INTERNET OF THINGS AND CYBER SECURITY

Rakesh Kumar Chawla[1], Prof (Dr) JS Sodhi[2], Prof (Dr) Triveni Singh, IPS[3]

[1]*Ph.D. Research Scholar, Amity Business School, Amity University, Noida; Technical Office, National Crime Records Bureau, Ministry of Home Affairs, New Delhi, India, rkconline@gmail.com*

[2] *Professor, Group CIO & Sr. Vice President-Amity Education Group, jssodhi@amity.edu*

[3]Superintendent of Police, Cyber Crime at Uttar Pradesh Police, 100triveni@gmail.com

Abstract

The world is changing at every single minute, and the generations have to keep up the pace. In this busy life everybody is trying to find a peace of mind and the technological advancements are giving a good grip to hang on the life. This is how busy the human race is, no time for food but nutrients can be taken in the form of supplements. In a similar manner the Internet of Things(IoT) is helping people by filling up the void in their daily life. Its all about connectivity, gone are the days when internet was all about certain webpage and websites. IOT is much more than that, its about sensors and software coordinating with other technology connected through internet. But with great power comes greater responsibility. As in IOT is all over the table, covering every aspect of life but there is a warning attached to it. Since everything is exposed to internet there is a possibility of data theft, hacking, phishing attack, etc. So the security is the biggest question now, since no matter how big the organization, data theft is a big deal but IOT is not restricted to few organizations instead it is available to each and every individual. The simplest example is the smart watch. Lot of development is going in the direction of IOT and its security zone and there are a lot of corners which are still unscathed. In other words, IOT has its advantages as well as some cumbersome data leakage that is still the biggest debate.

Keywords

IoT, Security, Internet of Things, IoT Projects, Global IoT Security Regulations, Cyber Security

Introduction

Internet of Things is explained as the basic amenity of human development. It gives a new direction to communication. It has given rise to new notion i.e. the smart world. “Internet” is a pretty common word but IoT stands for “Internet of Things”. So the other word “thing” is

very amusing. According to Samuel Greengard, there is a long way to go and the journey is filled with dark clouds, so survival mechanism needs to be strong enough. But irrespective of all these shortcomings IoT has gained immense popularity and is spreading across like wildfire. There is no such "thing" that is not connected through internet making lives better and comfortable with just few certain commands.

Kevin Ashton (MIT's Executive Director of Auto-ID Labs) took the initiative to name "Internet of Things" in 1999. He was the first person to acknowledge the beauty of IoT, but the definition of the IoT has taken several twist and turns nurturing the old meaning and evolving over time. But before that in 1980s, it was Carnegie Mellon University, which had a Coca Cola machine, local programmers used to connect to the refrigerated appliance with the help of internet, to check the availability and temperature of the colas. So far IoT has brought human life at ease and would continue to do the same because development and discoveries in this direction still has several light years to cover. Despite all these positive qualities there a lot of shortcomings too and the most challenging one is the security against cyber monsters.

Security is one of the most significant issues that exist today for IoT in the field of connectivity, communication and research. Security is not a simple term. To be discrete, security can be - security built within the device, security of data transmission, and data storage within the systems and its applications.

IoT

IoT stands for "Internet of Things", which means all the components help each other over internet to have a healthy communication environment within the snap of a finger. It deals with sensors, artificial intelligence, cloud environment, etc to deliver the best of services within the organization. Just like smart-phones, we can connect several devices through it and the wireless communication helps us to avoid any kind of helplessness. At the same time a smart-watch can be connected as well as a wireless headphone.

No doubt, over the short span of time IoT would rule the world because it is the demand of our hustle-bustle life. To cope up with our busy lives we need things that can remove the misogyny of time, but the rapid growth is also arising questions as to how safe is this.

IoT architecture

Architecture defines the efficiency of the project because it helps in proficient data collection and further planning although there is no universally defined architecture but there is a standard arrangement.

The architecture consist of usually consists of four layer-

- **Sensing layer**
- **Network layer**
- **Data processing layer**

- **Application layer**

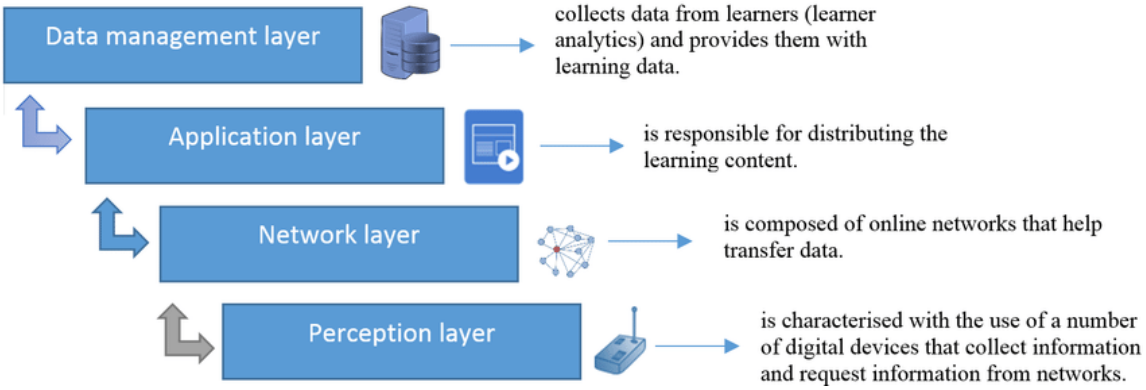


Figure 01

The Internet of Things is a novel concept in the modern day wireless technologies. The importance and gaining momentum of Internet of Things (IoT) is due to its presence around us in one or other form. For eg.- Mobile phones, tags, sensors, bar codes, etc. The simplest of our basic needs develop and start from IoT.

Undoubtedly, the greater the power of the IoT vision the greater the impact it will have on a few aspects of daily life and potential user behavior. From a private user perspective, the most obvious results of an IoT introduction will be visible in both the active and home fields. In this context, domotics, assisted living, e-health, advanced learning are just a few examples of application situations in which a new paradigm will play a leading role in the near future. Similarly, from the perspective of business users, the most obvious results will be seen equally in areas such as automation and industrial production, logistics, business / process management, human and logistics.

In fact, many challenging issues still need to be addressed and both technical and social knots need to be unraveled before the IoT concept can be widely accepted. Intermediate problems make full interoperability of connected devices possible, giving them a high level of intelligence by allowing them to adapt to their independent behaviour, while ensuring trust, privacy, and security. Also, the IoT concept poses a few new problems regarding network features. In fact, IoT-compliant features will be characterized by lower resources in terms of both calculation and power. Therefore, the proposed solutions require special attention to resource efficiency without obvious expansion problems.

Several industries, metrics and research themes are currently involved in the development of solutions to meet the highlighted technical needs. This study provides an overview of the current state of the art in IoT Specifically:

• provides students with an explanation of the different ideas of the Internet of Things paradigm of objects from different scientific communities;

• reviews the technology that allows it and shows the great benefits of the spread of this concept in everyday life;

• provides an overview of major research issues that the scientific community still has to deal with.

Through Internet of Things we are able to see the new era where everything seems to be interconnected. IoT allows the interconnection of embedded networks through wireless technology. It

leads to a highly distributed system of technology. IoT is currently opening various streams of opportunities for all sectors that promise to improve our standard and quality of life.

IoT can be easily used as a tool of global welfare. IoT is causing major digital divide. It encompasses a wide horizon of disparities and differences in various sectors. The perceived gap between those who have access to information technology and those who do not is called a digital divide. Digital divide is also closely linked with digital opportunity. Information technology is no longer a luxury but a development measure and tool. IoT might bring all parties to a level playing field thus leading to bridging the digital divide eventually.

IoT is not a new internet but it is actually an extension of the older one. IoT would not only change the face of the world but it will connect all devices the same way how humans connect through the web today. IoT will soon include all assets and real world elements. It is about the remote monitoring, control and about where these technologies are applied. IoT will automatically allow the assets of various enterprises and organisations to connect and gain profit accordingly. Simple machines and objects can be used more intelligently and effectively through IoT.

There is this benefit of every IoT oriented solution, that it comes with precision and much better efficiency. The IoT works on information from a lot of sources including sensor nodes, physical sources, data that is available in the open and private. Thus, this information and data becomes very complex. This complexity comes with a heavy cost. It can cause major security threats because it might get into dangerous hands. The question of security and privacy has to be dealt with accuracy and the quality of the information provided in the end has to be dependable.

IoT is basically innovation driven and it serves on multiple devices and multiple applications. It is very information and service centric. It works on the features of a data and information driven system. Its business is carried out in open market place. Also, it is very encouraging as it serves as a participatory and community driven system. It works on the principles of Business To Business and Business To Customer. It works between the emerging ecosystems and thus becomes an interactive space. It is an open web and service enabled system. Plus, it popularly works on cloud networking thus cloud deployment happens. The technology that works within IoT is a horizontal enabler approach. It also uses generic commodity devices. It strongly uses standards and open source in its working. In the process open APIs, web development, software development and data specifications are also used.

The increasing buzz around IoT has been created due to large markets and the growth around it. In IoT, the same information is used and reused again and again all thanks to the web based technology used in it. The steps towards IoT come through value based perspectives. This value is thought to be attached to IoT when it becomes a part of the information market. IoT value chains are to some extent enabled by open APIs. Open APIs allow information stored in different systems to become unembedded allowing many enterprises to combine their data till the time they have a proper interface to interact. The IoT value chains have a lot of inputs more than other such systems. Devices and sensors are the first and very important inputs in the IoT value chains. Open Data is the most important input in the value chain. Information is reused and recycled. New information will be made.

With IoT gaining momentum in daily life, comes with it the concerns related to IoT. The first concern that comes to mind is the compromise and vulnerability regarding its security. The compromise in privacy and threat to personal integrity is also constantly lingering with IoT. The collection of information from various nodes will allow identification of people and their identity even from

anonymous data. The information and data might also become out of beyond one's control due to so many complexities involved. With real life assets connected, there will be growing issue of a threat to people's lives, property and much more.

Not only the threats will be felt physically but also the costs in deploying IoT and its elements will be huge which will become major concern for the state and the people. Trust within IoT mostly means the amount of reliability that it can provide to its users. The amount of reliability points towards the data which IoT provides. The scale of dependability of the data will measure the effectiveness of IoT. So it clearly means that when building IoT solutions, it is important to ensure privacy of data otherwise it will become a source of threat. The amount of data that will be processes through IoT will be huge and its deployment will be very complex, thus it would have to be made sure that the data is not becoming infrequent and there is no effect on the performance of IoT.

IoT is the top notch that is the most needed right now. But this desirable asset becomes a threat when it comes to security and privacy. IoT has a lot to offer to the industry. It has a vast potential in its own. In the process of Internet of Things has been considered a new technology because devices don't need to be connected to the public Internet, they only need to be connected to a network and be recognized individually.

The field has seen dramatic evolution due to the convergence of various technologies. They include computing technology, commodity sensors, machine learning, artificial intelligence, embedded systems, etc. In the market based industry, IoT technology can be easily identified in products like smart home, smart watches, - These appliances support one or more ecosystems and can be controlled via devices related to that ecosystem. Smart phones, smart lights, smart air conditioners all use the same IoT technology that enable them to connect over a network and then work in cohesion. IoT is also popularly used in the healthcare system.

There are a huge number of concerns related to the increasing growth of IoT technology and its smart products. This risk analysis becomes even higher in the governance, infrastructure, international security, border relations, etc. It becomes a huge threat to privacy.

The growth of IoT has led to the increase in the number of smart devices. These smart devices are made to aid the customers. These applications work for a better and larger concept of home automation, connected health and appliances that can be controlled from a remote monitoring device.

In this broad spectrum of IoT working, home automation has a big role to play. It includes lighting, heating, air conditioning, security systems, etc. But this can have long term benefits which will include energy saving by switching off all electronic devices automatically without wasting electricity. It is actually based on hubs that control all home appliances. There are many examples of stand alone hubs which work and connect devices available at home. For ex. – Google Home, Amazon Echo, Apple's Home Pod, Samsung's Smart Things Hub, etc.

IoT products are also largely used for elderly care. Voice systems can be installed for people with visibility disability. Also, additional sensors and medical emergencies can be included in homes for creating it safe and secure for the elderly members of the family.

Thus, we can clearly see how IoT is leading its customers towards a new and higher quality of life. This quality life is the new aspiration of the gen Z. And thus this aspiration is extorted very fruitfully by the marketers to make a successful business. The term Enterprise IoT refers to devices used in

businesses and corporate offices. It is expected that EIoT will expand its business and worth to about 9.1 billion soon.

The Internet of Medical Things (IoMT) is basically the use of IoT in the medical and medicine related field. It includes research, data collection, monitoring, etc. In other words, it can also be called as Smart Healthcare because it includes creating a digitized healthcare system and then connecting it all over with all available medical resources, etc.

This healthcare will be very useful in times of emergency crisis management. The fit bands, advanced hearing aids, etc are some examples of very fine smart IoT based monitoring systems which are capable of monitoring blood pressure, heart rate, number of steps that you walk, and other specialized things. Specialized sensors can also be quipped within homes to aid the service of continuous monitoring of the ones in need and assistance. Then these reports can be directly shared with the doctor, and without going to the hospital, the doctor can see and tell the progress. This remote monitoring will make many things possible. It will help in managing the prevention of chronic diseases. Plus IoT also facilitates in creation of such beds in hospitals that reduce the need of the nurses in every little task. The beds can rotate and provide support required by the patient for getting up. It also contains particular alarms and sensors that can tell if they are able to walk properly and thus not fall.

IoT not only has the power to transform the medical system but it can also change the face of the transportation and communication system all over the world. Smart traffic control, smart parking, automated toll collection system, road assistance, etc are all very good basic examples of how different vehicles and traffic lights get connected to each other thus forming a network. This very useful data coaction and monitoring service of IoT is also being used in industries to help regulate and manage industrial set up. The IoT can also work wonders in the field of manufacture too. Network control, management, communication, asset control etc provide manufacturing with ease. The use of smart devices and automation help largely in the process. In this automated process, digital control systems create smart grids in which the industry functions independently using all safety and security measures within the purview of IoT.

There are a number of IoT applications that are associated with agriculture. They are mostly used for collection of data regarding the temperature, rainfall, humidity, wind speed, soil content, etc. This data can be further used to automate farming techniques, evolve new ones, etc. The ultimate goal is to increase productivity by combining the farmer’s experience and the aid provided by IoT. This will minimize waste and risks that are involved with traditional ways of farming.

A very good example can be taken from the August 2018 incident where Toyota Tsusho started a partnership with Microsoft to manufacture fish farming tools using the Microsoft Azure application suited for IoT technologies related to water management.

The bridges, railway tracks and wind farms use IoT on a large scale. They are the key applications of IoT. They are used to monitor and check for any structural change that might occur in any hazardous accident or might cause problem for the passers by. It can help tremendously by serving the industry on cost, time, energy and paper. It will make the repair very easy due to the real time situation data that it will provide. The IoT system will also help in reducing the number of accidents that can be caused.

There are many city projects that are coming up with an IoT deployment to make a new automated and smart city in countries like Korea, Spain, Singapore, etc. Many such projects with large

deployment are already in places like New York, San Francisco, etc. These large business deployments have smart lighting, smart heating, smart parking, smart WiFi, smart safety and security system, smart transports, etc.

The use of IoT can hugely help in the optimization of energy consumption as a whole. The lights, lamps, motors, pumps, other electrical appliances like mixer grinder, washing machine, air conditioner, etc already take up so much power. So, when IoT comes in the picture, it makes power generation very balanced and thus reduces on energy usage. The devices inbuilt with the IoT system have easy remote access with the users or the central authority via the cloud system. The cloud based interface allows remote scheduling of various devices. The formation of smart grid helps in the saving up of energy being used in the system. It is a utility side of IoT which prevents any wastage of energy and keeps charge of the efficiency of energy being used.

IoT is very helpful when it comes to the over exploited environment. The sensors used in IoT applications will help in assisting in the task of environment protection. It can easily monitor air quality, water quality, atmospheric or soil conditions, etc. The detection of earthquakes, tsunamis, floods and other natural calamities will also help in saving lives and livestock and act as an early warning system during emergency times.

The Internet of Things has huge prospects of being used in the military field. It will use sensors, machines, ammunitions, vehicles, etc equipped with special IoT battlefield mechanism which can alert the soldiers before hand and get them onto their feet. It can also be used under water, in the ocean for collecting data regarding all vessel activities, check for any attacks being planned, etc.

Other very effective usage of IoT can be seen in the smart packaging of products which allow you to scan a QR code and get to know everything about the product. These QR codes are basically unique and individual identifiers. This also happens in restaurants where you go and ask for the menu. The waiter in these restaurants will tell you that they are going paperless and you need to scan a QR code for ordering your meal. Thus, it points out how in every small detail of our lives, IoT has made a space for itself. And we are so used to it that we often tend to forget and even ignore how IoT has gripped the world in its changing atmosphere. These passive things are not the direct implications of IoT but they can be seen as small and basic digital enablers of IoT. This can also be seen as the first wave of IoT in India that we witness every day in 2022. But this should not be taken as granted because the same things of going online and ordering our meal was not possible till very recently in developing countries like India.

Technologies behind IoT

There are various technologies that help in the functioning of IoT. The idea of the Auto ID Center is based on RFID tags and unique recognition through Electronic Product Code. ADRC gives an application layer protocol and helping framework that can support in executing the IoT applications. Other technologies that support the system of IoT applications are short range wireless, medium range wireless, long range wireless, wired technologies like Ethernet, etc.

Some experts and scholars of various fields have argued that the IoT applications can also be used to create new models of civic engagement if device network are open to user control and inter usable platforms. It can be used to point out the ultimate beneficiaries of various schemes and policies.

IoT suffers from a lot of problems that cause criticisms to it. There is huge platform fragmentation in IoT which mainly happens due to the lack of common technical standards and the variation in hardware and software on which it runs. IoT devices are thus hard to maintain and an inconsistent

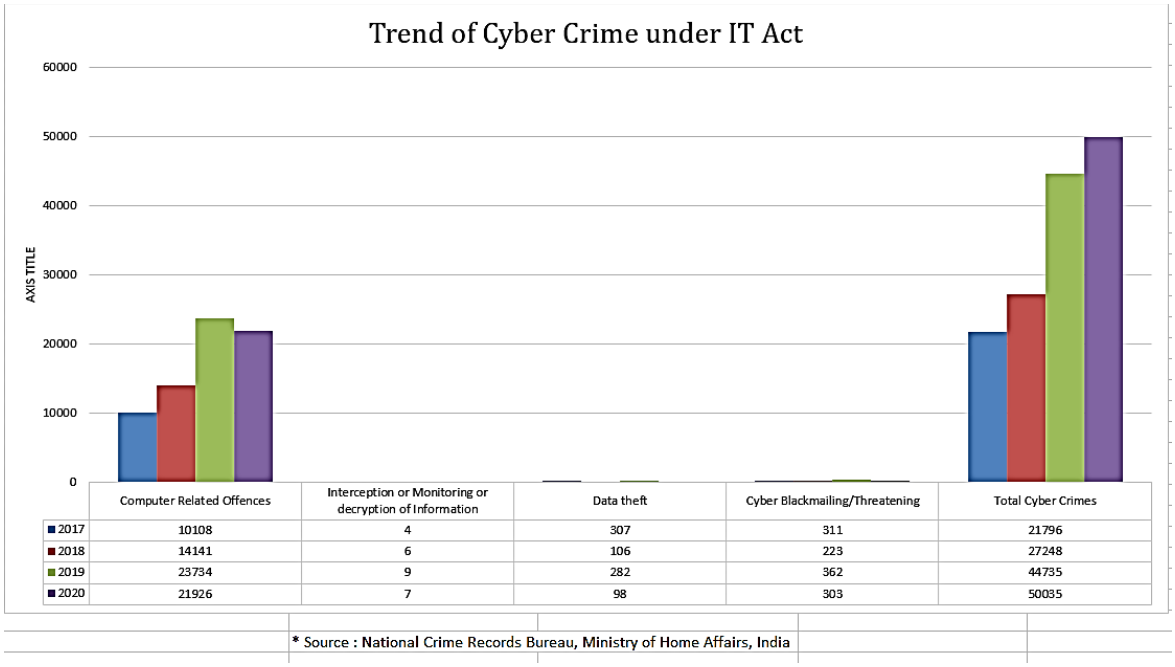
network is established. IoT has largely broadened information access to the common citizens. But this increased access causes a threat to individual privacy, thus, making information and data vulnerable. It may lead to social control and data manipulation. Concerns have led scholars to believe that Internet of Things is basically incompatible with the concept of security and privacy.

Also, many experts have argued that IoT technologies are not just an invasion to our privacy in public spaces but it also causes the rise of a normative behaviour by people from all walks of life. IoT devices misplace the user attention and usually make believe that IoT is all about human augmentation. IoT has made the notion in people's mind that IoT will be the end of privacy and also it will lead to rewriting of all privacy rules. Another issue with IoT producers is managing the vast amount of data already stored on the system. The various networks share the common data collected by sensor nodes which finally go to distributed system. When you have this huge amount of data with you, then the biggest issue is about its storage. Where will you sore this enormous data? The increasing storage capacity further causes a daunting challenge to energy and thus power generation. When you store your data, other questions like transparency, autonomy and others are considered too. These challenges are posed by manufacturing side. But if one has to extract optimal benefit from IoT products then it will have to keep in mind its data storage.

IoT Security Challenges

Security is yet another big question mark on the face of IoT, because security as a principle and basic need is not being discussed in the rapid development of IoT. Most of the security concerns related to IoT are similar to that of androids, servers, etc. These concerns include mishandling of security updates, not changing the default credentials, weak authentication, unencrypted messages being sent, etc.

According to Microsoft experts, India will be one of the top 3 countries for IoT malware infiltration in 2022.



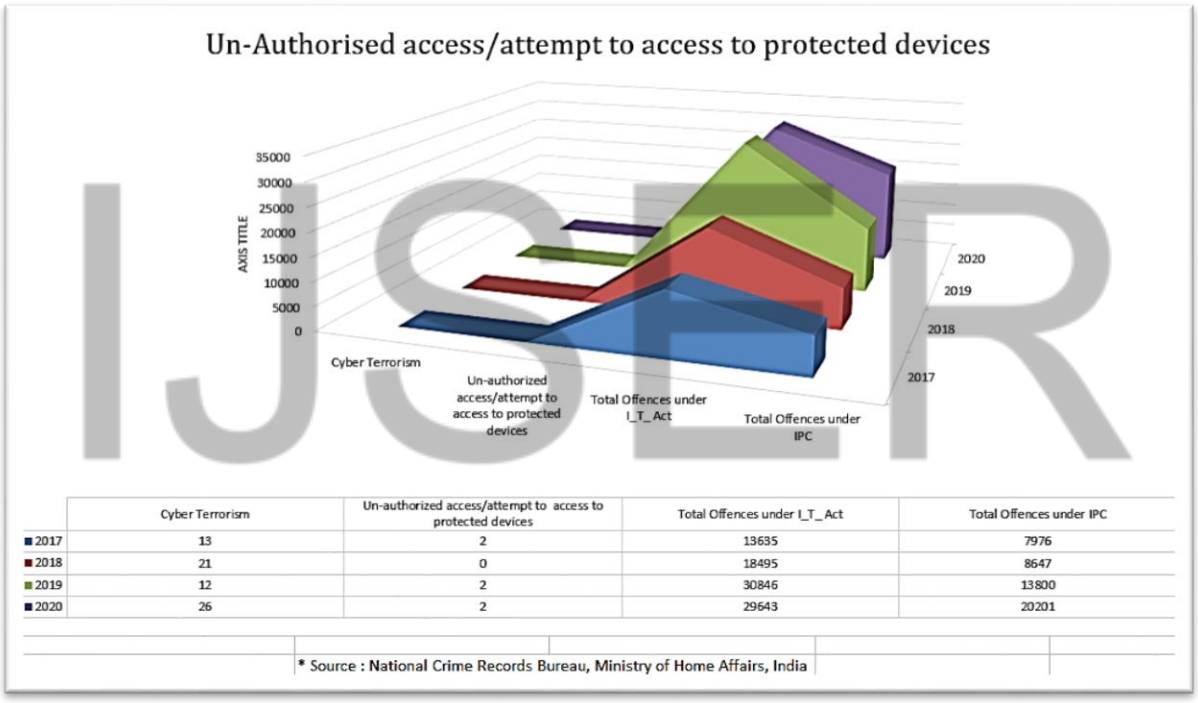
	Computer Related Offences	Interception or Monitoring or decryption of Information	Data theft	Cyber Blackmailing/Threatening	Total Cyber Crimes
2017	10108	4	307	311	21796
2018	14141	6	106	223	27248
2019	23734	9	282	362	44735
2020	21926	7	98	303	50035

* Source : National Crime Records Bureau, Ministry of Home Affairs, India

Figure 02

Apart from all other conventional attacks made on IoT, it is also popularly being threatened by fault injection. Fault injection attacks are physical attacks whereby the attackers try to introduce faults in the system. Faults sometime happen on their own due to electromagnetic field and noises also.

The risk of spying is also there with IoT devices because one device can manage other devices and they have access to a huge amount of data. Thus these devices become very easy and simple prey for cyber attackers. Thus many scholars feel that government restriction on IoT based products is very important. Due to the reliability of IoT, it also causes some unforeseen situations that might become very dangerous for the people around it. Detection of such flaws will require a holistic approach from the authority. The designing of IoT is another concern. Experts have argued that the successful accomplishment of IoT requires it to be more user friendly and integrated technology. IoT devices will bring major twists and turns in the field of environment. The environment which is in a very vulnerable state right now due to all the bad chemicals produced in the generation of electricity will increase moreover due to the over use of electricity day by day. Thus, major societal and environmental questions are highlighted towards IoT devices.



	Cyber Terrorism	Un-authorized access/attempt to access to protected devices	Total Offences under I_T_ Act	Total Offences under IPC
2017	13	2	13635	7976
2018	21	0	18495	8647
2019	12	2	30846	13800
2020	26	2	29643	20201

* Source : National Crime Records Bureau, Ministry of Home Affairs, India

Figure 03

A sample of a smart watch can be taken to see how the by-product of IoT is vulnerable to security concerns. Smart watches are the new fashion benchmark for all young and cool people in a country like India. These portable and easy to wear smart watches are very popular due to their multiple uses and well defined functions. They monitor our health specifications including the number of steps that we walk, our heart beat, pulse rate and what not. They even help us in making phone calls, send messages and check all notifications. This multiplicity of purpose that it provides is a result of Internet of Things. IoT has made possible the connectivity of devices over a network thus facilitating our needs.

But just like every other device of IoT, smart watches are also under vulnerability of attacks and risks that may cause data manipulation. At present there are not a lot of breaches related to smart watches but there have been a lot of attempts.

Here are some basic steps of keeping your IoT devices safe.

1. **Update your smart watch regularly** - Even though putting off all updates might seem very tempting but in the long run it can cost you your privacy and mental peace. So avoid doing this mistake and keep your smart watch updated.

2. **Keep a strong password** - Using easy to guess passwords like abc, 12345, 090909 are big mistakes. If you want your device to be safe from malicious attackers then use stronger and tougher passwords.

3. **Two factor authentication** - Now this is the most important step. You just have to switch on your two factor authentication. This provides a protective layer thus giving an extra valve of precaution to your device.

IoT projects

Smart LED Street Light Systems

Street lights are very important for perfect night vision of human eye and it helps one to avoid inevitable road accidents, which can be fatal and could also lead to loss of important life. Therefore, every organization, private as well as government is working towards road safety guidelines and is making efforts in this direction to uplift the current condition to get the road accidents happening every year under control.

Smart LED Street Light Systems is an important project in this path which will be worth the investment and will reduce energy consumption. It will be purely based on real time data and sensors which will ensure the smart off and on stage, i.e. intelligent management of light consumption and moreover, without regular human intervention. This will also seek the error detection and notify the faulty lights with the help of whole IoT system. LED's power saving feature combined with sensors and networking chain (IoT system) would prove to be a deadly combination benefiting in various ways.

Further, one can make it simple with more complex solutions, with the help of cloud computing and artificial intelligence, one can handle weather forecast and make real time weather reports available. On the other hand, one can also use it to detect real time traffic situations in the areas which will lead to less traffic jams and to help report accidents at the right time so that life can be saved and aid can reach on time.

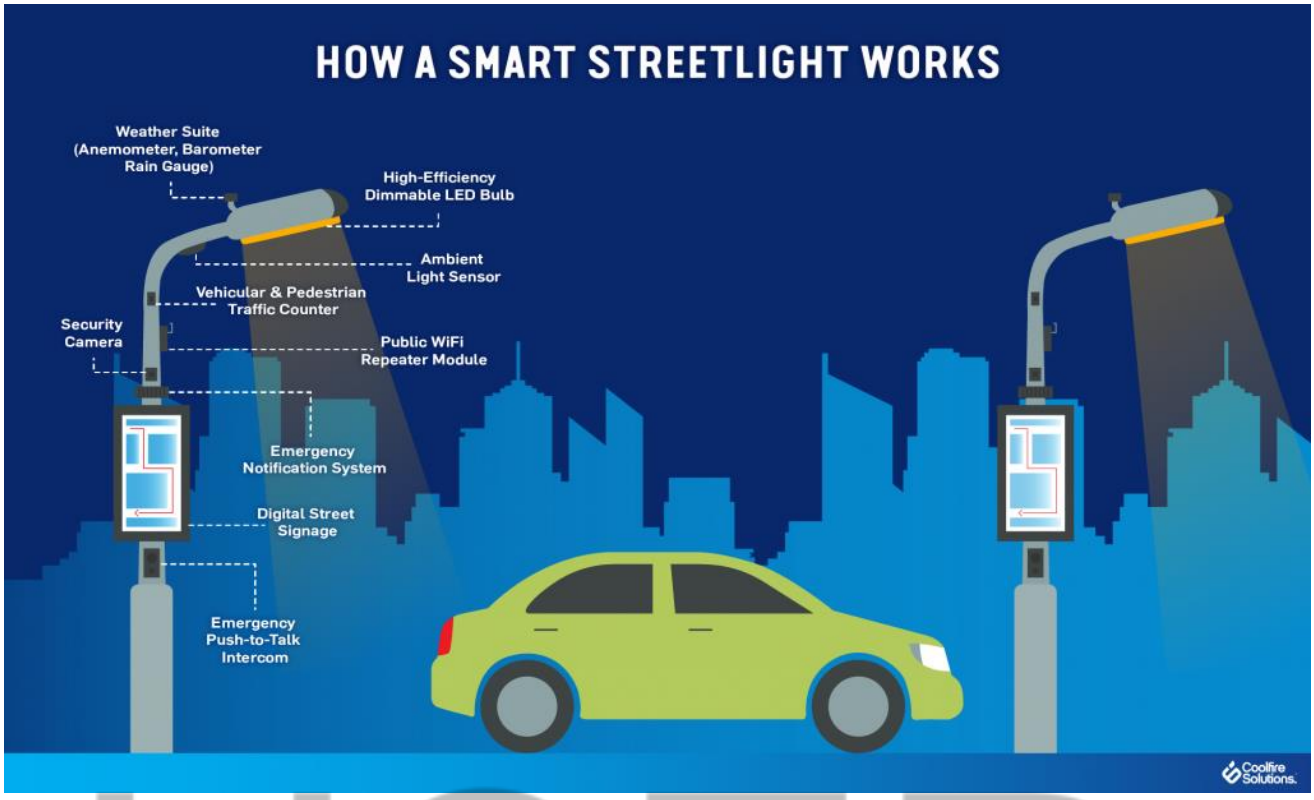


Figure 04

Award winning retarding basin monitoring

Global warming is the most debated as well as heated topic of every foreign meets or every other convention is based on environmental issues. Although earth's composition includes 71% of water but to be very precise the freshwater fit for human consumption is available less than 1%. This shows the scarcity of water and the need for conservation. Therefore, sustainable development is very important because there is a sufficiency in the world for man's need but not for man's greed (stated by Mahatma Gandhi).

Therefore, proper utilization and treatment of groundwater is a basic necessity because all the living flora and fauna require water for their survival. Moreover, groundwater is at a critical level.

Therefore, water authorities in Melbourne wanted to monitor the groundwater which was collected in the basins mainly due to heavy rainfall and man holes for proper consumption and for treatment of water. It was a challenging task to reach groundwater at difficult angles and test it for consumption. SAGE Automation came forward and formulated an inexpensive and reliable method to keep groundwater under check. This arrangement included cloud services, field sensors for visualization and understanding. It reduced manpower, difficult terrains became easy for further speculations.

In 2018, this IoT based project received several accolades including *Victorian Australian Water Association Infrastructure Project Award.*

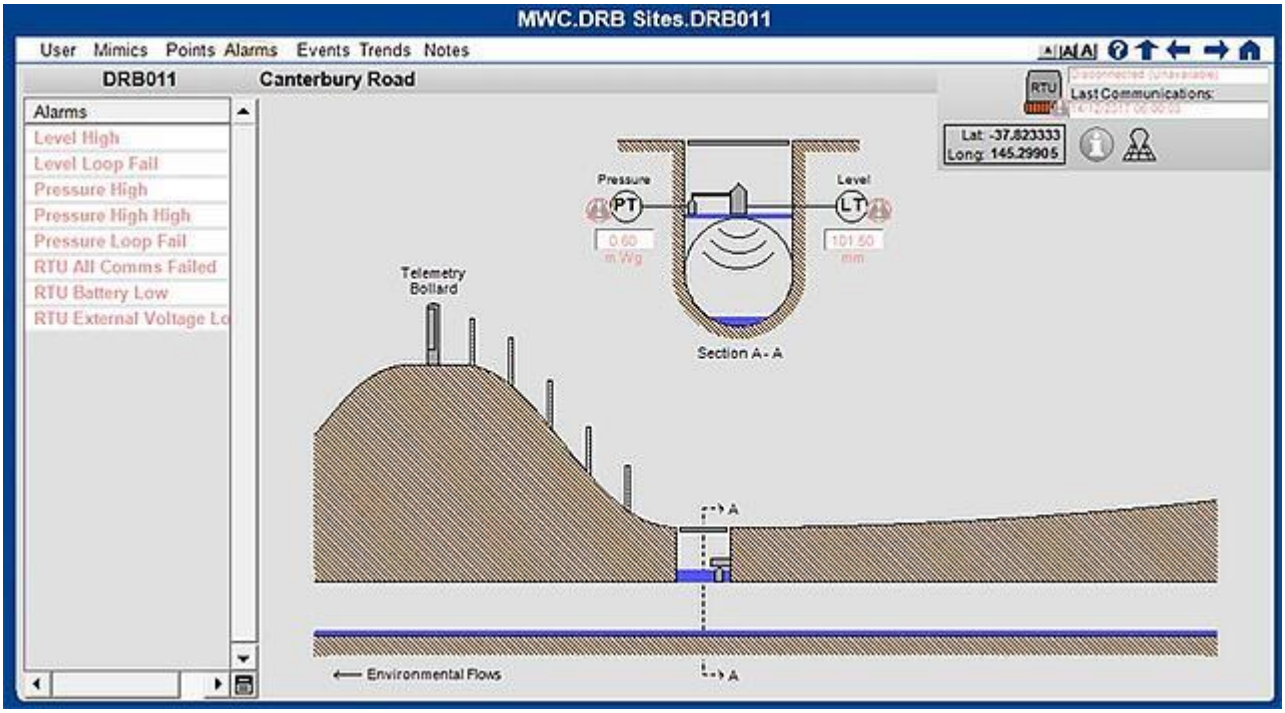


Figure 05

Smart Irrigation System

Population of India is increasing at a tremendous rate and therefore the available land is decreasing day by day. This is posing a great threat to the available cultivable land as a result the production of basic crops is also dropping drastically. Moreover, the bad weather is resulting in crop failure. Heavy rainfall or drought is ruining the cropping fields and also disturbing the soil fertility due to soil erosion or loss of moisture content. Lack of nutrients lead to bad quality of crops. Therefore, all this needs to be under proper constant check to reduce all the misfortunes and increase the yield of the crop.

IoT enabled device can help to monitor the health of the soil, to understand the moisture content, humidity, temperature and the water retention of the soil, to save water as well as make efficient use of available water to avail great quality crop. It also activates automatic irrigation system. With the help of sensors one can note the pattern of weather and rain to maintain the irrigation cycle. It uses humidity and moisture content sensors which are easily available.

Figure 06

Figure 07

Figure 08

Humidity and moisture sensor (Source - https://how2electronics.com/iot-smart-agriculture-automatic-irrigation-system-with-esp8266/)

Home IoT projects

1. Nest Learning Thermostat- at one click one can control the temperature of their house and save long bills on electricity
2. Smart home lighting- enables one to handle lights of the house from bedroom to garden through smartphone and helps monitor light when on long vacations too.

Through smart home projects, one can also handle all the devices and save electricity as well as any electrical short-circuit or damage can be avoided. It is also helpful in building children friendly atmosphere. Many patients or old people can be nursed back properly at home.

Peekaboo

It is a revolutionary application which will help to maintain consumer's privacy against smart home devices. When it comes to internet of things, the word security is obviously at risk and it is quite inevitable. But IoT is an important part of human life, making human schedule better and easier through augmentation, remote access and monitorisation. Basically, it is formulated as guidelines for the apps or device developers, that privacy is a very important bar and it needs to be respected at all costs. According to Jin, the developer of Peekaboo, "In the privacy world, we have a principle called 'data minimization'". Jin also added that all the companies should inform the user why are they collecting the particular data and should restrict the information collected used for their purpose. Same goes for the Peekaboo architecture, the developer has to make a proper declaration of the information needed and how or in what respect these data collected would be used further on the platform by the developer. This was done to give more power and right to the consumer over their piece of information. Jin says it is a kind of privacy nutrition label which is not only limited to a single device instead it can be applied to the entire home. This project was funded by Cisco, Infineon, the National Science Foundation, and CyLab's Secure and Private IoT Initiative. Peekaboo would prove to be a boisterous step towards security of IoT field. (Jin, 2022)

EU's General Data Protection Regulation (GDPR), Article 5 (1) (c) also states that "Personal data shall be limited to what is necessary in relation to the purposes for which they are processed."

IoT technology stack

IoT technology stack refers to the several layers involved with monitor, control and protection of internet. Multiple technologies cooperate together to exchange information or

rather they communicate with each other over internet at different layers and thus IoT technology stack is the basis of an admirable understanding of freedom and individuality of each and every device located over the network.

The basic layer of IoT technology stack includes

1. **Device Hardware**

The first layer of the IoT technology stack is device hardware, which acts as the mediator between the physical object and the server. The device software runs with the help of device hardware.

2. **Device software**

The second layer of the IoT technology stack is device software, it includes an operating system and application software. Device software runs with the processor. Operating system manages the device hardware which inturn provides a platform for application software to work perfectly.

3. Communications

- The third layer of the IoT technology stack is communications. In IoT architecture communication acts as the veins which circulates information among the devices involved in the IoT network. Some of the technologies or platforms used for the communication purposes are-
- Wired Network
- Wi-Fi
- Bluetooth
- Zigbee/Thread
- 2G/3G/4G/5G cellular networks
- LTE-M/NB-IoT cellular licensed LPWANs (Low Power Wide Arean Networks)
- LoRaWAN, Sigfox (unlicensed LPWANs)

All the communication devices should be at the same level for fluent information exchange and communication protocols make this task easy and arrayed.

4. **Cloud Platform**

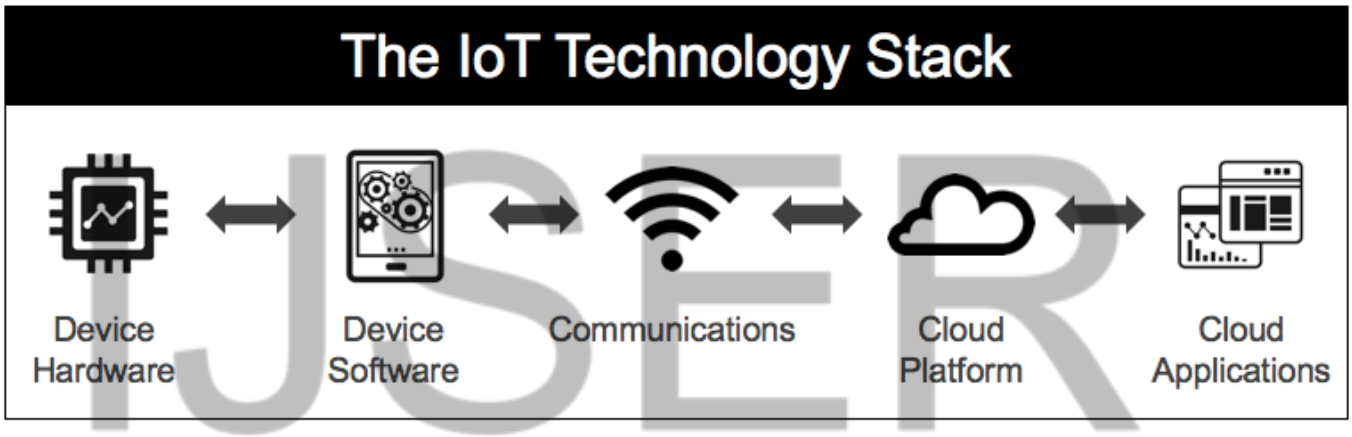
The fourth layer of the IoT stack is the cloud platform. Internet based data centers including the hard and soft parts of the actual project. It includes all the information assimilated in the IoT devices. Cloud computing is a vast word with a complex definition but it provides centralized services and database that can be assessed remotely. It provides scope of

development and improvement to the project with essential tools and services available. Few cloud services are-

- Bare Metal Servers
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

5. **Cloud Applications**

The final layer of the IoT stack is cloud applications. This layer supports the cloud platform and acts as a middle man between end user and the IoT network. It includes user interfaces.



(Source- https://www.trinetratsense.com/solution-overview/technology-stack-of-the-iot-platform/)

Figure 09

Global IoT Security Regulations

IoT is a big bucket of network with precise sensors and whole lot of information including a great flow of information. All these things together are giving IT industry a reason to move further deep and research thoroughly because competition is tough and everything needs proper attention and time. Homo sapiens are thrifty when it comes to sparing few minutes to the things which are much lower on priority index of human existence. IoT is flowing like a free river and it finally meets the vast ocean hence it knows no fathoms therefore, it is growing and maturing at great lengths. Surveys states that combined annual growth rate (CAGR) while reach 11.3% over the 2020-2024 time period. IoT is now the next reality or dream growth rate is good but now we need implementation and protection. The side effects of IoT are very dangerous and could cost one's privacy and survival. The global powers around the world are taking measures to protect the individuals through several important protocols.

Australia has encoded a "code of conduct" for IoT cybersecurity, having several protocols and boundaries for the manufactured devices related to IoT network, which ensures proper flow of information over the internet. It helps check the password authentication and authorization, credential protection. All the organization should declare the vulnerability disclosure policy with a strong uphold over the situation and if something goes out of hand, organization should be ready to face the consequences and take responsibility.

Singapore is rather going for a aggressive method, it is providing every enterprise with a guideline called "IoT Cyber Security Guide", to handle all of their IoT mechanism. Singapore also has convened "suite of IoT standards" to give brief idea to the corporate in the scenario about establishing a security labeling for the devices ringed to the smart devices, for better consumer experience.

UK has different division responsible for the development of departments like Digital, Culture, Media and Sport (DCMS). These department collects data of each and every individual registered on the platform but at the same point these information require protection and to ensure this all IoT devices involved are secure and protected, through unique passwords for all devices. All the platforms should have emergency contact details and this step is compulsory despite complex company policies.

European Union also has several countermeasure for security like IoT "Trust Label" which is used to ensure end-to-end personal protection of data in IoT system.

Brazil is taking an incentive based route to attract protection ideas for IoT services. Various tax reforms and money influx drives are designed to transform the face of IoT enabled devices and security. This step is actually giving an abrupt growth and edge to machine to machine (M2M) communication system. It has also promised to promote services and protection in secondary industries.

The main focus in **United States of America** is the "IoT Cybersecurity Improvement Act", which was signed into law in 2020, the legislation has shown intension of building yet another incentive based model. It is planning to incentivize the companies to enhance the security of all the devices they build and sell. All the guidelines for development, identity and configuration management for IoT devices are based on the standards builds by the National Institute of Standards and Technology (NIST).

Need for IoT security in India

IoT as the main dish on the menu is bursting with fresh energy and sizzling devices, which are being introduced in the consumer market every week, without any limits and that is quite amusing because nobody likes constraints but this freedom is coming at the cost of our privacy and security. So to overcome this bitterness, each and every individual has to think and learn some precautionary steps and be aware of their rights and the right platform to approach when in pain.

The first and foremost step is to bring certain level of legality in this ecosystem to prevent all the flora and fauna of this ecosystem from falling into the endless pit of pain and suffering. This is only possible when the government of the country is actively participating in the following debates based on IoT.

Government of India in 2015, drafted a IoT Policy with a visionary dream of connecting each and every corner of the country to smart IoT based system to boost our country's economy, society, environment and global needs and also to establish India as an active global country which is eager to learn and grow, it is also helping in fixing India's position in the global market as a country worth making investments, attracting several multi national companies (MNCs). (Chatterjee, 2018)

The 100 Smart city project was launched with the help of draft IoT policy,2015 with the aim to have India's very own smart city loaded with every basic facility. The launch of the Digital India Program brought new goals and vision which is a new target that the country is striving to reach, the possibility of having everybody connected at one platform with the help of training centre and governance committee to ensure proper application of effective governance policies and projects in India. This will aim to reconstruct the Indian society into a digitally empowered society and give new meanings to the blooming IoT industry in the developing country like India.

But the current wave is totally different from what is expected, with increasing internet connectivity people are exposed to many threats which are still not seriously addressed at national level like privacy, security, infrastructure, lack of standardization. There is an urgent need to protect because the data networks are sensitive and data clouds are still in developmental stage in India, hence storage of data in cloud services is still a hassle which could lead to questionable authorization.

After the surge of Covid quarantine, the interest of medical industry has spiked in the IoT network. The International Medical Device Regulators Forum (IMDRF) is keenly taking interest in spicing up the medical world with the pinch of IoT, by establishing a voluntary platform that brings together all the medical devices and their protocols from around the world to build an amazing medical facility loaded with every possible machinery. Making several impossible operations into reality and by opening several new doors to the study of human and human life.

Public key infrastructure (PKI) technology is a very important technology in terms of privacy and security of user devices. It displays an escalating factor by ensuring that an organization's devices and users are safely authenticated—and provide subtle protection for the information that is exchanged or taken into account, whether it is in transit or at rest mode.

There are several questions coming up against security related to IoT networks and connectivity, leading to problems based on authentication, authorization, privacy, leakage, etc. IoT is a framework

which enables one to communicate with certain established protocols. The main heated argument is the unfathomable connectivity of device over internet, since the world of internet has no boundaries it attracts moles (unwanted, uninvited guests) those are hungry for data to rupture an individual or an organization. Moreover, there is no sense of belongingness in terms of physical aspects, the networks are very abrupt and the channels are unknown. Complicated encryption and decryption also makes the data security a tedious task and IoT gives freedom to live life at a snap of a finger which makes it more vulnerable and indecent. There are many cases where big organizations were under the tables due to the shortcomings of IoT.

CASE STUDY-MIRAI MALWARE

Probably, everybody on internet is as very curious when it comes to learning something new and applying it in real life as soon as possible. Similarly, in the year 2016, an incident took place that was unexpected.

September, 2016, the owner of Mirai malware tried to overtake the website of a well-known security expert launching a DDoS attack. Although in return the expert overshadowed the attacker and opening a new world for other attackers by releasing the source code, which lead to mass duplication of the malware. The biggest attack took place in October 2016, breaking down the Dyn, the domain registration services provider.

Mirai malware plays all the games over IoT devices. It sieves the whole Internet for the devices that run on ARC processor (family of RISC CPUs). ARC processors are generally used with system on a chip (SoC) devices. Mirai easily breaks into the credentials and infect the system to the core, turning them into zombies. Generally, these zombies are “bots” that are controlled to corrupt the whole network and create their own network called “botnet” to handle DDoS attacks.

Since, Mirai’s birth was out of fraud because the company who was providing mitigation against the DDoS attack was the one creating the problem, to have extra ounce of penny in their hand. But Mirai malware is dangerous because it is mutating at tremendous level giving birth to new malwares and giving hard times to organizations.

CASE STUDY- UKRAINE POWER GRID ATTACK

It was a great blow to the electricity distribution companies of Ukraine. On December 23, 2015, there was a total blackout in many cities of Ukraine and the cause was unique it was a malware attack, taking the remote access of three big electricity suppliers of the country. It was an attack to establish political power play and these phenomena became frequent. Ukrainian spokesperson claimed that the attacks were directed from Russia and suspected that the Russian group known as APT28 (Advanced Persistent Threat 28 or “Fancy Bear”) was actively involved.

BlackEnergy malware was triggered through a mail. An employ received a mail and unfortunately opened it without knowing the threat, what happened next is history now. The soul purpose of the attack was to know the infrastructure and network properly for future malicious excursions. All the appropriate firewalls setup within the network became a laughing stock, because an inside device was a huge help and soon the malware was able to break into the network causing great loss.

They used Spear phishing to control the networks. They also used denial of service attacks on the call center so that nobody could inform or contact the authorities. Moreover, they used KillDisk malware to erase the traces of area attacked and other important logs and BlackEnergy malware was the main ingredient of the dish.

IOT LAYER'S ATTACK AND SOLUTION

PERCEPTION LAYER

Perception nodes RFID

*Attacks

Denial of services, privacy issues, spoofing, data interruption, eavesdropping, etc

*Solution

Encryption is one of the common solution, access control, cryptography, hashing, IPSec protocols, etc

Sensor nodes

*Attacks

Nodes are very sensitive and a disturbance in a single node can rupture the whole arrangement. Some of the attacks - Node failure, authentication, outage, unfairness, node message corruption, jamming, collisions, etc

*Solutions

Node authentication and deep level of privacy could protect the intricate sensor nodes.

Sensor gateways

*Attacks

Poor signal or signal lost, denial of services, fabrication, interruption, modifications, tunneling protocol (protocol responsible for communication or it is a communication protocol which facilitate the movement of data to and fro over the network),etc

*Solutions

Message security, clean onboard device and maintaining its security, integration security

NETWORK LAYER

Mobile communication

*Attacks

Deletion, eavesdropping, denial of services, corruption, bluesnarfing (data theft through the Bluetooth connection),bluejacking (method of hacking used to send unknown messages to a device within the given Bluetooth radius), interruption, jamming, etc

*Solutions

Involvement of public crypto keys, secure accessibilities, etc

Cloud computing

*Attacks

Complex system, unauthorized access, encryption and decryption issues, software configuration, etc

*Solutions

Location privacy, access authorization, cryptography with hash chain, etc

Internet

*Attacks

Hacking, theft, phishing, cyber crimes, spoofing, virus, Trojan, malwares, etc

*Solutions

Encryption and decryption, secure network, firewalls, cyber security, etc

APPLICATION LAYER

*Attacks

Data leakage, privacy, access control, authorization, etc

*Solutions

Authentication, secure user privacy, end to end security protocols, etc.

Conclusion

All the factors and statement about IoT environment shows that how it is an integral part of human society and it is very essential to safeguard the people entangled in it. Since, there some demerits of the IoT network but the need and necessity cannot be ignored and hence, this enchanting industry needs some legislation interventions and proper awareness and training centers for better understanding and proper utilization of the technology. The Internet of Things has emerged as a predicted trend in the growth of the information business. High-quality lifestyles will result from this. This article examined some of the most significant problems and obstacles related to the Internet of Things (IoT) from an Indian viewpoint, including what has already been done and what problems still need to be resolved.

References

Dey, Nilanjan; Hassanien, Aboul Ella; Bhatt, Chintan; Ashour, Amira S.; Satapathy, Suresh Chandra (2018). *Internet of things and big data analytics toward next-generation intelligence* (PDF). Springer International Publishing. Retrieved 14 October 2018.

Gillis, Alexander (2021). "What is internet of things (IoT)?". *IOT Agenda*. Retrieved 17 August 2021.

Raji, R.S. (1994). "Smart networks for control". *IEEE Spectrum*. **31** (6): 49–55.

Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). *CISCO White Paper*.

https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf

https://www.cloudflare.com/en-in/learning/ddos/glossary/mirai-botnet/

https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

https://www.researchgate.net/profile/Abdullah-Al-Hamdani/publication/334944162_Systematic_Review_of_Existing_IoT_Architectures_Security_and_Privacy_Issues_and_Concerns/links/5f97b76592851c14bceabdb9/Systematic-Review-of-Existing-IoT-Architectures-Security-and-Privacy-Issues-and-Concerns.pdf

https://www.researchgate.net/publication/320479860_Smart_LED_Street_Light_Systems_A_Bruneian_Case_Study

https://www.sageautomation.com/our-work-utilities-stories/iot-solution-provides-underground-monitoring?hsCtaTracking=3463a1f4-724a-4d5d-bcf0-80a02e3e0723%7C129d11b6-4945-45e2-8f97-87311b019e85

https://how2electronics.com/iot-smart-agriculture-automatic-irrigation-system-with-esp8266/

https://datafloq.com/read/iot-projects-that-will-change-the-world/

https://ncrb.gov.in/

https://www.crendoninsurance.co.uk/peekaboo-what-is-it-how-is-it-influencing-iot/

https://iotbusinessnews.com/2022/07/13/86750-what-is-the-iot-technology-stack/

https://securityboulevard.com/2021/06/understanding-global-iot-security-regulations/

https://www.congress.gov/bill/116th-congress/house-bill/1668

https://www.mondaq.com/india/telecoms-mobile-cable-communications/992586/internet-of-things-iot-policy-and-challenges-in-india