Internet of Things:Proposed Security Aspects for Digitizing the World

MANJU KHARI
Dept. of Computer Science
AIACT&R
Geeta Colony, Delhi- 110031
manjukhari@yahoo.co.in

MANOJ KUMAR
Dept. of Computer Science
AIACT&R
Geeta Colony, Delhi- 110031
manoj.g2408@gmail.com

SONAKSHI VIJ
Dept. of Computer Science
AIACT&R
Geeta Colony, Delhi- 110031
svij62@yahoo.com

PRIYANK PANDEY
Dept. of Computer Science
AIACT&R
Geeta Colony, Delhi- 110031
priyankpandeyrc@gmail.com

VAISHALI
Dept. of Computer Science
AIACT&R
Geeta Colony, Delhi- 110031
Vaishalig1012@gmail.com

Abstract—The Internet is a Heterogeneous entity which is constantly changing and evolving. The concept of "Internet of Things" (IOT) refers to extending the intelligent sensors in our day to day objects such as televisions, fridge, media players, heating appliances etc. This would help in extending the ability of the objects to provide feedback to the user. This enables the object to have some sort of consciousness.What we have today is the human interacting with the object and not vice-versa, but the IOT would help us to complete this loop. This kind of digitization would mean that our next generation of refrigerators would know more about our diet then our current dieticians. This would help in creating a "system of systems". Consideringacurrent scenario where the number of digital security threats and attacks are increasing day by day, the notion of IOT would be incomplete if we ignore its security aspects. In this paper, we would be exploring the various security aspects of IOT such as security ofremote frequency identifiers(RFID), wireless sensors etc. We have proposedataxonomyof the security aspects of IOT. We have also explained the basic concepts and motivation behind the evolution of IOT, its architecture, and applications.

Keywords— Internet of Things,RFID, Security, Wireless Sensors, World.

I INTRODUCTION

IOT represents a system in which real life objects are connected to their corresponding sensors and this system is in turn connected to the internet through wireless or wired connections. IOT is the concept that bridges the gap between day to day object, sensors, software and network connectivity. The gap is bridged by the collection and exchange of data. This feature allows the objects to be remotely controlled in a network framework. This, in turn, helps in bringing the real and electronic world closer.

The sensors used in this use a variety of LAN connections, for instance, RFID, Bluetooth, Zigbee, NFC, and Wi-Fi. The sensors are basically used for data collection purposes. As the world has moved from IPV4 to IPV6, hence it allows generating communication addresses for billions of devices. An Evenadvanced version of internet protocol IPV6 can arrange more addresses than atoms onthesurface oftheearth. Nowadays Wi-Fi and cellular wireless connectivity have become quite common hence this target of connecting the "animate" and "inanimate" has become easier. Before connecting everything up, we need to define the problem. This means that we need to get a clear idea in our mind that what "information learning" is to be done from the installed sensors [1]. After that, we build an IOT network by first laying its security foundations. Since IOT finds applications in a variety of domains hence the categories of vendors allotted for it also varies. But the fact still remains that there is no single vendor that has the capability to offer complete integrated solutions to this problem. IOT finds its applications in numerous domains, for example, healthcare, transportation etc.

IOT in general depicted as the internet and wireless sensors combination services which create unique things and this create a resultant utility. This utility not to be caught only visualizes if work on the aim of phenomenal aspects. The same aim can be visualized in Fig: 1. this visualization generates utility nodes at the rate oftheinfinite count.

The basic concept of IOT can be understood from Fig: 1. the internet and wireless sensors form the core of the method. They constitute millions of nodes. The computing utility nodes form the middle layer between the sensors and the physical devices. These utility nodes are billions in number. The physical devices/objects/appliances from the outermost layer that consist of trillion of nodes. These numbers of nodes are increasing day by day.

978-9-3805-4421-2/16/$31.00

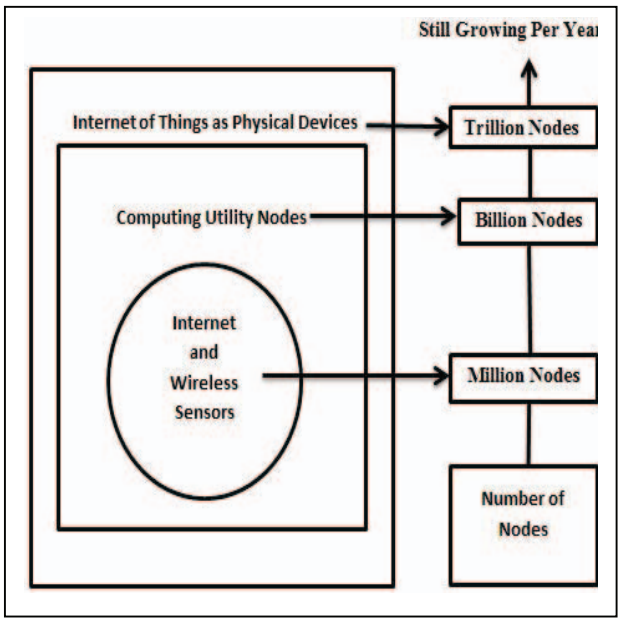

Fig: 1Visualization of IOT

The basic concept of IOT can be understood from this diagram. The internet and wireless sensors form the core of the method. They constitute millions of nodes. The computing utility nodes form the middle layer between the sensors and the physical devices. These utility nodes are billions in number and the physical devices, objects or appliances from the outermost layer that consists of trillion of nodes. These numbers of nodes are increasing day by day.

The rest of paper structured as section II describes the IOT recent scenario through which we can easily and directly depict the respected authors view regarding IOT. Section III describes the layered architecture of IOT. Section IV describes the how IOT actually works. Section V states the proposed general classification of security for IOT. In section VI, we conclude our study and provide appropriate future work.

II IOT LITERATURE SURVEY

TABLE I. PREVIOUS WORK DONE

S.no	*Proposals/Findings*
1.	In 2010, Y. Huang and G. Li provided an overview of the concept of "IOT". According to him, IOT is a new technology in which things and information are interconnected to each other throughtheinternet. He explained how IOT is an application of the semantic web [2].
2.	In 2010, L Tan and N. Wangexplainedthe basic meaning of "IOT". The communication ontheinternet is between two persons but in IOT, the communication will be "human and things" and "things and things". Hence, things will be creating the traffic. IOT will help in connecting various things at a time at any place [3].
3.	In 2011, L. Coetzee and J. Eksteenintroduced the concept of "IOT". Now a day's internet is very important for organizations, institutions etc. and is used by computers and humans. Hence by the emergence of IOT, the internet will further be used by things [4].
4.	In 2011, G. Gang, L. Zeyong and J. Jun stated that IOT is the future of upcoming IT industry. The function of IOT is to serve the different characteristics of things. The upcoming projects of IOT are a part of the small scale businesses that helpinraising the development standards of IOT. The paper is concerned with the application of IOT in a nation and to analyze the security risks prevailing in it [5].
5.	In 2012, Z. Yu and W.T. Ningillustrated the concept in which IOT offers to develop the equipment support in an interacting manner. This technology would help in reducing the expenses of the equipment support system. If once the equipment's are strengthened the army's battling capacities can also be improved [6].
6.	In 2013,K. Zhao and L. Ge focused on the issues related to the security of IOT that is actually based on the application of the system which is part of the IOT.This paper deals with the various security issues of IOT that are prevailing in the structure of the system. This paper also deals with the techniques of management of keys, protocols of security,thetechnology of data fusion, as well as on the authentication and access control [7].
7.	In 2013, X. Xingmei, Z. Jing and W. He reviewed about the popularity that IOT gained in the recent years which actually grabbed the attention of the scholars and experts from remote areas of the world as well as from several government sub-divisions. The author of this paper focuses on the various key technologies, the network architecture, problems related to security issues and fundamental characteristics of IOT such as RFID technology, sensor technology, network communication technology etc. The paper also provided a solution which would transform the information industry [8].
8.	In 2014,Y. Zhang, W. Zou, C. Yang and J. Caopresented the concept of "Power Internet of Things" (PIOT). The security considerations, including the policies and framework, are provided. This study is crucial from the architectural point of view. The paper also proposes a security framework considering both the perception and application layer [9].
9.	In 2015, Md. M. Hossain, M. Fotouhi and R. Hasan talked about the various IOT devices that are popular in different areas like health, Home, Commerce, trafficking etc. With the rise intheclassification of IOT devices in the real scenarios, in many cases, these are subjected to malevolent attacks that sacrificethe security mechanism of the IOT.The aim of this paper is to bridge the gap by detailed study of security tasks and problems. This paper presented a descriptive study of IOT attacks, threat forms, security issues, rhetoric and call out [10].
10.	In 2015, C. W. Axlrod stated the security in the IOT according to the 'Why' and 'What' of the system. The privacy and safety of IOT were explained but the 'How' of the system was missing. There are several reasons that why security in IOT is still an issue.In order to get an effective constraint on the set of characteristics, the author observed the implementation cost of IOT's safety, security and privacy and also about the frugal after come if not succeed. The author explored the various business, professional and government forms and patterns to achieve security in IOT. The author suggested a form that guaranteesasecure environment of IOT [11].

III LAYERED ARCHITECTURE OF IOT

IOT is a process of linkingaday to day objects like mobile, home and embedded applications to the internet in order to facilitate greater communication and computing capabilities. This makes use of data analytics to extract some meaningful information from the connected devices, making it an intelligent system of systems. This process can be easily stated by Layered architecture [12]. A layered architecture also implies that a team can individually work on various components of the system simultaneously. This means that various components of the system can be deployed independently. As shown in Fig: 2layered architecture of IOT. Layered architecture is essential for any system because it increases the scalability of the framework.

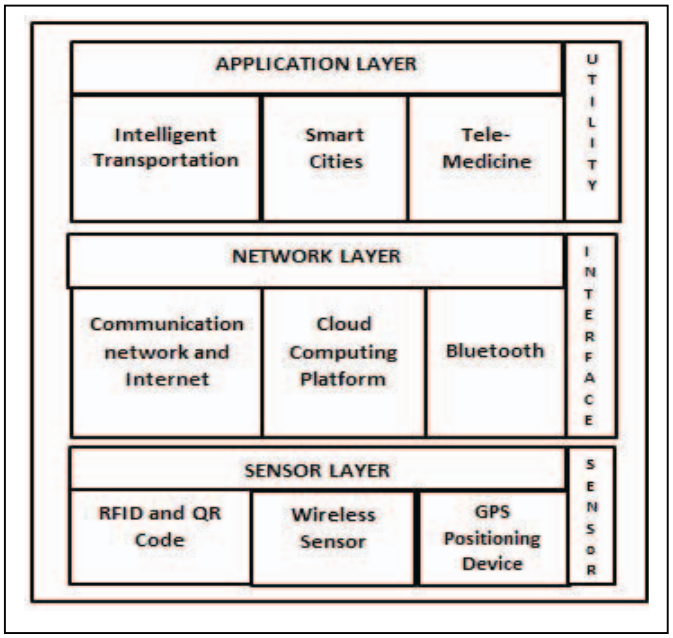

Fig: 2 Layered Architecture of IOT

Fig: 2 show the basic layered architecture of IOT which has three basic functioning layers. These layers coordinate with each other so as to provide the necessary outputs. These layers consist of the basic components of utilities, interfaces, and sensors.

A. Application Layer:

For the three-tier architecture of IOT, we have utilities positioned at the first layer. By utility, we mean the end products that are delivered with the help of IOT. The most common utilities are described as follows:

1) *INTELLIGENT TRANSPORT SYSTEM (ITS):*
It may be the best-taken example for these utilities. Congestion, pollution, and road accidents are the biggest faced problems of traffic system in this era. Intelligent transport system offers solutions to address these problems. Satellite navigation, electronic tolling, traffic and travel information systems, digital message signs are all active components of intelligent traffic systems.
"ITS" coordinates with the transport facilities by analyzing the "travel data" and by making more accurate decisions, every time it starts does so. It also improves the traffic management at transport corridors. It enhances the communication between the vehicles and the road network. It works by integrating each and every type of data related to any issue regarding transport. The intelligent transport system is also improving the road safety and security [5].

2) *SMART CITIES:*
Talking about smart cities, we can say that "what we can imagine for our purpose can be an element of our smart city." Here each and every device an element has some sort of connectivity to others of their types so that they can communicate effectively, and this is the key to smart city concept. Collected data from several resources, processed by different heterogeneous devices and element for effective extraction of useful information from them.
Smart cities are really going to change the way we are living. Either in terms of sustainability or efficiency, smart cities are better in every way. It can be a solution for sustainable electricity, sustainable environment or even for the time-saving methodologies. This is the fact that smart cities are not the concept that is only going to improve the lifestyle forahuman being, but they are the life changes for the society [8].

3) *TELEMEDICINE:*
It may be a key tothesuccess of IOT. In the present scenario, there still exist cases where we can't provide medical facilities due to several reasons. Considering these cases telemedicine is a great invention and is going to help a lot of people out there.
In telemedicine, the patient can send its live data related to his health issues directly via network channels to some concerned person and can get prompt and effective advice and medication. There are several cases when there is some constraint on timed for proper medication. In those cases telemedicine will remove the barrier of time and will provide prompt care [9].

B. Network Layer:

In the second layer of IOT, we consider media and communication channels. These channels are actually the backbone of any system. Any data or information goes through forth these channels. These channels contain several communication protocol suits and standards. The most common interfaces are described as follows:

1) *Communication network and The Internet:*
The Internet is a widespread system ofinterconnected computer networks which links billions of devices together. The Internet has been a life changer and aims at establishing numerous communications networks and channels to implement the concept of IOT [4].

2) *Bluetooth:*

This set contains data transfer standard for Bluetooth. Components like Bluetooth are categorized as mobile units and can easily convey the data information. They don't have compatibility issues in general [7].

3) *Cloud computing platforms:*
Considering the cloud computing platform one can assume a large repository of data and information on a day to day basis. This can be a channel for other devices to store and fetch information. Devices can then perform analysis on that data and information for meaningful information or results. The concept of IOT is integrating these all protocols, standards and devices in the number of trillions just to make things convenient, clear and easily accessible for everyone.

C. *Sensor Layer:*

IOT contains sensors and different data acquisition devices at its third layer. Sensors and devices for data acquisition are the key elements for integrating things. The most important thing in terms of processing and integrating things is data. Data is the most crucial term. These elements help a system to get data from various remote and connected locations. Processing and prompt action can only be done once we have the data. The sensors collect data from various sources. We can take an example of intelligent transport system utility [6]. There are several sensors and devices which are working on live locations to trace the data related to transportation. The traffic camera may be catching the whole scenario a feeding it to the transport headquarters. The most common sensors are described as follows:

1) *RFID and Quick response (QR) code:*
Talking about more mobile and complex type of sensors we can have RFID and the QR codes. These RFID'S can sense a specific frequency and make a signal totheconcerned unit [7].

2) *GPS (Global Positioning System):*
It is a well-structured example of the elements that guides the path / location layout with the help of over 26 satellites covering the whole planet [2].

3) *Wireless Sensors:*
They are the standard tools that are used for measurement purposes and are combined with transmitters in order to convert the signals received into a compatible mode for radio transmission. These signals are then interpreted by the user to get his desired output [1].

IV MECHANISM OF IOT

The overall mechanism of IOT can be understood with the help of Fig: 3.The object which has to be connected to our IOT system is analyzed to extract the object credentials. These credentials are then used to assign the RFID labels which are in turn connected to the internet [13]. The users can then remotely access these objects from anywhere around the world.

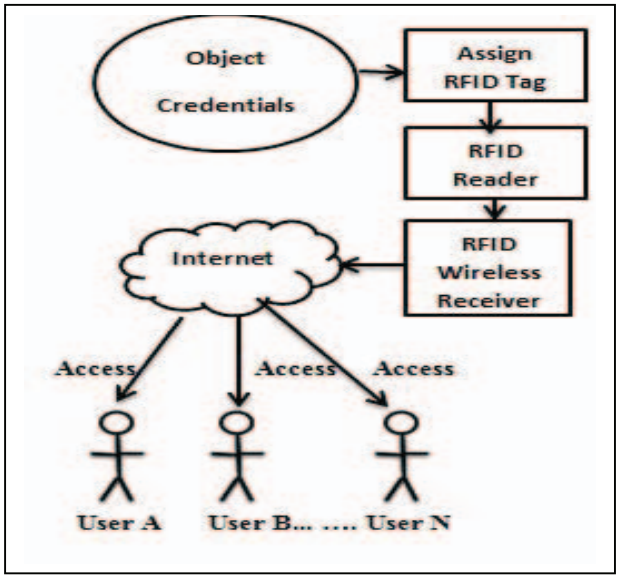

Fig: 3 Mechanism of IOT

RFID is the backbone of IOT architecture. It is a wireless technique of using the electromagnetic waves to transmit data for the automatic identification and tracking of the objects / things that are attached to that data. The tags or labels that are created consists of digitized characteristic information of the object.

Major applications of RFID tags include:

a) Access and location tracking system
b) Systems for tracking of goods
c) Collection of toll taxes at various remote locations
d) Object authorization
e) Object authentication

RFID offers various advantages as compared to the traditional bar code systems. For instance, it does not need to user to be in the LOS (Line Of Sight) of the tag. The tag is usually embedded in the object under consideration. It can easily be read even if the object resides in an opaque container. Hence, they can be considered as a method to implement "automated data capture as well as data identification".

RFID plays an important role in various industries. For instance, if we generate a tag for a car at the production stage then we can check its progress in the upcoming assembly line stages in the vehicular industry.

RFID Tags can be attached to objects such as:

a) Automobiles
b) Media playing appliances
c) Fridge
d) Microwave ovens
e) Heating appliances
f) Mobile phones

g) Computing devices

The object tags and labels could be active, passive or "battery assisted passive" in nature. The passive tags are generally low in cost because unlike their active counterparts, they do not have batteries attached to them.

V PROPOSED TAXONOMY FOR SECURITY ASPECTS OF IOT

The dimension of security is very crucial in any computing environment. The data needs to be secured from the unauthorized and unauthenticated users [14]. Individuals and organizations expect that their personal data which resides on the IOT products or systems should remain safe from unauthorized modification and should be available to them. The three major concerns of security are in maintaining for these needs are Data Confidentiality, Data integrity, and Data availability. In the target to achieve highly secure environment and ensuring to overcome these phenomenal loopholes of security in IOT. We proposed classified security aspects of IOT as shown in Fig: 4.

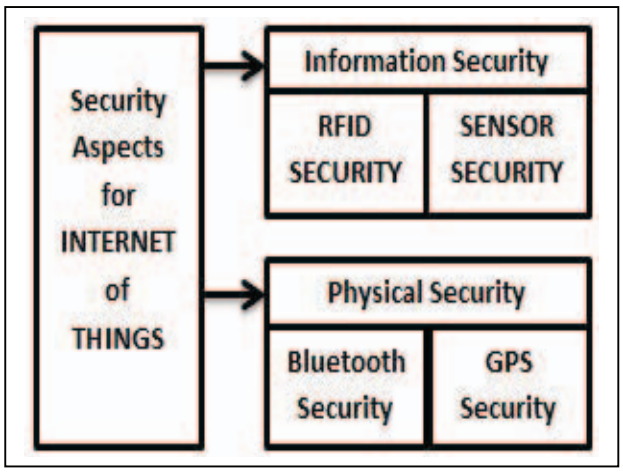

Fig: 4 Proposed Taxonomy for security aspects of IOT

As shown in Fig: 4, the security of IOT can be seen in terms of both information and physical device security. The information security component of IOT is concerned with RFID and sensor's security. On the other hand, physical security components deal with Bluetooth and GPS security.

A. Information Security

Information security refers to the practice of protecting our digital information from malicious users. This means that we aim at protecting our data from being disclosed, modified or destructed in any form [15] [16].

1) RFID Security:

The concept of RFID technology is exponentially growing across various industries. The corresponding security issues needaconsiderable amount of attention. It is a well-known fact that the RFID tags have numerous variants so we just cannot find a generic solution to RFID security issues. Some of the basic tags are not capable of executing cryptographic measures such as hashing, random number generation, encryption etc. Although these functions can be performed using some "high on cost" tags. These tags are also capable of performing symmetric encryption. Hence, the industries need to initially define their budget and then find the solution to their concerned security issues. However other measures are also possible regarding the security of the tagged data. This includes password protection as well. The tagged memory can also be physically locked.

2) Sensor Security:

The sensor attacks are generally initiated by the insertion of incorrect and malicious information by the constituent nodes of the network. Hence, we need to determine a way to detect these incorrect reports. But this, in turn, is an extensive research topic. Most of the models that are created forthesecurity of wireless sensors utilize the concept of the current network models. Also, the implementation of public key cryptography methods can enhance the security levels of the wireless sensors [17].

B. Physical Security

Physical security of IOT basically aims at improving Bluetooth and GPS security. Both these aspects are crucial for the development of IOT infrastructure as they form the backbone of the physical layer of the traditional IOT architecture [4].

1) Bluetooth Security:

Bluetooth is a "low on power" kind of short-range communication technology that is used in most of the today's generation handheld devices. Since they aim at implementing wireless networks, hence they also have certain vulnerabilities associated with them which may lead them to connect even to the unauthorized devices.Bluetooth technology lacks centralized administration and hence it faces some serious security issues. The Bluetooth specification is usually very complex in nature. Some of the tips that are to be kept in mind for implementing security in Bluetooth devices is:

a) Patch your Bluetooth device on a regular basis.
b) Use Bluetooth devices only when they are needed and not otherwise
c) Try to use the devices that support Class 2 / Class 3 Bluetooth transceivers
d) Keep both the connecting devices close to each other
e) Make your device universally discoverable only if it is required to do so
f) Try to use device firewalls
g) Try to implement 128-bit Bluetooth encryption when connection is made
h) Use sufficiently long pass keys

2) GPS Security:

GPS security has become essential when it comes to implementing IOT. The GPS security systems play a significant role in it. Usually, they work by using the tracker's GPS chip which is used to determine the location and connect to communicating satellites [18].

VI CONCLUSION

In this paper, we have discussed some of the basic notions of IOT. We have discussed in detail about the mechanism and layered architecture of IOT. We have proposedataxonomyof the security aspects of IOT. This taxonomy helps us to examine the various security considerations of IOT. This includes physical and information security. While the physical security deals with the Bluetooth and GPS security, on the other hand, information security handles the RFID and wireless sensor security. The security of the wireless sensors can be improved by applying various public key cryptography methods. Bluetooth security needs to focus on patching, device firewalls and the usage of long pass keys. We have concluded that RFID forms the backbone of the concept of IOT and hence its security is very crucial for the development of the IOT framework. The RFID tagged memory can also be physically locked to improve security.

IOT future is very bright and broad as our study depicted and in the near future much more intelligent sensors connect totheinternet and deliver smart utilities. No doubt there are many more technical concerns which need to be addressed to achieveahighly secure environment for IOT. So inthesecurityfield, there is a long way to making a real global field for IOT. After that, the IOT will serve more benefit to abroad category of people.

REFERENCES

[1] J.Gubbi, R.Buvya, S. Marusic and M. Palaniswami, "Internet of things: A vision, architectural elements, and future directions," in Elsevier, 2013, pp. 1645-1660.

[2] Y. Huang and G. Li, "A semantic analysis for Internet of things," in an international conference on intelligent computation technology and automation, IEEE,2010, pp. 336-339.

[3] L.Tan and N. Wang, "Future internet: the internet of things," in a 3rd international conference on advanced computer theory and engineering, IEEE, vol. V, 2010, pp. 376-380.

[4] L. Coetzee and J. Eksteen, "The internet of things-promise for the future? An introduction," in IST- Africa conference proceedings,2011.

[5] G. Gang, L. Zeyong and J. Jun, "Internet of things security analysis," in IEEE, 2011.

[6] Z. Yu and W.T. Ning, "Research on the visualization of equipment support based on the technology of internet of things," in IEEE, 2012, pp. 1352-1357.

[7] K. Zhao and L. Ge, "A survey on the internet of things security," in IEEE,2013, pp. 663-667.

[8] X. Xingmei, Z. Jing and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things," in a 3rd international conference on computer science and network technology, IEEE, 2013, pp. 825-828.

[9] Y. Zhang, W. Zou, C. Yang and J. Cao, "The security for power internet of things: framework, policies, and countermeasures," in an international conference on cyber- enabled distributed computing and knowledge discovery, in IEEE,2014, pp. 139-142.

[10] Md. M. Hossain, M. Fotouhi and R. Hasan, "Towards an analysis of security issues, challenges,and open problems in the internet of things," in IEEE world congress on services, 2015, pp. 21-28.

[11] C. W. Axlrod, "Enforcing security, safety and privacy for the internet of things," in systems, applications and technology conference (LISAT), IEEE, 2015.

[12] L. Atzori, A. Iera and G. Morabito, "The internet of things: a survey," in Elsevier,2010, pp. 2787-2805.

[13] A. W. Burange and H. D. Misalkar, "Review of the internet of things in the development of smart cities with data management and privacy," in an international conference on advances in computer engineering and application,IEEE,2015, pp. 189-195.

[14] R. H. Weber, "internet of things- new security and privacy challenges," in Elsevier, 2010, pp. 23-30.

[15] M. H. Asghar, N. Mohammadzadeh and A. negi, "Principal application and vision in the internet of things (IOT)," in an international conference on computing, communication, and automation, IEEE, 2015, pp. 427-431.

[16] Moghaddam, F. F., Alrashdan, M. T., & Karimi, O. (2013). A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments. *Journal of Advances in Computer Networks*, *1*(3), 238-241.

[17] M. Khar, & G. Shrivastava., (2011). Public Key Infrastructure and Trust of Web Based Knowledge Discovery. *International Journal of Computer Science and Security (IJCSS)*, *5*(3).

[18] M. Khari, M. Kumar, Vaishali., "Comprehensive Study of Cloud Computing and Related Security Issues" Computer Society of India (CSI), 50th Golden Jubilee Annual Convention, Springer, New Delhi, 2-5 Dec., 2015.