Safety and Security of Internet Of things

Israa S Mondany

Computer Department, High Institute of Administrative Services
Hawally,kuwait
is.mandany@paaet.edu.kw

Abstract— **Internet of Things is a new concept that arise, it's as many technologies have many benefits to the society as will as so many risks, relaying on this technology could be dangerous if we didn't take specific precautions to ensure the safety of it, in this research we discussed the risks from security overview to determine weather this technology is safe to use or not and we reach to a conclusion that following certain steps could make this technology safe.**

Keywords— **Internet of Things, risks, threats**

I. Introduction

Internet of things IOT is building a network that connect different objects, the network is build depending on the purpose of the usage. This network is used to create a comfortable environment for the user.

The objects of the network could be devices or even other network systems.

Smart houses are a simple example of internet of things, creating a system that connects your alarm with the coffee machine and even playing a morning sound while opening the curtain, after waking up and heading to the kitchen the toaster is just finished toasted your bread and all morning tasks are finished, and you are ready to go to work.

What about going further than that and all the previous system is connected to a traffic system that gives you the right time for you to wake up and to reach your work at the time and depending on that the alarm would set up automatically according to the traffic and wake you up earlier.

Another example if we want to use this technology at the education field, there are many ideas that we can create like connecting the students by special watch for example with the education institution so that their attendant is recorded when they just enter the gate, and all the activities of each one of them is recorded and can be analyze.

At the supermarket you will not need to do the same old routine, anything is taking from the roof is calculated directly and after you have finished all the shopping you can just walk out the door and the amount of money is deducted from you and even further from that your smart fridge would prepare your shopping list that you can adjust on it and send it to the supermarket to deliver your items.

There are so many ideas you can create using IOT technology in our lives but as any technology it has advantages and disadvantages.

II. Advantages of IOT

If we want to talk about the advantages, then the first obvious one for us is improving the quality of live, finding time to do our daily routine can be challenging with the accelerating rhythm of life so using this technology can free our minds from planning to these simple things and let us concentrate on the more important issues. Another example with the medical field a device that connect the person with the hospital or family could save his life where every second is in counter, differences in blood pressure or heart beats could give an early alarm and make it possible for early rescuing.

Another advantage for the IOT technology is collecting data, everything in our world depends on collecting and analyzing information, in all fields being able to reach these valuable data could help a lot in improving the work, IOT technology is based on this info so all what we need to do is to analyze this huge amount of information to reach our goal by analyzing the information then predicting and acting according to these predictions.

In the field of industry IOT technology could offer a huge benefit because of the accuracy and efficiency in performing tasks, any problem with the product itinerary for example could be discover early and repaired which saves time and money.

III. disadvantages of IOT

Let's move now to the disadvantages of Internet of Things technology, complexity is one of them, building a system requires several steps to ensure efficient work IOT technology depends on connecting objects or even systems to each other so any mistake of one of the steps for building a system could cause huge failure to it.

Job loss for most of the unskilled workers, applying this technology needs specific employees with precise skills and specialties so employees with simple knowledge will not be able to find work in any place that depends on the IOT.

Technology dominance, depending on this technology will cause a full reliance especially with the new generations, gaining experience in life with our simple things will not be necessary for them they will be addicted to this technology we need to put boundaries so that the technology will not take control of our lives.

IOT security and safety will be discussed in more details to determined if we can relay on it as an advantage or disadvantage.

IV. Security of IOT

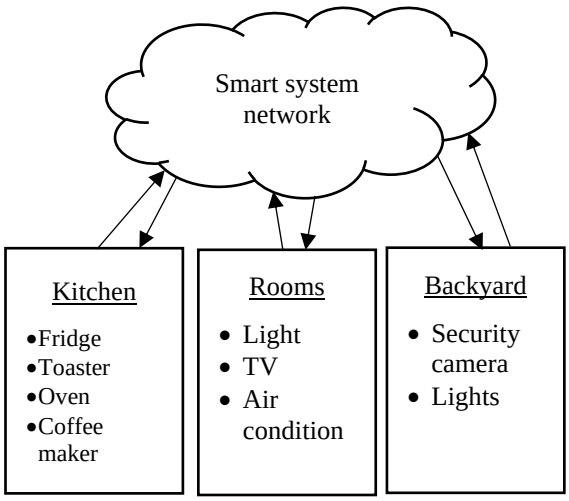
IoT security pertains to the safety of the actual hardware units and the network that connects them. It includes all the tools, technologies, procedures, and security precautions needed to protect IoT devices. Additionally, it guarantees that

programmers fortify the hardware against weaknesses and dangers.

With the help of techniques like access control, behaviour monitoring, and detachable networks, Internet of Things (IoT) security is intended to address vulnerabilities in IoT devices. These techniques defend against a variety of security problems, most frequently malware and information theft.

To identify the risks of IOT system we need to know first how IOT system works, An IoT system is made up of processors or sensors that link to a server or cloud over the internet. A piece of software processes the data before sending it to the server or cloud. When the procedure is finished, a signal is delivered to the sensor to carry out an operation, modify the sensor, or interact with other devices without the need for human intervention.

If we take smart homes as an example, smart home is a residence that has been created to maximize tenants' quality of life and customise their standard of living. A "smart house" can be remotely managed via a smartphone or manually controlled using pre-programmed settings or electronic gadgets. So we will see a system that is build from home devices that we use all day.



Smart houses are powered by IoT as its main technology. It allows for the connection and communication of devices, enhancing the ease, comfort, and safety of your home. You can automate and take control of your house using one application thanks to IoT's access to data and information. Your control centre is now your phone.

By controlling your home appliances, IoT enables you to save money and cut down on your energy usage. With a single app, you can manage them from anywhere in the globe and set up intricate routines that are carried out in accordance with your own requirements or a schedule. This will let you to do things like turn on the lights before rising, or pre-heat the oven while you're on your way home.

These devices will be able to manage by the people that live in the house whether they were in the house or outside, or these devices can communicate with each other through the system without human interfere.

These devices are connected to sensors that link to a server cloud, examples of sensors that can applied in smart homes are as mentioned in **https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/** web page:

A.Fire/CO detection.

There are several pollutants that can threaten the environment and air quality in our homes, all of which have the potential to cause property damage and harm to the occupants. For years, the basic fire detector has been beeping away at the first hint of smoke in the house. A carbon monoxide detector measures the amount of CO in the air and alerts users if the level is unsafe.

In addition to detecting smoke and CO, some modern sensors can also keep an eye on your home's overall air quality and look for contaminants including dust, soot, pollen, temperature, humidity, air staleness, pollution, and particles. The discounts that insurance companies provide when you employ these sensors make them even more alluring.

B.Window & door open and close

Door and window sensors can even turn lights on and off as doors are opened and closed, alerting you when people arrive and leave your home. Your first line of defense against home invasions should be door and window sensors; some of these devices can even tell when a window has been broken. These sensors warn you of prospective intruders as well as a rebellious adolescent. Once more, wireless technology enables you to receive alerts directly on your phone or tablet and to swiftly call for assistance if necessary.

C. Video doorbell

The video doorbell doubles as a theft-prevention device. You can check who is at your door from your smartphone with this amazing technology. Whether you want to check who is at the door when you are inside alone or whether someone is at your house while you are at work. You'll be aware. Thieves will avoid your home and forego the hassle of breaking in if you combine this with the door open/close sensor.

D. Smart thermostat

With the help of the smart thermostat, you can manage the heating and cooling in your house from anywhere. Smart thermostats are cool, but they can also save you money by keeping an eye on the humidity and temperature inside and outside of your house. Your home's temperature changes as you come and go, and a smart thermostat can vary the temperature based on how you behave and how the rooms are used. The greatest thermostats allow you to retain your preferred temperature when you are in the room and can default to an energy-saving mode when no one is around. They change the temperature on a room-by-room basis. A house is being made possible by using cognitive technology with these sensors.

E.Motion sensors

An area's motion and movement is detected by a motion sensor, as you might expect. When you aren't home, these sensors keep watch; they can let you know if there is motion

inside your house or if your doors or windows have been opened or closed. Motion sensors work as an extra set of eyes for you, letting you know if something is amiss in your home, like a teenager sneaking out (or in), or if a youngster visits a room that is off-limits, like the medicine cabinet.

Now what are the risks that would threaten a system like this, well we have so many risks like:

A. Theft of data.

The great majority of the data on an IoT device is specific to each user, including records of online browsing and purchases, credit card information, and details about their personal health.

This data is susceptible to theft on a device that is not adequately secured. Additionally, vulnerable devices can be utilized as access points to other parts of the network they are installed on, enabling the extraction of more sensitive data.

B. Unpatched vulnerabilities.

It is crucial to properly patch IoT and smart devices, and application vulnerabilities are frequently overlooked. Such patching is not just necessary at the operating system level.

Numerous infamous exploit kits aim to insert malware into Java, office productivity software, web browsers, and other frequently used applications.

While it might be challenging for end users to maintain all of their devices and applications patched, it can be even more challenging for an IT manager to keep hundreds or even thousands of IT devices properly updated and patched.

With the help of techniques like access control, behaviour monitoring, and detachable networks, Internet of Things (IoT) security is intended to address vulnerabilities in IoT devices. These techniques guard against a variety of security problems, most notably malware and information theft.

C. Weak authentication

IoT devices frequently use poor authentication techniques, which makes it simple for attackers to pose as authorized users and access confidential information. Additionally, a lot of devices have the same default passwords, which are simple for hackers to guess.

Applications including payment apps, communication platforms, and database management tools are frequently found on IoT devices. Because they contain sensitive information, these applications need to be fully safeguarded with robust security mechanisms including user authentication before access.

D. Use of outdated software and application

Software becomes old when there are no updates available to keep it up to date. It cannot function properly on new devices or connect with new applications.

The risks must also be considered. When flaws are discovered in outdated software, no updates are available, making it vulnerable to even more sophisticated cyberattacks. Due to the possibility of system failure as well as human malice.

E. Unauthorized access

The researchers discovered the presence of several third parties in apps connected to IoT wearable health and fitness devices. The information that some of these third parties gathered included persistent device identifiers, exercise routines, eating patterns, the length of one's walking stride, medical search histories, zip code, gender, and location. According to the that some IoT devices have the ability to "collect, transmit, and share highly sensitive information about consumer's bodies and habits."

As well as we have risks, we have threats also that could affect our IOT system, Threats can affect everything that is connected to the internet. We constantly risk being exposed to vulnerabilities, it is a fact. Depending on who is most exposed. We won't be able to take action to safeguard our computer system against these dangers unless we can identify these online threats. Any danger to IoT is motivated by a goal. Depending on the aim of the intrusion, the intent could change. Threats of IOT technology:

A. Botnets.

A network of connected systems known as a botnet is used to remotely manipulate a victim's system and spread malware. Cybercriminals use command-and-control servers to manage botnets that they use to launch DDoS and phishing attacks, steal sensitive information, and gather online banking information. Botnets can be used by cybercriminals to attack IoT devices that are connected to a variety of other devices, including laptops, desktop computers, and smartphones.

B. Worms.

IoT worms are currently more prevalent than botnets. Worms are self-replicating malware that can infect uninfected systems on a network by multiplying themselves.

C. Man-in-the-Middle.

In a Man-in-the-Middle (MiTM) attack, the communication link between two separate systems is breached in an effort to intercept messages being sent between them. Attackers seize control of their communication and deliver fraudulent messages to involved systems. IoT gadgets like self-driving cars and smart refrigerators can be compromised with such assaults.

Several IoT devices can be attacked via man-in-the-middle attacks as they exchange data in real-time. Attackers can use MiTM to intercept communications between various IoT devices, which can seriously malfunction. For IoT devices like industrial equipment and medical devices, such hacks might have disastrous results.

D. Social Engineering.

Hackers utilize social engineering to trick people into disclosing their private information, including passwords and bank account information. Alternately, thieves may gain access to a system through social engineering in order to covertly install harmful software. Typically, social engineering assaults use phishing emails to trick people, thus an attacker must create

convincing emails to do this. But with IoT devices, social engineering assaults might be easier to carry out.

E. Ransomware.

Attacks using ransomware have grown to be one of the most well-known online dangers. A hacker encrypts data that might be necessary for corporate operations using malware in this attack. Critical data will only be decrypted by an attacker after being paid a ransom. Using smart thermostats, researchers have illustrated the effects of ransomware. Researchers have demonstrated that hackers can use this method to low the temperature and hold it there until they are paid a ransom. Similar to how it can be used to target IoT and smart home technology. For instance, a hacker could target a smart house and notify the owner that a ransom must be paid.

F. Denial of service

By sending numerous requests, a denial-of-service (DoS) attack aims to intentionally overload the target system's resources. In contrast to phishing and brute-force assaults, denial-of-service attackers do not seek to steal important data. DoS can, however, be used to harm a company's reputation by slowing down or shutting down a service. For instance, a hotel that is subject to a denial-of-service attack won't be able to handle requests to make new reservations, check the availability of rooms, or cancel existing ones. In such circumstances, guests could choose different hotels. Similar to traditional security concerns, IoT security threats like denial-of-service attacks can harm a company's brand and income.

G. Advanced persistent threats

For many companies, advanced persistent threats (APTs) represent a top security issue. A targeted cyber attack that involves unauthorized network access and extended periods of time without detection is known as an advanced persistent threat. Attackers use sophisticated persistent threats to keep tabs on network activities and steal important data. These cyberattacks are challenging to stop, identify, or mitigate. Large amounts of crucial data are now easily shared across many devices thanks to the Internet of Things (IoT). These IoT gadgets could be the target of a cybercriminal looking to infiltrate private or business networks. Cybercriminals can steal private information using this strategy.

Now how can we adjust the security of our IOT systems to avoid or reduce the effects of the above risks & threats, will we have some points that have to be obvious to the user and the manufacturers of these devices both of them have to take responsibility to ensure the security of the system because the risks that will come from the system could be dangerous to the user it self and even to people around him.

A.Visibility.

Finding out the precise number of IoT devices on the network is the first step in IoT security. You can assess the risk profile of each connected device and how it interacts with the rest of the network by keeping an accurate, up-to-date inventory of all connected devices.

B.Network's segments

Your network's attack surface will be less the more segments there are. It will be more difficult for hackers to harm your entire network by compromising just one device if you divide it into two or more portions.

C. Authentication.

The majority of IoT devices ship with default passwords that are weak and simple to find online. When you connect an IoT device to your network, the first thing you should do is change the password to a more secure one.

D. Updates to Firmware.

Most Internet of Things (IoT) devices are not built with the capacity to repair security problems via routine updates, in contrast to IT systems. As a result, it's critical that you collaborate with the maker of your IoT device to develop a firmware upgrade plan and close security gaps before problems arise.

E. Constant Watching

You can quickly respond to security issues by installing a real-time monitoring solution that continuously examines the activity of all your Internet of Things (IoT) devices.

And when we talk about manufacturers responsibility security of Internet of Things devices starts with them fixing identified flaws in their goods, distributing updates to fix them, and disclosing when support stops. The design of IoT products must prioritize security, and manufacturers must undertake tests like penetration tests to make sure no flaws emerged during production. They also need to put procedures in place for accepting product vulnerability reports.

V. Conclusions

The IOT technology is developing greatly and will enter into many aspects of our lives. There are many areas in which we can rely on this technology, as it facilitates many things for us and even implements them with extreme precision, moving from its necessary presence in some urgent fields such as medicine, business and industry to its intervention in our lives. Ordinary, such as its presence in our homes or to entertain us, this technology enters into the small details of our lives that makes it have a great and dangerous impact in the event of a penetration, because it is like any other technology that uses the Internet communication, it is highly vulnerable to penetration, securing this technology will be the responsibility of the individual and society, It is necessary to spread full awareness at the level of individuals and manufacturers of the importance of following the highest levels of protection to secure it. There are many steps that can protect the individual and society, but that does not mean that it will be 100% safe, but due to the progress made at the present time, it cannot be stopped from spreading. Because of its importance

REFERENCES

[1] https://www.imperva.com/learn/application-security/iot-internet-of-things-security/
[2] https://home.sophos.com/en-us/security-news/2019/the-internet-of-things-is-it-safe
[3] https://authentatechsolutions.com/internet-of-things-iot-security-and-privacy/
[4] https://blog.dashlane.com/internet-of-things-iot/
[5] https://dangerousworld.soe.ucsc.edu/2018/03/25/the-dangers-of-the-internet-of-things/
[6] https://www.iso.org/news/2016/09/Ref2113.html
[7] https://www.avast.com/c-iot-security-risks
[8] https://sumatosoft.com/blog/advantages-of-internet-of-things-10-benefits-you-should-know#:~:text=One%20of%20the%20primary%20internet%20of%20things%20advantages,is%20logged%20and%20connected%20through%20an%20IoT%20network.
[9] https://www.linkedin.com/pulse/benefits-iot-internet-things-maktabiapp
[10] https://www.geeksforgeeks.org/benefits-of-internet-of-thingsiot-in-manufacturing-industry/
[11] https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek
[12] https://www.opswat.com/blog/iot-devices-unpatched-vulnerabilities-are-growing-danger
[13] https://www.parkersoftware.com/blog/the-security-risks-of-outdated-software/
[14] https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/security-for-internet-of-things-device-manufacturers
[15] https://www.fortinet.com/blog/industry-trends/examining-top-iot-security-threats-and-attack-vectors
[16] https://www.allerin.com/blog/8-types-of-security-threats-to-iot
[17] https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/
[18] https://iotblue.com/story-hub/iot-for-smart-homes
[19] https://www.geeksforgeeks.org/security-threats-to-iot-devices/