Final Report -02

SECURITY IN INTERNET OF THINGS
A1812485

Introduction to Computer Science Topic and Motivation

What is the Internet of Things?

The internet of things(IoT) is a concept for an ecosystem of electronics that aren't traditional computing devices but are web-enabled smart devices that use embedded systems, to collect, send and act on data they acquire.

How Big is IoT?

There are more than 50 billion IoT devices as of 2020, and these devices generated 4.4 zettabytes of data last year. By comparison, in 2013 IoT devices generated a mere 100 billion gigabytes. The market is estimated to rise to $14.4 trillion from $1.6 trillion by the end of 2025. (Josh Fruhlinger, 2020)

Examples of IoT devices

From a simple sensor that monitors the temperature of the room to smart home appliances are a part of IoT. IoT has a wide range of applications in consumer, industrial, infrastructural, and military sectors. Some popular IoT devices are smart bands, automated vacuum cleaners, autonomous robots at various industries, and autonomous vehicles. They all gather some kind of data and transmit the information over the internet and receive process outputs. One application, I am most fascinated with is Ocean of things. The idea behind it is simple, to have an internet of things across a large ocean area. The device will be equipped with a sensor that can detect the vessel's activities. The data is then sent to a cloud-based network to recognize unusual activities. (Mr. John Waterston, n.d.) Such innovations in the field of IoT fascinate me the most and motivate me to do some research on this topic.

Introduction to the Challenge and Motivation

Just like any other emerging technology, IoT also comes with lots of benefits and risks. One such risk that this report focuses on is security. As soon as an item becomes 'smart, it becomes open to being hacked. Hackers can choose one of the components of the ecosystem to introduce malware and to compromise the system. It raises many data privacy concerns as well. There have been many cases of data leaks, breaches, hijacking, and flooding. (Table 1) One such case is when hackers hacked into an automated vacuum cleaner. To get the virtual map it drew. The map was then sold to the thieves and they successfully executed a robbery. Such an attack is categorized as a data breach attack. (Table 1). These attacks happen at different phases of IoT architecture and table 1 contains the categorized data. It is a pressing issue and research are looking for ways to prevent it. Imagine a large-scale attack on the ocean of things. The hacker can

manipulate the data to show shadow vessels in some areas and the focus of the naval forces change and create an opening for enemy ships to enter.

Current Challenge Solutions

According to Mikhail Gloukhovtsev, there are three main domains under security - **trust, data confidentiality, and privacy**. (Image 1)

- **Trust** in IoT relates to the trustworthiness of IoT components throughout their lifetime. For example, a trustworthy firmware is that many embedded processors provide process encapsulation via memory virtualization. One current solution to this problem is to have trusted platform modules. Also, use of blockchain to develop trust in transactions and identity management to have secure and integrated management of data.
- **Data confidentiality** in IoT is related to the encryption of the data. It ensures that the data should not be compromised and integrity should be maintained via advanced encryptions. One current solution to this problem is Homomorphic encryption. It has recently gained attraction in the field of IoT and is effective in maintaining data confidentiality.
- **Privacy** is a significant concern. It involves the security of personal information and the ability to control what happens to the data. The level of privacy from the device is based on the type of information it collects. Privacy is currently being assured using data usage control.

Apart from these, there are various other solutions that revolves around these concepts to maintain security. Some of them are Managing updates to the device and to the installed IoT application, monitor and detecting, Authentication and authorization, and securing control applications.

The above problems are addressing the solutions quite well. However, there are some limitations to these solutions. One way to ensure the trust is to use blockchain as a mode of transaction. This can be a problem as several countries around the world have not identified cryptocurrencies as a legal way of making transactions yet. Further, a solution like identity management and using homomorphic encryption solutions to maintain data confidentiality are some good solutions and have recently been developed by the researcher. However, researchers have deemed homomorphic encryption as incredibly slow and non performant, and even after a year of work it still needs to be developed further. Data usage control, monitor and detecting systems, managing updates to the device, and having high security in the device are costly and time-consuming making them not feasible to use at a large scale. Additionally, one of the key characteristics of IoT is minimal human intervention, and using Authentication and authorization for each command makes it less preferable to use. Imagine a smart home that requires you to enter an authentication key each time you turn on the air conditioner, the autonomous vacuum cleaner, or opening the blinds. It can be irritating at times and the user might prefer to manually do things.

Solution To Challenge

There are two potential solutions to this challenge:

1. **Searchable Encryption** - Just like homomorphic encryption it is a way to maintain data confidentiality. Researchers have done some research around it however, it is currently not being used in the field of IoT. Searchable encryption allows a party to outsource the storage of its data to another party (a server) in a private manner while maintaining the ability to selectively search over it. There are three entities involved in this process. The data owner, who is the customer using the IoT device. The cloud server is a 3rd party responsible for storing the data. Finally, the data user or the service provider requires the data to be processed and then sends it to the device for output. The data owner encrypts the data using an application and specifies what data the data user can access. This helps in maintaining the privacy and the component has better security so the vulnerable information is much more difficult to hack. The data users can search for keywords or patterns in encrypted data for processing it. While keyword searches can be performed, the stored data cannot be decrypted and it is not possible to gain any knowledge of the underlying plaintext. Let's take the case of the same automated vacuum cleaners. However, in this case, searchable encryption is being used. The maps of the house cannot be accessed by the company. The customer asks the vacuum cleaner to clean the living room. The command is then sent to the company. The company then searches the encrypted data in the cloud server for the living room floor map. Then the map is sent to the device, decrypted and then the vacuum cleaner executes the command based on the decrypted data. The whole process makes it difficult for a hacker to hack the data. It can be divided into three phases. First, uploading phase, the data owner encrypts the data and uploads the encrypted data to the cloud server. Next, in the queuing phase, if the attributes satisfy the access structure, the data user could generate a trapdoor of some substrings and send the trapdoor to the cloud server. Lastly, the pattern matching phase, where the cloud searches the data using a matching operation between the cipher text and the trapdoor and returns the query to the data user. (Image 2) Some concerns are surrounding its application in IoT still need to be. IoT devices are often lightweight computing devices with low computing resources. It is difficult for these devices to perform heavy decryption operations and even if some devices are capable of doing that it would be really slow. This problem can be solved and this is what the second solution focuses on.
2. **Having a local server-** The world is looking forward to a future in IoT where we will be surrounded by several smart devices and will be dependent on them for our daily lives. Present security solutions don’t only make the devices more expensive but also make it difficult to use those devices. Enter passwords for each command you give to your devices and remembering different keys to all the devices makes it difficult to use these devices. Similarly, having the same level of security for each

device increases the cost of the device, and to tackle that we can have a local server that manages the communication with the main server at the company. A local server makes it easy to implement the current solutions. In the case of encryptions, both searchable and homomorphic one major limitation was the speed of decrypting and encrypting the data. If the local server does that work for the devices it can be faster and more efficient. Additionally equipping the local server with more trustworthy firmware makes it more secure and then the device can then have a lighter security system as the only device they can communicate to is the local server. The local server can be responsible for managing updates to the device and the installed IoT application, authentication, and authorization. At last, it will be easier to monitor and detect millions of servers rather than a billions individual of devices.

Discussion

The solution presented above still needs a lot of work to develop many milestones that need to be completed before they can be implemented in IoT. One of them is to convince the existing companies to collaborate with these 3rd party entities. It is one of the most crucial parts as many companies might not agree to store the data on a separate cloud server and allow a local server to process heavy data for their devices. Also, it is important to convince them that the server will have high security because hacking can not be eliminated but we can prevent it. If the server gets hacked all devices can be compromised. The company of the device will also be at blame and they wouldn't like that. To build this trust a proper architecture is required that is good enough to convince them.

Conclusion

IoT has revolutionized the way we use the internet in our daily lives. We see IoT devices almost everywhere from our homes, offices, shopping centers, schools, airports, and many other places to provide us with secure and on-demand services. However, security remains a challenge even after a year of work. There are many solutions to this problem that companies have implemented and many that are being researched to tackle future needs. The report addressed some of these solutions and their limitations. Further, some potential solutions were also discussed that can help provide better security. Searchable encryption proved to be one of them. It not only prevents hacking activities but also helps maintain data privacy. Another solution to the challenge discussed was having a local server. This can help support all the other solutions and make it easier to implement them. Both the solution proved effective against the given problem and if they are developed and implemented they can overcome the challenge.

References

Josh Fruhlinger, 2020. *What is IoT? The internet of things explained.* [Online]

Available at: https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

[Accessed 25 OCTOBER 2021].

Mr. John Waterston, n.d. *Ocean of Things.* [Online]

Available at: https://www.darpa.mil/program/ocean-of-things

Mikhail Gloukhovtsev, 2018. IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS. *DellEMC.*

XiSun, 2020. *Substring-searchable attribute-based encryption and its application for IoT devices.* [Online]

Available at: https://www.sciencedirect.com/science/article/pii/S2352864820302546

[Accessed 27 october 2021].

Li, S., 2019. *Searchable Encryption Scheme for PersonalizedPrivacy in IoT-Based Big Data.* [Online]

Available at: https://www.researchgate.net/publication/331489779_Searchable_Encryption_Scheme_for_Personalized_Privacy_in_IoT-Based_Big_Data

[Accessed 27 october 2021].

Tawalbeh, L., 2020. IoT Privacy and Security: Challenges and Solutions. *applied sciences ,* p. 17.

Appendix

Table 1

Attack Taxonomy According to the IoT Process Phases

Phase	Attack/Threat	Description
Data Perception: Various types of data collectors can be used. The device may be a static body (body sensors or RFID tags) or a dynamic vehicle (sensors and chips).	Data Leakage or Breach, Data Sovereignty, Data Loss, Data Authentication.	Data leakage can be internal or external, intentional or unintentional, involving hardware or software.
Storage. If the device has its own local memory, data can be stored. In the case of stateless devices, the data can be stored in the cloud.	Attack on Availability, Access Control, Integrity, Denial of Service, Impersonation.	Availability is one of the primary security concerns. Distributed denial of service (DDoS) is an overload condition that is caused by a huge number of distributed attackers.
Intelligent Processing	Attack on authentication	An IoT solution provides data analysis and intelligent services in real time.
Data Transmission	Channel security, session hijack. Routing protocols, flooding.	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
End-to-End Delivery	Man or machine. Maker or hacker.	Delivery of processed data on time without errors or alteration.

Image 1

Security Challenges and Requirements in Internet of Things

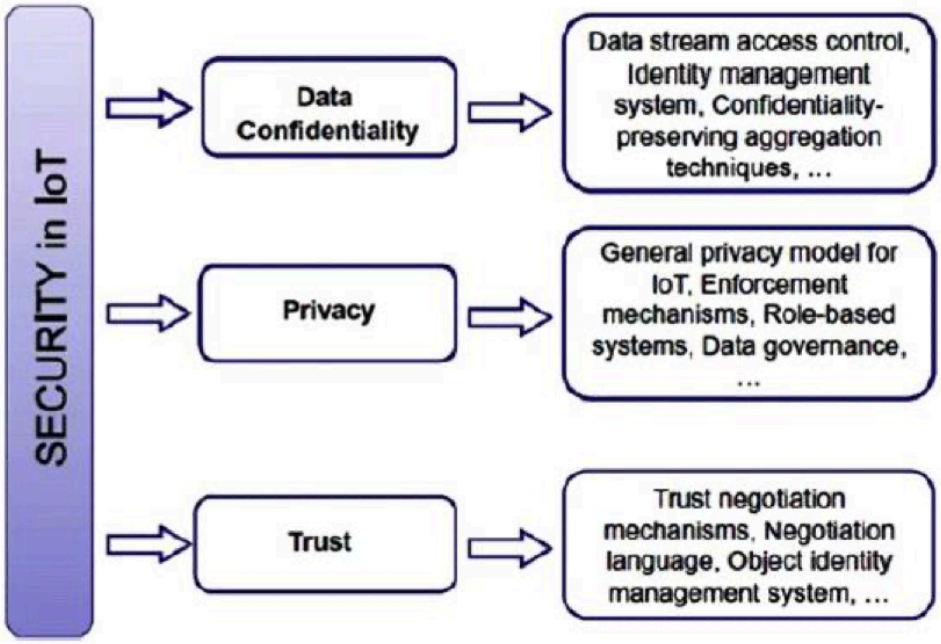

Image 2

System model.