TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

Popular Attacks on product modeling, fault detection of IoT Layers and its Countermeasures, Security Requirements and Open Issues

E.Sandhya, Assistant Professor, Dept.of IT, Sree Vidyanikethan Engineering College, Tirupati
Dr. Annapurani.K, Associate Professor, Dept.of CSE, SRMIST- Kattankulathur

Article Info
Volume 82
Page Number: 6195 - 6204
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 30 January 2020*

Abstract:
The interconnection of collaborative devices through internet as an interactivemedium is the basis forproduct modelling. The advent of IoT makes our lives smarter and better.At the flipside, IoT is still emerging technology and due to constrained environment; it is prone to several attacks, especially Distributed Denial of Service (DDoS) attack tops in list.We present a taxonomy that covers all possible categories of attacks that occur in IoT by product modelling.The paper exposes popular attacks layer wise in IoT fault detection.Also, the paper covers security requirements and measuresto tackle the threats in IoT environment.

Keywords: *Product modelling, IoT security requirements, DDoS,Fault detection, Attack Taxonomy.*

I. INTRODUCTION

Now days, IoT has become emerging trend and more complex in terms of opportunity. The world will adapt to the environment in terms of "any moment, any location, and any communication". IoT works on three principles i.e. to be identifiable, to communicate and to interact [3].IoT consists of four interrelated components i.e. humans, things, software and hardware [4]. Generally, the hardware platforms used in IoT are Arduino, Friendly ARM, Galileo, Gadgeteer, WiSense, Raspberry Pi etc and platforms include OS like Contiki RTOS, Tiny OS, Lite OS, Riot OS, and Android etc [4].The communication technologies used in IoT environment includes Radio Frequency Identification, Ultra Wide Band antenna, Bluetooth, Bluetooth Low Energy, IEEE 802.15.4,Near Field Communication, Z-Wave, Wi-Fi, LTE-A, ZigBee etc. [9]. IoT includes concepts like Machine–to-Machine (M2M) communications, Wireless Sensor Networks (WSN) and Cyber Physical Systems (CPS). So far, the world has deployed about 9 billion "smart things" connected to internet. Analysis say by 2020 there will be 50 billion connected smart devices(Fig.1). IoT is associating with technologies like Big Data, Machine Learning, Image Processing, Cloud Computing, Embedded Systems etc, for supporting various applications.

1.1 Definitions

IoT enables physical objects to see, hear, think and perform jobs by having then "talk" together, to share" information and to coordinate decisions". [2]. "Internet of things (IoT) is a collection of many interconnected objects, services, humans, and devices that can communicate, share data, and information to achieve a common goal in different areas and applications". [17]

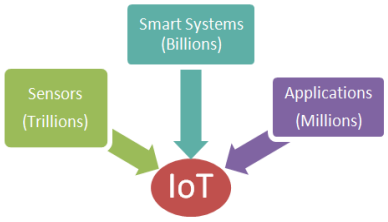

Fig.1. Building Blocks of IoT

"IoT covers all types of things associated to Internet. These "things" consist of dummy sensors, similar to

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

motion detecting sensors, temperature sensors, etc., to different types of smart objects, like smart phones, smart meters, self-directed cars, buildings, etc. The main idea is to connect all these devices to gather data, share data, and information, and at the end everything in this ecosystem act accordingly in smart ways so that our lives are easier, better, and in harmony". [12]

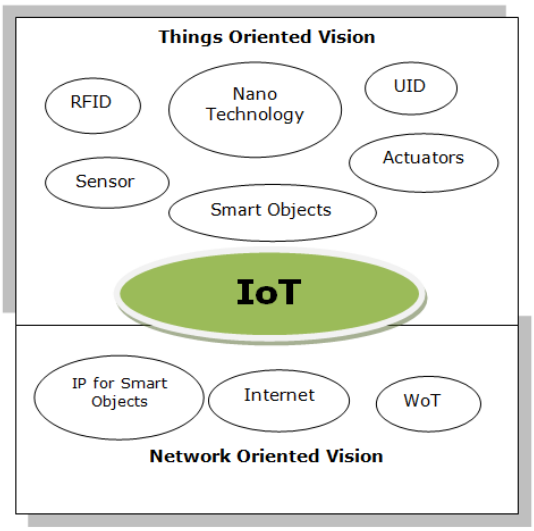

Fig.2. Vision of IoT Convergence

IoT consists of majorly two terms one is "Network" oriented vision and second one is "Things" oriented vision as shown in fig.2 [1].We need to take into account that "Internet" and "Things", when integrated results in modernization of environment into today's world."Internet of Things" means interconnection of heterogeneous objects which can be addressable uniquely based on traditional communication strategies.

1.2 IoT Architecture

Generally, IoT should be able to support interconnection of million numbers of heterogeneous devices through a network, so there is essential requirement for a layered architecture. Fig.3. represents a familiar architecture model.

a. Perception Layer

The initial layer, perception layer is also called as Object Layer. The perception layer represents collection of objects that gather and process information. This layer supports devices like sensors, actuators, transducers, RFIDtags to function various activities like location identification, motion identification, finding temperature, humidity, acceleration etc.

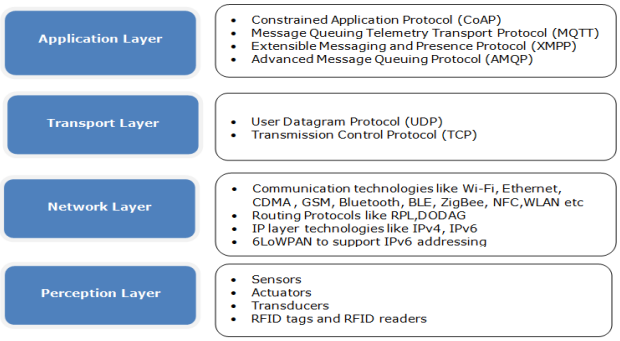

Fig.3. IoT Layered Architecture

b. Network Layer

This layer supports for transmitting data gathered in perception layer to application layer through various communication technologies. The various communication technologies used are RFID,3G/4G communications, GSM, CDMA, Wi-Fi, Bluetooth, ZigBee, Infrared, BLE, LTE, Z-Wave etc. This layer also guarantee in unique addressing of objects and making routing decision for supporting various heterogeneous platforms in the network.

c. Transport Layer

In IoT environment, the transport layer deal with end to end connectivity, bandwidth consumption and session maintenance .It is required to maintainefficient security features by this layer, since low power devices are more prone to attacks. The IoTapplications running in the application layer have tochoose the appropriate transport layer protocol.

d. Application Layer

The application layer supports in providingservices to users. This layer is responsible fordata formatting andpresentation. Generally, application layer worksbasedon HTTP protocol. In IoT, because of resource constrained nature HTTP is not suitable. Several application layer protocols are developed

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

such as CoAP, MQTT, and XMPP etc.It covers various applications such as smart home, healthcare, smart building, smart cities, agriculture, transportation, industrial automation, environmental monitoring, security and surveillance etc. The detailed IoT applications and its functions are specified in Table 1

Table1. IoT Applications and its functions

S.No	Applications	Functions
1	Smart Home	• Fire/Smoke Monoxide detection • Temperature Controlling • Smart Lighting • Smart Garage Door • Smart Locking System • Gas Leakage Detection • Water Leakage Detection • Appliance Monitoring and Controlling
2.	Smart Healthcare System	• Gait Analysis • BP Monitoring • Pedometers • Sleep Monitoring • ECG Monitoring • Body Temperature Monitoring • Assisted ambient living • Smart Medicine Box • Patients Surveillance
3.	Smart Vehicles	• Assisted Driving • Robot Taxi • Smart Parking
4.	Smart Agriculture	• Crop water Management • Pest Control and Monitoring • Food Production and Safety
5.	Smart Cities	• Smart Water and Waste Management System • Street Light Monitoring • Smart Meters • Traffic Monitoring System • Smart building • Smart Energy • Smart Roads • Public safety, security and crime prevention
6.	Smart Environment	• Fire Detection in forest • Air Pollution Detection • Monitoring of snow level • Detecting Landslide and Avalanche • Detection of quakes • River Floods Detection
7.	Retail Industry	• Payment using NFC in smart shopping application • Smart logistic Management

II. IoT Attack Model

Fig.4. specifies an attack model, the attacker first looks for an unaddressed threat. He targets the vulnerability to launch an attack. Upon successful attack execution, the attacker exploits by compromising the attack target. The attacker can

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

make use of readily available tools to look for vulnerable points and can launch the attack.

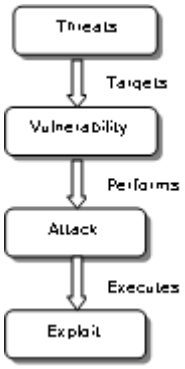

Fig 4: IoT Attack Model

2.1 IoT Attack Taxonomy

We have classified IoT attack taxonomy into four categories as shown in fig.5:

- Attacks on IoT Infrastructure: Targets the available physical infrastructure.
- Attacks on IoT Protocols: Exploits vulnerabilities in protocols.
- Attacks on IoT enabling technologies: Targets the technologies that surround IoT.
- Attacks on Information: A Data exchange in IoT is the main concern of such attacks.

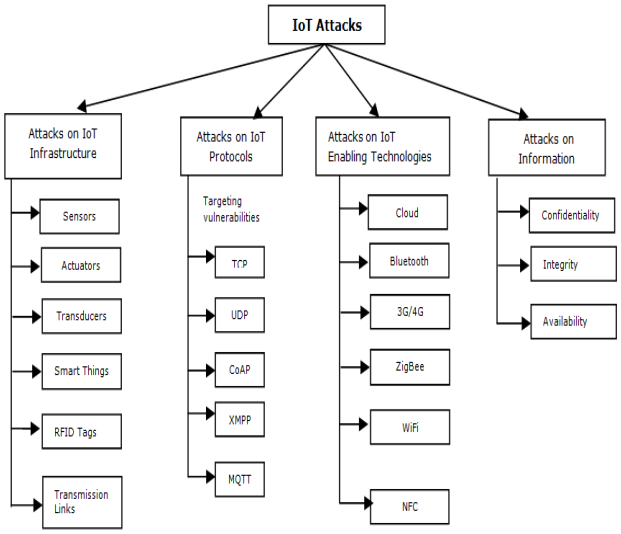

Fig.5. Classification of IoT Attacks

2.2 Security Attacks in IoT Layers

It is impractical to review realistic aspects of threat, vulnerability, and risk without examining the main components of information security, an essential sub-section of IoT security [5].

Briefly, they are as follows:

i. Confidentiality: Maintaining sensitive data secretly and protecting it from disclosure.
ii. Integrity: Guarantees that the data is consistent.
iii. Authentication: Make sure that the information is from a known trusted source.
iv. Non-repudiation: Guarantee that a transmitted message has been sent and received by the endpoints cannot later reject performed action.
v. Availability: Allowing Information accessibility whenever needed.

a. Attacks in the Perception Layer

Perception Layer in IoT deals with sensors and collection of information from it. The sensors and physical objects are prone to several attacks. An attack called node capture can simply and easily target a particular entity or the whole network communications by compromising gateways and by inclusion of malicious nodes. On the flip side, the attack such as man-in- the middle, timing attack and DoS attacks poses security threat to this layer. Replay attack is most commonly occurring attack under this layer that targets the authentication process of physical objects. To secure this layer, several security frameworks should be adopted.

The framework should focus on authentication and data integrity. The authentication and access control schemes were included to identify nodes in a network and their respective rolls. The data integrity and confidentiality schemes should be introduced to protect the collected data against tampering and publicizing [8]. Then, we also require key management schemes to develop the necessary keys and will be used for the purpose ofauthentication network objects, encryption of data that is being

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

collected, and generating signatures for transmitted messages [6]. Finally, it's a must to have intrusion detection systems to identify some malicious nodes and guard the network from attacks.

Popular attacks under perception layer include:
Transduction attack: they rely on analog signals to manipulate the data that prompts the computer system to take an action.
Node capture attack: It is a serious attack in which an intruder take control over a node and executes several operations over network and compromise it.
Replay attack: A legitimate message is frequently repeated to emulate malicious behaviour.
Relay Attack: An attacker initiates communication between two parties and relays messages between them.

Device tampering: Devices in IoT has little intelligence .They can be stolen easily without a notice. If a device went into the hands of wrong person or an attacker, he can tamper or manipulate the software or hardware. After performing such manipulations, the device might be introduced into the network to perform his tasks.
Signal Injection: attacker targets to change the sensed parameters of data by injecting fake data using electromagnetic signals to corresponding sensors.[13]

Wormhole attack: attacker gets a packet in one point in the network, tunnels it into another point of the network and again replays them into same network using that point. [14]
HELLO flooding attack: The malicious node is able to disturb the security of network by sending periodic hello packets with high signal strength.

b. Attacks in the Network Layer:
The basic responsibility of network layer is to transfer the information collected from sensors through WSN. Network layer has many security troubles and several kinds of attacks like eavesdropping, Packet sniffing, Denial of Service, replay attack, man-in-the-middle attack, routing attacks, security troubles in routing, as well as disclosure of privacy. Here, attacker aims to disrupt the packets using several means.

Popular attacks under network layer include:
Routing Attack: It is an attack that targets the weakness in the routing protocols and goal is to drop packets without making it to reach the destination by various means. [13]
IP Spoofing attack: It is related to IP packets, in which the packets originating from the attacker has someone else IP instead of attackers IP. It is used to hide the identity and it is used to perform several DDoS attacks.[10]
Flash crowd attack: A surge of increase in incoming traffic to a specific webpage or website makes it unresponsive and starts denying its intended services.
Man-in-the–middle attack: Attackers identifies the flaws in process of authentication and changes the messages exchanged between two communicating entities. They presume that they both are in fact interacting with one another. The attack focuses on integrity and confidentiality of the data exchanged between two parties.[13]

Eavesdropping: The passive attack in which the adversary silently listen to data exchange happening among the entities. It affects data privacy by deducing information from messages.
Reflection-based flooding Attacks: Attacker sends fake replicated request instead of genuine request to reflectors, arouting component. Then the reflectors send their reply to victim and exhaust the targeted resource. Attacker spoofs his IP address while performing this attack. e.g.: Smurfing.
Protocol Exploitation flooding attacks: Attacker uses vulnerabilities in protocols and targets specific features by using the bugs in the protocol. It consumes more amounts of targeted resources and can lead to DDoS attack .e.g.: SYN flood, TCP SYN-ACK flood, ACK PUSH flood etc.

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

Amplification-based flooding attacks: Attacker targets the application and generates series of messages in order to amplify the traffic towards victim. Usually in such attacks, we use bots o amplify the traffic. The main objective of this attack is to make system deny its services (DDoS).

c. Attacks in the Transport Layer:

Transport layer is responsible to transmit the information to Cloud or IoT application server. The transport layer transfers the data of sensors from perception to application layer and using networks such as Bluetooth, LAN, wireless links, 3G.It uses communication ports to achieve end to end communication.

Popular attacks under transport layer include:

Denial of Service attack: Most popular attack, where attacker attempts to put a stop to server or intended services to its legitimate temporarily or indefinitely.[13]

Port scanning attack: Port scanning aims to identify idle or open ports using scanning tools. Then attacker makes use of such ports to launch several attacks. Also we can identify services running using port scans .Attacker sends request to port addresses in server to find an active port. A variant to this attack is port sweep where multiple devices were scanned for an appropriate listening port.

UDP flood DDoS attack:It is a type of DoS attack, where large numbers of UDP packets were sent to victim server to drain its resource and affect its ability and response.

d. Attacks in the Application Layer:

Application layer deals with IoT Applications. Any vulnerability with respect to the application/service can be exploited through attacks like SQL Injection, Application Denial of Service, Attacks targeting application protocols such as MQTT, REST, XMPP, DNS etc., (application layer protocols).

Popular attacks under application layer include:

Application Denial of Service: Application DoS attack is more prominent attack in IoT and cloud. The attacker take advantage of flaws in the application layer design, Protocols and implementations in order to gain access to remote server and launch attack on victim's IoT application services. In this attacker looks for open Ports/Ideal ports present at server side to launch the attack. Applications, Services, Protocols were the targets.

Privacy Breach: A privacy breach occurs when there is illegal capturing, use and disclosing personalinformation. Most common privacy breach happen when personal information is mistakenly shared. The adversary can eavesdrop personal data through other sources such as repository and packet analysis.[10]

Elevation of Privilege: The attacker who's under privileged will try to gain privileged access to a specific device or service. With faked privileges, the attacker can gain administrator privileges, he can do anything that administrators can do [10].

Authentication & Identity: Due to heterogeneity and complexity of objects and network in IoT, traditional authentication and identity management methods are not applicable[7].

Table 2 Layer wise attack solutions

S.No	IoT Layer	Solution
1.	Perception layer	• Depends on type of sensors and devices. • Device specific resolution.
2.	Network Layer	• Security enhanced programming in routers. • Adapting tamper resistant router. • Effective packet filtering. • Monitoring packets through firewalls.
3.	Transport Layer	• Take appropriate action on open, idle ports. • Mitigating vulnerable

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

		ports. • Introducing port hopping techniques.
4.	Application Layer	• Improving programming standards and practices.

III. Security Requirements for IoT

Internet of Things can be easily compromised by various types of threats [13]. They could be introduced at different levels of the process. It can range from very passive attack like eavesdropping attack that exploits authenticity, confidentiality and integrity of the personal data. Due to such attacks, confidentiality of users in the IoT gets affected. One of the top rated attacks which identify the things is prone to resource exhaustion attack i.e. Denial-of-service (DoS) attacks. In this attack, the attackers flood the network by sending large number of unending request to concerned targets to diminish their resources. Thereby, the targets start denying its services to its intended users. Also the availability of several IoT resources and Network can also be disrupted by flooding large number of packets. Table 2 provide an overview of solutions in each layer.

Anything which is a part of Wireless Sensor Networks or in an IoT environment should be authenticated before being part of it. However, the identity management in IoT differs. The identity of things is not similar to the identity of its underlying mechanisms and they've various identification codes according to the type of the object and its service provisioning. IoT demands a Unique Identity using Global Unique Identifier (UID) that uniquely identifies a unique thing in the network [11].Also a hybrid identification scheme should be integrated to show entity location and an aggregation of IPv6 address. Thus, IoT should have specific identifiers like IP addresses to uniquely identify them and called for digital identity.

Also, there's a research gap in identifying the objects autonomously. The research should focus on proposing a framework which enables autonomous object authentication in order to verify its identity. The proposed work should also deal with the issue of device spoofing. Further, we are in need to develop security protocols that can take care of attacks targeting the information by combining security framework and various feasible cryptographic algorithms that covers digital signature ,hash algorithms and encryption algorithms, to deal with the Integrity, the confidentiality and the non-repudiation[1]. However, the security solutions for IoT will be far different from the traditional security solutions because of the constrained environment. In IoT, any security solution has to use very minimum resources, fairly low bandwidth, utilize very limited memory with nominal amount of computations. So the traditional security solutions will never work for IoT and demands optimal solution. Due to the resource-constrained environment with nominal bandwidth, little memory,restricted computations and energy available to IoT devices, traditional security protocols and mechanisms will not be feasible for the IoT. Thus, to secure IoT devices, it is must to have most favourable security mechanisms.

Further, the routing protocols in IoT should work for throughput, deal with high packet loss and variability in packet loss, has to coordinate with asymmetric link characteristics and has to take care of fragmentation of larger packets as they are susceptible to Denial of service attacks and also lead to fragment loss that degrades the network throughput[15]. Also, traditional cryptography using public key should never be used in IoT environment. Hence, cryptography mechanisms and security protocols should be optimized and modified such that it can be adapted to the highly constrained objects. Alternatively a completely fresh solution should be designed and integrated into the IoT.

In addition to issues with authentication and authorization, the vulnerabilities in software play a

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

critical role in current security research domain. Along with the functional and non functional requirements, it is advised to specify security requirements in order to make software fool proof [16]. While programming the IoT applications or IoT software's, programmers might commit mistakes and unknowingly introduce programming bugs and later they become potential threats and sources of attacks, if they were not addressed. They lead to several attacks that range from Zero day attacks to Application Denial of Service attacks.

The following are good considerations towards strengthening the security in IoT network.

1. Data should be encrypted on the application layer. End-to-End Security, cryptographic principles and key management are extremely important and should be carefully described.
2. Bug reporting system. The manufacturers who are into IoT should define a bug / defect reporting and tracking system together with response and resolution policy.
3. Manufacturers should provide a space to report discovery of vulnerabilities that pose threats to IoT applications
4. Much required to frame the workflows for assessing and dealing security incidents.
5. Maintain a common information sharing platform to share, discuss, and resolve different threats and vulnerabilities.
6. Always follow firm Password Policy. It is essential that all authentication systems demand strong passwords.
7. Use the modern concepts of design patterns to develop flawless design and implementation of IoT devices and networks to deal with security vulnerabilities.

IV. Countermeasures and Open Issues

4.1 Software Defined Networks (SDN)

It is equipped with SDN Controller that monitors and manages the entire network behaviour. It focuses on packet flow and provides faster solutions to security threats and attacks [17] .SDN supports both proactive and reactive mechanisms. It tackles security issues that are present in IoT environment in an effective way due to its own security and management strategies. Adapting SDN for provisioning security is considered to be finest solution. However, developing methodologies to detect and mitigate attacks is an open challenge.

4.2 Architectural security design for IoT

A Novel architectural design to satisfy security solutions are much required to achieve high level security and the need of light weight protocols and algorithms were discussed in [18]. The requirement of privacy preserving algorithms and safeguarding physical infrastructure were also specified. This deploys architectural security designs at: end-end, edge and distributed fashion.

4.3 End-to-End security at Things

End-to-End messaging is fundamental communication amonginterconnectednetworked systems [19]. IP protocol and 6LoWPAN were implemented to achieve this. Many security flaws can be addressed effectively using end-end security [20].

There are still many open research problems like Lightweight Protocols for End -to- End security, and to handle heterogeneity.

4.4 Mutual Authentication protocols for Lightweight systems

IoT is a constrained environment and demands mutual authentication among communicating entities. The [21] categorizes mutual authentication protocols into four classes .However, an effective testbed to test those protocols in real time has to be addressed.

4.5 Key management:

The importance of Key management schemes like RSAor DHKE, ECC [22] were discussed by many authors. However, adapting such cryptographic techniques to work under IoT environment requires optimization and is an open issue.

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

V. CONCLUSION

IoT technology is now playing a significant role in today's society.As per projection the estimated connected smart devices in the internet would touch 50 billion bythe year 2020.On the other hand, it has several security flaws and might become potential target to many attacks.We have exposed popular attacks on IoT as per each layer in IoT reference model. We have also presented an attack taxonomy that gives comprehensive coverage of IoT attacks. The layers can be strengthened by tightening packet filtering, firewallsand adopting tamper resistance routers. We have also addressed countermeasures to attacks targeting IoT ports by various port hopping techniques .Finally, we have presented several IoT related attacks and its probable countermeasures. It also covers security requirements and solutions to tackle such attacks. In future, the proposed security solutions need to be incorporated in such a way that it should support heterogeneous hardware and software platforms of IoT. The paper has addressed the open issues with respect to Software Defined Networks for mitigating attacks,designing of light weight protocols for achieveing End to End security, optimization of traditional algorithms for maintaining mutual authentication between the devices and key management.

VI. REFERENCES

1. Luigi Atzori, Antonio Iera, Giacomo Morabito,'The Internet of Things: A survey', Elsevier Journal on Computer Networks, Vol. 54, Issue 28,pp. 2787–2805, October 2010.
2. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, Fourth Quarter 2015.
3. Daniele Miorandi , Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac , "Internet of things: Vision, applications and research challenges", Elsevier Journal on Ad Hoc Networks , Volume 10, Issue 7, pp. 1497–1516, September 2012.
4. Jayavardhana Gubbia, Rajkumar Buyya,Slaven Marusic , Marimuthu Palaniswami ," Internet of Things (IoT): A vision, architectural elements, and future directions", Elseiver Journal on Future Generation Computer Systems ,Vol.29 ,No. 7, pp. 1645–1660, Sep 2013.
5. Rolf H. Weber," Internet of Things – New security and privacy challenges", Elseiver Journal on computer law & security , Vol.26 , Issue 1 , pp. 23-30, 2010.
6. Maha Saadeh, Azzam Sleit, Mohammed Qatawneh, Wesam Almobaideen, "Authentication Techniques for the Internet of Things: A Survey", IEEE Cybersecurity and Cyberforensics Conference, 2016.
7. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of Things (IoT) Security:Current Status, Challenges and Prospective Measures" , IEEE 10th International Conference for Internet Technology and Secured Transactions , 2015.
8. Mohamed Abomhara,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, 2014.
9. Minela Grabovica,Dražen Pezer, Srdan PopiC,Vladimir Kneževic, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey", IEEE International Conference on Privacy and Security,2014.
10. Ahmad W. Atamli,Andrew Martin , "Threat-based Security Analysis for the Internet of Things" , IEEE International Workshop on Secure Internet of Things, 2014.
11. Raja Benabdessalem,Mohamed Hamdi, Tai-Hoon Kim, "A Survey on security Models, Techniques and Tools for Internet Of Things", IEEE 7th International Conference on Advanced Software Engineering and Its Applications, 2014.
12. Omer Berat Sezer , Erdogan Dogdu, and Ahmet Murat Ozbayoglu," Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey", IEEE Internet of Things Journal, Vol. 5, No. 1, February 2018.
13. Jyoti Deogirikar, Amarsinh Vidhate, "Security Attacks in IoT: A Survey", International conference on IoT in Social, Mobile, Analytics

January - February 2020
ISSN: 0193 - 4120 Page No. 6195 - 6204

and Cloud, 2017.

14. Asma Alsaidi, Firdous Kausar, "Security Attacks and Countermeasures on Cloud Assisted IoT Applications", IEEE International Conference on Smart Cloud, 2018.
15. Qifeng Chen, Haoming Chen, Yanpu Cai, Yanqi Zhang, Xin Huang, "Denial of Service Attack on IoT system", 9th International Conference on Information Technology in Medicine and Education, 2018.
16. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao, "A Survey on Security and Privacy Issues In Internet-of-Things", IEEE Internet of Things Journal, Vol. 4, No. 5, 2017.
17. Flauzac Olivier, Gonzalez Carlos, Nolot Florent, "New Security Architecture for IoT Network", International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems, 2015.
18. Kewei Sha, Wei Wei , T. Andrew Yang , Zhiwei Wang, Weisong Shi, "On security challenges and open issues in Internet of Things", Future Generation Computer Systems, vol 83, pp. 326-337, Feb 2018.
19. Tobias Heer , Oscar Garcia-Morchon , Ren´e Hummen , Sye Loong Keoh , Sandeep S. Kumar and Klaus Wehrle," Security Challenges in the IP-based Internet of Things", Springer Journal on Wireless Personal Communications , Vol no.61 , Issue 3, pp.527–542, 2011.
20. Z. Shelby, C. Bormann, "6LoWPAN: The Wireless Embedded Internet", John Wiley & Sons, Vol. 43, 2011.
21. Aakanksha Tewari, B.B. Gupta," Security, privacy and trust of different layers in Internet-of-Things (IoTs) Framework", Future Generation Computer Systems, 2018.
22. Ashok Kumar Das, Sherali Zeadally , Debiao He, "Taxonomy and analysis of security protocols for Internet of Things", Future Generation Computer Systems , Vol no. 89, pp. 110–125 , 2018.