International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 2, Issue 3, July-September, 2023, Available online at: https://ijmirm.com

IoT Security Challenges and Solutions Research

Ali Saleh Altuwayjiri

Cybersecurity and Networks Trainer, at the Shinan Technical College, TVTC, Saudi Arabia

Abstract

IoT is one of the emerging technologies, which is getting attention in not only academic fields, but also in industries and household use as well. Connecting sensors embedded in different devices through the internet is integrating both the digital and physical worlds. IoT is offering huge business values to the organizations and providing different opportunities for applications like energy, healthcare, transportation, manufacturing. As a new emerging technology, IoT is facing many security challenges, including security breaking, unauthorized access to the devices, issues related to Data safety, botnets and malware attacks, and the hijacking devices.

To deal with the security issues, many solutions are introduced and being implemented, which include encryption of data, use of Software-defined networking architecture, different practices to keep data safe, and other security protocols. This paper discusses the IoT and its widespread, the importance of security for IoT, challenges for IoT security, and their solution and effect of devices' vulnerabilities on users.

Keywords: IoT, devices, security, protocols, network, solution, vulnerability, application, sensor, information, hackers, accident, user knowledge, social engineering attacks, encryption, viruses, malware.

What is Internet of Things?

Internet of Things (IoT) is a big net of devices, which are mutually connected. Data about the usage of these devices and the environment in which they are working is gathered and shared. This data is analyzed and used for different user applications. Data is collected using the sensors, which are embedded in almost all the physical devices. Almost everything you come across in day-to-day life, including smartphones, vehicles, electrical appliances, bar code scanner, traffic lights has embedded sensors thatsend data continuously about the conditions these are working in and other information about the environment.

IoT provides a common platform to all the devices to send their data and a common language is provided to all the devices to communicate with each other. After gathering data from different sensors, data is integrated and analyzed to extract the valuable information, which is used in the required applications. The result is when shared with other devices to get a better experience and improve efficiencies. For example, In an AC manufacturing company, the manufacturing machines and the belt has sensors embedded in them. Data is continuously captured using the sensors and sent to the manufacturer. This data may include the health of the machines and manufacturing products' specs and numbers. Using the information received, the manufacturer can identify the issues beforehand. A bar code or QR code is attached to every product, which has information about specifications and instructions of products and manufacturer.

Once the products are dispatched to inventory, the manufacturer can track the distribution of the products using the Bar code attached and can identify the shortage of any product before time. These products are then distributed to retailers or customers for use. Information about the product can be accessed using the bar code at any time. AC has sensors to keep checking the health of the compressor and temperature. This data is received and analyzed by the manufacturer continuously and customer care may contact the user about the repair or any other issue in time.(Dušan Marković, 2015)

The use of IoT is not limited to any field or sector. It is widespread over all the sectors and industries and being used domestically. It is approximately that there were almost about 26.66 billion active IoT devices in 2019, which may have reached 31 billion in 2020. It is said that 127 new IoT devices in a second are connected to the internet. (Lueth, 2018).

Applications of IoT include medical and health care, transportation, consumer applications, home automation, industrial applications, smart agriculture, infrastructure applications, energy management, environment monitoring and disaster management, military and defense applications, and many more. The rate with which the use of IoT is spreading shows that after a few years, each device will be linked to the internet. It was estimated that 9,1 billion IoT devices were being used in the industrial and corporate settings. (Feng Wang, 2015)

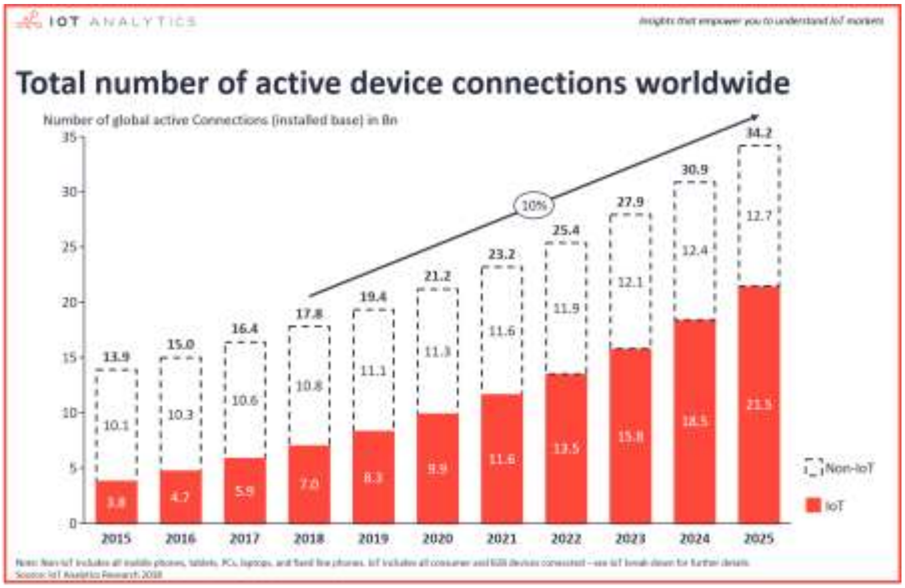


Figure 1: Total number of active device connections worldwide (Lueth, 2018)

Why is IoT security important?

A huge amount of data is being shared among different IoT devices over and this can be a target of hackers, fraudsters or anyone who wants to misuse it. In industries, data of customers are being shared through the IoT and if not secured, it may be misused. Moreover, some machinery is being used in a secure environment such as in the petroleum industry or defense industry where unauthorized access to the system or information may cause huge damage.

In smart homes, cameras are used to monitor and these are joined to the IoT. If someone hacks into the system and gets access to this recording, it can be used against the person using IoT as a hacker may break into the house when the owner is not at home. IoT is being used in vehicles and it can be controlled completely using the IoT. If someone hacks into the system, he may control it and cause an accident. As the information is being transmitted in an open network, it is important to keep it secure to avoid any kind of misuse.

IoT Security Challenges

The use of IoT is increasing enormously. At 2017, the IoT global market reached one hundred million dollars in revenue for the first time and it is estimated that it will reach $1.6 trillion until 2025. With the increase in popularity of the IoT, challenges also increase, as there become more opportunities for attackers to infiltrate and misuse the technology. The most important security challenges to IoT are discussed here. (Tawalbeh,2020)

Lack of Compliance in part of the IoT manufacturer

As the use of IoT is increasing, the demand for products from manufacturers is also increasing and they are manufacturing new devices every day. To complete a new product and make it available in the market early, the manufacturers don’t spend much time on the security of the product or they use many recourses for this purpose making the devices vulnerable to attacks. For example, manufacturers provide the devices with general and guessable login credentials and in many cases, the users do not change the login credentials and keep using the default one, which makes it easier to hack the devices.

One of the examples of such an attack is the Mirai attack, which used only a list of common login credentials and compromised about 100000 household devices. Sometimes, the devices were secured at the time they are manufactured but there is not any security update mechanism to update the security system of devices with new security threats which are usually more powerful than previous. There are sometimes hardware issues that make the devices at risk to attack.

Lack of user knowledge and awareness

Sometimes, it is easier to trick the human instead of attacking the IoT devices to get access to IoT devices. Although, the main threats are due to the manufacturers’ mistakes, still negligence and less awareness of users to use the

IoT devices may also cause great trouble. Targeting the human using IoT instead of targeting the device is called a social engineering attack.

The attacker uses that person to carry the virus or malware to the main system using which the attacker may get access to the network and misuse it. One of its examples is the Stuxnet attack which is carried out on a nuclear facility of Iran in 2010 which corrupted the 1000 centrifuges and plant was exploded. It was believed that the malware reached the main isolated network by a USB of users working there. (O'Donnell, 2020)

IoT Security Problems in device update management

Another main IoT security challenge is the use of outdated software and firmware. Although, at the time of manufacturing, the device has an updated security system It always needs to be updated according to the discoveries of new vulnerabilities. Sometimes, devices are not updated from time to time and are kept using for years with old software and security system which makes them unprotected and easy to new attacks.

Another issue is that a device may face a downtime while sending its backup to the cloud for updates. Now if the files are unprotected or the sending and receiving data is not encrypted, information can be stolen by attackers. Once they get the required information, they can hack into the device and then network and can misuse it.

Lack of Physical Hardening

If the devices are not physically protected, this may cause serious security issues. Most of the time, IoT devices are installed to work autonomously, and sometimes they are installed in remote areas where one cannot visit for a long time. In such cases, it is very important to consider the physical protection of the device. If the devices are not physically protected, someone can affect themin emotional way using malware through USB, as an example. Also, sometimes the victims, maybe have no idea if their devices such as USB, Hard Disk, have any kind of viruses or malware.

It is the responsibility of manufacturers to ensure the physical security of the devices. But it is always a challenging task for manufacturers to maintain a balance between the quality and the cost. It is also the user’s responsibility to consider the physical protection of devices while installing them. For example, if a video camera outside the house is not protected properly, someone can get it easily. (S.-K. Choi, 2018)

Botnet attacks

If a single IoT device is infected with malware, it is of no harm. But if hundreds of devices are infected with the malware, they become an army of zombies that are directed to attack the target by sending thousands of requests per second bringing down the target system. In the 2016 Mirai Bot attack, thousands of video cameras, routers NAS was hacked and were infected with malware and directed to send requests to DNS to bring it down. DNS was providing services to many important platforms, including GitHub, Reddit, Twitter and Netflix.

IoT devices do not have security and software update systems which make themexhibition to be hacked ormalware. They are easily infected by the attack, turning them into “infected zombies” and used to direct huge traffic to bring a system down. (Top 10 Biggest IoT Security Issues, 2020), (Kaspersky, 2015)

Hijacking your IoT Devices

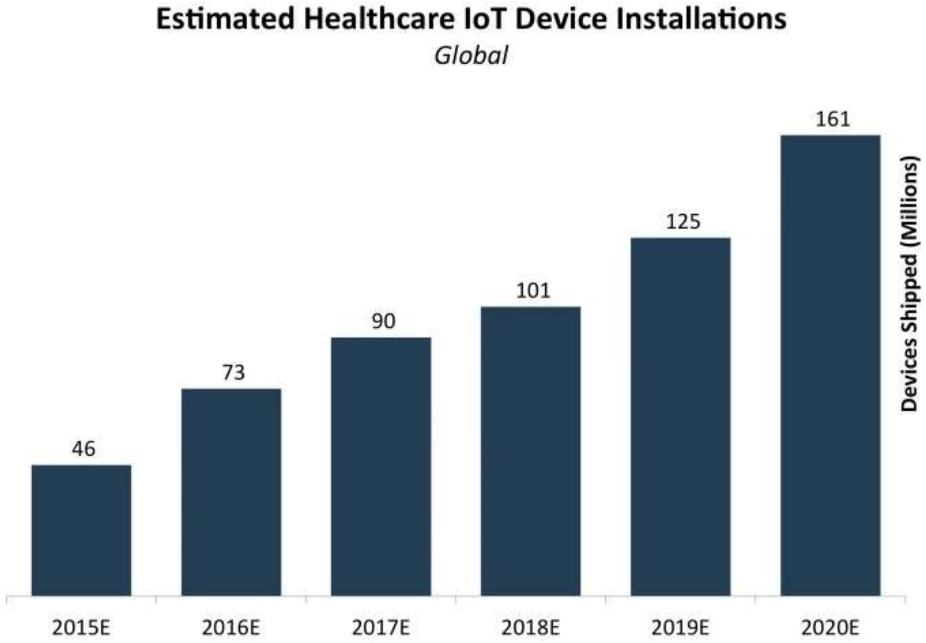
Ransomware is one of the types of malicious malware. When a hacker infects a device with ransomware, it does not harm or destroy the device or data in it, but it restricts the user’s access to the device and then the hacker asks for money in return to unlock the device. IoT devices with an insufficient security system can be an easy target for ransomware. Also, the IoT devices are not the primary targets for ransomware yet as most of the time, only computers and mobiles are being attacked using this, but with an increase in IOT usage devices will make it a primary target in near future.

Most of the data on IoT devices are stored in cloud memory, so this attack may not compromise your data, but it compromises the functionality of the device until you pay the hacker. For example, if your cars are attacked or hacked, you will not be able to start it until you pay the attacker. (Crane, 2020)

Data Integrity Risks of IoT Security in Healthcare

IoT Devices are usually receiving and transmitting data all the time. They send the data of their sensors to the cloud and receives the instructions or data used for decisions in IoT devices. Mostly, the sending and receiving data is not encrypted which enables the hacker to get access to information and the devices and control or change the data being received and sent. The false data can cause serious damage in healthcare as precautions are to be taken using the data being received.

Hackers may also control the devices to change the information related to the patient status and medicine status, which may cause trouble for the health of the patient. For example, the status of battery timing of medical equipment in an intensive care unit (ICU) is being monitored and hacker changes the status to 100% while it is about to end. (Anil Chacko, 2018)



Solutions to the Security Challenges of IoT

To get better use of IoT devices, there is a high need to solve its security and privacy problems to avoid any kind of damage. There are a lot of solutions proposed and being implemented to secure the privacy and security of the IoT devices. One of the main issues of using IoT is Data Integrity. This can be handled by using Data encryption. As in your IoT devices, sensitive data is being transferred from one device to another, so it is necessary that data is encrypting while transferring it.

Hackers are always looking for an opportunity to get access to the data and in the real case of encrypted data that can only be decoded by the user device itself. So, make sure to use Secure Socket layer (SSLs) protocols while dealing with your data online and use of firewall in case of web applications.

Customer Anonymity, secure session key establishment, and mutual authentication can be used for data authentication. To solve the hardware issues related to security, tech giants like Intel and ARM are spending more of their resources and time to build complex designs to ensure the security of IoT devices' hardware making these products expensive. One solution to many of the security issues of IoT is two-step verification while accessing the device which will make it difficult for an unauthorized person to access the device.

The manufacturers should not provide the devices with generic default login credentials, which are guessable. The practice of creating different and complex default login credentials should be followed by the manufacturers and the users should also change the credentials of devices once installed to better protect the privacy and avoid issues. Some of the protocols used to ensure the security of IoT include the public-key protocol, Identity-based Encryption, and Attribute-based Encryption.

To ensure the privacy of user's information different techniques are used including Data tagging, Zero Knowledge Proof, K-Anonymity Model. DoS or DDoS attacks on IoT devices are avoided using different methods including the IP traceback method which helps in DoS or IP flooding attack in real-time and artificial intelligence techniques in which models are trained to detect the DoS or DDoS attack and take precaution regarding that. Software-Defined Networking (SDN) is introducing new solutions for protecting the data and privacy of IoT. (Djamel Eddine Kouicem, March 2018)

How does device vulnerability affect the user?

If we look into the attacks on the IoT devices, we can observe that the vulnerability of devices directly affects the user. Vulnerable devices possible to be used to reach the target information or can be controlled to cause any damage.

Attackers may use the devices to weaponize the device or make target the device itself or use that device to spread the malware into the system. IoT botnets are an example to see how vulnerable devices affect users.

In 2016, Mirai is one of the clear examples of IoT Botnet took down many prominent websites in the DDoS campaign. In this attack, 100000 domestic IoT devices were compromised. These devices included a baby monitor, home routers, security cameras. Mirai used a list of 64 common usernames and passwords to hijack the devices. It was because of the weak security on these devices making them easy to attack.

Who is responsible for securing IoT devices?

To maintain the security and privacy of IoT devices is not the responsibility of a single company or person. This responsibility comes in the chain from the manufacturer to the end-user to ensure the protection and security of IoT devices by following the sufficient practices. Firstly, device manufacturers need to ensure security while building devices. Then the company which integrates the parts and creates the end-user product should ensure that steps are taken to protect the device.

The customer should take care of it while installing and setting up the device and especially when setting up the authentication codes or login credentials to access the device, they must keep this in mind to set such username and password which is not guessable and is not related to the information which other people know. With the advancement in technology, new threats to the security of IoT emerge which require new solutions.

Hence, it is the responsibility to keep that in check and with new threats, they must update the IoT software and security system. Customers should keep the devices safe physically so that no one unauthorized person could approach the devices and enter the malware into it. (Shaikh,2019)

Conclusion

Internet of Things is a new technology emerging nowadays connecting humans, smartphones, different objects, computers, and intelligent systems, and this connection of different physical objects through the internet will bring a new revolution.

In this paper, IoT and its widespread use, different security, and privacy issues of IoT, and their solutions were discussed. The best practices, which should be followed to avoid security and privacy breaking , are also discussed. Moreover, the discussion included the importance of security in IoT, the factors which are responsible for IoT security and privacy assurance, and the effect of device vulnerabilities on the users.

References

[1]. Anil Chacko, T. H. (2018). Security and Privacy Issues with IoT in Healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*.

[2]. Crane, C. (2020, February 28). *20 Ransomware Statistics You're Powerless to Resist Reading*. Retrieved from Security Boulevard : https://securityboulevard.com/2020/02/20-ransomware-statistics-youre-powerless-to-resist-reading/

[3]. *ddos-attack-dyn-mirai-botnet*. (2016, December 26). Retrieved from The Guardian: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[4]. Djamel Eddine Kouicem, A. B. (March 2018). Internet of Things Security: a top-down survey. *Computer Networks*.

[5]. Dušan Marković, R. K. (2015). Application of IoT in monitoring and controlling. *Acta Agriculturae Serbica*, 145-153.

[6]. Eman Shaikh, I. M. (May 2019). Internet of Things (IoT): Security and Privacy Threats. IEEE.

[7]. Feng Wang, L. H. (2015). A Survey from the Perspective of Evolutionary Process in. *International Journal of Distributed Sensor Networks*, 9.

[8]. Kaspersky. (2015, May 29). *Statistics on botnet-assisted DDoS attacks in Q1 2015*. Retrieved from SECURELIST: https://securelist.com/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/70071/

[9]. Lo'ai Tawalbeh, F. M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences* .

[10]. Lueth, K. L. (2018, Augugst 8). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. Retrieved from IoT Analytics: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[11]. O'Donnell, L. (2020, March 11). *More Than Half of IoT Devices Vulnerable to Severe Attacks*. Retrieved from threatpost: https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/

[12]. S.-K. Choi, J. K.-H. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. *KSII Transactions on Internet and Information Systems*, 906-918.

[13]. *Top 10 Biggest IoT Security Issues*. (2020, July 30). Retrieved from Intellectsoft: https://www.intellectsoft.net/blog/biggest-iot-security-issues/