IoT security issues and possible mitigation

Reece Watkins
Computer Science Student
Colorado State University
Fort Collins Colorado
watkins.d.reece@gmail.com

Sam Howard
Computer Science Student
Colorado State University
Fort Collins Colorado
sam.how44@gmail.com

Aidan Franklin
Computer Science Student
Colorado State University
Fort Collins Colorado
aidanf@colostate.edu

***Abstract*—This paper will investigate security issues within the internet of things stemming from its theoretical conception to the modern day implementations. It will then provide examples highlighting the main security risks in the industry today and possible future mitigations. Finally, this paper will discuss and explore how these solutions would help create a safer, more secure internet of things for the future.**

Index Terms - botnet, internet of things, IoT, mitigation, security, vulnerabilities

I. Introduction

The internet of things (IoT) is the term loosely used to describe the interconnection of computing devices embedded in everyday objects. This technology has been implemented in one form or another in almost every industry ranging from internet-connected ovens alerting when dinner is ready to battlefield soldiers helping to locate the positions of enemy troops based on the triangulation of gunfire. It has revolutionized how both humans and machines interact with each other, allowing for a more comfortable and efficient world. As with many technological advancements, security has been an aspect of the IoT that has been drastically underdeveloped and underutilized. Multiple substantial security risks exist in the current implementations of the IoT and their protocols including unencrypted data and data privacy. In order to create a safer and more secure future, we must understand the vulnerabilities of the IoT and be able to create realistic, effective solutions.

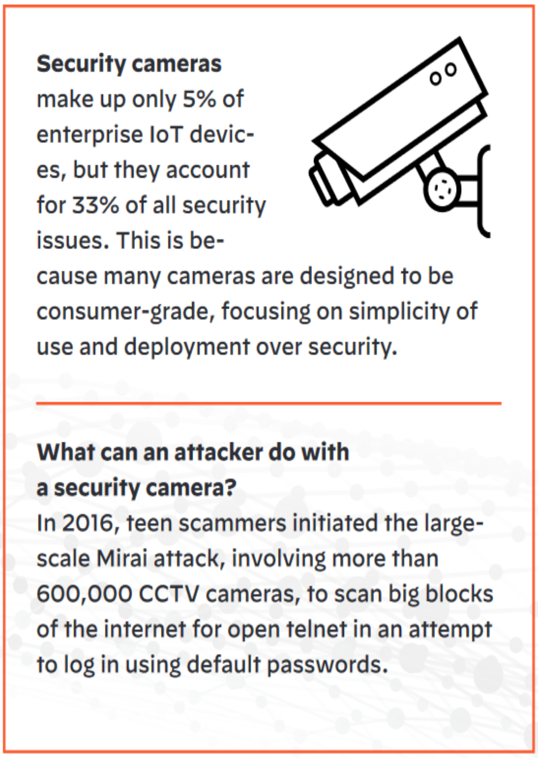
II. History

The first use of a connected device to solve a problem was in 1982 when a small group of Carnegie Mellon students attached some ARPANET-connected sensors to a coke machine to monitor its inventory. Throughout the late 1990s and early 2000s many individuals and companies created devices that were capable of interfacing over the internet and required less user-to-user interaction and relied more on device-to-device communications.

An example of this was the widespread development and adoption of RFID (radio frequency identification) technologies. In 2003, the United States Army deployed RFID tech in their Savi program to enable smart supply-chain and asset tracking capabilities [1]. In addition, in 2003 Walmart also deployed RFID tech throughout their chain for better logistics handling and product tracking [1]. These RFID deployments are an example of the early stages of IoT -- letting devices communicate with each other and minimizing the need for human interaction. A vast majority of these groups and devices did not think about security vulnerabilities in their implementations. Despite being a creative and logical solution, the idea of an interconnected network of computers and sensors generating and communicating data didn't gain mainstream attention until the early 2010s with the release of popular consumer products such as the Nest thermostat and Ring doorbell [2].

These early inventions paved the way for a whole new type of in-home gadget: the internet connected device. With the rise of smartphones in the early 2010s, many IoT devices could now be controlled from anywhere with an app or website since most people had a mobile computer in their pocket. The main focus in the IoT boom was pushing out new products quickly rather than diligently working on security. As a result, the lesson was learned that massively successful products didn't need good security to go mainstream. As a consequence of these precedents, bad security practices are still rampant in today's IoT tech. A 2020 report concluded that "98% of all IoT traffic is unencrypted, exposing personal and confidential data on the network" [3].

On October 21, 2016, a massive attack was launched on Dyn, an internet service provider, using an IoT botnet called Mirai. The malware spread from device to device logging into each using default usernames and passwords. Eventually, the vulnerabilities were patched, however alarming questions were raised about how mainstream devices had security issues as prominent as product-wide default usernames and passwords. The Mirai botnet was but one of many sophisticated attacks utilizing the expansive nature of the IoT. Others have targeted almost every conceivable weakness from specific device holes such as privilege escalation and brute forcing to eavesdropping and social engineering attacks. A chain is only as strong as its weakest link, therefore learning from past mistakes and creating a holistically secure IoT is the only way to secure a safer internet for the future.



Security cameras make up only 5% of enterprise IoT devices, but they account for 33% of all security issues. This is because many cameras are designed to be consumer-grade, focusing on simplicity of use and deployment over security.

What can an attacker do with a security camera?

In 2016, teen scammers initiated the large-scale Mirai attack, involving more than 600,000 CCTV cameras, to scan big blocks of the internet for open telnet in an attempt to log in using default passwords.

Fig. 1. Security issues relating to cameras

III. Current

Today's implementation of the Internet of Things is motivated similarly to David Nichols' development of the connected Coca-Cola machine -- automating monitoring and task execution to ease the lives of users (or steal all their users data). This approach naturally leads to positive and negative consequences. One benefit of IoT is its inherent simplicity. Nowadays there exist many consumer- and commercial-grade sensors, monitors, switches, microcontrollers, and microcomputers that can be standalone or integrated into an existing network. An example of this can be visualized as such: a homeowner installs a sensor to monitor soil and water conditions in their garden and connects the system to their existing local area network generated by their router. For the sake of this example, the sensor is not communicating back to any server or accessing the wider internet -- it is isolated within their LAN and only accessible by the user. The installation of this remotely-accessible sensor by the homeowner provides value to them and simplifies their gardening procedure -- exactly what IoT is supposed to provide for the consumer. This instantiation of a "miniature IoT" is an example of a safe and effective use of such technology because it avoids introducing security vulnerabilities that IoT devices commonly bring. However, most IoT implementations aren't as straightforward and minimally connected.

Many consumer-targeted IoT devices communicate with servers from their devices' manufacturers in addition to the user. This stream of data is aggregated by the manufacturers for analysis in usage statistics and error logging, for continual monitoring of software status and update potential, and for sale as "anonymized" data to data brokers. All of these uses by the IoT manufacturer are avenues for inappropriate security protocols and vulnerabilities. This in turn opens the door for personal data exploitation and breaches of privacy. An example of this can be seen by Amazon's Ring doorbell cameras. The Ring connected doorbell camera was first developed and released under the name Doorbot by Jamie Siminoff in 2013. Ring was built to allow users to receive a video stream captured by a camera on their front door for the sake of laziness, privacy, and security of its users. This is a useful service provided by a device in the IoT, but its poor implementation will compromise their security while also being valuable. The video streams captured and sent by the Ring camera to the user were sent in an unencrypted form and that unencrypted data was also sent to Amazon's Ring servers. It took 8 years, until the middle of 2021, for the Ring services to offer an opt-in option for end-to-end encryption, and this in itself is a half-step measure.

The majority of consumers who will be using the Ring camera IoT device either will not be properly educated and informed on information security, will not know the proper steps to better protect their data or connected devices, or will not care enough to remedy these vulnerabilities shipped and supported by the manufacturers. These facts have a larger impact than one might think. Companies like Ring and others generally don't care about security unless it affects their profit or public image. The apathy and ignorance surrounding security from consumers allow companies to have the same attitude. The people who care for security are generally too little and too late, with most people only caring about security after a hack has already taken place. This in turn promotes a certain attitude in tech companies and allows them to only implement security when something has already gone wrong, rather than baking the security into the product from the get go. While this may seem bleak, the attitude of the people is changing. As time goes on, the people will continue to care more and more about security. This is because data exploitation is rising and data privacy is becoming more and more of a virtue. Consumers caring more about security will force the companies to do the same, this trend will also force the government to take more action.

If there is not enough competition or public pressure, companies will not naturally change their business ways. Government regulations can hinder profits, but when implemented correctly, they protect consumers. Currently, there is not a national IoT set of standards for operation in the United States. Individual states such as California have specific privacy laws surrounding online data stating that “Californians have the right to know what personal information an organization is collecting about them”[9]. In order to protect data privacy around the world, bigger entities would have to enact similar laws such as the US federal government. One specific example is if US lawmakers require encryption by default for all potentially compromising data. This simple step would massively increase data privacy as currently anyone on a network can monitor the traffic and see the unencrypted data including passwords and other sensitive information. The government centered solution is not perfect, but combined with other mitigations it would increase the general security and data privacy on the IoT.

Although there is a lot that companies can do to their specific products that would create a safer network, like enforced encryption. Many issues within IoT security stem from the inherently wide structure and heterogeneity of devices and protocols on the IoT. Since the concept generally evolved naturally to fill a technological niche, there is not a main entity in control setting the standards for technical interactions of nodes from different places. This makes a one size fit all security solution next to impossible to create for security vulnerabilities exploiting the conglomeration of communication between different devices in different settings.

In order to address these concerns, some have broken down the concept of the IoT into 3 layers to get a better understanding of the structure of the IoT. The three most commonly cited layers are the perception layer, network layer, and application layer [4]. The perception layer consists of information gathering devices such as sensors and edge devices and is the main layer that connects with the physical world. The network layer refers to the connections between smart objects, sensors, servers, and other network devices. Finally, the application layer where the user interacts with the IoT. This includes the applications the user interacts with to control smart devices, but also smart houses if talking about the IoT on a larger scale than a home.

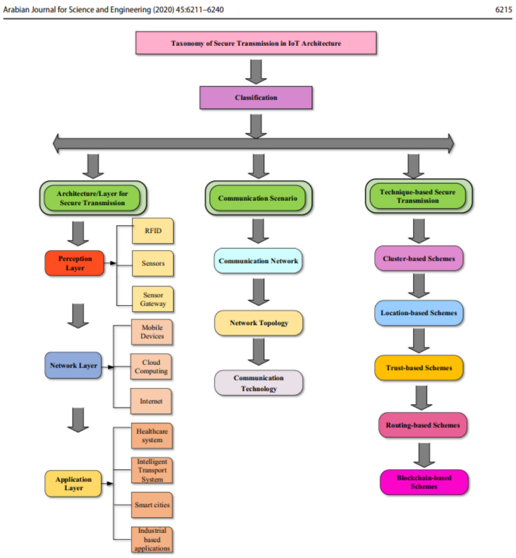


Fig. 2. Architecture of IoT transmission

Each of these layers provide an avenue of attack on IoT devices. The perception layer is the physical devices themselves. Insecure protocols, generic access credentials, and unfettered remote access all increase vulnerabilities within the devices. The network layer is possible to attack using man-in-the-middle attacks, and this is exacerbated by the industry-wide lack of encryption of data in motion. Finally, the application layer is ripe for exploitation. Most users control their IoT devices using proprietary software or applications from the manufacturers. A common adage is perfect code with no bugs is impossible to create. This applies to the software and applications created and sold by the device manufacturers. Common vulnerabilities in such software and applications are: improperly secured databases, improper access control, and plain unintended functionality of the code. All of these can be exploited by malicious users.

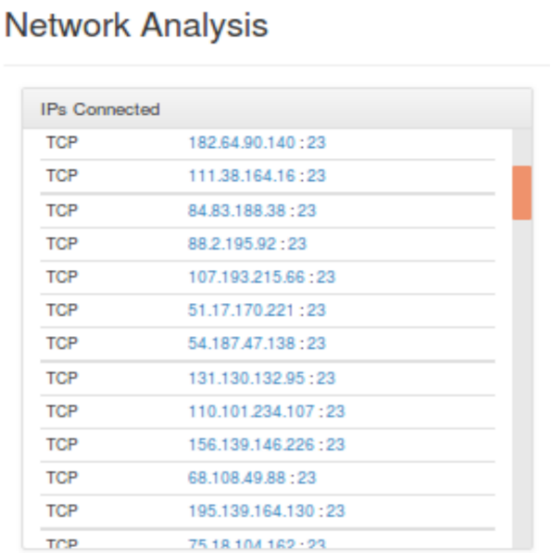
Since the IoT is a term to describe the interconnection of devices, sensors, and humans rather than a tangible thing, its natural evolution did not follow an ideal outline. Rather, the idea emerged and companies began integrating these types of devices into consumer products to make a profit. Since all industries began to adopt the idea, there emerged a multitude of different devices and protocols to service each need. This creates a large problem for researchers as it makes a one size fits all security solution much more difficult, if not impossible, to construct [5]. It only takes one small oversight to create a vulnerability exploitable on the entire network.

In order to decrease production costs and energy consumption, many smaller IoT devices -- especially within the perceptual tier -- were designed with only enough processing power and battery life to complete their basic functions. In fact, “Most IoT devices use a single-threaded microcontroller with a 2 MB Random Access Memory

(RAM) that is insufficient to run a full-fledged operating system or even a simple anti-virus”[6]. This means that for security researchers, all prospective solutions and mitigations must take into account the limited resources available to them [5].

There is both a benefit and a downside to developing IoT devices with limited computing functionality. Consider the garden sensor mentioned in the example above. It would be extraneous and unnecessary for such a device to communicate with other sensors or process and transmit large data streams like video or audio recordings. The only functionality it arguably needs is the capability to monitor the conditions in the soil using electric sensors and to send small data blocks to the users interface. By limiting the scope of functionality it reduces potential abuses of the devices and their data. If the physical capabilities of simple IoT devices do not allow for computing abilities beyond what is necessary, then it cannot be leveraged into malicious abuses. This is both a good and bad thing. It will mean that there will need to be specific, dedicated devices that are only designed and used for a singular task, therefore there will need to be many independent devices doing their one thing. This will introduce extra complexity into the IoT ecosystem -- and complexity is the opposite of security -- but this is a possible avenue for vulnerability mitigation. One way to reduce the complexity would be to introduce a hub into a consumer’s IoT ecosystem that will be a main controller/conglomerate of all the users data from their IoT devices.

An example of the problems potentially introduced by extra functionality in IoT devices can be seen with the proliferation of the Mirai botnet attacks using Telnet connections to DVR boxes and surveillance cameras [7]. This malware was written to autonomously expand its infected botnet by enlisting compromised devices to probe for vulnerabilities in internet-facing devices such as unchanged, default passwords or unrestricted firewalls and connection tables.



Network Analysis

IPs Connected	
TCP	182.64.90.140 :23
TCP	111.38.164.16 :23
TCP	84.83.188.38 :23
TCP	88.2.195.92 :23
TCP	107.193.215.66 :23
TCP	51.17.170.221 :23
TCP	54.187.47.138 :23
TCP	131.130.132.95 :23
TCP	110.101.234.107 :23
TCP	156.139.146.226 :23
TCP	68.108.49.88 :23
TCP	195.139.164.130 :23
TCP	75.18.104.162 :23

Fig. 3. Outbound Telnet connection attempts from a Mirai botnet infected device

Another issue with the restriction of resources available on IoT devices is the fact that in many of these devices there is no separation between user and kernel privileges and they often only have one unrestricted account. This user-interface being capable of any function on the device allows for potential unintentional capabilities from the user account. If this user account is compromised, the attackers will have full control over the abilities of the device. This can again be mitigated by limiting the ability of the device. In general this solution helps improve the security of the IoT by ensuring that a single node or device is only capable of doing what is necessary for its function.

IV. Future

In a world where efficiency and autonomy are valued so much, it is no wonder that devices connected to the internet are going to thrive. The IoT market is expected to grow from its current value of around 800 billion dollars to a whopping 15 trillion dollars by 2025 [11]. As IoT markets and their devices grow, so will the impact of their security vulnerablilities. Given the current state of IoT security vulnerabilities, it’s hard to imagine a future where personal privacy is respected by our IoT devices. In the tech industry, security is never the top priority and is often left on the back burner. There are many possibilities for what the future will look like. With the advent of smart homes, smart cities, and smart everything, the IoT has emerged as an area of incredible impact, potential, and growth, with Cisco Inc. predicting to have 50 billion connected devices by 2020 [12].

One hypothesized solution for increasing the IoT’s security is to use blockchain technology, specifically the public ledger which provides immutability and integrity to the data on the network. This structure allows for true decentralization which greatly increases the network's redundancy and fault tolerance. Generally, companies try to centralize all their data and proprietary software behind their company intranet to protect against unauthorized use and exfiltration, but this is intrinsically insecure because it allows for a single point of failure to compromise the data.

There are multiple ways to integrate the blockchain into the IoT, however the main security ideas behind most of the implementations revolve around using various proof algorithms such as Proof of Work, Stake, Authority, and many others to validate the transactions on the network [8]. Transactions are the communications and data shared between nodes on the blockchain network. Once an immutable record of transactions has been created, other parties know for certain the data they see is accurate and that any given certain party is who they say they are assuming the integrity and construction of the blockchain in question is concrete. One of the major problems with implementing a blockchain similar to the ones behind Bitcoin and Ethereum is that they are much too labor intensive for many of the small devices that make up the lower levels of the IoT. This constriction is already one of the reasons more secure algorithms aren't in deployment for modern IoT devices.

In order to create a feasible blockchain that can connect and secure all the devices on a network, the blockchain must be stripped of all non-essential properties surrounding coins and even change from slow, resource intensive validation methods like Proof of Work to faster methods such as Proof of Stake and Authority [9]. Integrating a blockchain to bolster IoT security is a radical yet partially needed solution. Blockchain has survived rigorous testing and almost a decade of scrutinous dissection, proving itself to be flexible and secure making it a viable candidate for an IoT security solution [8].

The future of IoT security is dependent on what steps we choose to take today to make it a safer place. Governments will need to take action in order to create a secure framework for how IoT devices and communications are created, maintained, and improved upon. Corporations must make ethical decisions to put their customers first and defend their data from those with malicious intents. Individuals will have the responsibility to educate themselves about data privacy and how they can protect themselves. On the whole, it is a monumental task to retroactively secure the IoT, but the possible futures that exist without these drastic actions overshadow any doubt that the effort is futile.

V. Conclusion

The IoT has changed the way we interact with devices allowing for a more interconnected world. Many home gadgets are now interfaceable from a mobile phone. One can change the temperature, check the door, and even preheat the oven while away from home. The IoT also allows for companies to streamline logistics and maintain efficiency by simultaneously checking and communicating between different nodes on the network, all contributing to a task. Unfortunately, many IoT devices lack even very basic security measures including encryption, nonstandard account credentials, and minimizing extraneous mutability [8]. These lapses create the potential for large attacks or data breaches that can affect millions of people.

If changes don't happen quickly, another big attack like the Mirai botnet is not just probable, it is inevitable. Furthermore, with the expansion of cyberwarfare, government sponsored hacking groups will be able to easily access devices and steal data from potentially anyone with an unprotected IoT device. It is hard to predict the future of an industry as large and fast paced as the IoT. The entire trajectory could be changed with a few simple decisions, however within 2-4 years we are likely to see the following:

(1) More and more companies will begin to defaultly encrypt data as the public's interest in protecting their privacy grows.

With the Senate's fairly recent "Anti-Encryption" bill, there has been a counter culture movement advocating for better data privacy. Furthermore, large data breaches will most likely happen from at least one IoT company and will make headlines. These factors will cause companies to slowly begin to encrypt data as a default for good PR but also mitigating the risks that accompany sending raw data over the internet in a world where anyone with a computer and bad intentions could access it.

(2) The rates of botnet DDOS attacks will continue to rise

Botnet DDOS attacks have been exponentially rising in recent years. Hackers can access and tweak existing viruses to exploit new vulnerabilities in IoT devices [7, 8]. These attacks have been frequently used for economic and even geopolitical purposes and have the ability to shut down large parts of the internet with a sufficient enough attack.

(3) Internet-connected chips will begin to be implanted in humans, cementing the new field of IoT health

There already exist hundreds of types of medical implants, but we will begin to see some of these providing real time feedback to medical professionals. One example is an implant that would provide continuous monitoring of glucose levels in the bloodstreams of diabetics. These devices could automatically communicate with doctors and be adjusted without a physical visit. When these chips are implanted, there will be a possibility of hacking someone's body and there will be numerous legal and ethical battles over real-life remotely-controlled health devices.

(4) Growing security concerns will cause the government to regulate the industry

The United States federal government is notorious for not addressing issues until massive damage has been done. The attacks of September 11, 2001 sparked massive changes in the way air travel was done. The TSA was created a mere 69 days after the terrorist attacks and now nobody can believe how relaxed security was in the preceding years. Furthermore, it took a mass poisoning of Tylenol bottles in Chicago in 1982 for medicine to have the bare minimum of an anti-tampering seal. In the next 2-4 years, there will be a large data breach that may affect members of the government, personally or economically, who have the power to implement restrictions and will do so. These restrictions will drastically change the structure of the IoT, requiring default encryption and full disclosure from IoT companies about their business practices and data handling ability.

(5) The field of IoT security will become its own distinct field of academic study

As mass acceptance of the IoT continues to gain prominence, many related subfields will grow as well. There already exist degrees available for the blockchain and blockchain management and the technology is a mere 13 years old. It is only a matter of time until formal education about the IoT is being offered as a concentration or its own distinct degree. In the age of the internet, ideas travel at light speed, and higher education must keep up both for their business model to attract new students and research as well as creating a next generation of knowledgeable, informed adults who can create solutions and keep the IoT safe and functional for everyone.

The IoT has transformed the way humans interact with the internet and the world around them. Never in history have data and communication become so integrated into our everyday lives. Unfortunately, there are massive security concerns surrounding the security of the IoT which have the potential to irreversibly alter the direction of the industry. Researchers have toiled over mitigations to these problems, however nothing will change unless the government, companies, and individuals involved in the IoT decide to take the actions necessary to secure its future. Actions such as governments creating regulations to ensure companies don't cut corners, practicing clean code and ensuring a device can only do what its meant to and implementing new technologies such as the blockchain will allow the IoT to reach its full potential of creating a smaller, more interconnected world.

References

[1] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," 2014 International Conference on Science Engineering and Management Research (ICSEMR), Nov. 2014, doi: 10.1109/icsemr.2014.7043637.

[2] K. D. Foote, "A brief history of the internet of things," *DATAVERSITY*, 18-Mar-2022. [Online]. Available: https://www.dataversity.net/brief-history-internet-things/#. [Accessed: 31-May-2022].

[3] Unit 42, Palo Alto Networks, "2020 Unit 42 IoT Threat Report," 2020. [Online]. Available: https://iotbusinessnews.com/download/white-papers/UNIT42-IoT-Threat-Report.pdf

[4] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[5] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.

[6]S. R. Zahra and M. A. Chishti, "A generic and lightweight security mechanism for detecting malicious behavior in the uncertain Internet of Things using fuzzy logic- and fog-based approach," *Neural Computing and Applications*, Jan. 2022, doi: 10.1007/s00521-021-06823-9.

[7] X. Zhang, O. Upton, N. L. Beebe, and K.-K. R. Choo, "IOT botnet forensics: A Comprehensive Digital Forensic Case Study on Mirai botnet servers," *Forensic Science International: Digital Investigation*, 29-May-2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281720300214. [Accessed: 21-Jun-2022].

[8] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[9] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917634.

[10]A. Aljeraisy, M. Barati, O. Rana, and C. Perera, “Privacy Laws and Privacy by Design Schemes for the Internet of Things,” *ACM Computing Surveys*, vol. 54, no. 5, pp. 1–38, Jun. 2021, doi: 10.1145/3450965.

[11] “Internet of things statistics for 2022 - taking things apart,” *Dataprot*. [Online]. Available: https://dataprot.net/statistics/iot-statistics/. [Accessed: 31-May-2022].

[12] M. binti Mohamad Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Computer Networks, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.