IOT Security Concerns and Mitigations

Maneesh Devanaboyina

Northwest Missouri State University, Maryville MO 64468, USA
S545394@nwmissouri.edu

1 Introduction

Every day, more devices are connected to the Internet of Things, and by 2025, the globe will have 64 billion IoT gadgets.This expansion has many benefits as it can change people's daily lives and affect the entire world. Smart lighting can reduce overall energy consumption and reduce electricity bills. Within a few years, cars will be able to communicate with each other using IoT. Healthcare and Modern Infrastructure everything is going to work on IoT.

However, with all of these advantages comes risk, as the growing number of connected devices provides additional access points for hackers and cyber thieves. Recently Hackers turned down the entire power grid and thereby causing a complete blackout with a cyber attack. Scientists are working hard to solve these problems and are trying to find new methods to provide more security.

1.1 Goals of this Research

In the last several years, the number of IoT application domains has exploded. While many are still in the early stages of development, several economically viable application scenarios cover a variety of domains. This paper describes the security issues of IoT and different techniques used by hackers to enter the IoT systems and what are being followed by the scientists to defend against these malicious attacks.

2 Related work

To create "A Smart World," the Internet of Things (IoT) plays a critical role in bringing users, computing systems, and objects with sensing and actuating capabilities together in unprecedented ways. IoT is being used in major sectors like hospitals, education, and industry and also to monitor environmental changes. Usually, the systems are more secure nowadays and highly Encrypted. It is very difficult to attack any system. The Challenges in IoT according to Shadi Aljawarneh and team[1] are confidentiality, Authentication, Access, Security and Privacy, Reliability, Heterogeneity, Performance, and Large Scale. To deal with these issues they must have to follow strong firewalls, Strong encryptions.

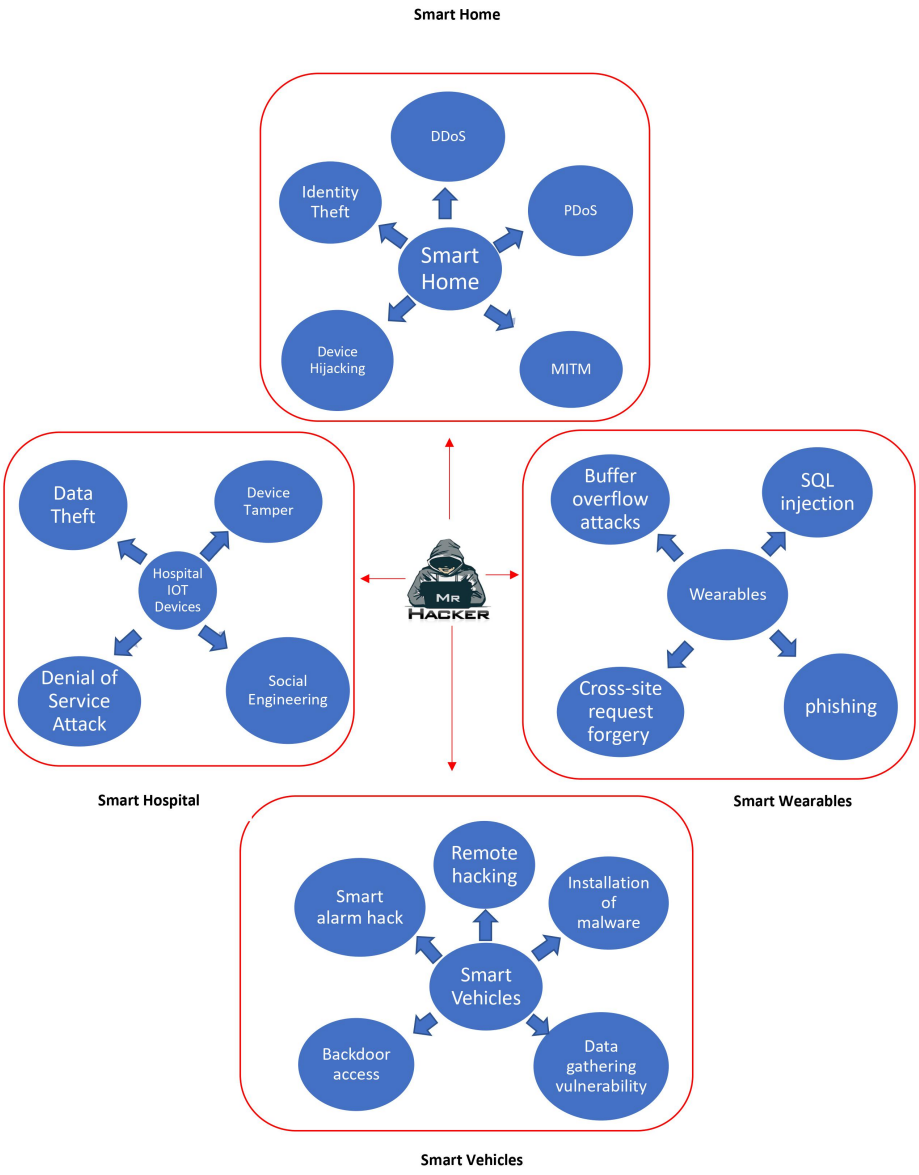

Fig. 1. Hacking techniques used by hackers for different IoT systems

3 IOT Applications

IoT is being employed in a variety of systems, particularly in Houses, hospitals, industries, monitoring the environment, smart gadgets, smart power grids, smart cars etc. Nowadays the entire house is connected to the IoT Devices. As a result, the residence may be monitored from anywhere in the world. Doctors are integrating sensors and equipment in the health sector in a similar way to monitor patients' health in real-time. Currently, the government is monitoring environmental changes, such as detecting Earthquakes and sending updates to citizens before risks. And there are many more.

So, to what extent can we rely on IoT? The processing of such large amounts of data exposes security flaws. If a data breach occurs, hackers would have complete access to all devices and will be able to utilize and control even government institutions, which would be a great threat to the country.

3.1 Attack Types on IOT Devices

As per Jibran Saleem and team[8] there are mainly 4 types of attacks which can be done on IOT devices.

1. Software Attacks
2. Network Attacks
3. Physical Attacks
4. Other Attacks

1.Software Attacks: These are the most common attacks nowadays on IoT Devices. Hackers will send a malicious piece of code to people, and as the target clicks on that code, they can take over the entire system. This is a virus attack. Some of the common Software Attacks are Virus Attacks, Logic Bombs, Worms, Trojan Horse

2.Network Attacks:

These days, denial of service (DoS) assaults and spoofing are very widespread. These tactics offer a significant network danger to software applications. These applications and connected IoT devices can be exploited by hackers. Some of the common Network Attacks are Node Capture, Node Manipulation, Routing Attacks, Denial of Service Attacks, Message corruption, etc.

3.Physical Attacks: Physical attacks are a sort of cryptanalysis, which is the study of information systems to uncover hidden elements of devices and systems by exploiting implementation peculiarities. Some of the common attacks are reverse engineering, physical probing, malicious damage, and decoys.

4.Other Attacks: In addition to the above attacks, there are other attacks performed by hackers to hack into the systems. Some of these attacks are Force Botnet Bondage, Timing Analysis, Ciphertext Attacks, and Man in the Middle Attacks.

4 Hacking techniques used by hackers for different IoT systems

Hackers will utilize the following attacks to break into IoT networks, as stated in the preceding section. Smart Houses, Smart Hospitals, Smart Wearables, and Smart Cars are among the most prevalent targets for cyber-attacks these days.

4.1 On Smart Homes

[5] IoT devices are mostly used in households in today's society. People are transforming their entire homes to run on Internet of Things (IoT) gadgets. They can control everything from the TV to the fan to the alarms, security cameras, and lockers with a single click or by using voice commands. A hacker can take control of the entire house if they find a little flaw in any of the components. They might even get their hands on their social security numbers and bank accounts, posing a major threat. The following are some of the most common smart home hacking efforts:

1.Identity Theft: As soon as the hacker gains access, they attempt to steal the person's identity. They'll use those credentials to gain access to their bank accounts and credit card information without their knowledge. After obtaining your identity, they can commit fraud and other crimes.

2.DDoS(Distributed Denial-of-Service): [5]For this attack, hackers employ many computers or machines to flood a target resource. Hackers can temporarily or indefinitely disrupting the services of a who are connected to the network, this sort of attack seeks to make a machine or network resource unavailable to its intended consumers. The smart home installation would be disturbed and unavailable if the communication between the components is jammed.

3.PDoS(Permanent Denial of Service):

A PDoS is the same as the hacking technique described above, in that it is triggered via hardware disruption. One strategy for launching these types of attacks is phlasing. Because so many businesses are shifting to the cloud these days, these attacks have become all too typical. This assault mostly damages the IoT Device physically.

4.MITM(Man-in-the-Middle Attack): [7]As per Rahimi and the team, this type of attack takes place between two victim nodes that communicate with one another. The attacker poses a false node as a valid node on the other side of each side. While communication is taking place between two victim nodes, the fake node in the center is capturing and understands the private information of both parties. The victims of this attack are unaware of the phony node, which makes it extremely dangerous.

5.Device Hijacking: By hijacking a device, an attacker gains control of it. These attacks are difficult to detect since the attacker does not change the device's basic functions. In addition, a single device has the potential to infect all smart gadgets in the home.

4.2 On Smart Hospitals

[3]The IoT is slowly encroaching on hospitals these days. Doctors are implanting sensors to the human body and monitoring the patients' health status remotely in real-time. They are even conducting operations remotely using the devices. Hackers can use the below attacks on Internet-connected devices to kill someone remotely or get valuable information about the patient:

1.Data Theft: Nowadays, data is everything. As previously stated, hackers can obtain personal information, including patient health information, through data theft attacks.

2.Device Tamper: Trying to interfere with a device's software or hardware is known as "device tampering." "Tampered State" refers to a gadget that has been tampered with. A "rooted device," a "device infected with malware," or a "device being observed by some malicious piece of code' are all examples of tampered states.

3.Social Engineering: Other severe dangers to smart hospitals include social engineering attacks like phishing and luring. Attackers take advantage of individuals to get beyond the target organization's defenses, and once inside, criminals can engage in a variety of destructive behaviors, ranging from data theft to sabotage.

4.Denial of Service Attack:

Due to a DoS attack, the entire system is brought down, and the device is no longer accessible to the intended users. Hackers send large amounts of data to the server at once, raising traffic and causing the system to crash. These types of attacks are all too typical these days.

4.3 On Smart Wearables

Small devices embedded with smart sensors and actuators that may be worn on the wrist, draped around the neck, or fastened to the body are examples of IoT-enabled wearable devices. They are used by a variety of industries, including entertainment, healthcare, sports, and the military. Bluetooth Low Energy (BLE) or other short-range communication technologies are typically used to connect them to smartphones and tablets. The devices must be secured from vulnerabilities that may occur as a result of their greater connectivity, particularly given the possible consequences of their unregulated use within businesses.[9].

1.Buffer overflow attacks: A buffer is a temporary storage region, while a stack is a data structure in which the most recently added item is the first deleted. As per Rahimi and the team, [7]in this assault, attackers make use of program flaws to breach code or data buffer boundaries. In reality, to cause the system to overflow, attackers place a large string of data in a specific location.

2.SQL Injection: [5]By inserting malicious code into a SQL statement and manipulating it, these types of attacks can provide an attacker with unauthorized access to a database. In a database, it can also be used to add, amend, and delete records. Once a hacker gets access to it, they can easily track, call, message, or even know a person's health condition.

3.Cross-site request forgery:

A online security weakness known as cross-site request forgery (CSRF) allows an attacker to deceive users into executing tasks they don't want to accomplish. It allows an attacker to get around the same-origin policy, which prevents websites from interacting with each other. These attacks are unintended.

4.Phishing: In this attack, attackers pose as legitimate users or approved organizations to obtain sensitive information from users, such as passwords and credit card numbers[7]. Smartphones and other mobile devices have smaller screens, making it more difficult for users to spot phishing emails and harmful websites.

4.4 On Smart Cars

The connection of objects in the outside world via wireless networks such as Wi-Fi, Bluetooth, NFC, or GSM introduces more risks that could impact the integrity and confidentiality of data as well as individuals' private lives; nowadays, many research efforts have been devoted to the definition of the various threats made during communications.[11]

1.Remote Hacking: Accessing a vehicle remotely by hackers is called "Remote Hacking." They can take full control of the vehicles. According to security experts, car manufacturers may have failed to incorporate effective cyberattack precautions into some situations. Threat actors could hack a vehicle to acquire sensitive data controlled by its components, either for sabotage or simply for personal gain.

2.Installation of malware: Hackers with access to a smart car's onboard computer may be able to install infected apps, spyware, and other security threats that inject malicious code and give the hacker complete control of the vehicle. By gaining access to the Jeep Cherokee's infotainment system, hackers were able to gain access to the vehicle. Others were able to insert a USB flash drive into the dashboard of a vehicle.

3.Data gathering vulnerability: If a manufacturer uses a third-party backend service to capture data or save data over the cloud, hackers may be able to gain access to the car.

4.Backdoor access: Mobile phone usage has skyrocketed, posing a severe cybersecurity danger to both individuals and enterprises. Because mobile phones have fewer security safeguards, a person with a weak phone who connects it to their smart car could give a hacker backdoor access through their phone.

5.Smart alarm hack: Researchers discovered serious cybersecurity flaws in two of the world's most popular smart alarm systems, affecting more than 3 million automobiles. Hackers were able to detect the weakness through penetration testing, allowing them to take advantage of the smart car's alarm system. They were able to unlock the car and obtain personal information about the owner as a result of this.

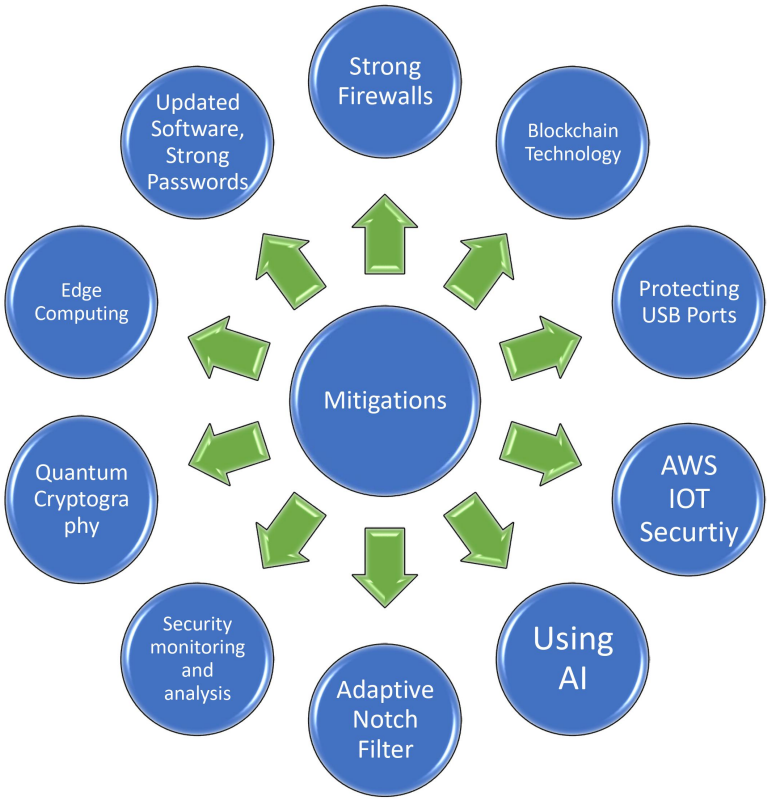

Fig. 2. Mitigations for the IOT attacks.

5 Mitigations

Scientists are striving to combat the hazards posed by hackers. They are developing new approaches, utilizing cutting-edge technology, and developing solutions for all possible threats. Manufacturers, Cloud providers, appropriate government agencies, researchers, and individual users all need to take active actions to secure IoT assets, given the varied spectrum of security threats mentioned in the previous section.[9]

5.1 Using Updated Software and Strong passwords

One thing to keep in mind is to create strong passwords. Hackers will find it difficult to break into systems if the password contains alphanumeric characters of sufficient length. Users should also update their software as often as feasible. This is because whenever a system is updated, there may be vulnerabilities. The company uses software updates to correct the issues.

5.2 Using Strong Firewalls

Firewalls are critical for protecting IoT devices. Internal and external threats, as well as network attacks such as DDoS and MiTM, are all protected by strong firewalls. As a result, in order to safeguard IoT devices, firewalls must be kept strong.

5.3 Using BlockChain Technology

[4]Blockchain is now being used in a variety of fields. By utilizing blockchain technology, we can make IoT systems more secure. The integration of IoT with Ethereum, according to Javaid and the team, not only stops rogue devices from gaining access to the server but also eliminates DDoS assaults by using static resource allocation for devices.

5.4 Protecting USB ports from unwanted access

[9] IOT includes dangers such as node capture, tampering, and side channels. To avoid node capture, camouflage the node, make it difficult to remove the storage medium, encrypt stored data at rest, make the device too small to disassemble, and protect USB ports from unwanted access are all viable options. When confronted with unexpected stress situations, the device should be able to collect perception and erase data.

5.5 AWS IOT Security

To interact with AWS IoT, each connected device or client requires a credential. All data going to and from AWS IoT is encrypted using Transport Layer Security (TLS). Data is protected as it transfers between AWS IoT and other AWS services thanks to AWS cloud security features.

5.6 Using AI

Machine learning is an artificial intelligence (AI) application that teaches computers to analyze data and test hypotheses about it to gain a "understanding" of it. If the ML algorithms are given the right parameters to work with and high-quality data to work with, they can provide useful insight.

One popular IoT security algorithm is Nave Bayes. It categorizes data based on anomalous data activities that are assumed to be the result of separate events rather than a single attack. The algorithm, named after the Bayesian theorem on which it is based, must be trained by human supervisors before it can be used to detect and flag anomalous and potentially malicious activity in live datasets.

5.7 Adaptive Notch Filter Mitigating Technique

The term "Adaptive Notch Filters" (ANF) refers to a variable notch filter with an adaptive algorithm that controls the notch frequency in real time. This adaptive mechanism automatically detects and removes an unknown sine wave embedded in a wide-band signal, such as white noise.This Technique is used against GPS jamming.

5.8 Quantum Cryptography

Quantum computing has excellent processsing power.Once they come into the market commercially hackers can easily break the current cryptographic algorithms. So Scientists have invented Quantum Cryptography in order to protect from Quantum hackers.

The semiconductor chips employ quantum techniques to generate a one-of-a-kind long cryptographic key for each device. This is possible with quantum random number generation (QRNG). It creates a source of noise with a high amount of randomness. It can create lightning numbers at a high rate using a quantum computer. As a result, communications and keys are kept safe and secure. This implies that each gadget has its own set of keys that are extremely difficult to crack. The only method to get the important information is to look at the device configuration. However, doing so on tamper-resistant devices without being detected would be extremely challenging.

5.9 Edge Computing

Using edge systems to do the processing necessary to establish a strong security architecture that can assist in the development of a secure IoT. The IoT systems become more safe through the simple adoption of edge computing, which uses edge systems to generate cryptographic keys and manage network security. To accomplish this, the edge system would need security agents on each of the IoT Network systems that perform the dedicated task of handling security and communicating with the edge server.

5.10 Mutual Authentication

It collects data about the overall state of the system, such as endpoints and connection traffic. The data is then analyzed for potential security issues and system threats. Once identified, some steps need to be taken as part of the system-wide security plan such as isolation of the device due to abnormal behavior. This monitoring analysis cycle can be run in real time or later to reveal usage trends and identify potential attack situations. End devices should be protected from tampering and data manipulation that can lead to false event reports.

6 Conclusion

IoT market has experienced a significant increase as a result of the current popularity of IoT devices. People are connecting their items to the Internet and staying in their comfort zones, entirely relying on IoT devices. The current state of the IoT industry poses a threat to the safety, security, and economic well-being of modern civilization. Cyber attacks are a global security threat that needs international collaboration. Unsecured IoT devices might provide a hacker with complete access to the entire system. This study focuses on the most prevalent attacks that occur on IoT devices these days. Hackers employed other forms of hacking attacks to infiltrate those devices, which were also described. It also included the most up-to-date tactics being used by scientists to counter those attacks.

[5] [3] [7] [8] [2] [1] [10] [6] [9] [11] [4]

References

1. Aljawarneh, S., Radhakrishna, V., Kumar, G.R.: A recent survey on challenges in security and privacy in internet of things. In: Proceedings of the 5th International Conference on Engineering and MIS. ICEMIS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3330431.3330457, https://doi.org/10.1145/3330431.3330457
2. Calderoni, L.: Preserving context security in aws iot core. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3339252.3340499, https://doi.org/10.1145/3339252.3340499
3. Jaigirdar, F.T.: Trust based security solution for internet of things healthcare solution: An end-to-end trustworthy architecture. In: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers. p. 1757–1760. UbiComp '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3267305.3277810, https://doi.org/10.1145/3267305.3277810
4. Javaid, U., Siang, A.K., Aman, M.N., Sikdar, B.: Mitigating Iot device based ddos attacks using blockchain. In: Proceedings of the 1st

Workshop on Cryptocurrencies and Blockchains for Distributed Systems. p. 71–76. CryBlock'18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3211933.3211946, https://doi.org/10.1145/3211933.3211946

5. Khawla, M., Tomader, M.: A survey on the security of smart homes: Issues and solutions. In: Proceedings of the 2nd International Conference on Smart Digital Environment. p. 81–87. ICSDE'18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3289100.3289114, https://doi.org/10.1145/3289100.3289114
6. Kozlov, D., Veijalainen, J., Ali, Y.: Security and privacy threats in iot architectures. In: Proceedings of the 7th International Conference on Body Area Networks. p. 256–262. BodyNets '12, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL (2012)
7. Rahimi, H., Zibaeenejad, A., Rajabzadeh, P., Safavi, A.A.: On the security of the 5g-iot architecture. In: Proceedings of the International Conference on Smart Cities and Internet of Things. SCIOT '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3269961.3269968, https://doi.org/10.1145/3269961.3269968
8. Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., Ande, R.: Iot standardisation: Challenges, perspectives and solution. In: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. ICFNDS '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3231053.3231103, https://doi.org/10.1145/3231053.3231103
9. Samaila, M.G., Sequeiros, J.a.B.F., Freire, M.M., Inácio, P.R.M.: Security threats and possible countermeasures in iot applications covering different industry domains. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. ARES 2018, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3230833.3232800, https://doi.org/10.1145/3230833.3232800
10. Sultan, A., Mushtaq, M.A., Abubakar, M.: Iot security issues via blockchain: A review paper. In: Proceedings of the 2019 International Conference on Blockchain Technology. p. 60–65. ICBCT 2019, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3320154.3320163, https://doi.org/10.1145/3320154.3320163
11. Tbatou, S., Ramrami, A., Tabii, Y.: Security of communications in connected cars modeling and safety assessment. In: Proceedings of the 2nd International Conference on Big Data, Cloud and Applications. BDCA'17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3090354.3090412, https://doi.org/10.1145/3090354.3090412