“Internet of Things and Data Security”

Dhatri Patel
S.ID: 010692526

Contents

Internet of Things(IOT) and Data Security

Introduction

There is one axiom which says that one cannot imagine his life without oxygen, same as one cannot imagine his life without technologies for this modern era. Nowadays, multiple technologies are developing at a rapid pace, beyond one's imagination to make an easier and efficient lifestyle of human-beings. In this paper, one of those recent technologies named "Internet of Things" are going to be discussed. Generally, the term "Internet of Things" is new in this advanced technological era. It is like most favorite and fascinating technology which is useful, not only for technological industries but also for ordinary people in their everyday life cycle. So, in this paper, various aspects of IOT, its various applications, its importance in day to day life and most important, data security and the Internet of Things are going to be discussed. But, it is necessary to understand the meaning of this new term and also working of it, before going into details of data security and the Internet of Things.

The Internet of Things

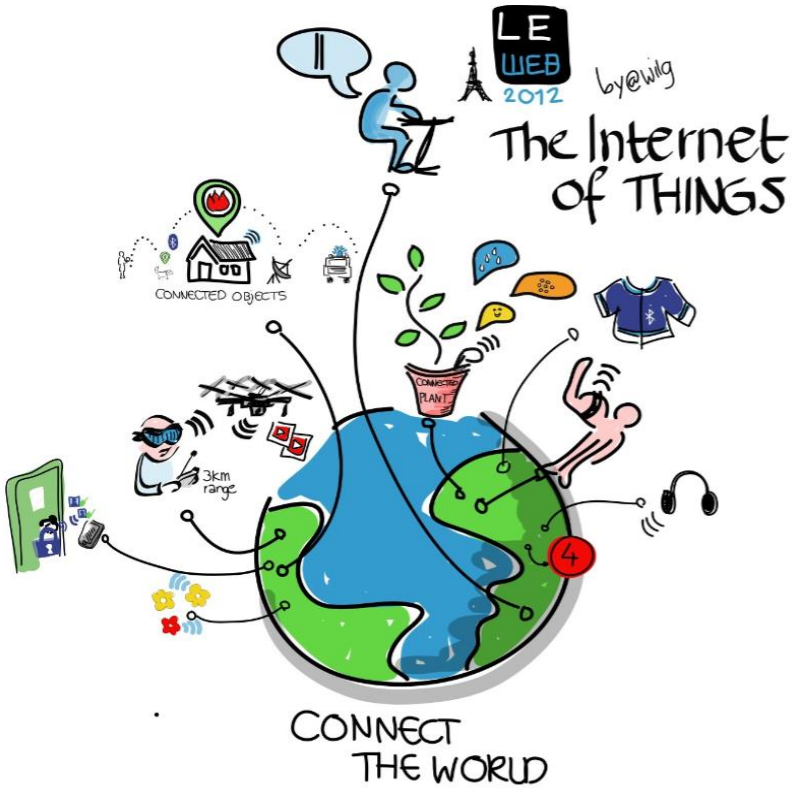

Fig. 1: IOT

The Internet is one of an important and transformative technologies ever invented in this world. Nowadays, people cannot live without the Internet. People use the Internet regularly. The Internet is a digital fabric which is weaving into the life of a person day by day. It is accelerating in one way or another way to increase productivity. Besides this, one new emerging technology is growing its seeds into the market, which is also known as new Internet. This is poised to change the world beyond the imagination of a human's brain. This Internet does not just connect the people but it also connects things and so it is named "Internet of Things". Thus, the simple meaning of it can be given as a concept of connecting things to the Internet to exchange information. Basically, it is the interconnection of physical objects to exchange or transmit information. Thus, the internet of things connects all things with people. It makes possible communication between people and things or between all things. Because of this new technology, it is possible for things or physical objects to share their experience with other physical objects.

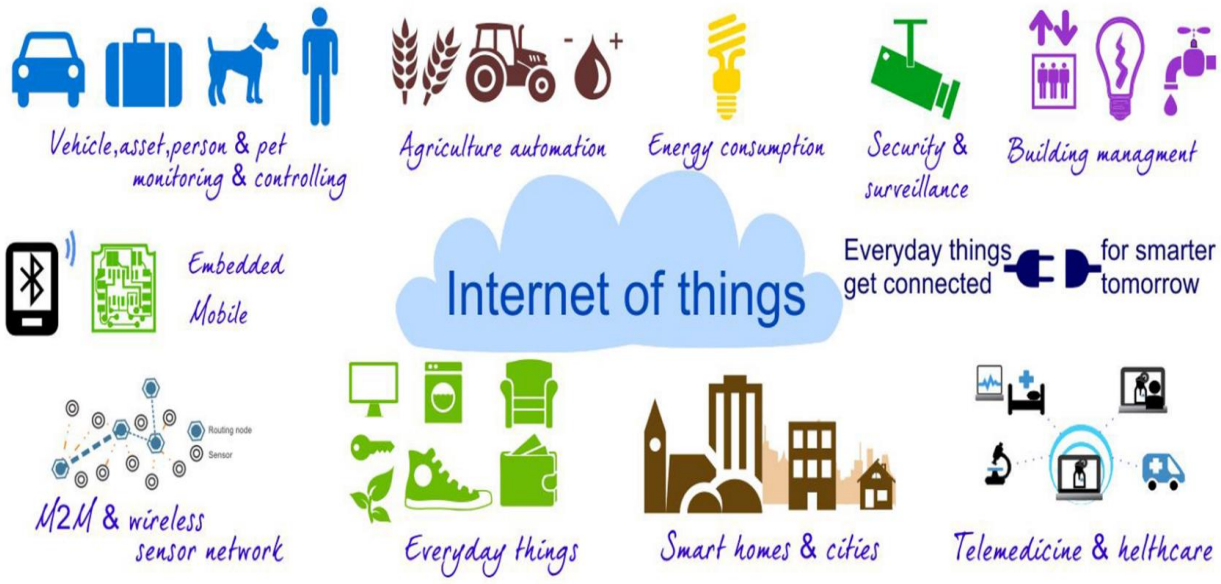

Fig. 2: IOT: Everything gets connected for smarter tomorrow.

The Internet of things (IOT) is a combination of Information Technology(IT) and Operational Technology(OT). Information Technology includes all computer-operated devices and Operational Technology includes managing plans and control systems that can control the whole system. The Internet of things is revolutionizing the way people live by transforming everyday objects surrounds into eco-system of information from home security to the smart refrigerator. Everything can become more technologically advanced. It promises to connect the whole world into one huge information exchange. Nowadays, the Internet of thing is growing rapidly beyond one's imagination. It changes a person's lifestyle.

IOT applies everywhere even in the smallest thing - necessary to complete one's routine. Everything can be connected to the Internet. For example, from the smallest things like a smart fork, a smart toothbrush, glucose monitoring, a smart piggy bank, a smart washing machine, smart Air Conditioner, Blood Pressure monitor, smart garage, smart garbage cans, smart door lock or even wearable devices like fit-bit, watches, clothing to industrial machines can be connected to each other. These physical objects can be able to gather data and transmit that data to other objects via the Internet.

This concept of the Internet of Things can be better understood by figure 2. Figure 2 shows that the Internet of Things is spread all over the world without any restrictions of size or type of physical objects. As explained above, every object like vehicles, commerce, or even a pet can be connected to a person for monitoring and controlling.

Moreover, all these things can be possible due to communication between machines. So, it is a machine to machine (M2M) communication that makes possible IOT. The Internet of Things can also be used in agriculture automation for monitoring the growth of plants and also to keep safe from bugs and insects. This new technology is very useful for energy consumption. For example, many buildings use sensors that can automatically sense the presence of persons and it can adjust heating and lighting as per requirements of a person in a building. It is also useful in healthcare because some wearable devices such as watches that can track the number of footsteps or clothing that can give feedback about a person's overall health information. Sometimes it is also possible in automobile engines. Cars that can communicate with each other, that can detect the running speed of a car and safer speed of a car or it can tell about the dealership or about maintenance what needs to be maintained. Isn't it crazy thing??!! ☺ In such cases, one can wonder when this interesting technology came into existence.

History of the Internet of Things

It is said that "Necessity is a mother of Invention". Same can be applied to an existence of the Internet of Things. In this modern era, due to the development of advanced technologies and due to the fast paced lifestyle of human beings, it became necessary to discover the Internet of Things to make more comfortable, automated and efficient lives of human beings. The potential of "Internet of things" is increasing in today's world due to advanced multiple technologies, but an entrepreneur, Kevin Ashton coined the term of "Internet of things" in the late 1990s. He is a founder of the Auto-ID center at MIT. Thus, this term became famous from the experiment of discovering the connection between objects to Internet through RFID tag at Auto-ID center. Kevin Ashton used this term "Internet of Things" in his presentation of this project of RFID tag and then this term stuck around the whole world. Thus, this concept of "Internet of Things" evolved as wireless Internet spreads all over the world, sensors improve it and one can understand that technology can be active participants. It can be either a personal tool or a professional one.

How "Internet of Things" works

As discussed above, the Internet of Things is a new industrial revolution. The Internet of things (IOT) is growing brilliantly at a rapid pace. For many people, it may be a new term. They may not be familiar with this technology. So, whenever they hear about IOT, it is possible that they may go into the wonderland of this technology. The most wonderful thing about this new technology is that the new category of devices can start to communicate with each other with little or no human intervention in this Internet of Things. One may get surprised for working of the Internet of things and possibilities of all these connections and communications between things. It is a big deal to connect all things together via the Internet. So, in this section, the basic concept of working of the Internet of things is going to be discussed.

The Internet of Things is altering the world in a way that it changes from how people drive to how people can make purchases and it also affects the way of getting energy for their homes. Basically, it can work by combining things and their ability to sense, communicate, touch and control. This is shown below, in figure 3.

Fig. 3: The basic concept of working of IOT

For all these things, sophisticated sensors and chips are embedded in physical things that surround people or environment. Each transmits valuable data. Data that can tell, that can better understand a way of working all these things together and a way of sharing a large quantity of data. Moreover, people put that information to work for improvement in products of a factory, for giving real time updates of city residents, and even for parking of cars. It is also helpful to monitor the healthcare area. It is a common IOT platform that brings every system together for work. It provides a common semantic for devices and applications to communicate with each other. The process starts with devices themselves so that they can securely communicate with an IOT platform. This platform incorporates a data from many devices and applies analytics to share that data with applications that address industry-specific needs or a person's everyday needs.

It can be explained by an example of a car. The driver of a car notices that light of check-engine turns on after taking a long trip. So, it is necessary to provide service to a car by a mechanic. But a driver does not know whether a car requires immediate attention or not. The sensors that trigger the check-engine light, monitor the pressure in a break line. These sensors constantly communicate with each other and also monitor various other parts connected to break line in a car. A diagnostic bus helps to gather data from all these sensors and then passes it to a gateway of a car which integrates and sorts the data from sensors. Thus, only relevant and diagnostic information can be transmitted to manufacturing platform. It collects thousands of bits of information constantly from the driver's car and thousands of other cars and builds a historical record and a secure database which is shown in figure 4. Furthermore, rules and logic are added to this

process. So, when a car senses a signal, below a recommended level, platform triggers an alert in a car. Now, the manufacturer uses the platform to create and manage applications that solve specific issues. In this case, the manufacturer organizes an application called the asset management system. This application monitors all of their other cars on a road as well as all parts in warehouses. For the present example, it uses a data from the driver's car to take an appointment time on his cellphone for servicing his car, directions to the nearest certified dealer and it also suggests a discount coupon on it.

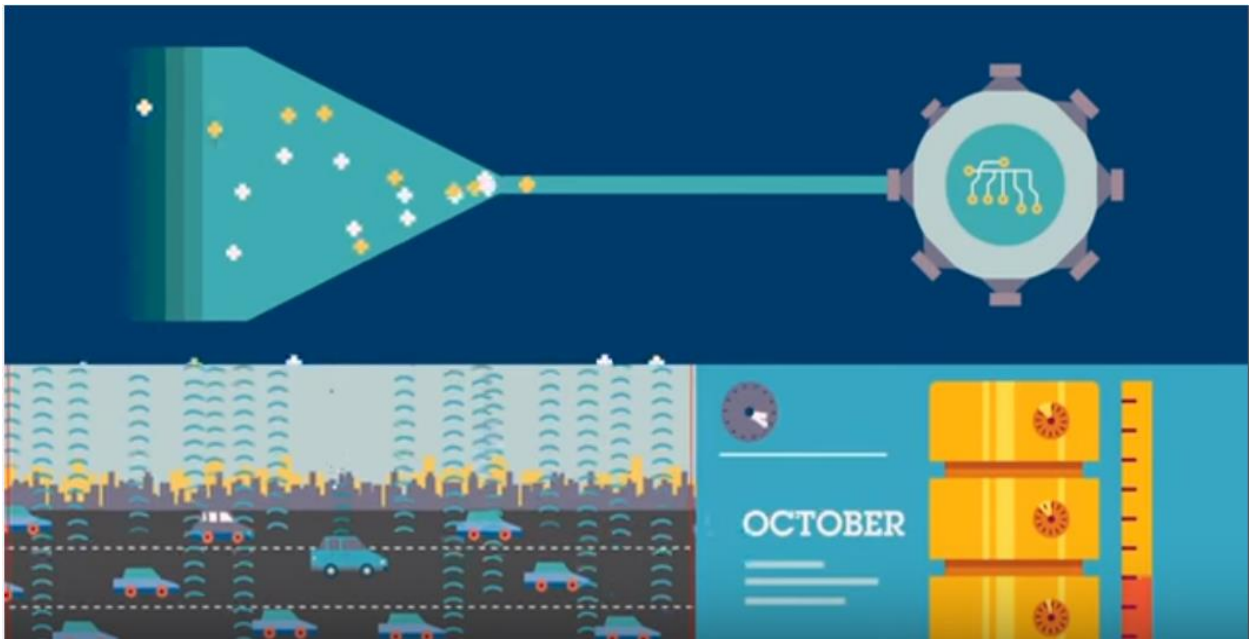

Fig. 4: Connection between cars and a platform with record of a secure database.

The cellphone ensures whether the defective part is covered under the warranty of a car. After this, the correct part is ordered and send to a service station. So, it can be ready when a driver arrives at the service station. So, the driver can back on a road faster and he can reach safely at his destination. But, the analysis of a manufacturer does not complete. They take this application into consideration also for thousands of other cars to improve the design and manufacturing process of a car itself. It can be helpful to see the location of a car factory and the date and time of assembling various parts of a car. So, from this whole process, dealer and manufacturer will get an advantage of better and safer cars. Thus, all these benefits or solution to problems can be accomplished due to an ability of sensing, communicating and acquiring data of the Internet of Things. There is one proverb, which says that "Precautions are better than cure". So, it is necessary to look over a data that is transmitted from one device to another for connection between devices. There should be secure communication without leakage of data between devices. Data integrity must be maintained all the way from a source to destination. Thus, apart from all these interesting facts about the Internet of Things, it is necessary to take care of security and privacy of data to get trust for this new technology. Because of this, various aspects of data security regarding the Internet of things are going to be discussed in the following sections. In next sections, data security for IOT, various security issues, security challenges for future IOT, solutions to this problem and opportunity of IOT to co-create the future are explained.

Data Security in the Internet of Things

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." Mark Weiser said this statement at the Scientific American in the year of 1991. It is 100% true. Technology is most useful when it disappears, when it weaves into lives of human beings, when it becomes indistinguishable from the lives of human beings. Then no conversation about the Internet of Things is complete without discussing security and privacy. Privacy and security both are very important. They are paramount in a field of the Internet of things due to following reasons:

- Highly personal, dynamic, persistent collection and transfer of data.
- A combination of devices, apps, platforms and cloud services.
- Multiple data flows, touch points and disclosures.

Fig. 5: Security in the Internet of Things.

Sensors in a host of physical objects are used in everyday life. They constantly gather, perform some operations and send data to other objects to make a life of human beings more convenient and more automated but also more vulnerable. These devices constantly generate a huge amount of data. So, it is necessary to use faster networks and large storage devices. Moreover, there is no separate eco-system to support all these connected devices to make them interoperable with other operating systems such as Windows, Apple iOS or Android ecosystems. This creates a simple dilemma regarding the ability to collect data overwhelms the capacity to protect it. The scope of a collected and communicated data encompass a wide range of sensitive information like purchasing patterns, access codes, driving habits, real-time locations etcetera.

Many technologies are repurposed for the Internet of things which are generally not intended for secure communications leaving networks and data vulnerable. A new automobile has various computational systems like GPS, diagnostic devices, remote locks, infotainment systems and connections to smart homes running million lines of programming code. The survey of automakers shows that nowadays most of the cars in a market include wireless technologies that may be inadequately secure. Some vehicle systems can even be hacked with a simple SMS text message on a cellphone. Even one vulnerable device leaves an entire eco-system open to attack which closes significant and potentially level dangers to individuals and organizations. Hacked smart cars can provide access to smart homes which can be dangerous to individuals. Managing risks are associated with increased data collection in the Internet of things which begins if data cannot be more secure against an expanding list of threats. Due to this, there can be an increment in the number of attacks on hardware and software severely. Thus, after understanding an abstract of a reason for consideration of security and privacy in the Internet of Things, now it is time to go into details of all aspects of security for the Internet of Things which is explained below.

Security Issues for the Internet of Things

IOT is an area of industry which is concerned with the protection of connected devices and connected networks of IOT. As discussed above, due to a large number of connections between physical objects, there can be a problem for the security of devices. This problem occurs because the Internet of Things is relatively new technology. So, it is possible that security cannot be always considered in product design for every network. Sometimes it is possible that these products can be sold with old or default passwords of unpatched software or operating systems on smart devices or if these passwords are changed, it can be failed to fulfill the requirements of strong passwords. So, the result can be very terrible. Due to this reason, there can be a problem of hacking of systems. In a survey by security agents, it shows that when any physical object becomes a part of a connected network of the Internet of Things, it can be a target for hackers to hack the entire network or system and already there are several attacks happened on various systems or devices. Now, as the number of connected devices in a system increases day by day, there can be a possibility of increasing risks of destroying the whole system. As the use of an Internet is increasing in a wide range, security becomes a critical issue to provide protection related to personal privacy, the threat of cyber theft or financial transactions. Likewise, IOT security also concerns for pharmacy labs or even for medical issues to prevent safety along with security to control any medical devices like a pacemaker which can create a threat to lives of human-beings. Furthermore, by understanding all of these, above mentioned issues related to security in the Internet of Things, sometimes technologist call it “Internet of Crappy Things”. So, some security issues which can be found in the Internet of Things system are explained below.

The Security Survey of Global State of Information, issued by “Price water house coopers” approaches to a conclusion that almost all of connected IOT devices have less fundamental security protection. Inherently, IOT products are getting vulnerable to threats. By taking real world example, since 2014, driverless cars have become legal and also some people are using it. But besides its advantages, the automated sensors can be affected by threats. Nowadays, along with cars, automated drive-through car washes can be controlled by IOT. Kaspersky’s expert validated security in fitness bands. These IOT products can be used by a latent attacker to retrieve information about the owner’s location. Moreover, beyond these threats, more dreadful condition can happen when there are threats in the Internet-connected insulin pumps and active pacemaker which is wireless transmission inserted in a patient’s chests.

According to a survey, devices can have different arrays of potential risks in the Internet of Things system. It can be better understood by taking an example of smart TV which can be used for surfing the Internet, for purchasing things or even for sharing photos to social networks. All these data are transmitted through TV. So, there is a possibility of risk of privacy of data. Furthermore, sensitive details of a bank card, personal data or passwords can easily assist identity theft. All this information is so sensitive that attackers can get their hands on easily.

Beyond these, there are also records of some wide range threats. Symantec, the IT security company discovered a new bug in a computer. Its target was traditional computers as well as some specific small IOT devices like web cameras, smart TVs, smart homes and home routers. By detecting all these damages, it was deduced that even wireless speaker system and smart refrigerators were also hacked. Thus, all these examples show that as the number of connected devices in IOT system escalations, it gives a chance to a hacker to attack the huge number of devices.

For present products of an IOT system, security versus efficiency is another dilemma. When resource constraints like insufficiency of battery and security of devices are considered, manufacturers always try to balance between some critical factors. At the moment, they cannot sure about the correct solution for implementing the integrity, availability measures and confidentiality without controlling the computational resources or optimization of energy. From all above-mentioned explanation, it can be observed that there are mainly four specific issues for the security of the Internet of Things.

- Unauthorized Access
- Encryption
- Updates and Patches
- Lack of Experience

Unauthorized Access

Providing protection against exposure to physical attacks is a challenging security issue for smart IOT devices. Sometimes IOT products are neglected for security. Because of this reason, these objects are easy prey for malicious attacker for capturing that objects and for extracting cryptography secrets. They can easily modify programming codes and make all those devices under his control and new devices are built such that it can capture login information of the user. For example, a device like USB chargers can hack a wireless keyboard. Due to this, it can be able to send data directly to the device of an attacker.

Unauthorized access can be very dangerous for creating potential risks to safety. According to a survey, it also affects to automated medical machines like insulin pumps. They can be hacked remotely so that they can be able to deliver the deadly dose of medicine and scheduled injections. Besides this, some series of experiments proved that an IOT system in a smart car can be accessed through a built-in unit wirelessly means without even touching the car. Some surveys or conferences have proven that even small wearable devices can be accessed illegally via Bluetooth radio. One research study proves that built in security features in IOT devices are not good enough by revealing various security defects in many IOT applications like TVs, door locks, web cameras, home alarms and various thermostats. Many of them undermine the factory made authorization features. Because of this reason, they can immediately detect for security threats. Most of them are failed due to lack of strong password authorization. It is said that “passwords are the lowest hanging fruit when it comes to authentication”. Because most of the IOT devices rely on it, there is a possibility of unauthorized access to these systems. Moreover, many devices of an IOT system have a

limited user interface without keyboards or screens. Because of this reason, by default, the system of password authentication can be weak. That is why many IOT smart applications can be sensitive to physical attacks. Thus, from this discussion, it can be said that in a world of the Internet of Things, where everything is connected to everything and everywhere, the working of the whole system looks like magic but in reality, it is completely different.

Encryption

Besides the issue of unauthorized access, there can be an issue of encryption for security in the Internet of Things system. The survey shows that there is a lack of encryption in many areas of IOT like data storage and communications, backdoor credentials, command-line interface on a port of network and accounts with weak passwords, bypass of authorization or privilege escalation. In such cases, it is possible that many security issues can be found simultaneously even in a single device. In a network of the Internet of Things, it is difficult to insert security measures like encryption because of small size, low power and the computational incapacity of devices.

This explanation for an encryption issue proves that there are some specific operational constraints for IOT devices and for these devices, various security measures should be taken into account. To support more secure measures for encryption for transmission of data, processing power is necessary. The survey for IOT shows that most sensors are not capable of finding an encrypted link because of some priority issues. It undermines the satisfaction of consumers for IOT products. For this, various alternative methods for a safety of data should be established. In such cases, it creates another issue. Machines are not always configured. So, it can be directly accessible through the Internet. Besides this, if the machines run with default settings or default passwords for a long time, then it can provide an easy and convenient access point to cyber villains.

Updates and Patches

For the security of the Internet of Things, there can be an issue of security if connected devices cannot be updated on a regular basis. If all the connected devices located in a network of an IOT system, is not updated regularly, then it welcomes extremely unsophisticated cyber threats. The risk of cyber-attacks can be increased due to this reason. One fact shows that many industries do not update their systems or IOT networks. The reason behind this is that firms which involve in a development of low-end devices can lack economic encouragements for giving continuous support. Because of this, there can be a decrease in consumers after the purchase from an unsupported IOT system with many security defects. Moreover, many of the IOT products are built from inexpensive chips and other materials. Due to this, manufacturers do not encourage to provide security patches for these industries. The other reason can be that there is a lack of technical expertise of IOT vendors for developing such updates. For some reasons, the fundamental issue is fewer communication channels for a company for remotely delivering the patches because of its convenience for such companies to let consumers download and install manually. This point undermines the consumer's satisfaction. Some of these consumers can experience difficulties for installing updates or a lack of awareness of their existence in first place. Some reports for IOT security show some cases for the security vulnerability and they show that for data controllers, it may not be easy to provide updates or patches to it and even if these cures do exist, many of the consumers may not find out about them.

Furthermore, if there is a presence of unpatched vulnerabilities, another weakness is that they can be addressed by specific search engines. In such cases, even if consumers are familiar with the presence of such vulnerabilities, they cannot be able to access updates of vendors due to some limitations of hardware or some limitations of technology which can be out of date and it can keep away the device from providing support for software updates. It is important to note that it can negatively affect all of the connected devices if there is a compromise of vendor's update. Because of this reason, the mechanism of firmware updates should not be automated for every device.

Lack of Experience

Sometimes, instead of PC hardware or software businesses, consumer goods manufacturers design the networks or devices of an IOT system. Sometimes there may be an issue of lacking proper experience of secure products and services. Besides this, from the above discussion, it can be said that it is more difficult to secure connected devices in IOT system than to secure conventional stationary computers because to design secure IOT products, it requires a huge number of multiple skills that can cover up all the areas like applications, the entire infrastructure, and all the devices without leaving the communication channel. The main obstacle for generating the secure environment for all these elements in an IOT system is a lack of experienced security experts specializing in IOT tech trends. New engineers or fresher may not have the experience to handle these security problems in IOT. Sometimes, in some tough security cases, it is possible that experienced or expert IOT manufacturers may find such problems hard to solve with a rapid pace of this new digital revolution. Because of this, it is possible that in an agenda of current IOT manufacturers, securing all the IOT connected devices and networks may not be a priority item.

Moreover, in reality, users of an IOT system generally do not bother with all these matters related to security. According to them, a connected air conditioner is still a simple air conditioner. For them, connected devices with a smart car are still operated normally and working properly through the car without any obstacles. Although aggressive marketing campaigns organized by various companies provide guidance to consumers, consumers rarely look at a connectivity option as something that can affect the real world. No matter how secure these applications or networks are, the company should provide guidance to users on using products safely through websites or advertisements or on packing. Moreover, company executives or experts should provide training to a small group of employees for the ability to teach costumers about usages of products and how to put on the best security practices such as how to manage access control the right way or how to change passwords of products on a regular basis and also for resolving critical security problems on their own.

Furthermore, last but not least, it is not necessary for IOT manufacturers or developers to focus only on security threats generating from outside like external hacking or any outside attack on a system, but they should also focus on specifications of products so that it can keep away products from external threats. It is necessary for IOT developers to attempt employee specific practices.

So, this is all about various security issues which can occur in an IOT system. Because of all these issues in IOT security, it is also necessary to be aware of different challenges for securing the Internet of Things systems. These security challenges are discussed below.

Security Challenges for the Internet of Things

Large number of data collection and Vulnerability

In an IOT system, more devices can be installed and connected to other machines through the Internet. Installing more devices most likely increases vulnerabilities. They are very sensitive to physical or cyber-attacks because of relying on wireless communication. Due to multiple connections between devices and transmission of multiple data between them through sensors, even a small single device or sensor in a whole network of the IOT system embodies a potential risk for that system or network. It destroys the confidentiality of collected data and the integrity of sent data. It makes the whole network vulnerable at multiple points of the network. Even if anyone line becomes weak, it can open up access to thousands of devices on a network. That creates a potentially hazardous condition for that system. For the security of an IOT system, the factor of vulnerability includes many IOT products, embedded software, communication channels, data transmission or reception platform or data centers for analysis of data etcetera. It is necessary to provide security to all of these platforms.

Providing protection against potential risks to all of these platforms is a serious challenge for industries. One security expert explains that to secure an Internet of Things system, it is necessary to secure IOT products and to implement multiple features at a system level like account management, access control, segregation of accounts and networks, secure protocols for transmission of data and management of antivirus updates. Thus, it is a serious challenge for securing the IOT system.

Data Integrity and Trust

Data Integrity means to maintain the data accurate and consistent throughout the system to make it reliable. Data integrity is a critical aspect of a secure network. For efficient data communication, data integrity is an important factor. In an IOT system, there is a bombardment of a huge amount of data between connected sensors. So, there can be a possibility of interference of data between devices and it will result in transmission of wrong information to a destination point. So, it breaks the concept of data integrity. If a destination gets the wrong data then, it is possible that the whole system cannot work correctly and there are no means of using such system. Moreover, due to issues of accessing other accounts and also issues of hacking the whole system, gaining trust for the use of an IOT application can be a serious challenge for the future. Trust is a foundation of an IOT system and it is necessary to be fortified by security and privacy.

By taking the example of utility companies, which automatically collect readings from smart meters. The survey shows that smart meters widely used in an industry were hacked for excessive use of energy. They were able to skit messages being sent from a smart meter to utility company, and it was result in sending a false data. In recent years, there are many anti-virus protection devices or software exist for the protection of PC or hardware devices. That security facility does not exist for most of the devices. In this case, it becomes a challenge to build security into the design of all these IOT devices and systems to create trust and to keep the integrity of a data for that system.

Data protection and privacy

The main goal or mission of this technology is to make the lives of human-beings easier, to increase the efficiency and productivity of lives of human-beings. There is a huge amount of data transmission and reception between devices in an IOT system. The collected data helps to make one's decision smarter. Despite this advantage, it also impacts on privacy expectations. There are no means of using automated IOT devices like smart homes, smart lock, smart car, smart bags or any personal IOT device which fulfills the requirement of humans efficiently, if it is hacked or if there is no privacy in it. All these personal devices have confidential information of a person or an industry. If IOT security will not take care of privacy or if there is a compromise in collected data by any devices in IOT system, it is possible to undermine the trust in a system of IOT. So, expectations from persons or industries for privacy in an IOT system challenges an IOT security.

Besides this privacy matter, it is also necessary to take care of a security that protects the Critical National Infrastructure (CNI) like air traffic control and oil fields. In such cases, there is a huge amount of connections. So, the Internet of Things crashes the separation between these infrastructures and the consumer world. Beyond this, it is possible that even household items can potentially be exploited by cybercriminals to gain access to Critical National Infrastructure. It is a biggest security challenge to protect all these CNI apart from household IOT devices or networks in any industries. Thus, it is necessary for any industries or businesses to identify the risk level for current and future exposure to IOT. Industries or businesses should also think about the privacy and security implications which are associated with the volume and type of data.

Other Challenges

Apart from all these challenges, there are some challenges in establishing the Internet of secure things which includes Critical functionality, replication, security assumptions, a long life cycle and industry specific security protocols. They are explained below in detail.

Firstly, the critical functionality of a network can be a serious challenge because in addition to simple devices or systems, IOT applications and networks can also control various systems like infrastructure, transportation, communication systems, utility grids. Secondly, once IOT devices are developed, there may be the production of thousands of identical devices. So, if hacker is able to hack one of those devices, then it is possible that the attack may be replicated across the whole system. Moreover, the third challenge is regarding security assumptions which explains that many of IOT developers have long assumed that IOT products cannot be the target of hackers. Due to this, they do not give priority to security in IOT devices. Now, connected devices in IOT ecosystem often use specific protocols. Sometimes, security tools cannot protect them. So, there should be protection against threats to such protocols. So, it is all about various security challenges can be found for securing the connected devices in a network of an IOT system.

It is said that "Nothing is Impossible" in a world of IOT. So, if there are problems in the world, then, there are also solutions to overcome that problem. Because, no technology can come into existence, without solutions to overcome its problems. Innovators of this new technology may be aware of security problems before they launch any product with new technology into a market. So, they have to find solutions for this negative impacts related to security of connected networks. In such cases, besides these security problems, there are also many solutions to provide advantages of IOT products to customers or consumers, or even to IOT developers which are discussed in the next section.

Solutions for the IOT security

The Internet of Things has become a ubiquitous term for today's world. There are a number of different sectors which serve for segmenting the IOT market such as buildings, energy, industrial, transportation, health care, life science, retail, security, public safety, Information technology and networks. Now, as explained above, in an IOT system, a large number of devices are connected and they can create services. Because of different sectors in which IOT applies, it is necessary to take care of the security of IOT devices in all sectors. It is possible that the solution to secure one sector may be different to a solution for another sector. It is also possible that one of many solutions for securing the network is different than another solution even within a sector. There are a number of IOT platforms and the purpose of these platforms is to put lots of applications on one platform by bringing them together. Thus, for IOT security solution, it is necessary to look at a data coming together from several different sectors because it is not only about individual machines, but it is about the whole environment around them that brings them together.

The underlying principle for securing the IOT system can be accomplished by using multiple layers of security protection. It is necessary to take care of security of data stored by IOT devices, secure communication, and it must ensure the protection against any attack like cyber-attack to devices. This goal of security can only be accomplished by including security in an early stage of design. To secure the IOT devices, there are some requirements which should be taken into consideration various parameters like the cost of security failure, the risk of attack and also the cost of applying a security solution. To secure the IOT networks, following features of solutions must be considered.

The first solution is to secure boot which can be accomplished through the use of an authorized code from a manufacturer. Hardware support is also necessary to verify the authentication of code. In this way, it ensures that the code is not altered. It also ensures that there is no malicious code in a system. Secondly, the system update is also an important solution for securing the IOT network. The method of secure code updates ensures that the device is updated for fixing the bugs, for security patches, etcetera. The system update also includes updated passwords for securing the device. All communications between IOT networks should be authenticated using strong passwords and strong secure protocols. Because to improve security, it is necessary for IOT devices to make restricted access to an IOT network, to disable default non-critical functionalities and also to disable the use of a untrusted software. It prevents an unauthorized access to a device and it gives benefits of encrypted data storage and encrypted communication. Thus, it contributes to narrow down the possibilities of attacks on a system and provides secure system.

Moreover, protection against cyber-attacks is also an important feature for securing devices. To achieve this, firewall settings should be modified. A firewall should limit the communication to only known and trusted hosts. It should be able to block hackers before their launch of an attack. A firewall can provide all these protections and some of them are also inbuilt for many applications. Besides this, IOT networks should be monitored to identify abnormal traffic. So, intrusion detection is another way to provide security to IOT system. Sometimes, IOT devices are attacked but no one knows that attack. An attacker or hacker can execute thousands of invalid login attempts without being reported the number of attempts. So, IOT devices can be able to detect and report the number of invalid attempts and other mischievous activities done by a hacker. The interesting feature is the ability of device damage detection. Nowadays, many new boards or processors have capabilities to detect the damage of a device. They can be able to detect the broken parts of a device. This helps to make the conclusion that someone may be attempted to tamper the device. Thus, all above discussed solutions help to prevent the security to an IOT system. It helps to protect all the devices connected in an ecosystem of the Internet of Things.

Opportunities for Security in the IOT market

If these solutions are managed in IOT system and if they are succeeded in establishing the secure environment in IOT system, then people can get many advantages of it. It can create many opportunities to enable smart services in the world of IOT.

Fig. 6: A smart city.

This can be helpful to enable smart city as shown in figure 6. Smart city can bring the whole collection of different services together. They can share different data among sensors that are scattered around the whole city. It also provides lots of services for citizens and frequent users of a system by taking advantage of various information coming together in the whole city. Moreover, huge security concerns can be in a transport system, energy, Information Technology (IT services) and so forth. The system can create an overall structure by putting all things together. There are many benefits due to this smart city. It can reduce cost, encourage new productivity and provide the Internet of secure things by providing secure environments.

Secondly, it is also useful to establish smart farming shown in figure 7, in which all of the devices, tools or vehicles can be connected by satellites through the low-power wide area or through Wi-Fi or cellphones. It connects all the devices together to provide efficient communication between them. Due to a large population in the world, it is necessary to improve production in farming and production of food. The Internet of secure things is able to find this opportunity.

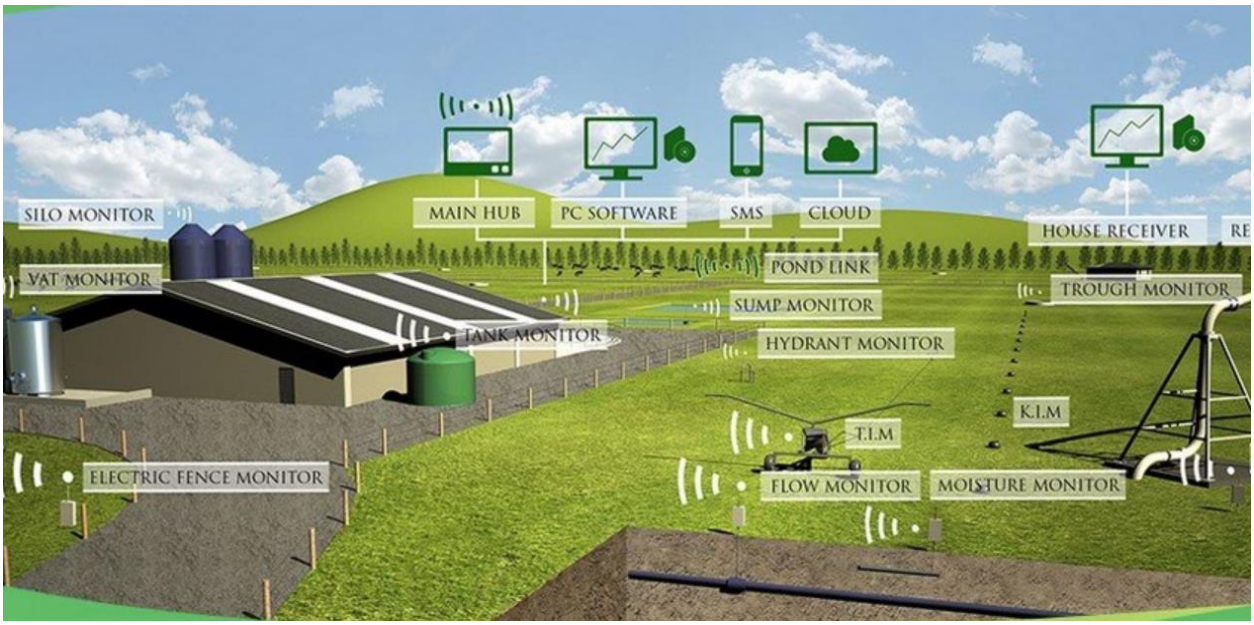

Fig. 7: Smart Farming.

Generally, the industrial sector has many connected devices to control many operations. In smart factories, lots of sensors are connected together. At that place, IOT security helps in optimization of operation and provides higher efficiency. The same concept applies in an energy sector to make it smart. There is a great opportunity for IOT to create optimized and low power IOT devices with long lasting efficiency and with less power consumption. For retail sector, it is also useful.

Moreover, if the issue of security is solved then, it will create a great opportunity for the area of healthcare. This area requires certified solution for security. It requires certified hospitals. It should ensure the condition of a patient whether patients are properly cared or not, operations are performed correctly or not. It is also necessary to take care of privacy of patients. Thus, all these tasks related to healthcare are very complicated. That is why there are lots of opportunities to enable smart healthcare.

In reality, everybody needs to way out of risks and costs. There should be some benefits when developing a new market. To develop a new technology, there should be adequate enable security in a system. Security is a fundamental key issue. It is a fundamental key enabler to market to create all these "Internet of Things" opportunities in real life.

Conclusion

In a nutshell, this paper shades a light on an intriguing technology – The Internet of Things along with data security in this ecosystem. The Internet of Things is a connection between the physical world and the digital world. IOT has the ability to sense, communicate, and wirelessly manage the huge number of connection between automated devices through the Internet. It is accelerating at a very fast pace from factory floor to hospital operating room to residential basement to even simple washing machine or microwave. In other words, everything can be connected and communicate with each other to make this world more electric, more digitized, more decarbonized and decentralized.

Behind this fascinating face of the IOT, there is a terrible face of IOT. The reason behind the ugly truth of this terrible face is Security. Security is a key issue for successful data transmission between devices. Without the security of data, there is no means of any benefits of IOT. If data is not safe or its integrity is not maintained, then it is possible that destination cannot get correct information. Such cases can cause many problems. It can create hazardous issues in various areas of IOT network. This paper explains various security issues like unauthorized access, encryption and system updates, which can be affected to security as well as the privacy of an IOT system. Due to these issues, there are many security challenges such as data protection, data privacy, vulnerabilities at multiple points and data integrity. They should be taken into consideration to secure the IOT system. On the other side, every problem has solutions. There are many solutions for securing IOT networks like authentication, regular secure updates or use of secure protocols. By means of these features, it is possible to prevent IOT networks safe from hackers.

Finally, if all these issues related to security are solved, then there will be great opportunities to co-create the future. IOT can provide solutions to every problem by connecting all things together. It can enable smart communication between all devices. Due to this technology, it is possible to convert imagination of smart cities, smart farming, smart factories, smart health care into reality. This can give many benefits for human-beings. It makes human lives more efficient, convenient and easier. So, at the end, Life will be good…. ☺

References

1. "Internet of Things (IOT)." *What Is the Internet of Things (IOT)*. Web 09 May 2016. http://www.sas.com/en_us/insights/big-data/internet-of-things.html

2. "Security Challenges in the Internet of Things (IoT) – InfoSec Resources." *InfoSec Resources Security Challenges in the Internet of Things IoT Comments*. 2015. Web. 09 May 2016. http://resources.infosecinstitute.com/security-challenges-in-the-internet-of-things-iot/

3. "The Internet of Secure Things – What is Really Needed to Secure the Internet of Things?" *Icon Labs*. Web. 09 May 2016. http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things

4. UKNMI. "The Opportunity for Security in the IoT Market." *YouTube*. YouTube, 2016. Web. 09 May 2016. https://www.youtube.com/watch?v=wXKy5pw-Pls