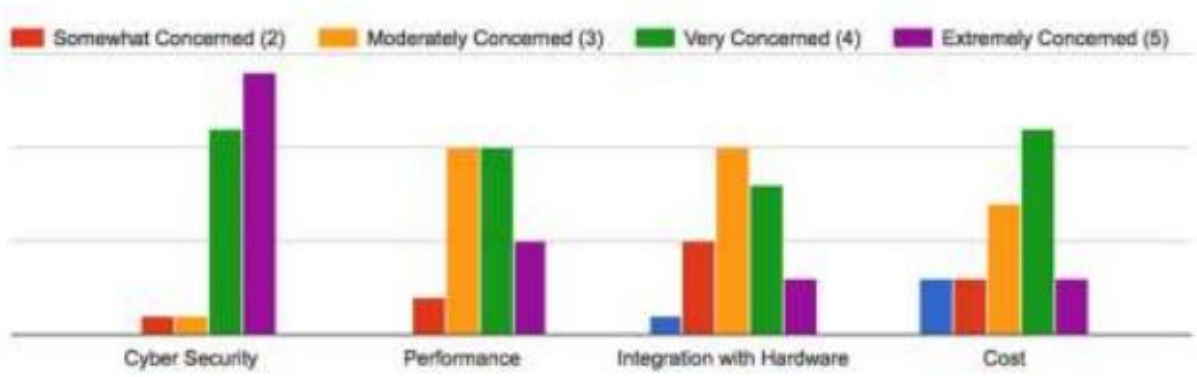

Figure 16. Cyber security is important to business

4.6 Impact of Cyber Security Concerns on Business

According to respondents, 65.5% of people said that cybersecurity issues would prohibit them from purchasing an IoT gadget, while 34.5% of people still want to adopt the newest technology breakthroughs despite cybersecurity concerns.

4.7 Awareness of Devices Vulnerabilities

Cybersecurity worries are growing as IoT adoption grows. The security of IoT devices is only seen favorably by 3.7% of individuals, leaving the other 96.6% as prime targets for hackers.

4.8 Belief in the power of IoT

In contrast to the 10.3% of respondents who said they didn't think IoT was valuable to them, 89.7% of respondents said they had positive impressions of it and could see how it was affecting their lives, businesses, and industries.

4.9 Most Popular IoT Devices

Smartphones, laptops, and tablets were recognized as the most popular Internet of Things (IoT) devices in 2016, with 100%, 97%, and 83% of the time, respectively (Figure 17). Every participant in the survey has a certain type of smartphone. Desktop computers and TVs are ranked as the next two most preferred devices by 75% and 65% of individuals who responded to the study, respectively. Gaming consoles and wearable technology came in second with 31% of the market. The additional devices are less common than these others, with radio coming in at 28%, health-related devices at 24%, kitchen appliances at 7%, and PDAs at 4%.

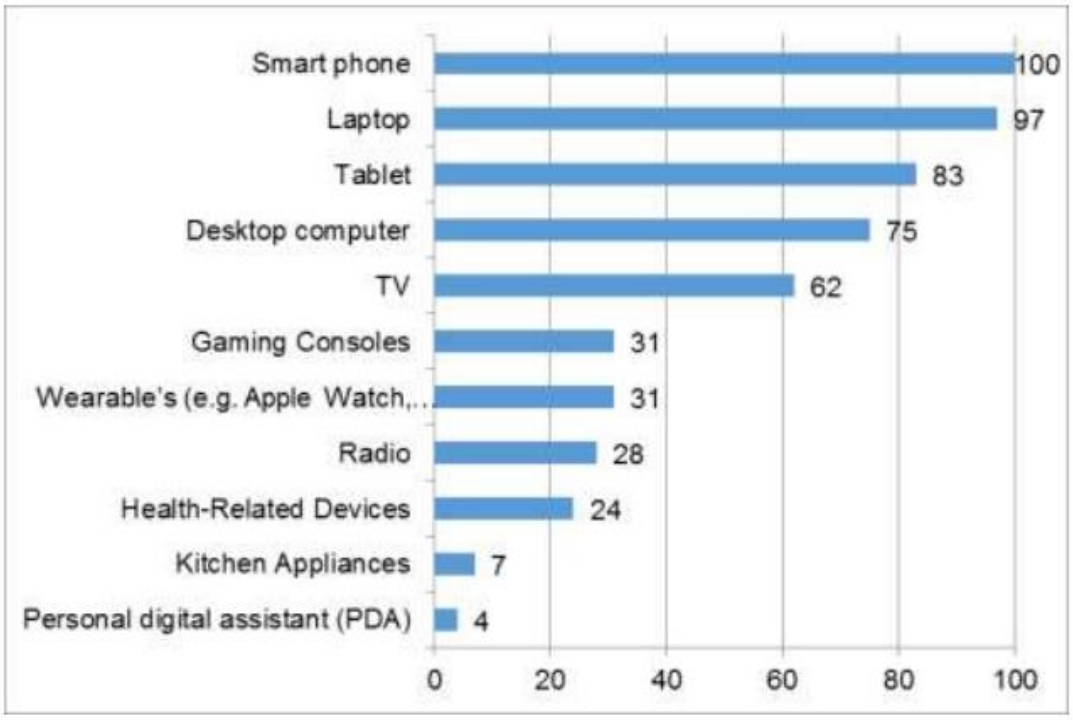

Figure 17. Most Used IoT Devices in 2016

4.10 Use of Credit/Debit Cards on the Internet

While 10.3% of respondents think using their credit or debit cards is safe, 89.7% of respondents are aware that they could be compromised. Considering that the problem of credit/debit card election hacking has not yet been solved, awareness of the problem is a big step in the right way.

4.11 Public Awareness of Credit Card Breach

10.3% of respondents think using credit or debit cards is secure, even though the fact that 89.7% of respondents are aware that this is a possibility. Even though the credit/debit card hacking problem has not yet been solved, awareness of the problem is a big step forward in the right direction.

4.12 IoT Manufacturers' Security Concerns

Users' awareness of cybercrimes has grown recently. Only 20.7% of respondents are happy with the security offered by IoT manufacturers, according to respondents, who represent 79.3% of the total sample. These respondents think that manufacturers need to do more to improve the security of their devices.

4.13 Most Sensitive Data in IoT

Everyone wants their personally identifiable information to remain private. It follows that it is not surprising that, as shown in Figure 18, 62.1% of survey participants believed that personal data was the most vulnerable type of information in the Internet of Things. Concerns regarding corporate information (10.3%), emails (3.4%), IoT devices (3.4%), and passwords (24.1%) were next in terms of frequency of mention (which will connect to so many devices as well as link them with a password).

4.14 Top Security Threat in IoT

Figure.19 demonstrates that the DDOS attack was viewed as the primary offender by a resounding majority of respondents (51.7%). Phishing is the second most prevalent option, with a citation rate of 48.3%. Nevertheless, 31% of the respondents brought up the ransomware epidemic among businesses. Like this, internal threats and attacks by nation-states were stated in 20.7% of cases, while cyber exploitation was highlighted in 27.6% of them.

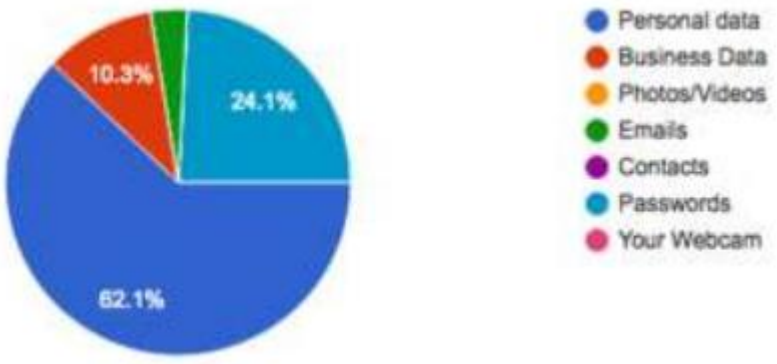

Figure 18. Most Sensitive Data in IoT

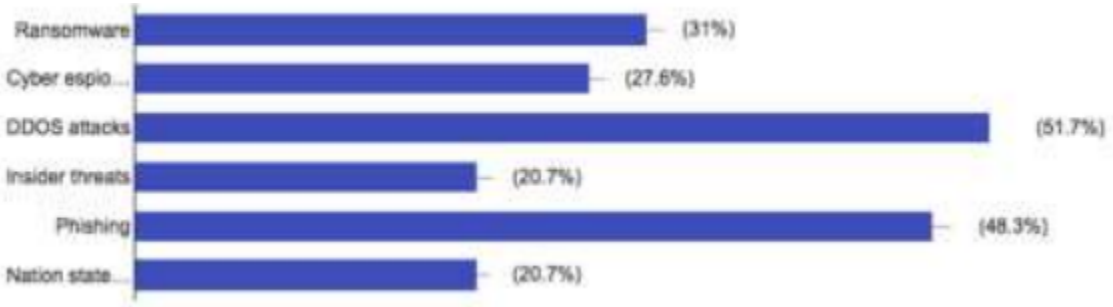

Figure 19. Top cybersecurity threats in IoT

4.15 Leading Sources of Cyber Threats

Malicious outsiders and accidental loss were recognized as the two leading reasons for data leakage, accounting for 31% and 17.2% of all cases, respectively. The results found in the literature closely match our outcome. Other attacks received 17.2% of all citations, making them the source that was cited the second most frequently. With 13.8% of all occurrences coming from malevolent insiders, they were the second most frequent source of breaches. Figure 20 shows that states and hacktivists were responsible for 10.3% of attacks.

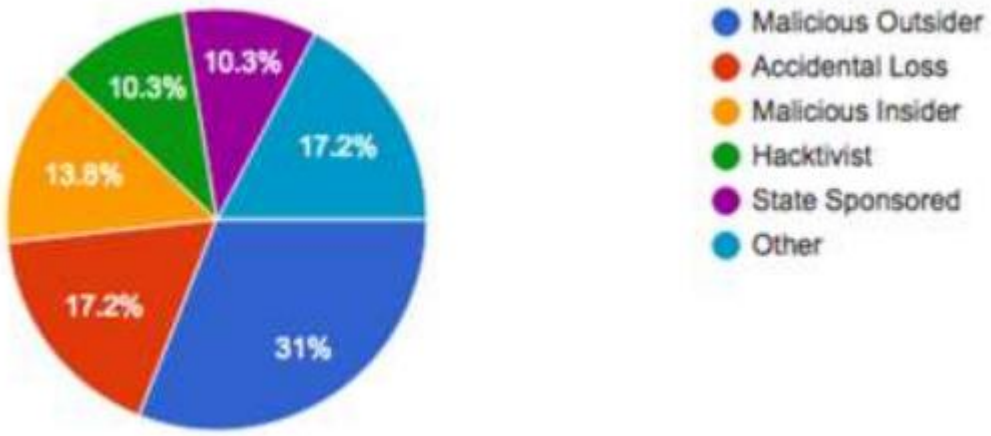

Figure 20. Leading Sources of Cyber Security Threats in 2016

4.16 Key Recommendations for IoT Users

Cybersecurity is the brain of our electronics [23]. By putting the following advised security measures into practice, device security will increase:

- As alternatives for two-factor authentication, choose the firewall, Touch ID, and HTTPS.
- The default login and password should be changed every 30 days using strong characters.
- Avoid revealing private information like your date of birth or home address unless it is necessary.
- Set your device's pin or password.
- Make logging possible on your device.
- Set notification preferences for security alerts to active.
- Make that the software or firmware of the gadget is up to date when updating it.
- Deactivate any unneeded physical ports.

FUTURE DEVELOPMENTS IN THE AREA

1. Construction of the Future IoT – commercial and academic efforts to design and build innovative new “things” that others will use
    - Devices
    - Materials and Material Processes
    - Automation and Artificial Intelligence
    - Software
2. Users of the Future IoT – industrial users and consumers who use these “things”
    - Industrial Plant Users
    - Consumers
3. Support for the Future IoT - services and collaborative efforts to support the ability of users to use the new “things”
    - Computing and Infrastructure
    - Government and Industry Guidance and Collaboration

CONCLUSION

The Internet of Things (IoT), which is now the technology with the quickest growth rate and is the subject of a lot of studies, is covered in this chapter. With its numerous applications, IoT simplifies people's life. Most IoT devices use the internet to perform this function, making them immediately susceptible to internet threats. As a result, to make the IoT environment secure, all IoT stakeholders must work together, adhere to standards, and improve IoT environment security.

Issue	Reasons for Issue	Prevention Steps
Poor Physical Security Weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present when USB ports or other external ports can be used to access the device using features intended for configuration or maintenance. This could lead to easy unauthorised access to the device or the data.	• Access to Software via USB Ports • Removal of Storage Media.	Ensure following • Data storage medium cannot be easily removed • Stored data is encrypted at rest • Device cannot be easily disassembled • USB ports or other external ports cannot be used to maliciously access the device • Only required external ports such as USB are required for the product to function • The product has the ability to limit administrative capabilities.
Insecure Software/Firmware Devices should have the ability to be updated when vulnerabilities are discovered and software/ firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/ Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. The inability of software/ firmware being updated means that the devices remain vulnerable indefinitely to the security issue that the update is meant to address. Further, if the devices have hardcoded sensitive credentials, if these credentials are exposed, then they remain so for an indefinite period.	• Encryption Not Used to Fetch Updates • Update Not Verified before Upload • Update File not Encrypted • Firmware Contains Sensitive Information • No Update functionality or OTA option	Ensure following • The device has the ability to update • Update file is encrypted using accepted encryption methods • Update file is transmitted via an encrypted connection • Update file does not expose sensitive data • Update is signed and verified before allowing the update to be uploaded and applied • Update server is secure.
Insecure Network Services This relates to vulnerabilities in the network services that are used to access the IoT device that might allow an intruder to gain unauthorized access to the device or associated data.	• Vulnerable Services • Buffer Overflow • Open Ports via UPnP • xploitable UDP Services • Denial-of-Service • DoS via Network Device Fuzzing	Ensure following • Services are not vulnerable to buffer overflow and fuzzing attacks • Only necessary ports are exposed and available • Services are not vulnerable to DoS attacks which can affect the device itself or other devices and/or users on the local network or other networks • Network ports or services are not exposed to the internet via UPnP for example
Lack of Transport Encryption This deals with data being exchanged with the IoT device in an unencrypted format. This could easily lead to an intruder sniffing the data and either capturing this data for later use or compromising the device itself.	• Unencrypted Services via the Internet • Unencrypted Services via the Local Network • Poorly Implemented SSL/ TLS • Misconfigured SSL/TLS	Ensure following • Data is encrypted using protocols such as SSL and TLS while transiting networks • Other industry standard encryption techniques are utilised to protect data during transport if SSL or TLS are not available • only accepted encryption standards are used and avoid using proprietary encryption protocols
Insufficient Authentication/ Authorization Its due to ineffective mechanisms being in place to authenticate to the IoT user interface and/or poor authorization mechanisms whereby a user can gain higher levels of access then allowed	• Lack of Password Complexity • Poorly Protected Credentials • Lack of Two Factor Authentication • Insecure Password Recovery • Privilege Escalation • Lack of Role Based Access Control	Ensure following • The strong passwords are required • Granular access control is in place when necessary • Credentials are properly protected • Implement two factor authentication where possible • Password recovery mechanisms are secure • Re-authentication is required for sensitive features • Options are available for configuring password controls

Issue	Reasons for Issue	Prevention Steps
Insecure Web Interface Web interfaces built into IoT devices that allows a user to interact with the device, but at the same time could allow an attacker to gain unauthorized access to the device.	• Weak Default Credentials • Account Enumeration • Credentials Exposed in Network Traffic • Cross-site Scripting (XSS) • SQL-Injection • Session Management • Weak Account Lockout Settings	Ensure following • Default passwords and ideally default usernames to be changed during initial setup • Password recovery mechanisms are robust and do not supply an attacker with information indicating a valid account • Web interface is not susceptible to XSS, SQLi or CSRF • Credentials are not exposed in internal or external network traffic • Weak passwords are not allowed • Account lockout after 3 -5 failed login attempts
Privacy Concerns It generated by the collection of personal data in addition to the lack of proper protection of that data. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.	• Collection of Unnecessary Personal Information	Ensure following • only data critical to the functionality of the device is collected • Any data collected is of a less sensitive nature • Any data collected is de-identified or anonymized • any data collected is properly protected with encryption • Device and all of its components properly protect personal information • Authorized individuals have access to collected personal information • Retention limits are set for collected data • End-users are provided with "Notice and Choice" if data collected is more than what would be expected from the product.
Insufficient Security Configurability It is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is apparent when the web interface of the device has no options for creating granular user permissions or for example, forcing the use of strong passwords. The risk with this is that the IoT device could be easier to attack allowing unauthorised access to the device or the data	• Lack of Granular Permission Model • Lack of Password Security Options • No Security Monitoring • No Security Logging	Ensure the ability to as following • Separate normal users from administrative users • Encrypt data at rest or in transit • Force strong password policies • Enable logging of security events • Notify end users of security events.
Insecure Cloud Interface Related to the cloud interface used to interact with the IoT device. Typically this would imply poor authentication controls or data traveling in an unencrypted format allowing an attacker access to the device or the underlying data	• Account Enumeration • No Account Lockout • Credentials Exposed in Network Traffic	Ensure following • At the first time setup, default usernames and password must be changed. • Password reset mechanisms should not be vulnerable. • There must be some mechanism to lockout account after few failed unauthorized access attempts • Cloud-based web interface is not susceptible to XSS, SQLi or CSRF • In wireless networks connection, IoT object must send their sensitive information in secure way. • Implement multi factor authentication.
Insecure Mobile Interface Similar to the Cloud Interface, weak authentication or unencrypted data channels can allow an attacker access to the device or underlying data of an IoT device that uses a vulnerable mobile interface for user interaction	• Account Enumeration • No Account Lockout • Credentials Exposed in Network Traffic	Ensure following • At the first time setup, default usernames and password must be changed. • Password reset mechanisms should not be vulnerable. • There must be some mechanism to lockout account after few failed unauthorized access attempts • In wireless networks connection, IoT object must send their sensitive information in secure way. • Implement multi factor authentication.

References

[1] B. Intelligence, "https://www.businessinsider.com/.," June 2016. [Online]. Available: https://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5.

[2] W. S. Christopher, "hbr.org," June 2013. [Online]. Available: https://hbr.org/2013/06/cyber-security-in-the-internet.

[3] C. J. R. a. W. Stephenson, "Cyberentity Security in the Internet of Things," March 2013. [Online].

[4] C. W. Axelrod, "Enforcing security, safety, and privacy for the Internet of Things," 2015 IEEE Long Island Systems. [Online]. Available: https://ieeexplore.ieee.org/document/7160214/authors#authors.

[5] Microsoft, March 2016. [Online]. Available: https://architectcorner.yolasite.com/products.php.

[6] Intel, February 2016. [Online]. Available: http://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html.

[7] Google, "cloud. google," Oct 2016. [Online]. Available: https://cloud.google.com/architecture/iot-overview.

[8] C. A. J. Lawrence Miller, "IoT Security for Dummies".

[9] . E. G. "A Study of Vulnerable Devices on the Internet of Things (IoT), in Intelligence and Security Informatics Conference,2014 IEEE Joint," 2014. [Online].

[10] A. Meloan, "business insider," Aug 2016. [Online]. Available: https://www.insiderintelligence.com/insights/internet-of-things-devices-examples/.

[11] K. O. Security, "Krebs on security," 29 November 2016. [Online]. Available: https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060.

[12] J. Murdock, "http://www.ibtimes.co.uk/," Feb 2016. [Online]. Available: https://www.ibtimes.co.uk/los-angeles-hackers-demand-3m-ransom-hospital-unlock-vital-files-1543962.

[13] B. News, "https://www.bbc.com," Oct 2016. [Online]. Available: https://www.ibtimes.co.uk/los-angeles-hackers-demand-3m-ransom-hospital-unlock-vital-files-1543962.

[14] A. Greenberg, "https://www.wired.com/," Aug 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[15] P. M. a. T. Grance, "www.nist.gov," July 2009. [Online]. Available: https://www.nist.gov/system/files/documents/itl/cloud/cloud-def-v15.pdf.

[16] A. Pasick, "https://qz.com/," April 2015. [Online]. Available: https://qz.com/393909/american-airlines-planes-are-grounded-because-their-pilots-ipads-have-crashed.

[17] S. HELTON, "https://21stcenturywire.com/," April 2015. [Online]. Available: https://21stcenturywire.com/2015/04/13/remote-control-aviation-expert-says-germanwings-9525-could-have-been-hacked-electronically/.

[18] D. Harwell, "https://www.washingtonpost.com/," May 2015. [Online]. Available: https://www.washingtonpost.com/business/economy/fbi-probe-of-plane-hack-sparks-worries-over-flight-safety/2015/05/18/8f75e662-fd69-11e4-805c-c3f407e5a9e9_story.html?utm_term=.66213252e33d.

[19] B. Krebs, "https://krebsonsecurity.com/," April 2016. [Online]. Available: https://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/#more-34596.

[20] Gemalto, "http://breachlevelindex.com/," 2016. [Online]. Available: http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf.

[21] none, "https://contenteratechspace.com/," [Online]. Available: https://contenteratechspace.com/8-common-cyber-attacks-in-the-iot/.

[22] E. M. 360, "https://em360tech.com/," [Online]. Available: https://em360tech.com/continuity/tech-features-featuredtech-news/top-10-cybersecurity-challenges-in-iot#:~:text=Top%2010%20Cybersecurity%20Challenges%20in%20IoT%201%20Cryptomining,Espionage%20...%208%20Updating%20Issues%20...%20More%20items.

[23] OWASP, "https://owasp.org/," [Online].