ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

A STUDY ON SECURITY ISSUES AND CHALLENGES IN IoT

A.Vithya Vijayalakshmi*[1], Dr. L. Arockiam[2]
[1]Ph.D. Scholar, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli – 2.
[2]Associate Professor, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli – 2.

Keywords: *Internet of Things, IoT architecture, Key Technologies, Security issues of IoT.*

ABSTRACT
The Internet of Things (IoT) is a modern paradigm, with emerging modern wireless communications. The technologies such as RFID sensors and wireless sensors network offered by the IoT make possible of device communication with each other or with human. With the great potential of IoT, there comes all kind of challenges. This paper provides an overview of IoT, IoT architecture, key technologies in IoT and application scenarios of IoT. Various security issues and challenges in the IoT environment are also discussed and presented.

INTRODUCTION
Now-a-days our society is moving towards the "always connected" system. The rapid growth of advanced technologies has changed the life style of human beings, mainly the recent and most popular "Internet of Things" (IoT). It is a rapidly emerging paradigm where variety of objects get connected in such a way that they can interact over the Internet. The Internet of Things research and innovations team defines IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities use intelligent interfaces and are seamlessly integrated into the information network" [30]. The Internet of Things (IoT) completely transforms connectivity from "anytime", "anywhere" for "anyone" into "anytime", anywhere" for "anything" [5]. The goal of IoT may be to form a smart city, provide smart healthcare, offer smart transportation etc. There are many possible application areas for IoT. With the rapid growth of the IoT applications, several security and privacy issues are observed [21].

1.1 IoT ARCHITECTURE
The IoT environment should be capable of interconnecting large number of heterogeneous objects through the Internet. So, there is a need for elastic and adjustable layered architecture. The general IoT architecture is divided into three layers such as Perception layer, Network Layer and Application layer. Figure.1 shows the three-layer IoT architecture.

Perception Layer
This layer collects information through the sensing devices such as RFID, Zigbee and all kinds of sensors. Radio Frequency Identification (RFID) technology enables the design of microchips for wireless data communication and helps in automatic identification of anything they are attached to, acting as an electronic barcode [22]. The collected data are transmitted only through wireless network transmission (WSN). Some common attacks that occur in this layer are: Node capture, Fake node or malicious data, Denial of Service attack, Reply attack etc. [4].

Network Layer
This layer supports secure data transfer over the sensor networks and responsible for routing. It transfers the information through wireless technology such as Wi-Fi, Bluetooth, and Infrared etc. [23]. Hence, this layer is mainly responsible for transferring the information from perception layer to upper layer. There are some common security problems in LAN, Wi-Fi, and Internet. They are: illegal access network, eavesdropping information, confidentiality and integrity damage, DoS attack, Man-in-the-middle attack etc.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Application Layer

This layer is the topmost layer of the IoT architecture that provides the delivery of all services in various fields. It includes cloud computing, intelligent transportation, environmental monitoring etc. Application layer has some security problems such as data security, cloud platform security, data protection and recovery etc. To solve the security problems of this layer, authentication and privacy protection are needed. Particularly, password management is very important for data security [1].

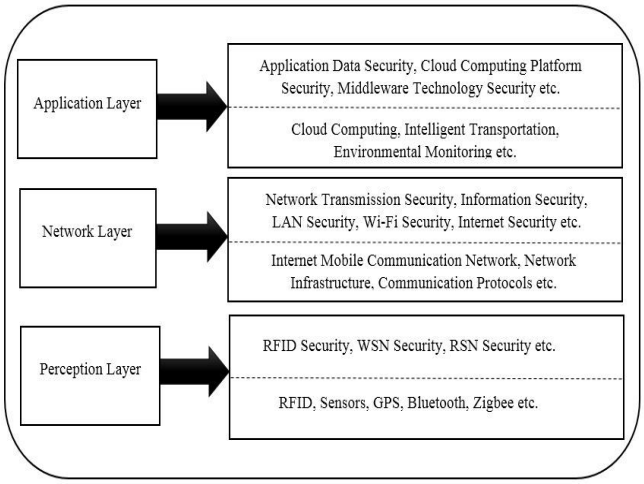

Figure 1: Three-layer IoT Architecture

1.2 KEY TECHNOLOGIES IN IoT

Identification, sensing and communication technologies

Identification methods are electronic product code (EPC) and ubiquitous code (uCode). In IoT, objects' address refers to the address within a communication network that includes IPv6 and IPv4. RFID technology is the main factor in the embedded communication technology [28]. It can be used to monitor objects in real-time, without the need of being in line-of-sight. This is helpful for mapping the real world into the virtual world [25]. Sensing refers to gathering of the data from IoT objects within the same network and sending it to the database or cloud. Objects can interact with the physical environment either passively or actively (performing sensing operations or performing actions) [27]. The IoT sensors can be smart sensors, actuators or wearable sensing devices [24]. IoT communication technologies connect heterogeneous objects together to deliver specific smart services. The communication protocols used by IoT are Bluetooth, Wi-Fi etc.

Middleware

In IoT, middleware is a software layer or a set of sub-layers interposed between the technological and the application levels. It is also named as IoT transaction basis middleware [25]. Embedded middleware are modules and operating environments which support different communication protocols [10]. It is responsible for providing services to the customers, besides ensuring interoperability, scalability and abstraction. Also, it authenticates the user to provide more secure environment along with efficient delivery of services [23].

Zigbee Technology

ZigBee is a wireless network protocol formulated by ZigBee Alliance. It is a two-way wireless access technology of close distance, low power consumption, low data rate, low complexity and low-cost. It is mainly suitable for automatic control and remote monitoring. ZigBee is highly reliable wireless data transmission network, which is similar to CDMA and GSM networks. ZigBee data transmission module is similar to the mobile network base station. ZigBee technology constitutes wireless data transmission network platform up to

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

65000 wireless data transmission modules [26]. ZigBee is widely used in home automation, digital agriculture, industrial controls, and medical monitoring [29].

Cloud Computing

Cloud computing is the integrated product of traditional computer technology and network technology, such as grid computing, distributed computing, parallel computing and utility computing etc. [26]. In Internet of Things, there is a large scale, massive amount of data need to be processed. So the data processing capacity is in high demand. The data collected by IoT devices are stored in the cloud environment. Integrated IoT and cloud computing applications enable the creation of smart environments such as smart cities, smart home etc.

1.3 APPLICATIONS OF IoT

The following table lists some of the IoT applications:

Table 1: Applications of IoT [23] [25]

FIELD OF APPLICATION	EXAMPLES OF APPLICATION
E-Health	Patient monitoring, Doctor tracking, Personnel tracking, Real-time patient health status monitoring, Predictive expertise information to assist doctors and practioners.
Retail & Logistics	Supply Chain Control, Intelligent Shopping Applications, Smart Product Management, Item Tracking, Fleet Tracking.
Smart Transportation	Smart transportation through real-time dynamic on-demand traffic information and shortest-time travel path optimization.
Smart Environment	Comfortable Homes/Offices, Industrial Plants, Smart Museum and Gym
Energy Conservation	Smart Devices, Smart Grid
Smart Home	Energy use, Water Use, Remote Control Applications, Intrusion Detection System.
Environmental Monitoring	Air Pollution, Noise Monitoring, Waterways, Industry Monitoring.
Green Agriculture	Green Houses, Compost, Irrigation Management, Soil Moisture Management
Futuristic	Robot Taxi, City Information Model, Enhanced Game Room

REVIEW OF LITRERATURE

Hui Suo et al. [1] reviewed the research progress of IoT and discussed the security issues. Detailed discussion on security architecture, security features, security requirements in each level of IoT was made. Various issues viz. authentication, privacy, multi-party computation, DDoS, encryption, key agreement in the IoT layers namely perception layer, network layer, support layer and application layer were discussed. An exploration on the research status of IoT was made. Eventually, several key challenges in IoT were also summarized.

Chen Qiang et al. [2] discussed various security issues such as RFID tag security, wireless security, transmission security, privacy protection and information security. Existing researches on network security were investigated. Based on that, a new security method for IoT was provided. The difficulty in processing massive amount of IoT data and ensuring security and reliability of the data was highlighted. The need to solve security issues to avoid a big security risk on the application of IoT was also stressed.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Security problems in each layer of IoT were analyzed by Qi Jing et al. [3]. The cross layer heterogeneous integration and security issues were discussed in detail. The comparative analysis of security issues in IoT and the traditional network was done. Also, various open security issues of IoT were deliberated. Security issues of RFID technology, WSN technology, RSN technology were discussed and the corresponding solutions were offered. The features of the given solutions were analyzed using the technology involved. Finally, an overall security architecture for IoT system was given.

Kai Zhao et al. [4] discussed several security issues of IOT that exist in the three-layer system structure and also offered solutions to the security problems in each layer. The common attacks such as node capture, false node and malicious data, denial of service, timing attack, routing threats and replay attack in perception layer were elaborated. Cryptographic algorithms and key management techniques were deployed to solve these attacks. The compatibility and cluster security problems were resolved using WPK1, PK1 and key agreement mechanism. The common security problems such as data access permission, identity authentication, data privacy, and software vulnerabilities etc. in the application layer were also discussed.

The architecture, protocols and security issues of IOT were discussed by Surapon Kraijak et al. [5]. The evolution of IoT in day today life, widely used protocols security and privacy issues in IoT applications were explained. Using Arduino device, the implementation of IoT system was done. The future trends of IoT were also clearly shown. The generic IoT architecture was divided into five layers namely perception layer, network layer, middleware layer, application layer and business layer and the functions of each layer were described. The tradeoff between the security and permission policies were also discussed

Mahmud Hossain et al. [6] explored security challenges and open problems in IoT. The need for a systematic study of the security challenges in IoT was propounded. A detailed analysis of IoT security challenges was done to bridge the gap in the existing scenario. A series of open problems in IoT security and privacy was provided. An overview of IoT architecture and interoperability between interconnected networks, the critical security problems and the mitigation methods in IoT were presented. Five major components of IoT ecosystem viz. IoT devices, coordinator, sensor bridge, IoT services and controller were examined to understand IoT security issues.

Gupreet Singh Matharu et al. [7] described the general layer architecture and briefed several challenges in IoT such as robustness in connectivity, interoperability and standardization, naming and identity management, safety and security of objects, data confidentiality and encryption. Security issues related to all the four layers of the IoT architecture were discussed, analyzed and determined. Finally, the strategies for solving security issues were suggested.

Omar Said et al. [8] discussed the research challenges and open problems related to the Internet of things. The concept of IoT database was introduced and IoT database architecture was suggested. The six layers namely IoT layer, data collection layer, data warehousing layer, event processing layer, data mining service layer and application layer of IoT database model and their functions were discussed and demonstrated. The future vision of IoT was also discussed. The two IoT architectures viz. three layer architecture, five layer architecture and other special purposes architecture were presented. Numerous challenges and open problems in IoT were discussed.

The various enabling technologies in IOT and also the major issues faced by the researchers were discussed by Eleonora Borgia [9]. The enabling technologies such as identification, sensing and communication technologies were elaborated. Various attacks in IoT were clearly explained. The key features and the driving technologies of IoT were presented. The research challenges and the open issues in the IoT application scenarios were identified. The fundamental characteristics of IoT were defined and the IoT technologies were described.

Xu Xiaohui [10] elaborated the basic concepts, the security issues and key technologies in IOT. The evolution of IoT was divided into three stages: information perception, intelligence material and intellectual interaction. Security issues related to perception layer and the key technologies involved were discussed. Various security problems in sensor networks such as counterfeit attacks, malicious code attacks were highlighted. Certification

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

and access control are the two key technologies used to ensure secure communication between objects. The need to make IoT network into an open, secure, trusted network was propounded.

Jorge Granjal et al. [11] discussed various security issues in IoT and also surveyed existing protocols. Existing protocols were analyzed to offer security in communications between IoT devices. Several existings protocols were explored to enable security in physical (PHY), Medium Access Control (MAC) layers low-energy communications, network layer, routing, and application layer with CoAP. Possible ways to offer novel security mechanisms were provided based on security requirements.

Raja Benabdessalem et al. [12] explored different methods to address security and privacy issues. The security requirements viz. confidentiality, authentication, integrity, authorization, non-repudiation and availability in IoT were analyzed to ensure privacy, data protection and security. Discussion on various kinds of threats such as eavesdropping and denial-of-service attacks was made. Several cryptographic algorithms were scrutinized to ensure secure data communication between IoT devices.

Ahmad W. Atamli et al. [13] discussed IoT features and the three major entities viz. Malicious User, Bad Manufacturer, External Adversary that pose risks to the security and privacy in IoT . Various attacks were analyzed and security concerns for each IoT device actuators, sensors, RFID tags and network NFC were discussed. The need to build a novel security framework for IoT was propounded. The security properties namely tamper resistant, protected storage and access control, data exchange, identification and authentication and availability needed to ensure confidentiality and integrity of the system as well as privacy properties to prevent revealing information about users, devices were emphasized.

Rwan Mahmoud et al. [14] analyzed general security issues of internet of things and also security issues specific to each layer. Two types of issues namely technological and security issues were explored. Technological issues in wireless technologies to ensure scalability and consume low energy were stated. Security challenges such as confidentiality, authentication, integrity etc were specified. Attacks in perception layer such as replay attack, timing and node capture attack and also attacks in network layer such as man-in-the-middle attack were reconnoitered.

Emmanouil Vasilomanolaki et al. [15] discussed four different IoT architectures and analyzed security and privacy components and its requirements. The traditional systems were examined and the distinguished properties such as uncontrolled environment, heterogeneity, scalability and controlled resources were identified. The security and privacy requirements such as network security, identity management, privacy, trust and resilience for each compound were listed and four different IoT architectures proposed by various authors were compared. Finally, security needs of each architecture and the strength and weakness of the four most dominant IoT architectures were described.

Zhi-Kai Zhang et al. [16] discussed ongoing research on internet of things such as authentication and authorization of IoT, privacy in IoT, malware in IoT etc. and mainly focused on security issues in IoT. The major security issues namely object identification issue in IoT to ensure the integrity of the records; authentication and authorization to certify the user to use the IoT objects were highlighted. The need to preserve the privacy of collected data through data anonymization was stressed. Lightweight cryptosystems and malwares in IoT were also explored.

DU Jiang et al. [17] offered three ways to analyze the existing information security of Internet of things M2M. Possible security threats in M2M's structure, which consists of front-end sensors and equipment, networks, back-end IT systems were explored. Eight major standards such as access control, privacy protection, user authentication, no arrived patience, data confidentiality, communication layer security, data integrity, and availability at any time needed to ensure security in IoT systems were described. The privacy and credibility (data integrity and confidentiality) issues of the internet of things system were examined.

Subho Shankar Basu et al. [18] discussed security issues and design challenges such as heterogeneity, connectivity, mobility, addressing and identification, spatio-temporal services, resource constraints, data

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

interchange, resource and service discovery related to IoT applications. The threats such as spoofing, tampering, repudiation, information leakage, DoS, user privacy and replay attacks were also described. An effective security framework was proposed to prevent threats.

Glenn A.Fink et al. [19] discussed various kinds of vulnerabilities in IoT and also societal effects of IoT such as standards and privacy and security. Discussion on the security system related to crime, cyber welfare, emergent behavior, scientific and technology challenges, social and regulatory challenges etc. was made. Various kinds of vulnerabilities were discussed and techniques to mitigate such vulnerabilities were provided.

Sye Loong Keoh et al. [20] focused on communication security for IoT, specifically the standard security protocols. Four modes namely NoSec, PreShared Key, Raw Public Key and Certificate based on the configuration of IoT device were described. Deployment of DTLS which is considered as the main security suite for IoT was done to provide security functionalities to the IoT devices.

Table 2: Issues and Challenges in Internet of Things

AUTHOR	DESCRIPTION	ISSUES AND CHALLENGES
Hui Suo et al. [1]	Discussed Security in each layer: 1.Perception 2. Network 3. Support 4. Application	1. Power and storage 2. DDoS attack 3. Authentication and confidentiality 4. Privacy Protection
Chen Qiang et al. [2]	Discussed 1. RFID Tag information security 2. Wireless communication and Information security 3. Network Transmission of Information Security 4. Privacy Protection	1.RFID identification, communication channel, RFID reader security issues 2. Radio signals attack 3. Internet Information security 4. Private Information Security
Qi Jing et al. [3]	Explored 1. Security issues in RFID 2. Security issues in Wireless Sensor Network.	1. Uniform coding, conflict collision, privacy protection, trust management. 2. Limited resources including small amount of storage, poor calculation ability.
Kai Zhao et al. [4]	Explained security issues in each layer: 1.Perception layer security issues 2. Network layer issues 3. Application layer issues	1. Node capture, false node and malicious data, denial of service, timing attack, routing threats and replay attack. 2. Compatibility problems and cluster security problems. 3. Data access permission, identity authentication and data privacy.
Surapon Kraijak et al. [5]	Provided an overview of: 1. Security in Information transmission 2. Privacy Protection	1. Eavesdropping, denial of service attack. 2. Privacy in device and storage.
Mahmud Hossain et al. [6]	Discussed Security Constraints Limitations in: 1. Hardware 2. Software 3. Networks	1. Computational and energy constraint, Memory constraint. 2. Embedded software constraint, dynamic security patch. 3. Mobility, scalability, multiplicity of devices.
Gupreet Singh Matharu et al. [7]	Described 1. Interoperability and Standardization	1. IOT devices differ in technologies and services. 2. A unique identification for each object over internet.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

	2. Naming and Identity Management 3. Security of objects 4. Data confidentiality	3. Unauthorized person can cause physical alteration. 4. Secure transfer of the data
Omar Said et al. [8]	Explained 1. Security in Information gathering 2. Security and Privacy of information 3. Things Communication Problems	1. Gathered by RFID 2. Due to wireless transmission 3. Addressing of things & RFID problems in reading, writing and transmission of objects information.
Eleonora Borgia [9]	Explored Security in M2M communication, routing, end-to-end reliability, device management, data management and security of IoT data	Communication between IoT objects/ machines. IoT device management & Security of data while transmission and storage
Xu Xiaohui [10]	Discussed Wireless Sensor network security problems & Information transmission and processing security.	Counterfeit attacks, malicious code attacks.
Jorge Granjal et. al [11]	Discussed Security in IoT: 1. PHY and MAC layer communications 2. Network layer communications 3. Security in Routing 4. Application layer communications	1. Communications with IEEE Standards 2. Security in 6LoWPAN 3. Security in RPL 4. Security in CoAP
Raja Benabdessalem et al. [12]	Explored 1. Eavesdropping attack 2. Denial-of-service attack	1. Compromise the authenticity, integrity and confidentiality of personal data 2. Attackers send incessant requests to deplete their resources.
Ahmad W. Atamli et al. [13]	Provided an overview on 1. Threats 2. Attacks on system	1. Malicious user, Bad manufacturer & External adversary 2. Device tampering, Information Disclosure, Privacy Breach, Denial-of-service, spoofing & Elevation of Privilege.
Rwan Mahmoud et al. [14]	Discussed 1. Technological Challenges 2. Security Challenges	1. Wireless technologies, scalability, energy and distributed nature. 2. Authentication, confidentiality, integrity etc.
Emmanouil Vasilomanolaki et al. [15]	Discussed 1. Network Security 2. Identity Management 3. Privacy 4. Trust	1. Confidentiality, integrity, authenticity and availability. 2. Authentication, authorization, accountability and revocation 3. Data Privacy, anonymity, pseudonimity and unlink ability 4. Device trust, entity trust and data trust
Zhi-Kai Zhang et al. [16]	Explained	1. Ensure naming system cause man-in-the-middle attack

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

	1. Object Identification 2. Authentication and authorization 3. Privacy	2. Infeasible to issue a certificate to a object in IoT 3. Privacy in data collection and anonymization requires access control and cryptographic schemes
DU Jiang et al. [17]	Discussed Information security of IoT M2M	Security threats in: 1. Front-end sensor and equipment 2. Network 3. Back-end IT systems
Subho Shankar Basu et al. [18]	Discussed Security Challenges: Heterogeneity, Connectivity, Mobility, Addressing and Identification, Spatio-temporal services, Resource constraints, Data interchange, Resource and Service discovery	Threats in Security Challenges: Spoofing, Tampering, Repudiation, Information leakage, DoS, User Privacy, Replay Attack etc.
Glenn A.Fink et al. [19]	Described 1. Standardization 2. Privacy 3. Security	1. Protocols to be used 2. Data location privacy 3. Crime, cyber welfare, emergent behavior
Sye Loong Keoh et al. [20]	Discussed 1. Standardization 2. Communication Security	1. Interoperable Security 2. Datagram Layer Security

MOTIVATION

IoT has become one of the most significant elements of the future Internet with a huge impact on social life and business environments. IoT applications and services are unsecured in most of the application domains as discussed in Table 2. To secure IoT against those issues, a secured technology is needed in these application areas. More specifically, authentication, confidentiality and data integrity are the key problems of IoT security. The main motivation behind this survey is to provide a detailed study about the security issues and challenges in IoT.

CONCLUSION

IoT gives tremendous changes in the usages of Internet and also provides many number of research opportunities in real-world. Although a lot of research on IoT security issues has been carried out, still there is a need for more security solutions. This paper discusses various security issues and challenges. It is evident that there is no maximum protection in many IoT areas. To resolve these existing issues, more research should be done.

REFERENCES

1. *Hui Suoa, Jiafu Wana and Caifeng Zoua, Jianqi Liua, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, 2012, pp. 649-651.*
2. *Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, "Research on Security Issues on the Internet of Things", International Journal of Future Generation Communication and Networking, 2013, pp.1-9.*
3. *Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qui, "Security of the Internet of Things: perspectives and challenges", Springer, Wireless Networks, vol. 20, Iss.8, pp. 2481–2501.*
4. *Kai Zhao and Lina Ge, "A Survey on the Internet of Things Security", IEEE, International Conference on Computational Intelligence and Security, 2013, pp. 663-667.*
5. *Surapon Kraijak and Panwit Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends", Proceedings of ICCT, 2015, pg.26-31.*

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

6. *Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", IEEE World Congress on Services, 2015, pp. 21-28.*
7. *Gurpreet Singh Matharu,Priyanka Upadhyay and Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues", IEEE, International Conference on Emerging Technologies (ICET), 2014, pp.54-59.*
8. *Omar Said and Mehedi Masud, "Towards Internet of Things: Survey and Future Vision", International Journal of Computer Networks (IJCN), Vol.1, Iss.1, 2013, pp. 1-17.*
9. *Eleonora Borgia, "The Internet of Things vision: Key features, applications and open issues", Elsevier, Computer Communications, 2014, pg. 1–31.*
10. *Xu Xiaohui, "Study on Security Problems and Key Technologies of the Internet of Things", International Conference on computational and Information Sciences, 2013, pp. 407-410.*
11. *Jorge Granjal, Edmundo Monteiro and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communication Surveys and Tutorials, 2015, vol.17, no.3, pp. 1294 – 1312.*
12. *Raja Benabdessalem, Mohamed Hamdi and Tai-Hoon Kim, "A Survey on Security Models, Techniques, and Tools for the Internet of Things", International Conference on Advanced Software Engineering & Its Applications, 2014, pg. 44-48.*
13. *Ahmad W. Atamli and Andrew Martin, "Threat-based Security Analysis for the Internet of Things", International Workshop on Secure Internet of Things, 2014, pg. 35-43.*
14. *Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pg. 336-341.*
15. *Emmanouil Vasilomanolakis, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier and Panayotis Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems", International workshop on Secure Internet of Things, 2015, pg. 49–57.*
16. *Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen and Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities", IEEE International Conference on Service-Oriented Computing and Applications, 2014, pp.230-234.*
17. *DU Jiang and CHAO ShiWei, "A Study of Information Security for M2M of lOT", IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp.576-579.*
18. *Subho Shankar Basu, Somanath Tripathy and Atanu Roy Chowdhury,"Design challenges and Security issues in the Internet of Things", IEEE Region 10 symposium, 2015, pp. 90-93.*
19. *Glenn A. Fink, Dimitri V. Zarhitsky, Thomas E.Carroll and Ethan D.Farquhar, "Security and Privacy Grand Challenges for the Internet of Things", IEEE, 2015, pp.27-34.*
20. *Sye Loong Keoh, Sandeep S.Kumar and Hannes Tschofenig, "Securing the Internet of Things: A Standardization Perspective", IEEE Internet of Things Journal, 2014, pp.265-275.*
21. *Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things: Current Status and Open Issues", IEEE International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014, pp. 1-8.*
22. *Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT)" A Vision, architectural elements, and future directions", Elsevier, Future Generation Computer Systems, 2013, pp. 1645-1660.*
23. *Gurpreet Singh Mathuru, Priyanka Upadhyay and Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues", IEEE International Conference on Emerging Technologies (ICET), 2014, pp. 54-59.*
24. *Ala Al-Fuqaha, Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", IEEE Communications Surveys & Tutorials, 2015, vol.17, Iss. 4, pp. 2347-2376.*
25. *Luigi Atzori, Antonio Iera and Giacomo Morabito, "The Internet of Things: A survey", Elsevier Computer Networks, 2010, pp. 2787–2805.*
26. *Wang Rui1, Wang Jingu and Wang Na, "Analysis of key technologies in the Internet of things", International Conference on Material, Mechanical and Manufacturing Engineering (IC3ME), 2015, pp. 938-941.*

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

27. *Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: Vision, Applications and Research Challenges", Elsevier Ad Hoc Networks, 2012, pp.1497-1516.*
28. *Mohsen Hallaj Asghar, Nasibeh Mohammadzadeh and Atul Negi, "Principle Application and Vision in Internet of Things (IoT)", International Conference on Computing, Communication and Automation, 2015, pp. 427-431.*
29. *Xian-Yi Chen, Zhi-Gang and Jin, "Research on Key Technology and Applications for Internet of Things", Elsevier International Conference on Medical Physics and Biomedical Engineering, 2012, pp.561-566.*
30. *"Internet of Things – From Research and innovations to Market Deployment", River Publishers Series in Communication, Editors: Ovidiu Vermesan and Peter Friess, 2014.*