12th International Conference on Recent Innovations in Science, Engineering and Management
Sri Venkateswara College of Engineering & Technology,Etcherla, Srikakulam (ICRISEM'18)
17th February 2018 www.conferenceworld.in ISBN: 978-93-87793-01-9

INTERNET OF THINGS - A BUDDING TENDENCY

B.V.Hemalatha[1], R.Vijayalatha[2]

[1]Assistant Professor, Department of Computer Science & Information Technology,
Theni Kammavar Sangam College of Arts & Science, Theni, Tamilnadu, India)
[2]Research Scholar, Manonmaniam University, Tirunelveli (India)

ABSTRACT

In the recent years, people need to use Internet at anytime and anywhere. Internet of Things (IOT) allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. IOT can be distinguished by various technologies, which provide the creative services in different application domains. This implies that there are various challenges present while deploying IOT. The recent development of communication devices and wireless network technologies continues to advance the new era of the Internet and telecommunications. The various "things", which include not only communication devices but also every other physical object on the planet, are also going to be connected to the Internet, and controlled through wireless networks. This concept, which is referred to as the "Internet of Things (IoT)", has attracted much attention from many researchers in recent years.

Keywords— Internet of Things(IOT), RFID, WSN, ICSS, MEMS.

I INTRODUCTION

In the recent years, Internet has become the most important thing in people's life. Around two billion people around the world use Internet for sending and receiving emails, using social networking applications, sharing large amount of data, playing games and many other things. As the use of Internet is growing day-by-day, another big area is emerging to use Internet as a global platform for allowing the machines and smart objects to communicate, compute and coordinate, called Internet of things (IoT). IoT is a technology where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via the Internet.

With the rapid development of Internet technology and communications technology, our lives are gradually led into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. However, human beings live in a real world, human activities cannot be fully implemented through the services in the imaginary space. It is the limitation of imaginary space that restricts the development of Internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and real-world on a same platform which is called as Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models. Apart from benefits of IoTs, there are several security and privacy concerns at different layers viz; *Front end, Back end and Network*. In this paper, the survey is in several security and privacy

concerns related to Internet of Things (IoTs) by defining some open challenges. Then, discussion on some applications of IoTs in real world [1].

The motivation behind IoT is to create, Smart city, to optimize use of public resources, increase the quality of services offered to people and decrease the operational costs of the services. The ultimate goal is to create „a better world for human beings, where objects around us know what we like, what we want and what we need and act accordingly without explicit instructions.

The term IoT is used to refer (i) the global network which interconnects smart objects by using Internet technologies (ii) set of supporting technologies such as Radio Frequency Identifications(RFIDs), sensor/actuators, machine-to-machine communicating devices etc. (iii) combination of application and services using such technologies for business purposes.

The IoT depends upon three building blocks, based on the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) to communicate (anything communicates) and (iii) to interact (anything interacts). The focus of IoT is on the data and information, rather than point-to-point communication [2].

II IOT OVERVIEW AND BACKGROUND

2.1 What is the Internet of Things?

As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. They are "Material objects connected to material objects in the Internet".

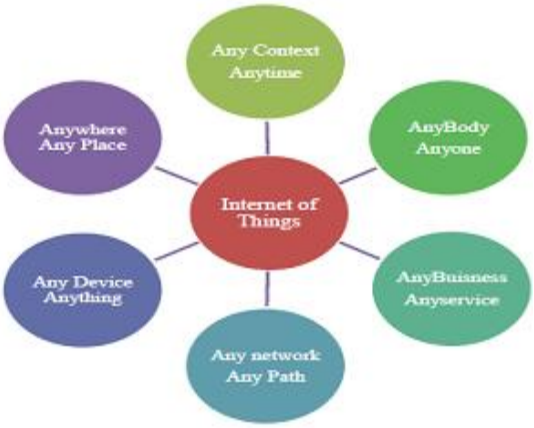

Fig. 1. Definition of Internet of Things.

For example, through RFID, laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object for communication services and data exchange. At last, to reach the smart devices to be tracked, located, and monitored and to handle the network functions, to make the IT infrastructure and physical infrastructure consolidation IoT is the most needed one.

2.2 Evolution

Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in Fig. 2, in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and formed the mobile-Internet. With the emergence of social networking, users started to become connected together over the Internet. The next step in the IoTs is where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via the Internet.

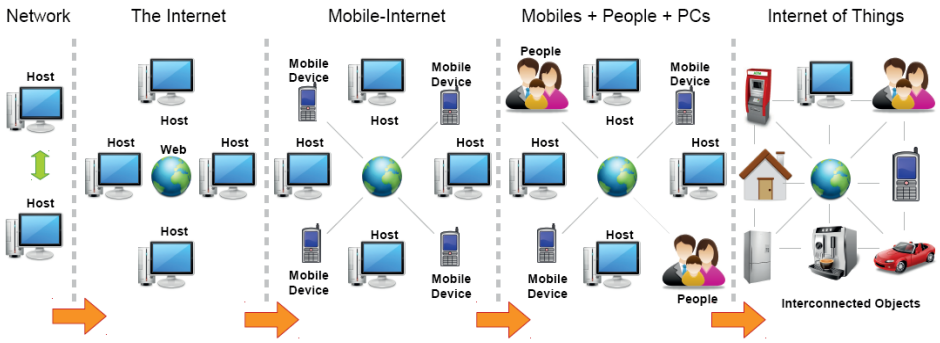

Fig.2. Evolution of Internet of Things

IoT promises to create a world where all the objects (also called smart objects) around us are connected to the Internet and communicate with each other with minimum human intervention. The ultimate goal is to create "a better world for human beings", where objects around us know what we like, what we want, and what we need and act accordingly without explicit instructions [1].

III ARCHITECTURE OF IOT

More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980, cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols. Without a proper privacy assurance, IoT is not likely to be adopted by many. Therefore protection ofdata and privacy of users are key challenges for IoT. The six layers of IoT are described below as shown in Fig.3:

3.1 Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects.

3.2 Perception Layer

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

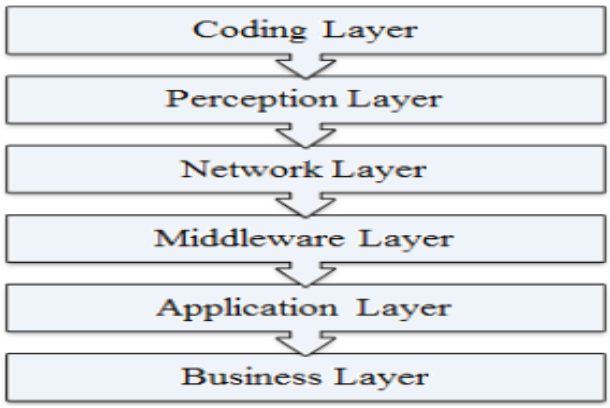

Fig.3. Six-Layered Architecture of IOT

3.3 Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth,WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

3.4 Middleware Layer

This layer processes the information received from the sensor devices. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

3.5 Application Layer

This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the development of IoT so this layer is very helpful in the large scale development of IoT network. The IoT related applications could be smart homes, smart transportation, smart planet etc.

3.6 Business Layer

This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies[3].

IV TECHNOLOGIES OF IOT

The development of a ubiquitous computing system where digital objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which automated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other. In this section we discuss the relevant technologies that can help in the large-scale development of IoT.

4.1 Radio Frequency Identification (RFID)

RFID is the key technology for making the objects uniquely identifiable. Its reduced size and cost makes it integrable into any object. It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application. Active tags have a battery attached to them due to which they are always active and therefore continuously emit the data signals while Passive tags just get activated when they are triggered. Active tags are more costly than the Passive tags however they have a wide range of useful applications. RFID system is composed of readers and associated RFID tags which emit the identification, location or any other specifics about the object, on getting triggered by the generation of any appropriate signal. The emitted object related data signals are transmitted to the Readers using radio frequencies which are then passed onto the processors to analyze the data.

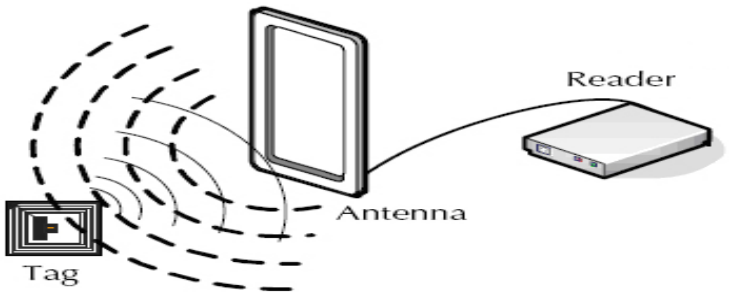

Fig.4. RFID Scenario

Depending on the type of application, RFID frequencies are divided into four different frequencies ranges, which are given below:

(1) Low frequency (135 KHz or less)

(2) High Frequency (13.56MHz)

(3) Ultra-High Frequency (862MHz 928MHz)

(4) Microwave Frequency (2.4G, 5.80)

Bar Code is also an identification technology which has almost the same function as an RFID but RFID is more effective than a Bar Code due to a number of its benefits. RFID being a radio technology doesn't require the reader to be physically in its vision while Bar Code is an optical technology which cannot work unless its reader

is placed in front of it. Moreover, an RFID can work as an actuator to trigger different events and it has even modification abilities which Bar codes clearly don't have.

4.2 Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, built from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc and then pass on to the processing equipment. The sensing nodes communicate in multi-hop each sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a communication, actuation and sensing unit respectively along with a source of power which could be both battery and any energy harvesting technology. A typical sensing node is shown in the figure below:

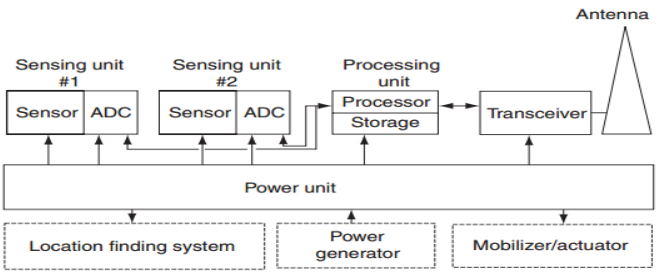

Fig.5. A typical sensing node

Wireless Sensors Network technology and RFID technology when combined together opens up possibilities for even more smart devices, for which a number of solutions have been proposed. An example solution is provided by the Intel Research Labs in the form of Wireless Identification Sensing Platform (WISP). WISP is a passive wireless sensor network with built-in light, temperature and many other sensors. Both WSN and RFID Sensor Networks have their own advantages but RFID Sensor Networks have a low range and their communication is Asymmetric while WSNs have a comparatively longer range and their communication is Peer-to-Peer. Moreover most of the WSNs are based on the IEEE 802.15.4 standard, which specifies the Physical and MAC layer of Low-Rate Wireless Personal Area Networks (LR-WPANs).

The technologies that enable the integration of WSN with the IOT are a hot research topic, many solutions have been proposed for that including that of a 6LOWPAN standard, that allows IPv6 packets to be transmitted through the networks that are computationally restricted. Also there's ROLL routing standard for end-to-end routing solutions.

4.3 Cloud Computing

With millions of devices expected to come by 2020, the cloud seems to be the only technology that can analyze and store all the data effectively. It is an intelligent computing technology in which numbers of servers are converged on one cloud platform to allow sharing of resources between each other which can be accessed at any time and any place.

Fig.6. A typical Cloud Computing Scenario

Cloud computing is the most important part of IoT, which not only converges the servers but also processes on an increased processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity. But this is just a beginning of unleashing the true potential of this technology. Cloud computing interfaced with smart objects using potentially millions of sensors can be of enormous benefits and can help IoT for a very large scale development so researches are being carried out since IoT will be totally dependent on the Cloud Computing.

4.4 Networking Technologies

These technologies have an important role in the success of IoT since they are responsible for the connection between the objects, so we need a fast and an effective network to handle a large number of potential devices. For wide-range transmission network we commonly use 3G, 4G etc. but As we know, mobile traffic is so much predictable since it only has to perform the usual tasks like making a call, sending a text message etc. so as we step into this modern era of ubiquitous computing, it will not be predictable anymore which calls for a need of a super-fast, super-efficient fifth generation wireless system which could offer a lot more bandwidth. Similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc.

4.5 Nano Technologies

This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a system by enabling the development of devices in nano meters scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and the resulting network defines a new networking paradigm which is Internet of Nano Things.

4.6 Micro-Electro-Mechanical Systems (MEMS) Technologies

MEMS are a combination of electric and mechanical components working together to provide several applications including sensing and actuating which are already being commercially used in many field in the form of transducers and accelerometers etc. MEMS combined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc.

4.7 Optical Technologies

Rapid developments in the field of Optical technologies in the form of technologies like Li-Fi and Cisco's BiDi optical technology could be a major breakthrough in the development of IoT. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide a great connectivity on a higher bandwidth for the objects interconnected on the concept of IoT. Similarly Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multifarious devices of IoT [3].

V APPLICATIONS OF IOT

A survey done by the IoT-I project in 2010 identified IoTs application scenarios which are grouped in 14 domains viz; Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy. This survey was based on 270 responses from 31 countries and the scenarios attracting the most interest were: smart home, smart city, transportation and health care. In this paper, the focus will be briefly on the IoTs applications in medical (health care), smart home, intelligent community security system (smart city).

5.1 IoTs in Medical Application

Due to population growth, rural urbanization, declining birthrate, population aging, economic growth and social unbalanced resource utilization, some social problems have become increasingly apparent in the healthcare field.

- The health management level and the incapability of responding to emergency is a pressing social problem.
- There is a serious shortage in medical staffs, institutional facilities especially in rural areas, lack of medical facilities, low level of treatment, inadequate healthcare system.
- The imperfect diseases prevention system cannot meet the national strategy requirements to safeguard the health of the citizen becoming heavy burden on economy, individuals, families and state.
- Inadequate disease prevention and early detection capability.

To address these issues, Remote Monitoring and Management

Platform of Healthcare information (RMMP-HI) can provide monitoring and management of these lifestyle diseases so as to reach the purpose of prevention and early detection.

Regardless of restrictions of location, time, and user' activity state, RMMP-HI can collect human body medical information timely through a variety of body medical sensors loaded in the human body or surrounding space and extract useful information by data encryption, storage, comparative analysis and processing. When abnormal appearance is found, users are notified to take early treatment; this enables the early detection and prevention.

Fig.7. The framework of healthcare service

Through real-time monitoring, when user is in emergency agencies or relevant authorities, which improve medical emergency treatment and response capacity. Furthermore, it is also efficient to establish national health management records, to provide prevention and decision making basis for lifestyle diseases, epidemic and regional disease through monitoring, comparing analyzing and processing healthcare information of associated group. In this way, capabilities of disease prevention, early detection and early treatment are improved enormously.

Body medical sensors can register and delete, constituting Medical Body Area Network (MBAN) automatically. As shown in Fig. 7, short-range wireless communication sensor module will transmit human medical information to 3G mobile phone or home gateway. This medical information is uploaded to data storage and processing center timely. Then the important health guidance will be fed back to the patient, family members of patients or medical institutions after analytical processing of expert system or the inspection of professional medical staff in health service center. In the state of emergency, first-aid notification is delivered to medical institution by health service center to provide emergency services to patients.

5.2 IoT in Smart Home

Now a days, smart homes are becoming more and more cost effective and intellectualized with continued progress and cost reduction in communication technology, information technology, and electronics, which connects the Internet with everyday devices and sensors for connecting virtual and physical objects through the data capture and communication capabilities development.

Reading of remote meters can be attained through these smart home systems. That implies, the data related with home power, telecommunications, gas and water can be sent automatically to their corresponding utility company to enhance the efficiency of the work. In addition, by virtue of smart home systems, windows, home ventilation, doors, lighting, air conditioning etc., can be controlled by remotely. Each electronics devices such as refrigerator, washing machine, oven etc., can be manipulated by remote platforms or programs. Entertainment

equipment's like radios and televisions can be connected to common channels which are in remote. In addition, home security and healthcare are also important aspects of smart homes.

Fig.8. IoT Smart Home.

For instance, health aid devices can help an elder individual to send request or alarm to a family member or a professional medical center. In the smart home design, the house and its different electrical appliances have been equipped with actuators, sensors as shown in Fig. 8. The home devices functions in a local network but on certain occasions connected to a remote management platform in order to do processing and data collection.

5.3 Intelligent Community Security System (ICSS)

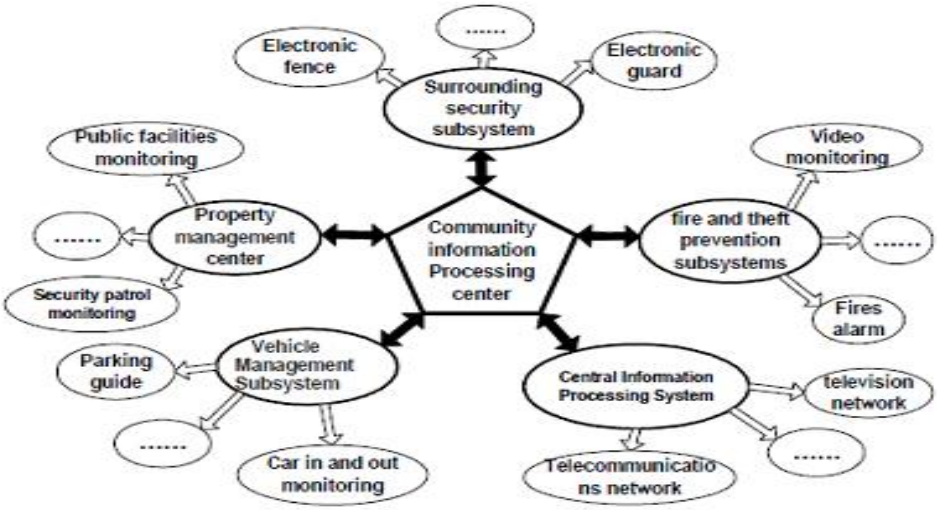

Fig.9. Intelligent Community Security System (ICSS)

As shown in Fig. 9, the intelligent community security system (ICSS) holds several subsystems, such as Vehicle Management Subsystem (VMS), Surrounding Security Subsystem (SSS), Central Information Processing System (CIPS), Property Management Subsystem (PMS), Fire and Theft Prevention Subsystem (FTPS) etc.

Through wireless the information of each subsystem is messaged to the CIPS implies automatic adjustments and timely warnings in order to maintain the community security. The details about ICSS subsystems are as follows:

1) Vehicle Management Subsystem of the ICSS

The Vehicle Management Subsystem in ICSS adopts IPR, sensor network technologies and RFID. Image registration can be taken by RFID card and video camera which is given to the vehicles, as shown in Fig.10. The vehicle license information will be messaged to the CIPS, when it enters the communities.

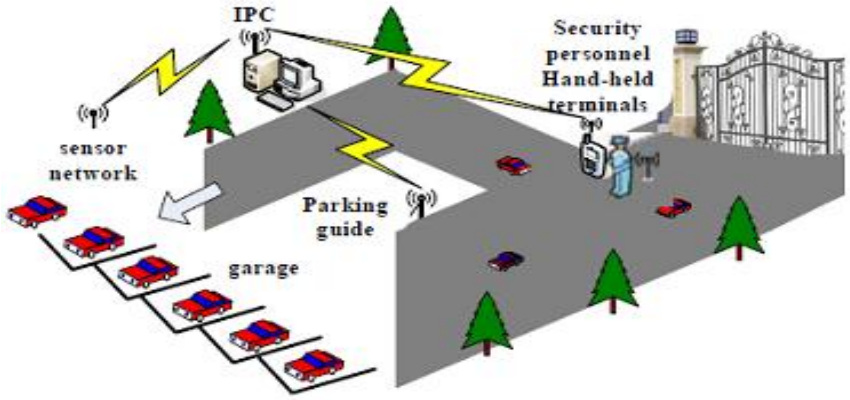

Fig.10. Vehicle Management Subsystem

The visitors are allocated with the temporary parking places. The record data and the information of the driver' RFID card must be coherent, when the car leaves. This guarantees the security of cars and prevents theft occurrences. In the garages video monitoring devices will prevent stealing or damage to assure the vehicles safety. Through the Human-Computer interface system CIPS can controls the garages to facilitate and observe the vehicle management.

2) Surrounding Security Subsystem (SSS) of the ICSS

As per the requisites of security surroundings to establish an intelligent and enclosed community, sensing terminals such as Power Network, Unicode Infrared Laser and Sensor Optical Fiber etc are installed. As shown in Fig. 11, wireless and sensor networks gather the useful information and feedback to the CIPS at regular time intervals.

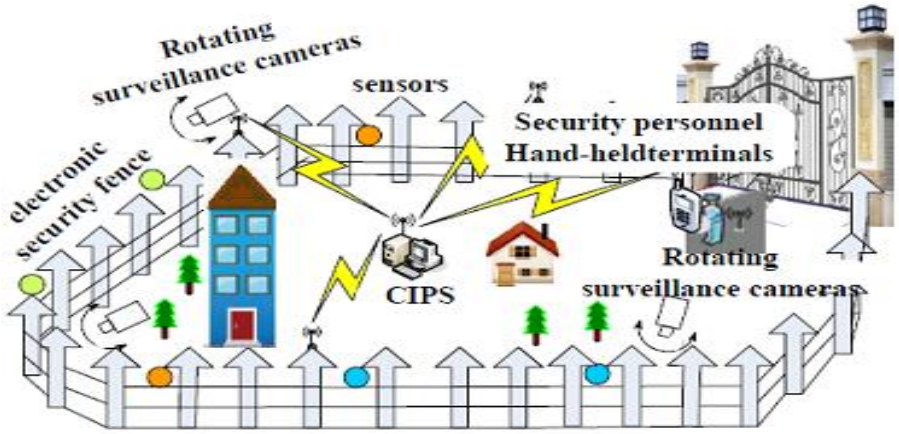

Fig.11. Surrounding Security Subsystem

The SSS contains electronic access controls, electronic fences and rotatable monitoring cameras. It can be utilized to avoid illegal enter or intrusive behavior into communities. The subsystem can find the exact location of the accident by using sensing terminals which can automatically omit untrue signals. The rotatable cameras will track the people or objects by IPR technology; simultaneously they triggers alarm to the handheld devices of the security personnel and CIPS through the sensor network.

Intruder's location could be verified on the CIPS electronic map and electronic alarm is triggered. The accident images can get by clicking the handheld devices of security personnel and can rush to the crime scene as early as possible. The CIPS will give lighting facilities and begin to monitor systems to tape the whole process in order to ensure the security of the area particularly in the places which is beyond the security personnel' sights.

3) ***Property Management Subsystem of the ICSS***

A humanized and efficient property management system provides more convenience and happiness to the residents. As shown in Fig. 12, the IoT technology can get better residential property management which is more standardized and scientific.

- Public Facilities Monitoring System use the unified coding sensor network technology which provides real-time monitoring of the public facilities such as the public transportations, swimming pools, emergency exits, residential elevators, community basketball courts and so on. In case somebody is injured or public facilities are damaged, the terminals triggers alarm information will sent to the CIPS which can thoroughly go through the situation or circumstances and the accurate location automatically. To ensure the safety and smooth of the public areas security personnel can verify and repair the facilities at regular intervals.
- Management for electricity, water and gas uses the unified coding sensor network technology which provides the real-time detection and also controlling of working conditions, such as the power distribution system, the drainage, water supply and elevators. Through the wireless network the information of failed operations will be sent to the CIPS at regular intervals. The unexpected cutting off of electricity, water or gas can be determined or resolved as early as possible.

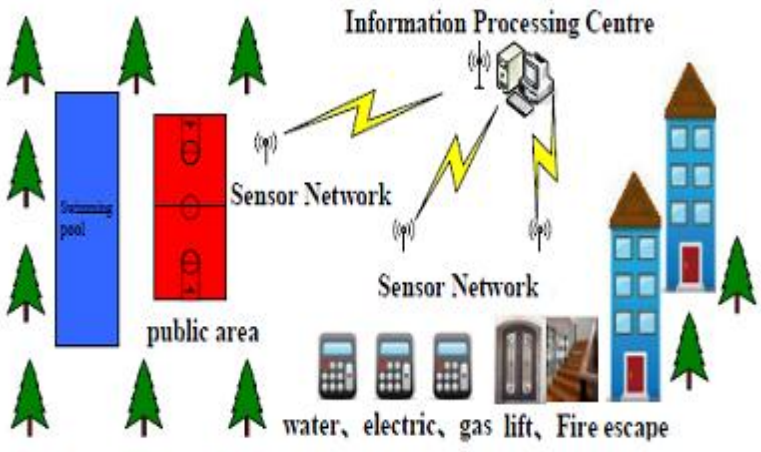

Fig.12. Property Management Subsystem of the ICSS

4) Fire and Theft Prevention Subsystem (FTPS) of the ICSS

Electrical equipment's and appliances may induce huge potential dangers. The FTPS can be used for the indoor security. As shown in Fig. 13, it contains anti-theft and anti-fire alarm system, video monitors and emergency alarm functions, etc. The system primarily use the uniform coded of sensing window fences, monitor cameras, entrance guard devices, emergency calling devices, temperature sensors, and smart detectors of smoker combustible gas. To form the network of this subsystem home network, sensor network and the CIPS were used [1].

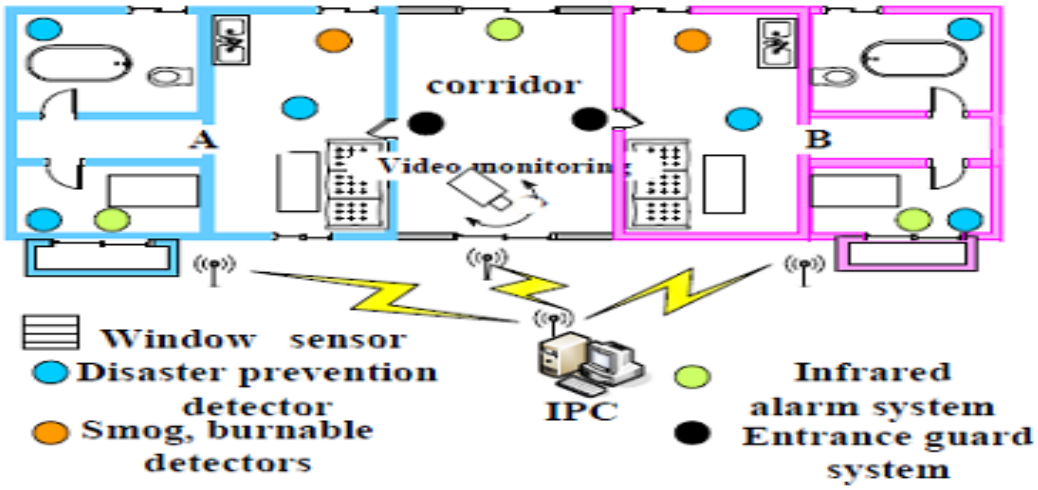

Fig.13. Fire and Theft Prevention Subsystem of the ICSS

VI SECURITY AND PRIVACY CONCERNS IN IOT

6.1 Security Concerns in IoTs

Internet of Things virtually is a network of real world systems with real-time interactions. The development of the initial stage of IoT, is M2M (Machine to Machine), having unique characteristics, deployment contexts and

subscription. Unattended operation without human intervention is possible for long periods of time by the wireless area network (WAN) or WLAN. Though providing improvements in social efficiency it creates an array of new problems concerning breach of privacy and that information security. The various threats in the security of IoT is shown in the below Fig 14.

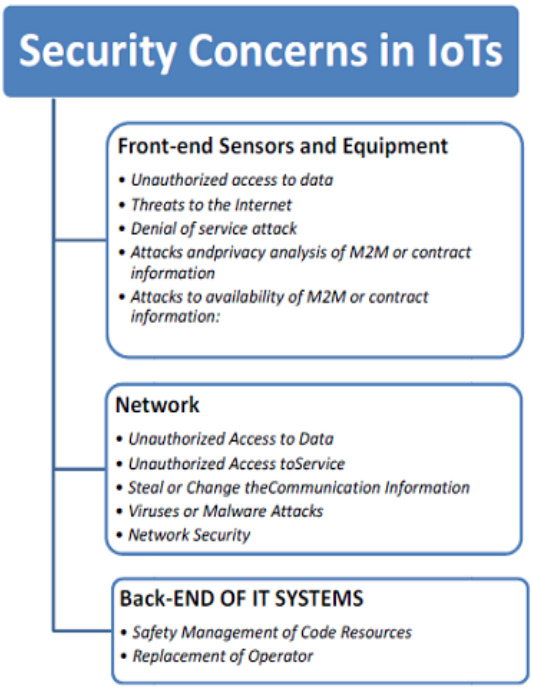

Fig.14. Security Threats of IOT

1) Front-end Sensors and Equipment

Front-end sensors and equipment receives data via the built-in sensors. They then transmit the data using modules or M2M device, thus achieving networking services of multiple sensors. This methodology involves the security of machines with business implementation and node connectivity.

Machine or perception nodes are mostly distributed in the absence of monitoring scenarios. An intruder can easily access these devices which imply damage or illegal actions on these nodes can be done. Possible threats are analyzed and are categorized to unauthorized access to data, threats to the Internet and denial of service attack.

2) Network

Network plays an important role providing a more comprehensive interconnection capability, effectualness and thriftiness of connection, as well as authentic quality of service in IoTs. Since a large number of machines sending data to network congestion, large number of nodes and groups exist in lOTs may be resulted in denial of service attacks.

3) Back-end of it systems

Back-end IT systems form the gateway, middleware, which has high security requirements, and gathering, examining sensor data in real time or pseudo real-time to increase business intelligence. The security of IoT system has seven major standards viz; privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time.

6.2 Privacy Concerns in IOTs

The Internet security glossary defines privacy as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

Typically in IoTs, the environment is sensed by connected devices. They then broadcast the gathered information and particular events to the server which carries out the application logic. This is performed by Mobile or/and fixed communication which takes the responsibility.

Privacy should be protected in the device, in storage during communication and at processing which helps to disclose the sensitive information. The privacy of users and their data protection have been identified as one of the important challenges which need to be addressed in the IoTs.

1) Privacy in Device

The sensitive information may be leaked out in case of unauthorized manipulation or handling of hardware and software in these devices. For example, an intruder can "re-program" a surveillance camera could such that it sends data not only to the legitimate server, but also to the intruder. Thus, for devices that gather sensitive data robustness and tamper-resistance are especially important. To ensure IoTs security trusted computing technologies including device integrity validations, tamper-resistant modules and trusted execution environments are useful.

In order to provide the privacy in the devices, there exists so many problems one need to address such as it could be the location privacy of the device holder , non-identifiability means protecting the identification of the exact nature of the device, protecting the personal information in case of the device theft or loss and resilience to side channel attacks. Location Privacy in WSN is achieved by using the algorithm Multi-Routing Random walk in the wireless sensors, in the case of the Protecting of display privacy and Protection of personal Identifiable Information(PII) in case of device loss, theft could be achieved by having QR codes(Quick Response Code) technique were selected. In the case of Non-Identifiability and side channel attacks adding randomness or noise, having synchronous CPUs, Blind values used in calculations could be used.

2) Privacy during Communication

To assure data confidentiality during the transmission of the data, the most common approach is encryption. Encryption on certain occasions adds data to packets which provides a way for tracing, e.g. sequence number,

IPsec- Security Parameter Index, etc. These data may be victimized for linking packets to the analysis of same flow traffic. Secure Communication Protocol could be the suitable approach.

During the communication Pseudonyms can be replaced for encryption in case it is not feasible to the device's identity or user's in order to decrease the vulnerability. One of the long familiar examples is Temporary Mobile Subscriber Identity (TMSI). Devices should communicate if and only if when there is a need, to derogate privacy disclosure induced by communication. In 3GPP machine type communications, in order to avoid unnecessary collection of location information by the network after a certain period of inactivity the devices will detach from the network.

3) Privacy in Storage

For protecting privacy of information storage, following principals should be considered.

- Only the least possible amount of information should be stored that is needed.
- In case of mandatory then only personal information retained.
- Information is brought out on the basis of "need-to-know".

To conceal the real identity tied with the stored data Pseudonymization and Anonymization could be used. Without disclosing any specific record, a database could allow access only to statistical data (sum, average, count, etc.). To ensure the output (typically aggregate queries) is independent of the absence or presence of a particular record adds noise called as differential privacy could be the appropriate technique.

4) Privacy at Processing

It is mainly of two folds. Firstly, personal data must be treated in a way that it should be simpatico with the intended purpose. Secondly, without explicit acceptance and the knowledge of the data owner, their personal data should not be disclosed or retained to third parties.

By considering the above two points, Digital Rights Management (DRM) systems is most suitable which controls the consumption of commercial media and defends against re-distribution illegally. One can define privacy policies for personal data in a rights object or license instead of excising principles for commercial media which must be obeyed during the data processing. DRM requires trusted devices, secure devices to work efficiently and effectively.

User's permission and their awareness are requirements for distribution of personal data. User notification aids to avoids abuse [1].

VII FUTURE PERSPECTIVE OF IOT

In the future, things may be controlled not only inside the network that they are the parts of but also with the condition of the other network scales. In such situations, it is necessary to consider the way to efficient utilize the new type of IOT systems.

A. Requirements of Next Generation IOT systems

1) Large Address Space

2) Network Scale based security frameworks

3) Data Processing

VIII CONCLUSION

IoT is the next step towards using Internet anywhere and anytime. IoT allows connecting people and devices (things) anytime, anyplace, with anything and anyone.

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us.

The IoT technology draws huge changes in everyone's everyday life. In the IoTs era, the short-range mobile transceivers will be implanted in variety of daily requirements. The connections between people and communications of people will grow and between objects to objects at any time, in any location. The efficiency of information management and communications will arise to a new high level. The dynamic environment of IoTs introduces unseen opportunities for communication, which are going to change the perception of computing and networking. The privacy and security implications of such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT.

In this survey, we presented Internet of Things with architecture and design goals. We surveyed security and privacy concerns at different layers in IoTs. In addition, we identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. We also discussed applications of IoTs in real life. And also this paper described the present state and future prospects of IoT. In future, research on the IoTs will remain a hot issue. Lot of knotty problems is waiting for researchers to deal with.

The future research directions mainly consist of how to deal with the challenges may be related to security issues, faced by IoT. We hope this paper will be helpful in order to allow a valuable deployment of IoT systems and in suggesting the future research direction.

REFERENCES

[1] J.Sathish Kumar and Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications (0975 – 8887), Volume. 90 – No 11, March 2014.

[2] Ashvini Balte, Asmita Kashid, Balaji Patil, "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and software Engineering, Volume 5, Issue 4, 2015.

[3] M.U.Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal, "A Review on Internet of Things (IoT)," International Journal of Computer Applications (0975 – 8887), Volume. 113 – No 1, March 2015.

[4] Yen-Kuang Chen, "Challenges and Opportunites of Internet of Things," IEEE, 2012.

[5] Yuichi Kawamoto, Hiroki Nishiyama, Nei Kato, Naoko Yoshimura, Shinichi Yamamoto, "Internet of Things (IoT): Present State and Future Prospects," Special Section on Frontiers of Internet of Things.