A Comprehensive Study on Different Types of Security and Privacy Challenges in the Field of IoT

Kartikeya Uniyal[1] And Dr. Goldi Soni, Professor[2]

[1]*Student (B.Tech) Department Computer Science and Engineering, Amity University Chhattishgarh.*

[2]*Department of Computer Science and Engineering, Amity University Chhattisgarh*

Abstract

The idea of connecting normal devices such as appliances, machines, sensors etc to the internet has become a mainstay in our modern world. From your refrigerator being able to know what food you consume to your car knowing where the closest café or petrol pump is. The idea had been in the Zeitgeist since the late 1960s but still seemed far away since even 20 years ago.

The integration of IOT on every possible mechanical, electrical and compute device seems to be a definite future. With dreams of a smart home which can anticipate its owner's needs and desires and adjust accordingly being realized with the combination of Artificial Intelligence by technologies such as Google Home.

The logical conclusion of this is to convert billions of our normal devices into smart devices which are connected, that will cover and take over almost every aspect of our lives. The IoT consists of smart devices or machines that employ sensors to record data that is used to interact and communicate with other machines, objects or infrastructure. Since all of this data is collected and recorded, it can be further processed and used as good information to 'command and control' itself to make our lives better.

Keywords - Internet of Things,, Security in IoT, Attack Surface, Man-in-the-Middle Attack, Trusted Execution Environment.

1. Introduction

Internet of things abbreviated IoT is a system which is based on the concept of connecting digital, mechanical and computing devices to a network or the internet to send and receive signals while being able to act by itself or by executing commands from the cloud.

The Cloud consists of a network interconnected with various Data Enters which hold vast amount of servers, that is connected to the internet. They can perform a large variety of tasks and easily service the public, governments, military and Universities.

The most common private cloud providers are Google, Amazon, Microsoft etc. These provide hosted services for compute, storage and application development.

2. History of IoT

An IoT Framework comprises of 'devices' that can communicate with each other and the cloud with some kind of connectivity. When the information is sent to

the cloud it is processed and after that an operation may or may not be committed on it.

As an example, a caution is sent to the cloud by the temperature sensors stating a high ambient

temperature, while the cloud processes and decides to drop the temperature inside the home.

It was Kevin Ashton, in 1999 using 'Internet of Things' as a title for a presentation on a sensor project that the term was first used, which got adopted swiftly.

The concept of IoT originates in 1832, after the invention of the first electromagnetic telegraph, which allowed direct communication between the two devices with the usage of electric signals. The phrase although came about in the mid to late 90s. However the true history of IoT begins after its invention during the mid to late 1960s..

The First Internet of Things device was invented during the 1970s by a group of students at Carnegie Melon University. They had created a way by which the campus Soda vending machines would report on its contents via the University network and save them a trip if it was out of soda. They also installed micro switches to count the number of cans and report whether they were warm or cold.

John Romkey was the first one to connect a toaster to the internet in 1990. A group of students in 1991 at the University of Cambridge, to find out the amount of coffee left in their Computer Lab's pot, used a web camera.

The 2000s were the time when consumer electronics with IoT started to get introduced in the consumer market. LG Electronics in 2000 sold the world’s first refrigerator connected to the internet. Which had features such as the ability to order groceries over the internet or make calls.

One of the First conferences on ‘Internet of Things’ was held in 2008 in Switzerland.

3. How it Works

A common ecosystem of IoT contains sensors/devices, network(connectivity), Data Processing and UI.

- Sensors: In IoT sensors are used to detect changes in physical circumstances and then provide a signal that represents the change in magnitude of the variable being monitored.

Sound, light, heat, air/water pressure, distance even video are a few examples that can be monitored using sensors. Some examples of sensors are as follows:

- ◦ Pressure sensors
- ◦ Motion sensors
- ◦ Level sensors
- ◦ Image sensors
- ◦ Proximity sensors
- ◦ Water quality sensors
- ◦ Temperature sensors

- Connectivity: The Data from the smart devices needs to be either processed locally or sent to the cloud. This were connectivity comes in, connecting various smart devices with each other and to the internet.

There are various ways of connecting smart devices with each other and the internet such as Wife, Bluetooth, NFC, Ethernet etc.

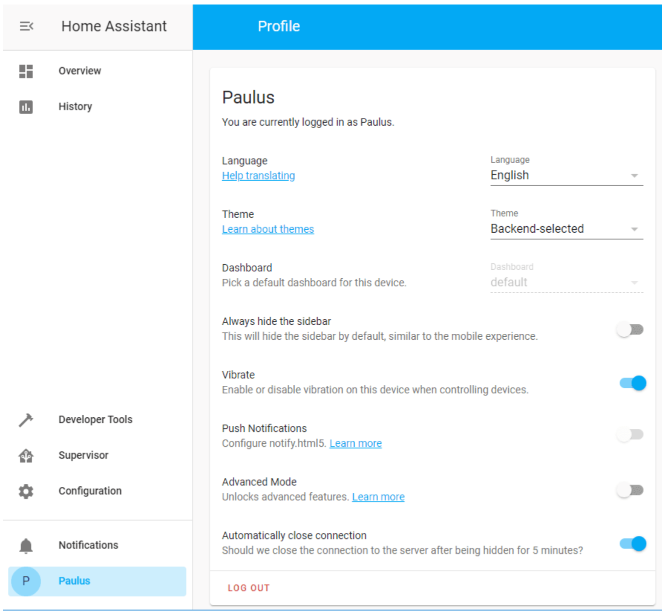
Each of these has its own trade-offs between bandwidth, range, power consumption.

- Data Processing: When Data is received in the cloud, it needs to be processed and handled.

The level of processing could be very simple, like checking whether the air pressure or temperature has not crossed the limit. It could also require massive amounts of compute, like using it to identify objects using the camera sensor.

The user is not brought into or informed of this until an intervention is required.

• User Interface: After the Data is processed, it needs to be sent to the end user. This can be a caution signal or a status update sent via E-mail, MS or a notification on your phone. For example a text based status update of your temperature.



Paulus

You are currently logged in as Paulus.

Language
Help translating
Language: English

Theme
Learn about themes
Theme: Backend-selected

Dashboard
Pick a default dashboard for this device.
Dashboard: default

Always hide the sidebar
This will hide the sidebar by default, similar to the mobile experience.

Vibrate
Enable or disable vibration on this device when controlling devices.

Push Notifications
Configure notify.html5. Learn more

Advanced Mode
Unlocks advanced features. Learn more

Automatically close connection
Should we close the connection to the server after being hidden for 5 minutes?

LOG OUT

An IoT system may also have a UI Client which allows the end user to pro-actively monitor the system. It could be a web-based one that can be accessed easily on the web browser.

There is might also be other ways to monitor and modify various parameters of the system using other methods remotely, such as a Mobile Application easily accessible on your smart phone. An example would be changing the temperature of your home using a mobile application on your phone while you're at work.

Most Systems also allow usage of rules which can modify parameters automatically. Requiring no intervention from the end user. A rule could be created in a smart home that it would drop the temperature to 200 C when it detects a specific ambient temperature.

Moreover, these systems can also be used to notify both you and the authorities during unusual activities in your home as recorded by the camera sensors or any other systems that could help, as set by the predefined rules.

4. Applications Of IoT

IoT is playing an important in various fields, with more and more fields adopting it to increase productivity, analytics, etc.
Some fields in which IoT plays an important role are as follows:

- Monitoring of Environments
- Infrastructure Management
- Manufacturing
- Agriculture
- Energy Management
- Medical and Health-care
- Building and Home automation
- Transportation
- Metropolitan-Scale deployments
- Consumer Applications

Infrastructure Administration
IoT devices are used for the observation and control of various important infrastructure frameworks, such as extensions, rail road tracks, bridges.
An IoT system could be utilized for checking any occasions or changes in basic conditions that can trade off well-being and increment hazard.

Manufacturing
IoT has emerged as a potential solution to the problems of the manufacturing sector. IoT has the potential to increase efficiency and productivity while reducing costs. An IoT system integrated into a manufacturing plant can greatly reduce downtime while giving opportunities to optimize production..

Health-care
Previous to the introduction of Internet of Things, doctor-patient interactions were relegated to visits, telephone and text communications. IoT devices became the first way doctors and hospitals could continuously monitor their patients' health enabling them to make recommendations. ITT-enabled devices have made remote monitoring in the health-care industry possible and empowering physicians to deliver superlative care. Since patients can be remotely monitored hospital stay lengths could be radically reduced, IoT devices would also help save health-care costs.

5. Advantages of IoT

Some advantages of IoT systems are as follows:

• **Data Collection**: Once your IoT network is up and running it will collect and store large amounts of data on-site or on the cloud. The information provided by these devices is a lot, like sensory or status-information, from the amount of milk in your fridge to the time you return home.
• **Instant Data Access:** Almost all IoT devices and ecosystems have a feature where you can access the devices and your data off-site via the internet, using a laptop, smart-phone or tablet.
• **Improved data-based decision making:** The greater the information you posses the better chances of you making a better decision. Whether it is a simple call of changing the colour of the lights or a systemic decision as needing to alert staff of changes in processes or productivity to work out.

- **Reduction in maintenance costs:** IoT as an emerging technology can be very useful for maintainers in production or usage in heavy equipment.

As an example, IoT devices can be told to pro-actively send status alerts so that maintenance can be scheduled before any problems arise.

- **Improved Quality of Life:** Almost all applications of IoT result in improved quality of life changes for the end user, while being accessible from the palm of your hand.

6. Disadvantages of IoT

Some disadvantages of IoT systems are as follows:

- **Compatibility:** At the moment, there is no standard that help on compatibility for IoT. This causes hardware from different manufactures to often malfunction or refuse to communicate with one another, forcing the user to either lock in to using their manufacturer's devices or a small list of compatible ones.
- **System Complexity:** A large IoT system is a very complex system with various points of failure. Although when working any IoT system can handle its tasks easily, the system is not invulnerable and issues such as either a bug in software or a power outage can cause catastrophic damage.
- **Security and Privacy:** Since IoT devices are interconnected, any of them can be targets of over the network or physical attacks. Cybersecurity being of paramount importance to develops and manufacturers of IoT systems, doubts about security and privacy remain.

Think of the information generated by all IoT devices and systems such as household appliances, industrial machines, medical products such as pacemakers.

- **Connectivity and Power:** An IoT system is basically a network of electronic devices connected to the Internet. Which means it needs to have around he clock electricity and a connection to the internet. Having IoT devices without redundancies would make the whole IoT infrastructure crash during a power or connectivity outage.

A modern smart home could be easily shut down if the Wi-Fi Network is disrupted or compromised, causing your smart devices to shut down or start malfunctioning.

7. IoT Security Challenges and Problems

Driven by low-cost computing and the cloud, the Internet of Things has become of the most ubiquitous connected technology with billions of instances deployed over the globe. Such proliferation of this technology has caused a vast amount of security challenges. There are large volumes of flaws regularly detected in IoT systems.

IoT security vulnerabilities are found in everything from smart grids, smart home devices to vehicles and watches. Researchers have frequently found it easy to hack web cam systems.

As shown above, issues with security of IoT devices is a major and valid concern that when ignored can lead to disastrous situations. Some major challenges in IoT security are as follows:

- **Problematic Access Control:** Services offered by an IoT device or system should only be accessible to the owner and/or people in the immediate environment whom permission has been given by the owner, this however is often unsuccessfully enforced by the security system of the device.

IoT devices may also in their default configurations trust the local network so that no authorization is required. This becomes an regular issue as these devices are often connected to the internet as well, making it vulnerable to the rest of the world.

Another common problem is that many of these devices hold similar default passwords ("admen", "password123") across model ranges and brands. Since the firmware and default settings are usually the same often that being the case, the credentials are public knowledge, making access to these devices by a third party a non-issue.

IoT devices often have only one privilege level or account, both exposed to the user and internally. Meaning when privilege is gained there is no barrier to further access control, the whole device gets compromised.

- **Large Attack Surface:** Each new connection a system makes increases its attack surface by providing more opportunities to be attacked. Each new service on an IoT device offers over the internet the more it increases its attack surface.

A device may have open ports that have services running which are not in use, an attack against that service and the device could easily be prevented by shutting down the service. Development and debug services such as Tenet SSH or a debug interface may be required during development of the device but if unneeded must be removed.

- **Outdated Software:** As security vulnerabilities are discovered and resolved, constant software updates are necessary for an IoT device. It is also important to distribute these devices with the latest up to date software. They also must have an update functionality that would make software and security updates possible post deployment of the device.

There has been instances of a security vulnerability being patched but a year later that exploit remains successful as devices have not been updated.

- **Encryption:** When a device sends/receives data in plain text, all data being exchanged is can be obtained by a Man-in-the-Middle attack(Mitm). Sensitive data such as login credentials can be obtained by anyone capable enough to access a network point between a device and its endpoint.

An example of a common problem that occurs is usage of a less secure protocol like http instead of https which is the encrypted version of the protocol.

Even if encryption is present, it is necessary that it is complete and configured correctly, for example a device may fail to verify the authenticity of the other party, it can be intercepted via Mite even though the communication was encrypted.

- **Vulnerabilities in Software:** Software bugs may be able to affect functionality of a device in such a way that the developer had not intended, making the attacker able to execute his own code over the device.

The first step in fixing this issue is by the acknowledgment that fixing software bugs is an important step in securing devices.

Security vulnerabilities like bugs is impossible to avoid during developing software, mitigations may include following methods well known that either reduce vulnerabilities or the possibility of one.

- **Trusted Execution Environment:** Almost all IoT devices are and use general computer hardware to run specific software, making it easier for attackers to install their own software that grants them functionality that the developers did not extend. A common result is the attack installs a software that performs a D Dos attack.

By intentionally limiting the devices' functionality and the software it can run, the possibilities to abuse the devices reduces. This may reduce the D Dos attack ineffective since it can no longer connect to arbitrary target hosts.

To stop the device from running software aside from the vendor's a cryptographic hash is used to sigh the software. Since only the vendor has the private keys only he is able to successfully run software on the device.

To further restrict the running of code on a device, the implementation of code signing to the boot process can be followed, with the help of hardware. This is a difficult to process to implement with various devices getting 'jailbreak' such as Microsoft Box, Sony Play station, Apple i Phone due to faulty code signing implementations.

- **Vendor Security Support:** The reaction of the vendor when and if security vulnerabilities are found determines its impact.

The vendor must play a role to receive input on potential vulnerabilities, while also acting to develop the mitigation and the deployment of it. The Vendor security support often depends on whether the vendor has a process in place to deal with security issues.

The consumer primarily perceives the increase in vendor security support through communication, when a vendor does not provide contact information or instructions to proceed during one, it does not help mitigate the issue.

- **Privacy Protection:** Consumer devices store sensitive information, devices are deployed on a wireless network store their own passwords and other sensitive information. Cameras deployed in a network if accessed by attackers can result in serious privacy violations.

IoT devices must after the end user's consent correctly and securely handle sensitive consumer data, this must be applied to on site and cloud storage as well.

The also plays an important role in privacy protection, other than a malicious attacker, the vendor or any other third party software might be responsible for a privacy breach.

The vendor or service provider of an IoT device might decide to gather information from consumer behavior without explicit consent for various purposes.

Several instances of IoT devices such as Smart TVs' have been observed listening to conversations within a household.

- **Intrusion Detection:** When attackers successfully gain access to a device, it goes unnoticed. These devices are not equipped to measure excess network and compute usage. The ability to either log or send an alert automatically.

This results in making the users assume the device is functioning as it should but instead is compromised and unable to be make any mitigations.

- **Physical Security:** If the attackers have physical access to the device, they can open and attack the hardware. For example, if the memory can be read, any and all protection software can be bypassed. Commonly devices also have a debugging contact, accessible after opening the device providing the attacker with more opportunities.

Since physical attacks can only be used on a single device by a single attacker at the same time while also requiring physical interaction, the scope when compared to en-mass network based attacks from the internet becomes pretty low.

8. Conclusion

The continued proliferation of Internet of Things systems, has the potential to greatly improve the availability of information which should be able to transform industries, companies, organizations and even governments over the world.

As such finding ways to leverage IoT systems for these organizations will be factored into their strategic objectives regardless of the focus of any industry.

Challenges in security and privacy remain that require vendors and developers to work closely to provide protection from software bugs and security vulnerabilities while also remaining a consent based partnership regarding data collection from the end user.

This technology although still new in the time-line of computing has a lot of potential in providing many advantages to any field its applied to. More research and development time must also be spent in the securing of these systems and devices.

9. References

i. Naeini, Pardis Emami, et al. "Privacy expectations and preferences in an {IoT} world." Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). 2017.

ii. Nakamura, Emilio Tissato, and Sérgio Luís Ribeiro. "A privacy, security, safety, resilience and reliability focused risk assessment in a health iot system: Results from ocariot project." 2019 Global IoT Summit (GIoTS). IEEE, 2019.

iii. Sfar, Arbia Riahi, Zied Chtourou, and Yacine Challal. "A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges." 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C). IEEE, 2017.

iv. Zhou, Jun, et al. "Security and privacy for cloud-based IoT: Challenges." IEEE Communications Magazine 55.1 (2017): 26-33.

v. Andrade, Roberto Omar, et al. "A comprehensive study of the IoT cybersecurity in smart cities." IEEE Access 8 (2020): 228922-228941.

vi. Bilogrevic, Igor, and Martin Ortlieb. "" If You Put All The Pieces Together..." Attitudes Towards Data Combination and Sharing Across Services and Companies." Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. 2016.

vii. Nurse, Jason RC, Sadie Creese, and David De Roure. "Security risk assessment in internet of things systems." IT professional 19.5 (2017): 20-26.

viii. Kunz, Immanuel, Angelika Schneider, and Christian Banse. "A Continuous Risk Assessment Methodology for Cloud Infrastructures." 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2022.