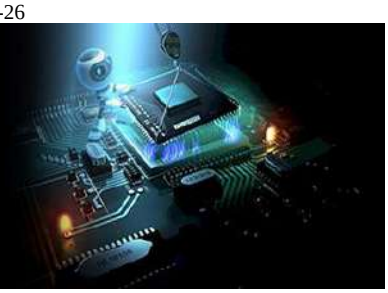
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2019; 1(2): 16-26
Received: 06-05-2019
Accepted: 10-06-2019

Bashar Ibrahim Hameed
Assistant Lecturer, Master of Information Systems, Iraqi Sunni Affairs, Iraq

Corresponding Author:
Bashar Ibrahim Hameed
Assistant Lecturer/Master of Information Systems/Iraqi Sunni Affairs, Iraq

An overview of internet of things (IoT): Definitions, architecture, security, applications and future directions

Bashar Ibrahim Hameed

DOI: https://doi.org/10.33545/26633582.2019.v1.i2a.15

Abstract
The use of technology has been constantly increasing in our lives and it is affecting it greatly. There has been no doubt in this claim that technology is headed in the direction of automation and is making steady progress. If we look at the definition of technology, it can be described as an act of progress that makes it easier to complete a task. Isn't it the very basic principle of technology to make our lives easier by leaving fewer things to be explicitly done by us? It might be making us all lazier every day, or one might argue that it is giving us far greater time to pursue whatever we desire. Whatever might be the effect, there is no doubt that automation is the future and the place that it is happening the most significant is right in our homes. Internet of things (IoT) makes our lives easier by automating every task at our homes starting from turning lights ON or OFF to opening or closing doors. The use of IoT is not restricted to homes but is also used in autonomous vehicles are commonly known as self-driving cars and many other applications. In this paper; Firstly, various definitions of IoT are introduced; Secondly, the architecture of IoT is discussed; Thirdly, the major challenges in the security of IoT which need addressing by the research community and corresponding potential solutions are investigated; Fourthly, some open issues related to the IoT applications are explored; Finally, discussion of IoT and future directions are systematically reviewed.

Keywords: Internet of Things (IoT), Service-oriented Architectures (SoA), Internet of smart living (IoSL)

Introduction
IoT stands for the Internet of things and there is no standard definition of it. Many organizations such as the Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IEFT) and National Institute of Standards and Technology (NIST) are working on making a standard definition of IoT but all of them have their differences and hence have different definitions.
According to IEEE, the definition of the Internet of Things is stated as:

> *"A network of items—each embedded with sensors—which are connected to the Internet."* [1].

IEEE P2413 also deals with the prospects of IoT in the market. The stakeholders of the IoT and IoT market are shown in figure 1.
According to IETF, the definition of IoT is different from what IEEE has proposed and they also have their definitions of "Internet" and "things".
The definition of IoT is:

> *"The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones makes it possible to materialize IoT which interact and cooperate to make the service better and accessible anytime, from anywhere."*[1].

The definition of "Internet" is:

> *"The original 'Internet' is based on the TCP/IP protocol suite but any network based on the TCP/IP protocol suite cannot belong to the Internet because private networks and*

telecommunication networks are not part of the Internet even though they are based on the TCP/IP protocol suite. In the viewpoint of IoT, the 'Internet' consider the TCP/IP suite and non TCP/IP suite at the same time."[1].

The definition of "Things" is:

"In the vision of IoT, 'things' are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc. These things are classified as three scopes: people, machines (for example, sensors, actuator, etc.) and information (for example, clothes, food, medicine, books, etc.). These 'things' should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. In here, if the 'thing' is identified, we call it the 'object.'"[1].

According to NIST IoT can be considered as cyber-physical systems and physical cyber systems. They also have given two definitions of IoT. One definition was presented by the team "Smart American Global Cities Challenge" and the other one was presented by Chris Greer who is a NIST senior executive for cyber-physical systems.
The Smart America/Global Cities Challenge description of IoT:

"Cyber-physical systems (CPS) – sometimes referred to as the Internet of Things (IoT) – involves connecting smart devices and systems in diverse sectors like transportation, energy, manufacturing, and healthcare in fundamentally new ways. Smart Cities/Communities are increasingly adopting CPS/IoT technologies to enhance the efficiency and sustainability of their operation and improve the quality of life."[2].

Greer's description of IoT:

"Cyber-physical systems, also called the Internet of Things, are the next big advance for our use of the web. They allow complex systems of feedback and control that can help a robot coordinate with a dog or human in a search and rescue operation or help health care providers evaluate the recovery of patients after they leave the hospital"[3].

IoT is going to affect our lives on a much wider and bigger scale than most of the scientists have imagined. It will affect every aspect of our lives and will help make things much easier and simple. It aims to reduce the workloads of humans by automating things. For example, solutions for traffic flows can be achieved with the help of IoT, reminders about daily tasks such as maintenance of vehicles, taking care of energy consumptions and monitoring energy usage. Monitoring that helps with diagnosing and sensing maintenance issues and prioritizing maintenance based on the severity of the damage. It also affects the field of transportation by the introduction of driverless vehicles which as the name states do not require a driver but drive themselves based on various sensors. In the sector of health, it can be used in tracking devices that monitor and store the data of the patient and with the help of that data they can diagnose health problems and monitor the state of the patients in a much better way. It can also be used to monitor the data of a specific area such as a metropolitan or a cosmopolitan and will help them operate in a much better way. The data analysis systems will make it easier to predict the traffic preventing traffic jams. Waste management can be done with the help of these systems. The law enforcement departments and pollution control departments can also take the help of these data management systems and make the cities safer and cleaner.
It can be considered as the next level linked devices so they can help people in their homes such as the refrigerator can give you alerts that there is no food or we can turn devices ON and OFF with the help of our voice. We can also cater for security issues such as that we can access the locks of our homes remotely and in case of any break-in or theft we can get a notification indicating the threats. We can also allow guests to access our homes remotely.
Since these devices will be used on such a large scale the amount of data will also increase substantially. This is where we will need Big Data and this will help us in dealing with such massive amounts of data. Big data and IoT go hand in hand. Big Data helps manage a huge amount of data that is generated by the device operating on IoT. Internet of Things and Big Data are vital subjects in many industrial and commercial applications. Big Data refers to the data generated by the IoT devices and it stores and manages it. Big data study this data and tries to find trends and meanings out of this data. This trend will then help consumers make decisions that will be helpful in the future.
It was in the relatively recent past that we imagined places of things to come where things would be done alone lights going ahead without anyone else's input, espresso being fermented only the manner in which you like as you are going to wake up and your shower knowing the climate outside and changing the water temperature likewise. Also, presently we are at a point where innovation to accomplish the total of what that has been around for some time and has now turned out to be moderate. Consequently, it's anything but especially enormous amazement that we are seeing some stunning things occurring in the realm of computerization [4].

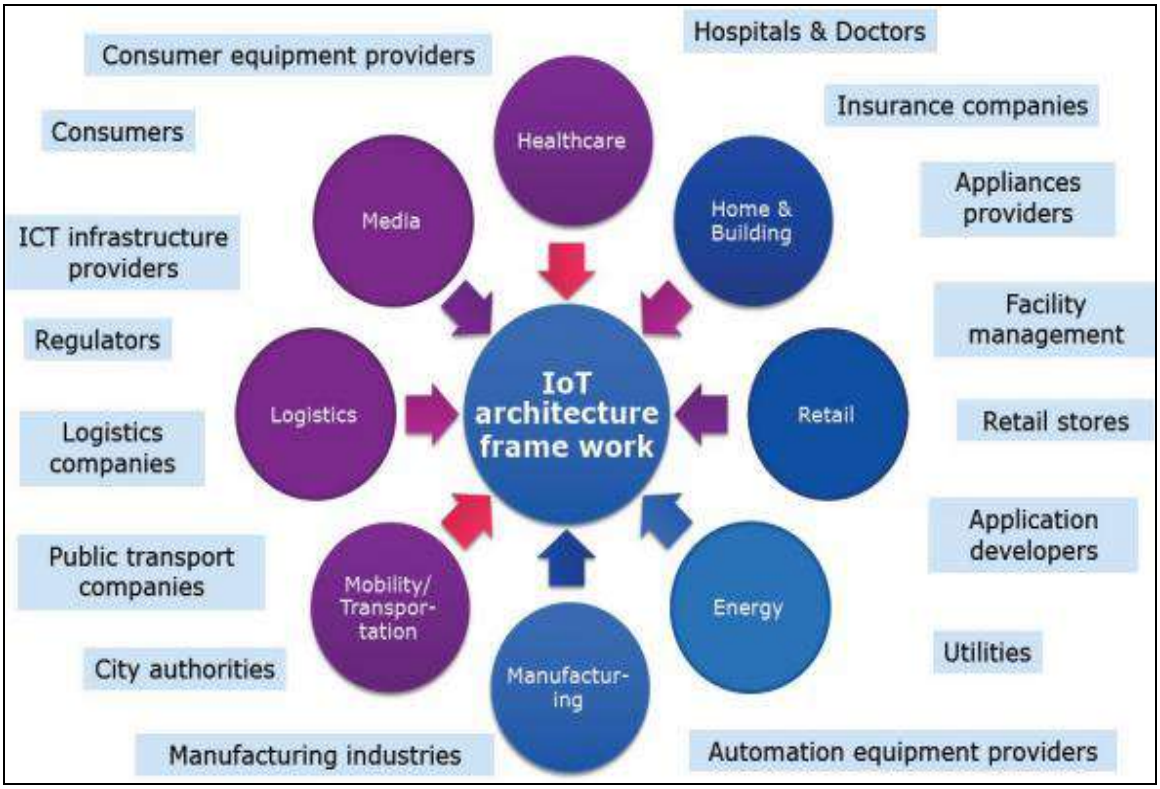


Fig 1: IoT markets and stakeholders

2. Architecture of IoT

This section of the paper deals with different types of architectures that are related to IoT.

2.1 Three-layer architecture

Generally, the architecture involved in IoT has three layers and these layers are considered to be the basis of the architecture [5]. The layers are the application layer, perception layer, and network layer. These layers are further explained as:

2.1.1 The perception layer is also referred to as the sensor layer of the IoT architecture. It is present at the bottom of the IoT architecture and is the lowermost layer [6]. The purpose of this layer is to interact with physical devices with the help of smart devices such as RFID, sensors, acutators, etc. It helps connect the IoT network with other things as well as to measure, collect and process the information of the state of such things with the help of smart devices. It transmits all this information from physical devices into upper layers with the help of layer interfacing.

2.1.2 The network layer is also referred to as the transmission layer of the IoT architecture. It is present in the middle of the IoT architecture hence it is the middle layer of IoT architecture [7]. It consists of many integrated networks and the task of this layer is to receive data from the sensor layer and the determine the destination and the path of the data towards their respective IoT hub, devices, and applications. The devices that are integrated into this layer include hubs, gateways, cloud computing performance, switching, etc. The various communication technologies that are integrated into this layer include Bluetooth, Long term Evolution (LTE), WiFi, etc. The inclusion of such important devices and technologies makes it the most important layer in the IoT architecture.

2.1.3 The application layer is also termed as the business layer of the IoT architecture. It is the topmost layer of the IoT architecture [7]. This layer receives data from the network layer and based on that data, it performs specific services and tasks. For instance, the application layer can predict the future of the state of a physical device with the help of analysis services. It also provides the service to backup data into databases. Various applications are a part of this layer and each application has its own set of requirements. Some of the examples are smart cities, smart grid. Transportation, etc. [8, 9]

This three-layered architecture that we have discussed is the basis of IoT structure and it has been implemented and used in several systems to achieve various tasks [8]. The architecture of the IoT may seem simple but it performs complicated and diverse functions that are performed in both the network layer and application layer. For example, the application layer has to provide services to the clients and customers devices but also help them by providing data services such as data mining, data analysis, etc. The network layer, on the other hand, has to transfer data to the application layer and set up routes for the transfer of data. Therefore to develop a universal and tangible architecture for IoT, a service layer is to deployed between the network layer and the application layer which will help in providing data-related services in IoT. Service-oriented Architectures (SoA) have been introduced recently to support IoT [10, 11].

2.2 SoA-based architecture

SoA is a component-based model which means that these models are made according to the need of the user. They are designed in such a way that they combine different functional units and then, as a result, makes the user able to perform certain tasks and application via protocols and interfaces [12, 13]. One of the biggest advantages of SoA is that they allow us to re-use hardware and software. This task

is achieved by constructing workflows of coordinated services and help improve the feasibility of using SoA in IoT structure designing [12, 11]. Hence, SoA can be arranged in the basic IoT three-layered structure. It is integrated in such a way that the data services that are provided by the network layer and the application layer can be taken into a new layer known as the service layer which is sometimes called as the middleware layer or interface layer. Therefore, in SoA there are four layers in the IoT architecture that interface with each other [14]. The layers are perception layer, network layer, service layer, and application layer. In some cases, the service layer is further divided into two sub-layers which as service composition sub-layer and service management sub-layer. The business layer acts as the upper layer of the application layer and deals with providing complex service requests. The business layer is extracted from the application layer [16].

The perception layer in the four-layer SoA-based IoT architecture is the lowest in the architecture and it is used to measure, gather and extract data that is present in the physical devices connected to the IoT [15]. The network layer helps in determining the routes and help in data transmission via integrated networks [12, 16]. Next is the service layer that is present between the network layer and application layer, and it provides services with the help of which it supports the application layer [12]. The service layer is made up of services such as service discovery, service composition, service management, and service interfaces. The purpose of service discovery is to find the service request that is desired, service composition helps to interact with connected objects, and divide or integrate services to meet service requests efficiently, service management helps to manage and find out the trust mechanisms to fulfill service requests, and service interfaces help support interactions to all services that are being provided. The application layer helps identify the service requests of the users. The application layer can support a number of applications, including smart grid, smart transportation, smart cities, etc. [16], see figure 2.

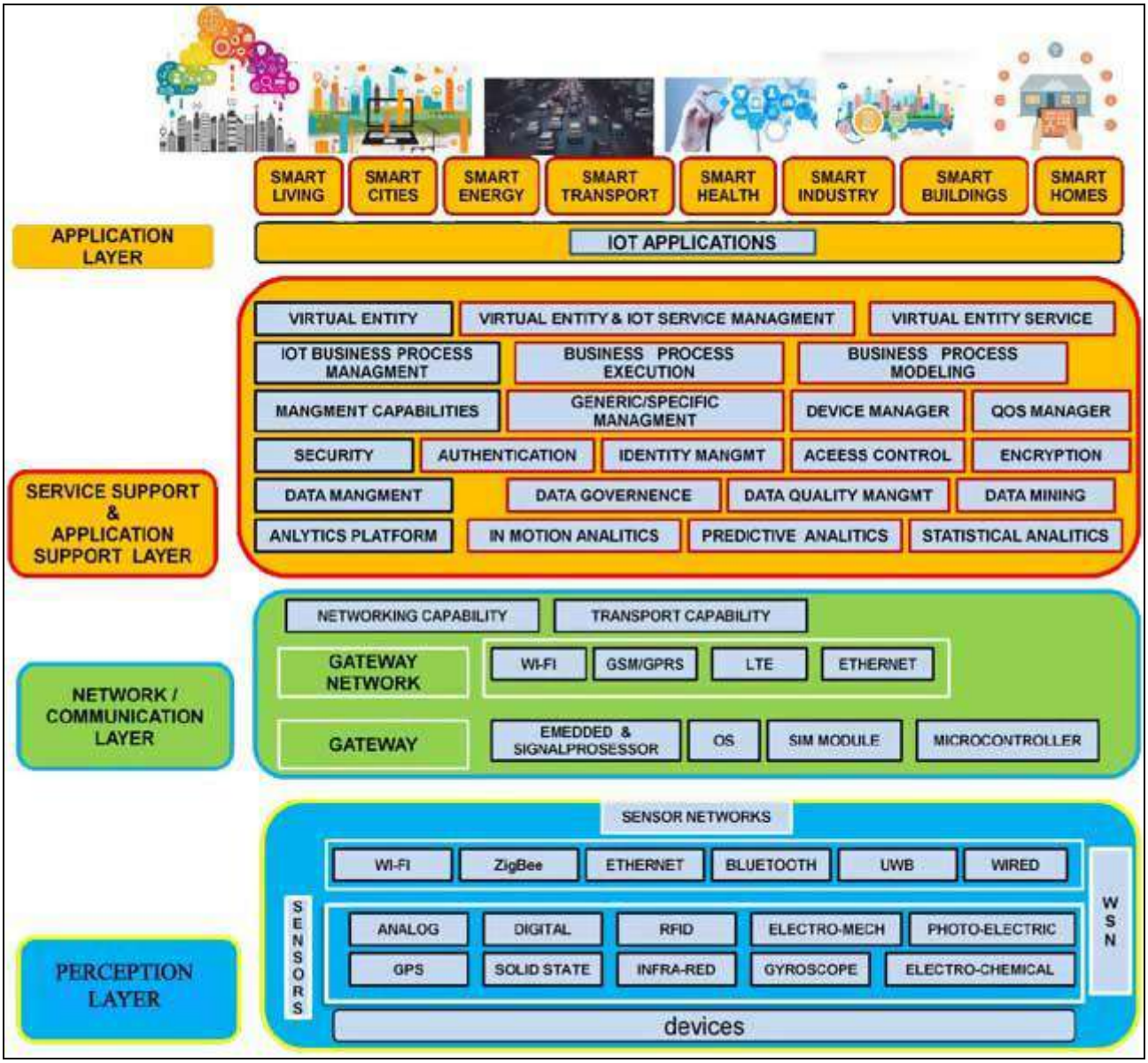


Fig 2: Architecture of IoT

3. Security of IoT

This section deals with the features of security of IoT, the security issues that are faced and lastly the solution to those problems.

3.1 Security features of IoT

3.1.1 Confidentiality: Confidentiality means that the data is only accessible to authorized users and nobody else. The data remains safe throughout the transmission process and is not altered or lost due to the interference of any unauthorized individual. In IoT, confidentiality is considered to be a very basic and crucial security aspect because IoT deals with the majority of measurement devices such as sensors, RFID, etc. Therefore, it is very important that the data that is collected by the measurement device is safe and will not leak any important information that can result in any sort of loss. To make our systems more confidential and safe different techniques are used such as secure key management mechanisms and better encryption techniques [18].

3.1.2 Integrity: Integrity means that the data that was sent is the same data that is received. The data was not tampered by any external source during its transmission and accurate data is received at the receiving end making sure that the integrity of the user's data is kept. The integrity of data is very important in the case of IoT as if tampered data is received than IoT will perform wrong operations and wrong feedback commands will be made. To ensure the integrity of data mechanisms such as false data filtering schemes should be implemented. Secure data integrity mechanisms should be used [19].

3.1.3 Availability: Availability makes sure that when the authorized user or authorized device demands the data it is provided to them. This means that the data should be readily available to all the authorized personals and devices. In IoT, services are requested in a real-time fashion. Therefore, the data should be readily available so that the requested services can be provided at the requested time professionally. This makes availability a very important aspect of security in IoT. Denial of Service (DoS) attack is a threat to the availability of data. Secure and efficient routing protocols should be used to cater to such threats and ensure the availability of data in IoT [20].

3.1.4 Identification and authentication: Identification makes sure that only authorized person or device is connected to the IoT and authentication makes sure that the data that is being given to the IoT is legitimate and the devices that have requested to get this data are also authorized and legitimate. In the case of IoT authenticating and identifying every data set is very difficult as the data that it receives is massive and consists of diverse objects. Therefore to cater for that we have to design mechanisms that are efficient and critical [21].

3.2 Security

Now we will discuss the security threats that the IoT structure faces. In IoT structures that are based on SoA, the service layer is created by extracting the data services and its functionality from the network layer and application layer. Hence, the security threats and challenges faced in the service layer can also be taken as the challenges faced in the network and application layer [16]. Now we will discuss the security challenges faced in the application layer, network layer, and perception layer.

3.2.1 Perception layer: The main aim of this layer is to collect data hence the challenges faced by this layer are mostly related to the security of data. The job of this layer is to keep the data safe and prevent any unauthorized user to forge or falsify the data of authorized devices and users. Some of the security challenges faced are given below as:

3.2.1.1 Node capture attacks: In this type of security attack the attacker can capture the node through which the IoT system is communicating with a physical device. This can be done by physically replacing the node or by tampering the device and hardware of the node [22]. The capture of the node means that important information such as communication key, radio key, matching key, etc. are exposed making the whole transmission process vulnerable. Another threat that is related to capturing of the node is that the attacker can get the information related to the captured node and then make a fake malicious node and trick the IoT system into thinking that it is the actual node and get all the information. This attack is known as a node replication attack. This attack is a very serious threat to the network and it causes major damage to the network. To fight against this attack we need to develop schemes that monitor and detect malicious nodes [23].

3.2.1.2 Malicious code injection attacks: The attacker can also control a node or a device with the help of a malicious code that has to be injected into the memory of the device or its node. This injection of malicious code as a form of attack is known as a malicious code injection attack [24]. This malicious code can get access to the whole of the IoT system present in the network and then can make it perform any specific function that it can perform. Code authentication schemes and methods should be applied to save the device from such malicious codes [24].

3.2.1.3 False data injection attacks: If the node in an IoT system has been compromised than the attacker has the ability to replace the normal data with the data of its own choice that can result in corrupting the data set or file that has to be transmitted across the IoT network and in this way it can make the IoT system perform unwanted tasks [19]. False data filtering technique can be used to defend against such type of attack as this technique filter out any malicious data or false data at the receiving end [25, 26].

3.2.1.4 Replay attacks (or freshness attacks): To obtain the trust of the receiver of the data in the IoT network the attacker can send authorized identification information and passcodes to gain the trust of the receiver [22]. Such a type of attack is usually performed during the authentication process and it aims to destroy the certificates of validity. Secure time stamp schemes should be used to avoid such types of attacks [27].

3.2.1.5 Cryptanalysis attacks and side-channel attacks: Such type of attacks try to break the encryption technique that is used to keep the data safe. It tries to obtain the ciphertext or the key that is used for the encryption of data [28]. This attack is less effective as the encryption keys made

today are highly secure and they need massive computing power to break them. Side-channel attacks are sometimes used by the hacker and attackers. A type of side-channel attack that is used frequently is known as timing attack and in this attack, the attacker tries to find out the key from the time the encryption algorithm takes to execute the algorithm. To cater to such attacks the encryption techniques used should be very complex and the key management systems should be protected with complex allgorithms [18].

3.2.2 Network layer: The purpose of the network layer is to send the collected data onto the channel. The security challenges faced by this layer are mostly concerned with the availability of data. Most devices in an IoT network are connected through a wireless channel so most of the security challenges that this layer caters for are related to wireless network channels.

3.2.2.1 Denial-of-service (DoS) attacks: It is a type of attack in which the attacker sends massive service requests to the IoT device which is not able to handle such massive traffic which results in delay or blockage of service to the users [84]. It is the most common type of attack and it results in the loss of services of the IoT system. Therefore, DoS attacks can be created by attack schemes such as Ping of Death, SYN flood, Tear Drop, Land Attack, UDP flood, etc. To defend against DoS attacks, attacking schemes need to be carefully investigated first, and then the efficient defensive schemes to mitigate attacks need be developed to secure IoT systems [30].

3.2.2.2 Spoofing attacks: These sorts of attacks aim to gain access to the IoT system and then send malicious data of their own choice into the system [31]. The types of attacks related to spoofing in IoT systems consist of RFID spoofing [33], IP spoofing [32], etc. These sorts of attacks work based on IP addresses. The attacker in case of IP spoofing gains access to the IP addresses of authorized devices in the IoT network and then send malicious data to the IoT system making the malicious data appear as valid data coming from an authorized source. In an RFID spoofing attack, the attacker aims for the information of a valid RFID tag and once it gains access to that it then sends malicious data with this authorized valid tag ID to the IoT system. To defend against such spoofing attacks we need to have proper identification and authentication procedures [21, 34].

3.2.2.3 Sinkhole attacks: In such type of attack the attacked hole acts as a powerful node and hence the other neighboring nodes and devices choose this node for communication or as a forwarding node in the process of data routing acting as a sinkhole and everything is attracted to it [35]. This compromised node then can get all the data before it reaches the IoT system and can compromise the confidentiality and integrity of the data. It also affects the availability of data making it a starting step of DoS attacks. To defend against such attacks we have to use multiple routing techniques and multiple routing protocols [36].

3.2.2.4 Man in the middle attack: As the name states it is a type of attack in which the attacker acts as a part of the communication system between two nodes or devices of an IoT system [37]. By doing that the malicious device can act as a bridge between the two devices and the two devices would not even know that their data is first being transferred to an attacker and would carry on believing that they are receiving the data that was sent to them by the authorized devices. Such a type of attack is a threat to the confidentiality, integrity, and privacy of the data of the authorized users and devices in the IoT system. The attacker can gather the data, tamper it and also control the communication between two devices hence making them a great threat to the system and its data. These type of attacks does not need any physical tampering whereas, they can be launched by knowing the protocols of communication of IoT networks. Using secure communication protocols and key management schemes, that make sure that the identity of the normal devices is not lost, should be used as they can be effective against such attacks [17].

3.2.2.5 Routing information attacks: Such type of attacks aim to get the routing protocols that are followed in the IoT system. By gaining access to the routing protocols they can then manipulate the routing techniques and destinations which will result in looping of paths in data transmission networks. This looping will result in the delay of end-to-end data transmission in the IoT network [31]. To prevent these attacks from happening secure routing protocols should be implemented. Also, ensure that the IP addresses and other identifying information are not leaked.

3.2.2.6 Sybil attacks: In such attacks, the attacker gets hold of the information of many authentic users in an IoT network and then impersonates them and makes replicas in the IoT system [38]. The malicious device that does all this is known as a Sybil. As such devices have many authentic identities so the malicious data sent by the Sybil device is accepted by the neighboring devices in the IoT network. It also if any device selects the Sybil device as a forward path then it may seem as the data is going through various devices but in reality, it is going through just one device. All the data will go through the Sybil device and this can then be used for jamming and DoS attacks. To prevent such attacks we need to have proper identification and authentication mechanisms in IoT systems [21].

3.2.3 Application layer: Application layer is used to support the services that are requested by the authorized users. Hence, most of the threats that are faced to this layer are focused on software attacks and some of these attacks are explained as:

3.2.3.1 Phishing attack: In such attacks, the attacker spoofs the data of the authentic users and then obtains their usernames, e-mail ID and passwords. The attacker makes a fake e-mail or website and then the authentic user is log in through that website resulting in their data being stolen [31], [39]. Secure authorization access points, as well as identification, can lessen phishing attacks [31]. The most efficient way to stop these attacks is to make the users more aware and informed about such online websites. This is mainly an issue as machines are dumb so they cannot differentiate but humans can so they need to be vigilant.

3.2.3.2 Malicious virus/worm: A virus or a worm is a self-propagation attack that tampers the data of the users and is a major challenge for the IoT devices [31]. Worms, Trojan

horse, etc. are the types of malicious viruses that forge confidential data. To cater to these viruses firewalls and virus detection techniques should be used [40].

3.2.3.3 Malicious scripts: These are the scripts that are added to the software of the systems that are in an IoT network and once these scripts are added into the software they are modified and then deleted and this results in damaging the functionality of the system [31]. As all the IoT systems have access to the internet and their applications are also internet-based so the attacker can fool the users into running these malicious scripts resulting in improper functionality and data loss. These scripts can also result in a lockdown of the system. The techniques that can be used to cater for these scripts include honeypot, static code detection and dynamic action.

4. Applications of IoT

IoT has numerous applications in practical life. It has the potential to influence all the fields of life and can revolutionize our day-to-day life. It has the potential to influence enterprises, businesses, and society as a whole. The application of IoT is in the domain of smart environment and smart spaces. This domain includes things such as smart buildings, smart cities, smart transportation, lifestyle, etc. some of the applications of IoT devices are shown below [41].

4.1 IoSL (Internet of smart living): It doesn't take a genius to figure out what home automation entails: it's pretty much just the usage of smartphones and other easily available computing devices to automate and control household items and devices-from electrical appliances to lights to doors-with the help of hardware that can be controlled remotely. Most home automation begins small-people start with controlling simple binary devices, that could either be in an "on" or "off" state. But it's when these devices are hooked up to the internet that they become truly smart and enter the realm of the internet of things. Most automation systems nowadays use their internet=enabled abilities to record and analyze usage patterns of devices, mostly lighting and heating systems, to reduce monthly electricity bills and overall energy expenditure.

While setting up a home automation system, the best place to start investing in is your nuisances, for many people, the most obvious problem is their electricity bill, so most people purchase a few smart lights as their first home automation product. Or if you are the kind of person who is constantly paranoid about whether they left the geyser on, smart switches would ease your paranoia. From there, you slowly build up a full lighting system that can be remotely controlled and would respond to human presence, or an automated home theatre comprising a smart TV with smart ambient lighting.

Any smart home automation system today is generally a central hub that can be configured to control a bunch of smart devices, sensors, and switches, all of which communicate with the hub using certain communication protocols. The hub, in turn, is instructed through an app or the web. The main takeaway is the distribution of monitoring and computing functions between the hub and the remote app. For example: in a smart lighting system, a hub would act as the central interface between multiple smart devices, say, a bulb and a door contact sensor [42].

4.2 IoSC (Internet of smart cities): It has various uses in the smart city which are stated as:

1. Structural Health: Keeping an eye on the structural integrity of the buildings. Monitoring the condition and durability of the materials used in the making of the building and monuments.
2. Lightning: Smart lights that are considerate about the weather and adapt according to the weather condition.
3. Safety: Monitoring of areas using digital cameras. Management of fire and fire control, automatic and smart public announcement speakers.
4. Transportation: Intelligent roads and high-ways that have cautionary signs which depict the condition of the road, affect of weather on the road and any sudden accidents or diversions.
5. Smart Parking: Smart parking systems that will enable the users to find out about the availability of parking space in the city or the nearest area.
6. Waste Management: Smart dustbins that perform the task of recycling trash and garbage. RFID tags on bins and cans that will help the cleaning and sanitation department to see where they have to get this garbage from [43].

4.3 IoSE (Internet of the smart environment): It has various uses in the smart environment which are stated as:

1. Monitoring air pollution: The air pollution generated by transport can be monitored. Carbon and its emissions from factories can be monitored.
2. Forest Fire Detection: Observing zones that have high levels of inflammatory chemicals and gases and mark them as danger zones so that people can stay away from them.
3. Weather monitoring: Observing conditions of weather such as temperature, wind speed, humidity, rain, and pressure.
4. Water Quality: Checking the quality of water at different water resources to see if the water is drinkable or not.
5. River Floods: Observing the sea level and water levels in various water resources such as rivers, dams, and reservoirs to see if there is a threat of flood.
6. Protecting wildlife: Using tracking devices such as tracking collars to help find wild animals and protect them if they need saving [43].

4.4 IoSI (Internet of smart industry): It has various uses in the smart industry which are stated as:

1. Explosive and Hazardous Gases: Observing and monitoring the levels of different hazardous gasses in the industrial environment that can result in an explosion. Checking gas leakages and leakage of hazardous materials. Observing the gas levels of oxygen in mines to see if they are safe for workers to work there. Keeping an eye on the levels of gas, oil, and water to keep everything in order.
2. Maintenance and repair: Having an overview of the equipment so that we can predict any future failures or malfunctions that can lead to loss of life, money or equipment [43].

4.5 E.IoSH (Internet of smart health): It has various uses in smart health which are stated as:

1. Patients Surveillance: Observing the health of patients

and people who need to be under care all the time. Monitoring old homes.
2. Medical Fridges: Temperature controlled fridges that are used to store important medical-related things such as medicines, blood, organs, etc.
3. Fall Detection: Observing and assisting old people who live alone by keeping an eye on their credentials.
4. Dental: A smart device that is connected to the toothbrush and the phone of the user. It gives details about the condition of the teeth and also tell us about any dangers or dental diseases.
5. Physical Activity Monitoring: Smart sensors that are wireless and are placed in the bed of the patient. They track all the vital movements such as breathing rate, blood pressure, heart rate, etc. All this information can be viewed with the help of a smartphone [43].

4.6 IoSE (internet of smart energy): It has various uses in smart energy which are stated as:
1. Smart Grid: Observing the amount of energy consumed and also managing the energy according to the needs.
2. Wind Turbines/ Powerhouse: Observing how much energy is produced by the powerhouses or wind turbines. Meters that keep track of how much energy is used and how much of it is produced. Analyze patterns in the data of energy use and make decisions according to that pattern.
3. Power Supply Controllers: Determine the amount of energy required with the help of controllers. Provide sufficient and efficient energy that is not wasted but is enough to fulfill the needs of the people.
4. Photovoltaic Installations: Observing the performance of solar energy plants and solar energy sources [43].

4.7 IoSA (internet of smart agriculture): It has various uses in smart agriculture which are stated as:
1. Green Houses: Observe the optimum conditions required to produce maximum amounts of fruits and vegetables and then maintain those conditions to obtain desirable results.
2. Compost: Prevent the growth of decaying matter such as fungus and other microbial organisms in hay, straw, etc.
3. Animal Farming/Tracking: Locating different animals and identifying them to see for what purpose can they be used. Observe the quality of air and gases in farms to maintain optimum conditions for cattle and farm animals.
4. Offspring Care: Observe and control the conditions in which the animals grow improving their chances of survival and growth.
5. Field Monitoring: Decreasing the wastage of land and waste of crop by monitoring the conditions of the soil and fields in which they are grown. Finding out weaknesses in the soil and then replenish them again so that the crops are not lost and gone to waste [43].

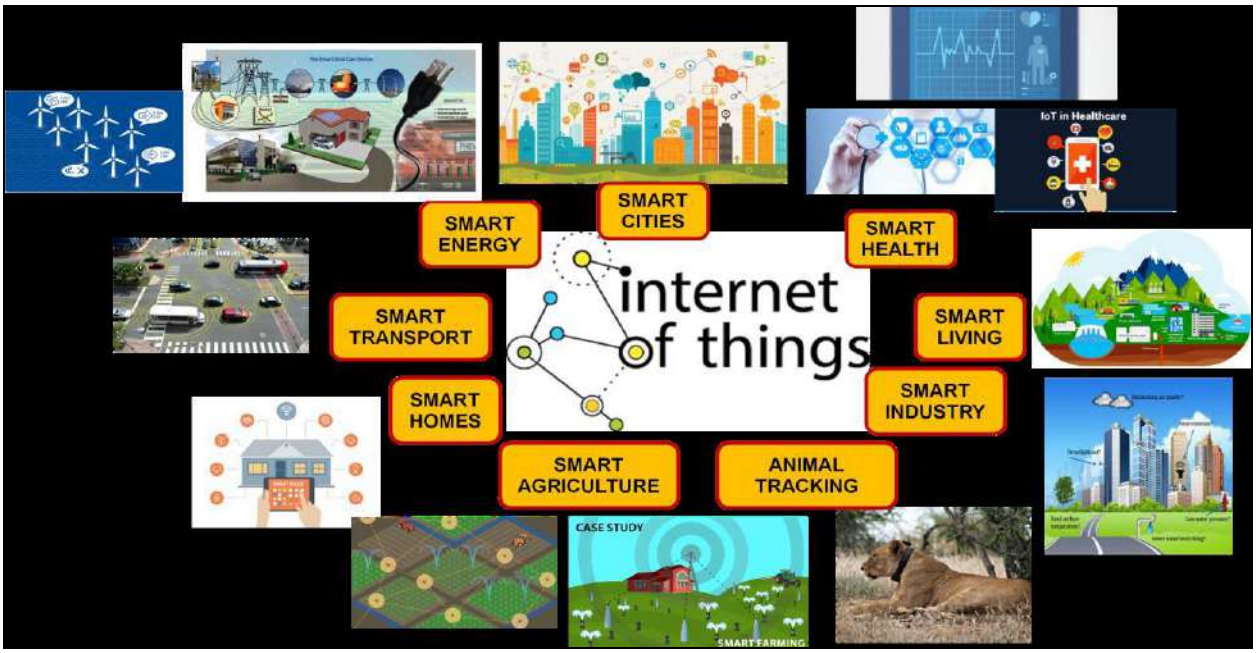


Fig 3: IoT applications

5. Discussion of IoT and future directions

Now we will discuss some concerns related to IoT. Before we demonstrate the future direction of IoT, we first give an example: With the introduction of 5G cars will be able to send and receive signals 10 times faster than they are now. According to a report, the car market globally will increase from 5.1 million units to 37.7 Million units by 2022 [44]. With the steady increase in the technology and induction of telematics units, the experience of driving has changed drastically in a positive way. This advancement has led us to create safer vehicles and improvements in cybersecurity taking us forward into an era in which cars are connected globally. China has been anticipated to be the next big market for autonomous vehicles. Mass adoption of new technology has been seen as a new trend as it has already happened with smartphones so it is anticipated that the trend of autonomous cars will also be accepted provided that the prices are comfortable. We will discuss these issues in detail and are stated as:

1. Safe Driving: The introduction of connected cars can be a plus point for the insurance companies as now they can offer deals and incentives to the drivers such as they will offer them lower premiums if they will drive responsibly. This will help make the road safe for

people and everybody will benefit from this. This can also be used to see how are the drivers driving and can help observe their skills and based on this analysis they can see their mistakes and improve themselves. Big data can solve the problem of traffic jams by predicting better routes for everyone and making traffic work in such a way that there are fewer traffic jams.

2. Predictive Maintenance: The owner of the cars will now be able to see if there would be any fault in their car so they will be able to take precautionary measures before anything bad happens. This will result in a reduction of vehicle breakdown cases and will help the drivers to take care of their vehicles better. Better maintained vehicles have a very low emission rate so this will help the environment as well.
3. The Data Opportunity: A research that was conducted recently shows that automated vehicles will be able to generate approximately 10 times more revenue than the conventional vehicle. The future of the market will not depend on the number of vehicles sold but it will depend on the amount of data generated and stored by the vehicle. This concept is still very fresh and has a lot of room for improvement but it is the future of the automobile industry [45].

A trend can be seen that IoT is headed in the direction of automation of everything and it aims to make everything work like a robot. This is not an easy task as science has not advanced that much and to make everything in human life automated, we need massive capitals which nowadays is not possible [46, 47]. Science wants to achieve full smartness which means that technology which is made up of hardware and software components should act like humans and have similar behavior to that of humans. To achieve that we need equipment and technology that is extremely smart. To develop such technology, we have to make such programming codes that have never been made before and are highly complex. This means that to achieve total smartness we have worked a lot in programming such codes that have never been made before [48]. This is a gradual process that will not happen at a snap of a finger but it will take time.

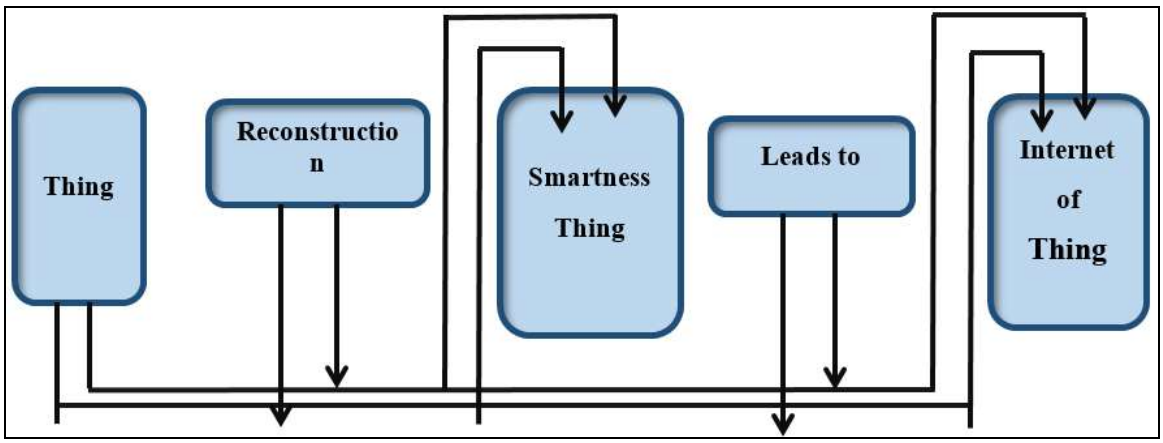


Fig 4: Live cycle of thing to be in the IoT system.

A major problem that will arise by achieving total smartness and that is standardization. Standardization means that the hardware and software of the IoT device or system can be changed according to the needs of the user. Each system has its hardware and software and they are not compatible with other systems as they both are made for different purposes. For example, the task of refrigerators varies from places to places. If they are used in homes they have the task to keep the food fresh and if they are used in hospitals then their task is to keep the organs and blood at the required temperature level as well as release certain gases and chemicals that will keep them from decaying. So we will have to set standards as to how we can use certain equipment in certain conditions. This will help reduce the complexity of IoT and make the devices more compatible and less expensive.

6. Conclusion

IoT can enhance the availability of data and information drastically which will help in transforming all the major companies and organizations into a virtual industry. IoT can help many companies in reaching their industrial as well as strategic goals. It can do that with the help of data analysis and influence the strategic goals of an organization. The amount of numerous innovations required for the further development of the IoT places a premium on interoperability and has brought about broad accomplishments to construct guidelines and specialized details that help reliable and steady correspondence between IoT gadgets and segments. The joint effort between different standard improvement gatherings and the combination of some present endeavors will inevitably bring about more noteworthy clearness for IoT innovation organizations. A self-driving car can pick you up at a scheduled time and also find out the best route to home with the least traffic. 5G can make communication 10 times faster that will improve awareness in devices and will give devices the ability to make faster and quicker decisions. This is what the future will be like. The main purpose of this paper is to provide a clear and deep understanding of IoT, especially security issues and suggest solutions to address them and highlighting areas of use IoT applications, to additional advance the improvement of IoT.

7. References

1. Roberto Minerva ABR. IEEE, Telecom Italia SPA, 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

2. Challenge SAG. NIST, 2014. [Online]. Available: http://www.nist.gov/.
3. Greer C. The Internet's Next Big Idea: Connecting People, Information and things, 2014. [Online]. Available: http://www.nist.gov/el/20140611_internets_next_big_idea.cfm.
4. IEEE-SA. Internet of things ecosystem study, IEEE, 2015. [Online]. Available: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/iot_ecosystem_exec_summary.pdf
5. Mahmoud Rwan *et al*. Internet of things (IoT) security: Current status, challenges, and prospective measures. 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015.
6. Atzori Luigi *et al*. The social internet of things (IoT)-when social networks meet the internet of things: Concept, architecture, and network characterization. Computer networks. 2012; 56(16):3594-3608.
7. Leo Marco *et al*. A federated architecture approach for Internet of Things security. Euro Med Telco Conference (EMTC). IEEE, 2014.
8. Wu Miao, Ting-lie Lu, Ling Sun, Hui-Ying Du. Research on the architecture of Internet of things, in advanced Computer Theory and Engineering (ICACTE), 2010, 484-487.
9. Tan Lu, Neng Wang. Future internet: The internet of things. 3rd international conference on advanced computer theory and engineering (ICACTE). IEEE, 2010, 5.
10. Al-Fuqaha Ala *et al*. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials. 2015; 17(4):2347-2376.
11. Da Xu, Li Wu He, Shancang Li. Internet of things in industries: A survey. IEEE Transactions on industrial informatics. 2014; 10(4):2233-2243.
12. Atzori Luigi, Antonio Iera, Giacomo Morabito. The internet of things: A survey. Computer networks. 2010; 54(15):2787-2805.
13. Miorandi Daniele *et al*. Internet of things: Vision, applications and research challenges. Ad hoc networks. 2012; 10(7):1497-1516.
14. Suo Hui *et al*. Security in the internet of things: a review. international conference on computer science and electronics engineering. IEEE, 2012, 3.
15. Ilie-Zudor, Elisabeth *et al*. A survey of applications and requirements of unique identification systems and RFID techniques. Computers in Industry. 2011; 62(3):227-252.
16. Han Chong *et al*. A cross-layer communication module for the Internet of Things. Computer Networks. 2013; 57(3):622-633.
17. Lin Jie *et al*. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal. 2017; 4(5):1125-1142.
18. Capkun Srdjan, Levente Buttyán, Jean-Pierre Hubaux. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on mobile computing. 2003; 1:52-64.
19. Yang Xinyu *et al*. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. IEEE Transactions on Computers. 2013; 64(1):4-18.
20. Maheswari Uma S *et al*. A novel robust routing protocol RAEED to avoid DoS attacks in WSN. International Conference on Information Communication and Embedded Systems (ICICES). IEEE, 2016.
21. Chuang Ming-Chin, Jeng-Farn Lee. TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Systems Journal. 2013; 8(3):749-758.
22. Zhao Kai, Lina Ge. A survey on the internet of things security. Ninth international conference on computational intelligence and security. IEEE, 2013.
23. Bharathi Vivekananda M *et al*. Node capture attack in Wireless Sensor Network: A survey. IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2012.
24. Yang Xinyu *et al*. Towards a low-cost remote memory attestation for the smart grid. Sensors. 2015; 15(8):20799-20824.
25. Lin Jie, Wei Yu, Xinyu Yang. Towards multistep electricity prices in smart grid electricity markets. IEEE Transactions on Parallel and Distributed Systems. 2015; 27(1):286-302.
26. Lin Jie *et al*. On false data injection attacks against distributed energy routing in smart grid. Proceedings of the IEEE/ACM Third International Conference on Cyber-Physical Systems. IEEE Computer Society, 2012.
27. Cho Chang-Hyun *et al*. Design of RFID mutual authentication protocol using time stamp. Fourth International Conference on Computer Sciences and Convergence Information Technology. IEEE, 2009.
28. Zhang Jing *et al*. Differential power cryptanalysis attacks against PRESENT implementation. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE, 2010, 6.
29. Yang Bo, Kaijie Wu, Ramesh Karri. Scan based side channel attack on dedicated hardware implementations of data encryption standard. International Conference on Test. IEEE, 2004.
30. Maheswari Uma S *et al*. A novel robust routing protocol RAEED to avoid DoS attacks in WSN. International Conference on Information Communication and Embedded Systems (ICICES). IEEE, 2016.
31. Andrea Ioannis, Chrysostomos Chrysostomou, George Hadjichristofi. Internet of Things: Security vulnerabilities and challenges. IEEE Symposium on Computers and Communication (ISCC). IEEE, 2015.
32. Mukaddam Ayman *et al*. IP spoofing detection using modified hop count. IEEE 28th International Conference on Advanced Information Networking and Applications. IEEE, 2014.
33. Mitrokotsa Aikaterini, Melanie Rieback R, Andrew S. Tanenbaum. Classifying RFID attacks and defenses. Information Systems Frontiers. 2010; 12(5):491-505.
34. Chen Ray, Jia Guo, Fenye Bao. Trust management for service composition in SOA-based IoT systems. IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2014.
35. Soni Vinay, Pratik Modi, Vishvash Chaudhri. Detecting Sinkhole attack in wireless sensor network.

International Journal of Application or Innovation in Engineering & Management. 2013; 2(2):29-32.
36. Kalnoor Gauri, Jayashree Agarkhed. QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2016.
37. Padhy Rabi Prasad, Manas Ranjan Patra, Suresh Chandra Satapathy. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011; 1(2):136-146.
38. Zhang Kuan *et al*. Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal. 2014; 1(5):372-383.
39. Jagatic Tom N *et al*. Social phishing. Communications of the ACM. 2007; 50(10):94-100.
40. Sahoo Abhaya Kumar, Amardeep Das, Mayank Tiwary. Firewall engine based on graphics processing unit. IEEE International Conference on Advanced Communications, Control and Computing Technologies. IEEE, 2014.
41. SINTEF. Ovidiu Vermesan, and P. F. Norway. Belgium, Internet of Things–From Research and Innovation to Market Deployment‖, 2014.
42. Research B. The future of retail through the Internet of Things (IoT), Intel, 2013. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/future-retail-through-iot-paper.pdf.
43. Patel Keyur K, Sunil Patel M. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing. 2016; 6:5.
44. Research B. The future of retail through the Internet of Things (IoT). Intel, 2013. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/future-retail-through-iot-paper.pdf.
45. Karen Rose SELC. The Internet of Things: An overview. Internet Society, 2015. [Online]. Available: https://pdfs.semanticscholar.org/df53/501af80026c4379a3467b551caaf7589a1db.pdf?_ga=2.111088646.2296748 93.1565134891-667184256.1565134891.
46. Kiritsis Dimitris. Closed-loop PLM for intelligent products in the era of the Internet of things. Computer-Aided Design. 2011; 43(5):479-501.
47. Kortuem Gerd *et al*. Smart objects as building blocks for the internet of things. IEEE Internet Computing. 2009; 14(1):44-51.
48. Said Omar, Mehedi Masud. Towards internet of things: Survey and future vision. International Journal of Computer Networks. 2013; 5(1):1-17.