iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5356

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Internet of Things Security: Challenges and Opportunities

Dhananjay M. Kanade[1], Lalit A. Patil[2]
[1, 2]*Computer Engineering, KKWIEER, Nashik*

Abstract: ***Internet of Things (IoT) is the technology used to interconnect human, things and services which interact with each other as components of IoT system. In the next future, there are billions of IoT devices connecting to the Internet and this dynamically increasing number has focused attention on the IoT security. As an ongoing technology, IoT can be used in various fields, such as Mobile to Mobile (M2M) communication, Wireless Sensor Network (WSN), Radio Frequency Identification (RFID) and Supervisory Control And Data Acquisition (SCADA). It has been changing our world and the way we live and think. In IoT the large amount of data flows into the systems that demands a security architecture that ensures the protection of all layers of the system, including the communication channels and APIs used to integrate the applications and IoT devices. However, IoT has been lacking in security perspectives, there are different kinds of attack such as Physical attack, tag cloning, Sybil attack, sinkhole attack, denial of service attack, malicious code injection, man in middle attack, replay and redirect attacks, wormhole attacks and Data Transport Layer Security (DTLS) lacking. IoT devices are more vulnerable to attacks because it is simple and some security measures cannot be implemented. The paper analyses security challenges and opportunities in the IoT.***
Keywords: Internet of Things (IoT), Mobile to Mobile (M2M) communication, security challenges, security architecture, Wireless Sensor Network (WSN)

I. INTRODUCTION

The Device, the thing and object with regard to the IoT, thing is defined by ITU-T [1,5] an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks. Some other terms used by the research community are ‘smart objects’, ‘devices’, ‘nodes’. While the device by the ITU is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture data storage and data processing. More generally, the device from a technical view [2] is a set of electronic components with low computation capabilities, in addition to communication devices connected to the Internet or other types of network to interact with the real world not only with sensor nodes but also actuators.

As an emerging technology, Internet of Things (IoT) is defined as a network with everything that can connect to the Internet, such as light bulbs and temperature sensors. Gartner [3] says that here are more than 6 billion IoT devices connecting to the Internet and the number will be more than 26 billion. And the IoT industry will generate about 300 billion revenue by 2020. IoT technologies can be applied in different fields, such as agriculture, healthcare, manufacturing, energy, retailing and transportation. Therefore, IoT has been changing the world, the way we live and companies do business.

A. Some Interesting Definitions of IoT

The IoT is defined by Cluster of European Research Projects (CERP) [4], the Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. Definition by ITU-T [5] , the IoT is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

The IoT adds many dimensions like "Any THING communication" to the information and communication technologies which already provide "any TIME" and "any PLACE" communication. The another detailed definition of IoT [6], 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 and use intelligent interfaces, and are seamlessly integrated into the information network.

This paper is structured as follows: Section 2 presents security background, Section 3 will cover organization for IOT security. In Section 4, represent the challenges in IoT security. Section 5 presents the opportunity in IoT security and Finally, Section 6 conclusion and future work.

II. SECURITY BACKGROUND

Everything is a double sword, means the development of IoT can bring us both good service and bad effects. In Oct 2016, a Domain name system (DNS) service provider, encountered a severe DDoS (Distributed Denial of Service) attacks which disrupted uninterrupted service of many important websites such as Amazon, Twitter, Facebook. The source of the attack is partly from the Mirai botnet with thousands of compromised IoT devices. This attack used more than 5000 devices from the university campus, ranging from light bulbs to vending machines to launch attacks on DNS queries [7]. Thus, protection must be there without it, IoT devices are more likely and easily to be attacked and used for malicious purposes. So, we should take more consideration on IoT security and privacy protection. IoT provides security functions (e.g., authentication, verification) through its service interface technology [5]. Now a day, IoT-related researches are being carried out in various fields (e.g., medicine, automotive, house, etc.) and cause appearance of related products. The increasing interest in IoT, many attacks (e.g., denial of service (DoS), sniffing, modification, man in the middle attack), which occurs in conventional network system and it can also be occurred in IoT environment [8].

A. Vulnerabilities of IoT

The IoT devices goes through various stages in its life cycle right from the manufacturing of the device to the removal of the device from the IoT base systems. Throughout these stages various vulnerabilities might occur in the device and IoT base application. There are some issues such that information manipulation, unauthorized access, Denial of Service Attack, Distributed Denial of Service attack, Theft of resources (man in the middle attack) and information disclosure.

B. Security Requirements

To solve the aforementioned problems there is a need of security, such as Authentication, Data confidentiality, Access control, Trust management, Availability of resources, secure storage and secure software deployment.

C. Security model for IoT

Security model [23] for IoT represents the security features that should be followed by an IoT application. The security model shows Fig 1, can be represented by a cube with three dimensional representation that is security (Authorization), Trust (Repudiation) and Privacy (Respondent).

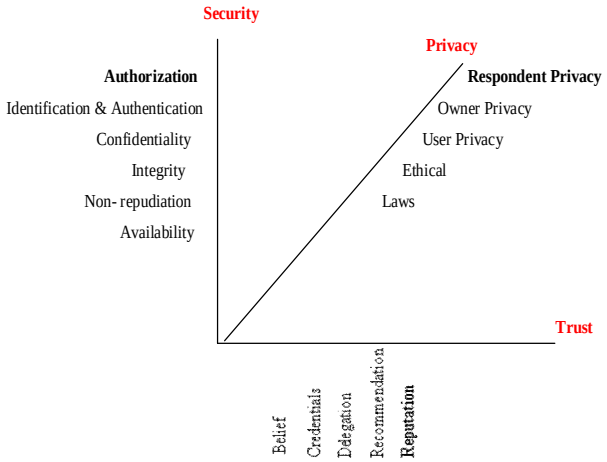


Fig 1 Security model for IoT

D. IoT Security Tomography

IoT security tomography represents the various attacks at the communication layer of transmission. As Table I, shows the different layers and their attacks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Table I IoT Security Tomography

	LAYER	Attacks
[1]	Transport Layer	Send wrong message, inject incorrect control packets
[2]	Network Layer	Routing Loops, wormhole attack, Network Partitioning
[3]	MAC Layer	Spoofing, Buffer Overflow, Eavesdropping
[4]	RF Layer	Complete Jamming, Eavesdropping, H/W or Sensor level threats

III. ORGANIZATIONS FOR IoT SECURITY STANDARDIZATION

There are lots of organizations working for IoT security standardization, some of them are mentioned below,

A. National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce publishes the FIPS standards applicable under the Federal Information Security Management Act (FISMA). NIST is actively developing a high level IoT guide covering organizational process and roles [16].

B. IoT Security Foundation

A new organization tries to holistically address IoT security through best practices guide and planned self certification schemes the Best Practice User Mark. The organization doesn't believe on the fact that only manufacturer is responsible and roles of other players are also taken into consideration[15].

C. Industrial Internet Consortium

The Industrial Internet Consortium (IIC) works on use cases for industrial. The IIC connects, controls and integrates the resources with people, processes and data by using general architecture , interoperability and open standards. The Industrial Internet Security Framework (IISF) is the in detail cross- industy-focused security framework which comprises of expert visualization, knowledge and security best practices [17].

D. Prpl Foundation

The Prpl Foundation works on next generation open source software from data centre to the device. prpl endorses OpenWrt and endeavours to support the OpenWrt community. They have a framework note for IoT security, a guide for critical areas in embedded computing.

Prpl works are pragmatic about security and collaborating with Continental Automated Buildings Association (CABA) in evolving IoT security. CABA is an international not-for-profit industry association dedicated to the advancement of intelligent home and intelligent building technologies [15].

E. Broadband Internet Technical Advisory Group (BITAG)

The outbreak of IoT insecurity is studied in the report of Broadband Internet Technology Advisory Group and certain recommendations are made to deal with it. The report motivates its recommendations with over 150 informative references and footnotes on IoT risks, vulnerabilities and remedies. It covers the home segment [18].

F. Open Web Application Security Project

The Open Web Application Security Project is well regarded for their work. The top 10 threats issued by OWASP have been very well received. They approach cyber security, especially at the web application layer protocol like HTTP, HTTPs. Recently they have started a project for IoT [12].

G. IPSO

The IPSO Alliance has been working for some time on data and functions for Smart Objects. It consists of design pattern and an object model, that can effectively use the IETF CoAP protocol to provide high level interoperability between Smart Object devices and connected software applications on other devices and services. It extends the smart objects devices networks along with security[14].

H. AllSeen

AllSeen alliance includes AllJoyn and Open Connectivity Foundation. The devices and apps can discover each other easily using AllJoyn, open source software framework and the communication between them becomes simple. The The AllJoyn system provides a security framework for applications to authenticate each other and send encrypted data between them [19].

I. online trust alliance alliance

The online trust alliance (OTA) works on consumer trust and online brand reputation, including privacy, identity theft and internet governance. They are a successor to efforts to combat spam emails through Email Senders and Provider Coalition (ESPC). They have developed a IoT trust framework [20].

J. Internet Engineering Task Force

The Internet Engineering Task Force (IETF) produces high quality, appropriate technical documents that influence the way people design, use and manage the Internet and makes the Internet work better. They are responsible for numerous standards around security, including X.509, Public key etc. [21].

K. Open Trust Protocol

Open Trust Protocol (OTrP) is a protocol for installation, updation, deleting applications and for managing security configuration in a Trusted Execution Environment (TEE) [12].

L. Manufacturers Usage Description

The draft Manufacturers Usage Description is a RFC intended to help reduce the vulnerability surface using a simple network policy. The scope for malware injection and the air firmware updates being hijacked is reduced. It also tries to cover devices no longer actively maintained by the original manufacturer [12].

M. Open Interconnect Consortium (OIC)

The OIC is a consortium founded in 2014, announced only a week before Thread, focused on creating a standard specification and an open source project to address the push for interoperability of IoT devices. The OIC wants to connect the next 25 billion smart devices that are expected to emerge by 2020 by defining a full and standard communications framework to enable all applications over a broad range of vertical markets. As with the other standards groups mentioned, the OIC believes that interoperability between objects is necessary and a standard, open source implementation is the best way to do this [22].

IV. CHALLENGES IN IOT SECURITY

There are lots of challenges facing by IoT system, some of them are mentioned following,

A. Establishment of Identification

The establishment of identification in IoT is one of the greatest challenge due to the number of devices. To identify every last gadget in the network like the web page over a web. In web to identify any resource require unique identification system such as a Uniform Resource Identifier. This kind of system need to be designed in IoT [11].

B.Authorize and Authenticate Devices

Authentication and authorization of devices is critical for securing IoT systems. Devices must establish their identity before they can access gateways and upstream services and apps. However, there are many IoT devices that fall down when it comes to device authentication, for example, by using weak basic password authentication, or using passwords unchanged from their default values. Adopting an IoT Platform that provides security by default helps to resolve these issues, for example by enabling two factor authentication (2FA) and enforcing the use of strong passwords or certificates. IoT Platforms also provide device authorization services used to determine which services, apps, or resources that each device has access to throughout the system [11].

C. Data Management

Recognizable proof of billions of devices and their forwarding can be viewed as a noteworthy issue in IoT. As indicated by estimations, by the year 2020 more than 50 billion devices will be associated with the internet. Dealing with the devices and their

forwarding will be troublesome notwithstanding for IPv6.There are techniques that can be utilized for recognizable proof of the items in IoT. Some of them are Bar code identifiable evidence, vision based object identification
and so forth. RFID and NFC innovations are utilized for filtering purposes [9].

D. Heterogeneity

The greatest security and protection issue is by a long shot the problem of device heterogeneity. Issues should be handled appropriately to make IoT more secure and robust. Administering hundreds of distinctive sorts of devices with each has their own security problems and necessities. Each object should be handled contrastingly which makes it hard to apply a single resolution to all. It will be an extreme assignment to secure each sort of the device from various kinds of incidents. It makes it harder to supervise the items. Every device imparts and works distinctively when contrasted with other objects. Device heterogeneity can influence numerous different perspectives also, for example, trouble in combination, security, and distinguishing proof and so on [9].

E. Ensure data privacy and integrity

While or after transmission of data across the network it should be stored and processed securely. The data privacy includes redacting or anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. The data that is not in used should be disposed of securely. Maintain legal and regulatory framework for storing data is also an important challenge. Along with privacy data integrity is also important which may involve employing checksums or digital signatures to ensure data has not been modified. Now a days, some organizations are using Blockchain – as a decentralized distributed ledger for IoT data for offering a scalable and resilient approach for ensuring the integrity of IoT data [11].

F. Physical Security

The sensor nodes (mobile phones, embedded chips, RFID tags) are vulnerable to theft and misplacement. Therefore, anti-theft policies should be introduced and applied to the nodes. And if theft occurs, then steps should be taken to immediately block the stolen device to avoid any unauthorized access to the sensitive data [10].

G. Heterogeneous Networks

Various types of networks (WSN, LAN, RFID, sensor networks) communicate with each other in an IoT environment. The interoperability among various networks might pose some risk to the security, privacy and trust. Therefore, there is a need to explore security solutions during interoperability [10].

H. Detect and manage VULNERABILITIES and Incidents

It is challenging to assess the repercussions of a vulnerability or the extent of a breach in order to manage its impact. Despite best efforts, security vulnerabilities and breaches are inevitable. There is a number of techniques to detect vulnerabilities and breaches include monitoring network communications and activity logs for anomalies and ethical hacking to expose vulnerabilities, and applying security intelligence and analytics to identify and notify when incidents occur [11]. Also, for managing the devices a device manager require which is used to maintain a register of devices.

I. Secure Routing

The information from sensor devices is sent over the wired or remote transmission network. The communication framework ought to have the capacity to deal with information from a vast number of sensor devices without bringing about any information loss because of system clog, guarantee legal security measures for the transmitted information and keep it from outside intrusion or checking [10].

J. Predict and Preempt Security Issues

A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to predict and proactively protect against potential security threats. To predict security issues threat modelling is a one of the approach. Other approaches include applying monitoring and analytics tools to correlate events and visualize unfolding threats in real-time, as well as applying AI to adaptively adjust security strategies applied based on the effectiveness of previous actions [11].

K. Secure web, Mobile, and Cloud Applications

Web, mobile and cloud apps and services are used for managing accessing and processing IoT devices and data. So as part of a multi-layered approach to IoT security they must be secured. When developing IoT applications, be sure to apply secure engineering practices to avoid vulnerabilities such as the OWASP top 10 vulnerabilities. Apps should support secure authentication, both for the apps themselves and the users of the applications, by providing options such as 2FA and secure password recovery options [11].

V. OPPORTUNITY IN IoT SECURITY

This section discusses the opportunities in the IoT security. There are different methods used to provide security in IoT such as cryptographic solutions, security frameworks, authentication protocols, routing protocols, privacy preserving protocols. Besides a number of solutions still there is a research gap. Following are some solutions which can lead to some solutions.

A. Application Specific Solutions

The IoT has heterogeneous applications. Different industries have different application requirements with different security requirements. For example, data privacy is more important for smart transportation, health, home, positioning. Whereas for Smart urban management, data
authenticity is more important. Therefore, security solutions should be designed specifically for an application.

B. Huge Data

IoT systems like temperature sensors, traffic sensors, weather monitoring, etc. generates lots of data. This huge and heterogeneous data have to be stored securely and analyzed as per user's needs. To handle this amount of data, Big Data techniques can be applied to IoT. While doing so, data security is of utmost concern. Hence, by securing data enough security can be provided to the IoT applications.

C. Physical Security

The sensor nodes (mobile phones, embedded chips, RFID tags) are vulnerable to theft and misplacement. Therefore, anti-theft policies should be introduced and applied to the nodes. if a theft occurred, then next steps should be taken to immediately to block the stolen devices to avoid any unauthorized access to the sensitive data.

D. Heterogeneous Networks

Various types of networks (WSN, LAN, RFID, sensor networks) communicate with each other in an IoT environment. The interoperability among various networks might pose some risk to the security, privacy and trust. Therefore, there is a need to explore security solutions during interoperability.

VI. CONCLUSION AND FUTURE WORK

The development of the IoT exposed many new challenges, including the lack of clear architecture and immature security methods. To meet these challenges, the proposed acting security methods can hopefully balance the desires from different parties, can open the door of opportunities for future IoT security. The future of IoT will be expected to be unified, seamless, and pervasive. The hugh efforts need to be taken within a set of security methods. Thus, the developments of IoT as an intelligent system can be proceeding with interoperability, energy sustainability, privacy, and security.

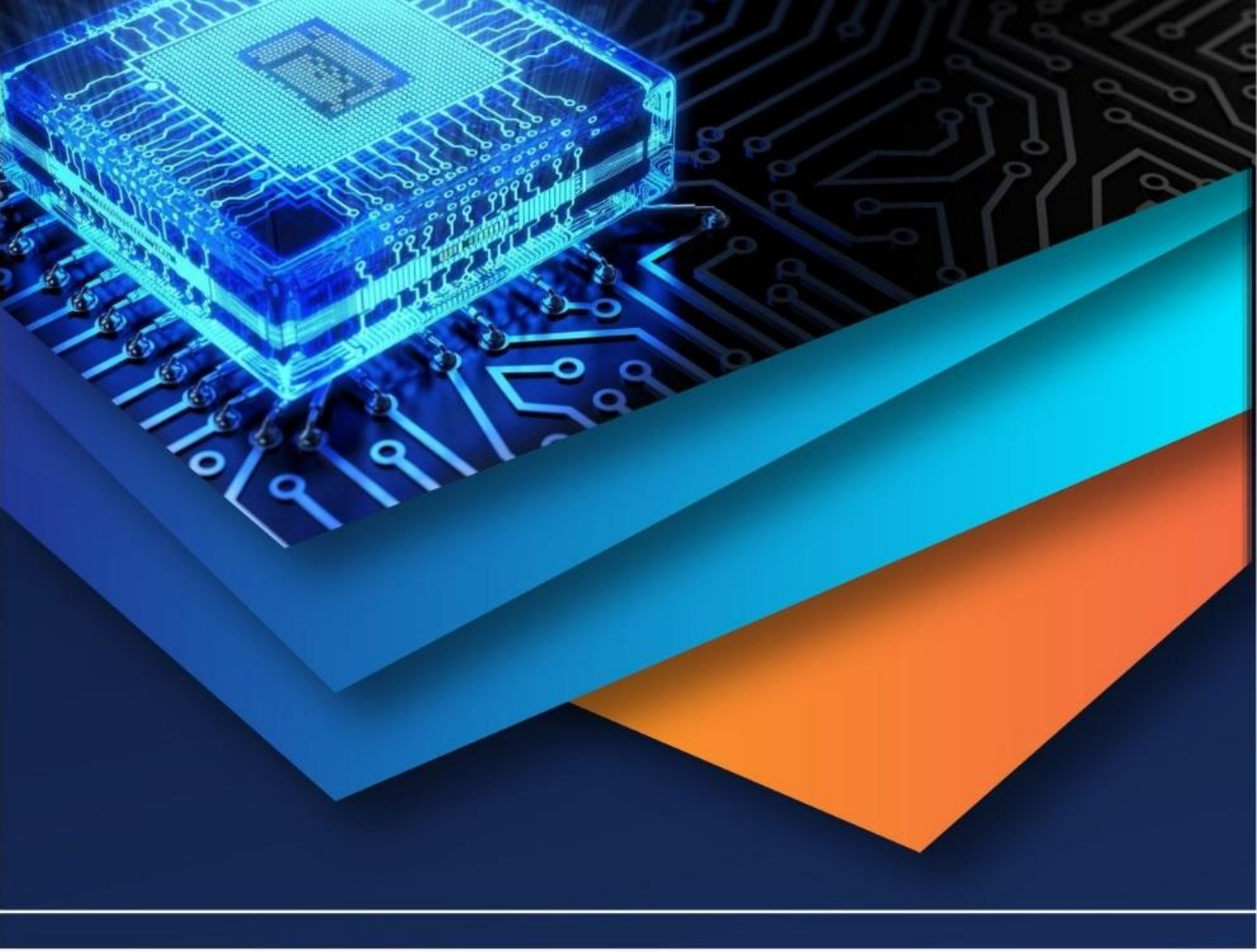
V. ACKNOWLEDGMENT

The Authors would like to thank Prof. Dr. S.S. Sane, Head of Department of Computer Engineering, Prof. Dr. S.M. Kamalapur, KKWIEER, Nashik and Swati R. Chaudhari, Datamatics Global Services Ltd, Nashik for their kind support and suggestions. We would also like to extend our sincere thanks to all the faculty members of the Computer Engineering.

REFERENCES

[1] H. Kim, D. Kim, "IoT Technologies and security", Review of KIISC, 2012
[2] L. Zhou and H. Chao, "Multimedia traffic security architecture for the internet of things" Network, IEEE, no. June, pp. 35–40, 2011
[3] http://www.gartner.com/newsroom/id/2684616
[4] O. Vermesan, F. Peter, G. Patrick, G. Sergio, B. Harald, Sundmaeker Alessandro, J. Ignacio Soler, M. Margaretha, H. Mark, E. Markus, and D. Pat, "Internet of Things: Strategic Research Roadmap," Internet Things Strateg. Res. Roadmap, pp. 1–50, 2009.
[5] International Telecommunication Union (ITU), "Overview of the internet of things", 2012
[6] Ian G Smith,Ovidiu Vermesan, Peter Friess and Anthony Furness, " The Internet of Things 2012 New Horizons", published in Halifax, UK, 2012

[7] Honbo Zhou, “The Internet of Things in the in Cloud A Middleware Perspective”, CRC Press Taylor & Francis Group, Boca Raton, FL 33487-2742
[8] M. Hossain, M. Fotouhi, R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things”, IEEE World Congress on Services, New York, USA, pp. 21-28, 6. 2015.
[9] A. u. Rehman, S. U. Rehman, I. U. Khan, M. Moiz and S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS), vol. 8, no. 3, pp. 147-157, 2016
[10] Aanchal Punia, Dr. Daya Gupta, Shruti Jaiswal ”A Perspective on Available Security Techniques in IoT”, 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, Indi
[11] https://developer.ibm.com/dwblog/2017/iot-security-challenges/
[12] http://www.cisoplatform.com/profiles/blogs/survey-of-iot-security-standardshttp://www.openinterconnect.org
[13] https://www.ipso-alliance.org/about-us/members-committees/
[14] https://iotsecurityfoundation.org
[15] https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.
[16] http://www.iiconsortium.org/
[17] https://www.bitag.org/documents/TWG_Governance_Manual_v3.1.pdf
[18] https://openconnectivity.org/developer/reference-implementation/alljoyn
[19] https://otalliance.org/initiatives/internet-things
[20] https://www.ietf.org/
[21] https://openconnectivity.org/
[22] https://www.researchgate.net/figure/IoPTSsecurityauthorization-trustreputation-privacyrespondent_fig1_46572265



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY