IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review on IoT Applications and its challenges and limitations of existing solutions

Amit Kumar Bind, Avtar Singh

M. Tech Scholar, Assistant Professor

Department of Computer Science & Engineering,

Dr. BR Ambedkar National Institute of Technology, Jalandhar, India

***Abstract*- Internet of things (IoT), is the 24/7 interconnected sensors nodes generating data to the cloud. The cheap price of the sensors and RFID enabled the IoT in vast area of application in almost each and every field of daily life which makes the many things automated and can solve many daily life problems and makes the term smart. Like smart city smart energy etc. IoT enables the use of compact devices consist of various sensors from medical to mechanical sensors, it includes almost every type sensor like human can sense or even more. There are wide range of devices available widely in size, energy, use, capacity and computation power. The integration of these wide range smart things into the standard internet introduces many security challenges regarding architectural design and because the of many internet technologies and protocols were not designed to support IoT. Many researchers have explored about such type of security issues and design challenges and many open problems in IoT. This paper briefly explains the Application of IoT, Challenges and Issues in IoT, existing methods for providing security solutions and their limitations.**

***Keywords — RFID (Radio-frequency identification),* IoT (Internet of Things), Smart devices**

I. INTRODUCTION

The internet of things (IoT) term has become very popular in recent years. IoT does not have a specific type or standard definition. The IoT word was first discovered in 1998. The IoT means the 24/7 interconnected sensor nodes generating the data to the cloud. The main objective of IoT is to make "A easy and convenient World for human beings" , in which objects will be smart enough so it can sense our need. Based on various application domain, IoT applications can be classified into mainly in five categories such as smart Home automation services, smart medical services, smart city, smart energy and smart enterprise. The many technological advancements in the computer science and electronics field led to an exponential increase in the number of small compact interconnected sensing and computing devices (smart devices). As a consequence, the large number of potential threats and possible there adversely effects against security or privacy of things or an individual has grown rigorously. For giving a large number of reliable services, designers face several challenges in particular, in security and also design issues in architecture of the devices. It is unfortunate that these threats and general privacy issues. This survey briefs about applications and challenges and issues and existing solutions and their limitations.

- Motivations for IoT Issues
- Key Layers of IoT
- Applications IoT
- Issues in IoT.
- Solutions and their limitations.

II. MOTIVATION FOR IOT ISSUES

The IoT issues is the most trending research area now days. As the IoT become very popular in last few years and it is getting implemented in each and every possible field and as the adverse effect of the IoT becomes very cheap and any one can design this compact device. There is no any standard architecture defined for this device to design and the there are no any standard protocols defined for this compact device. So they are large number of the security threats to this smart compact devices. As the devices or the embedded board used for making these compact devices are open source design and ae very vulnerable to the various security attack. There also privacy issues arise as some vendors using the default passwords for this device and so user may or may not changes the passwords and this device get exposed to the attackers. There is also a design related issues occurred as there is no any standard architecture defined for the its architecture. It will be problematic for the other users to understand the architecture of the device. There is also power management issues arises as many of this compact devices are battery powered so the power management for this devices is also an issue.

III. KEY LAYERS OF IOT

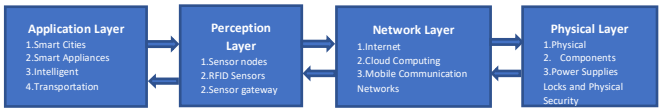

Fig 1. IoT as a layered approach

As shown in the Fig 1 we can divide the IoT in four layers for achieving the objective of creatin IoT [16]

- Application Layer: It has the various services and applications that is provided by the IoT. Applications include such as smart cities, smart home, transportation, utilities and healthcare.
- Perception Layer: It has the different types of sensors technologies like temperature sensor or RFID's which allows device to sense the others entities values according to the type of sensors used.
- Network Layer: This layer includes the network software's and also the physical components such as network nodes and servers and network component which enables the communication. Its main work is to transmit data between devices and from the devices to receivers
- Physical Layer: It is the layer which consists of various underlying hardware components. Power supplies which is the backbone for the networking in IoT devices.

IV. APPLICATIONS OF IOT

There are vast applications exist for the IoT. They broadly divided into five categories: - Smart Home Automation, Smart Medical services, Smart City, Smart energy, Smart Enterprises. Below Tables includes the field of applications and there examples.

SL	Field of Application	Examples of application
1	Smart Home Automation [11]	Smart doors. Smart Surveillance camera which can detect the unusual activities in absence of the owner
2.	Smart Medical Services	Smart health monitoring system
3	Smart City	Auto Traffic signal control. Automated challan of vehicle.
4	Smart Energy	Energy billing on the basis of the energy estimations on the basis of the load delivered by the sensor's nodes
5	Smart Enterprises	Energy and Production & Resources management: Smart farming through accommodating increasingly complex and interconnected farming equipment (Example Heat watch is a cattle monitoring solution that records the activities of each animal
6.	Smart Agriculture	Smart irrigation, infection detection and use pesticides on selected area only, Smart greenhouse management using sensors

V. ISSUES IN IOT AND SOLUTIONS WITH LIMITATIONS

The IoT become so popular as this providing compact solutions to many problems and its very cheap to build. So, the design of the implementation is open and as result it is also open to many security threats. As per there is not any security standard and no vendors are providing the any cryptographic security.

So, there are the following Issues in IoT:

A. Standardization

The Standardization is very important and major challenge to the application design in the IoT devices. It is the main thing of the IoT devices. There are no any such standards defined for the IoT design and for its architecture.[18]

Type	Issue	Solution	Limitation
Architecture	No any standard architecture defined for the IoT devices and lead to many vulnerabilities in devices	Many standardisation bodies are involved in making framework for the IoT	Due to vast range of open source embedded system it is difficult to implement
Protocols	There is no specific protocol for the message communication between the IoT devices	The use of the MQTT and the CoAP protocols for the messaging and	Due to lack of standard protocols it may be not much suitable

B. Loop Holes in Software

There are wide range of vendors available and they are using their own firmware's or open source firmware and they are vulnerable to many known security threats. It can be hacked by hackers. Recently it was

So, to make it less vulnerable the FOTA method that are being used by phone companies and many other vendors for updating the software's regarding the security patches and the loop holes patches. So, it can be used in IoT devices firmware update also to remove the existing loop holes or making it mor secure.[20]

It also has it limitation as that very limited vendors provides the firmware updates and it is not so automated and a user need to update the firmware by checking its own or so it has this limitation.

C. Power Management

The power plays a major role in IoT devices as mainly sensors nodes are battery powered and They are connected to the internet 24/7 and generating the data in fixed interval of time so there may be power needed for 24/7 time. So, where the battery enabled devices are used there a problem arises of recharging those devices.

Type	**Solution**	**Limitation**
Recharging Battery	Gather power from natural resources like solar heat or vibration.	The natural resources have their own limitations
Power Consumption	Limit to the only running critical processes to save the energy consumption.	As Sensors nodes generating data 24/7 so it can utilize power consumption 24/7

D. Scalability

As in the past years the number of IoT devices increase and the data generation by this device also increases and year by year its increasing rapidly and needs the processing and the storage. So the devices should be scalable to this type things and the horizontal scaling can be done or as well as vertical scaling should also be increase.[17]

E. Interoperability

Data sharing is huge now days and it is increasing day by day in very large amount. So, this data can be managed securely. We need this data at various devices and we access this data. So their issues arises on the interoperability of data as the same data is used at various places and accessed. Therefore, standards which include interoperability among these smart devices are needed.[18]

F. Privacy

The privacy is a big concerned now days and we need to ensure the privacy wherever we are putting our data or using our data for making accounts and we need to read their privacy policies first how they are going to use our data. As IoT devices concern it's also generates lots of data and some devices using 3rd party cloud services for saving the data so their privacy concern may arise so where ever the personnel data is used the privacy issues arises.

In IoT we have the following five type of privacy issues Device privacy, Privacy during communication, Privacy storage, Privacy in processing and Privacy in ownership.[17]

G. Security

There many security threats IoT devices as they using the mostly the wireless standard that is Wi-Fi which makes the term smart devices or appliances.

Now the following are the security threats or issue to the IoT as follows

i. Security Issues in the Application Layer

There are security issues present in the application layer due to which the services at the application layer can be compromised and shutdown. Because of this the applications failed to rum the services they are programmed to do and also run authenticated services in incorrect manner. Due to the malicious code attack in this layer causes bugs in application programs code that triggers malfunctioning of an application. As numbers of devices categorised as application level entities arises a very dangerous concern. Common threats to Application layer are:

- Malicious Code attacks: In this type of attack the attacker spread the malicious "worm" in the internet attack embedded devices having a particular OS for e.g. Linux. This type of worms can attack a range of interne enables small devices such as routers at home security cameras. The worm uses a known vulnerability of the software to spread across the internet.
- Tampering node-based applications: There are some attacks that can lead by hackers to exploit the vulnerabilities in the application on this smart device and instal malicious root kits. So, this security design should be tampered resistive or at least tampering avoidable. Some manipulations to the environment can act as threats to this device as the little change in the environment can change their sensors values such like if we have temperature sensors, we can manipulate it to a single continues value by changing the environment of temperature sensor
- No security patches: Same the vendors did not give updates to these compact devices and in case of like nuclear reactors, if there exist a bug in its firmware then it may result in very danger consequences.
- Hacking into the smart meter/grid: A smart meter responsible for sending the usage of a particular user to the provider for the electricity bill and if the usage data is changed then it may loss economy in large amounts and also loss to a particular user if someone changes its value to some high value.

ii. Security Issues in the Perception Layer

Security threats in this layer are at node level because the nodes are combination of different sensors, they are the major targets from hackers, who like to replace the device software with malicious software. In this layer the mainly threats comes from the outsource entities with respect to sensors mainly and data collecting utilities. Common threats are:

- Eavesdropping: The mode of communication between this smart compact device is wireless and through Internet, so these devices are vulnerable to eavesdropping attacks as the smart devices generally left unattended. So, the smart home and smart health domain are compromised in this type of attack to send push notifications to users and try to collect private information.
- Sniffing Attacks: In this the attacker sniffs the data by placing other malicious sensors near the normal sensors. The smart environment is made for the human to detect the physical activity to some accuracy so the insight can deliver so if there is any sniffing of this data can lead to some serious issues.
- Noise in data: Data in this smart device is transferred mainly through the wireless medium so there may be a possibility that the data may consist of the noise. So, this noise may lead to some serious problem or false news.

iii. Security Issues in the Network Layer This layer is highly vulnerable to attacks because it carries a large number of data. This leads to large amount of network congestion. In this layer the most of the security threats issues are is related to integrity and authentication of the data that is transmitted in the network.

Attack by hackers and malicious nodes that compromises devices in the whole network is a big issue. Common threats are:

- DoS (Denial of Service) attack: The devices or any server are flooded with some unusual automated requests from the attackers to a particular service so that that service is not available to use by the users. DoS attacks that may shutdown the transfer of data between smart devices. So, overflow of information is sent to these devices that may lead to the shutdown its processes. Services with lower bandwidth networks lead to life-threatening risks and business loss.
- Gateway Attacks: This type of attack cut off the connection between different sensors nodes and the Internet infrastructure. This attack includes DoS attack or attacks launched in the gateway that results in wrong information's transmitted through the sensors nodes through the Internet. So, it leads to malfunction of the subdomains such vehicular or smart cities.
- Unauthorizes access: Some owners expect that the smart devices are in their physical control when left unsecured. But in actual they are open to all. For example, the pacemakers which is implant in human bodies and any unauthorised access with these devices can lead to many serious issues to health of that person.
- Storage Attacks: The large amount of vital information of users are collected through these devices and stored on the storage device or sent to the cloud's services connected to these devices. Both can be vulnerable to the security threats and can be hacked. The different replication of the data increases the risk of various area of attacks.
- Injecting fake Information: The hackers or attackers can transfer the false data to these smart compact devices through the Internet causing theses system to react inappropriately. This may also be used by the attacker to frame such type of threats.

iv. Security Issues in the Physical Layer This layer is vulnerable to the physical damage of the devices. And there are many security issues present in IoT systems at this layer.

There is great need of new technologies to making safeguard power sources to these devices and physical security methods to prevent the physical damage to this device. Devices needs to be secured against the weather and individuals' perspectives. They also take precaution for the efficient power and make capable of relying on battery power in absence of power failure. Recharge these devices quickly to keep running this smart device.

Common issues are:

- Physical Damage:
  Considering an example in this type of attack is physical devices such as sensors and nodes that can be physically damage by the attackers or by malicious activity. This cause sensors to not work or may lead to permanent damage and may lead vulnerable to other risks of security.
- Environment attacks: Considering a situation in this type issue the sensors are highly effected by the natural phenomenon like heavy rain/snow/ or wind. This cause the sensors to lose its expected ability to sense properly and becomes vulnerable to the other security threats.
- Loss of Power: Sometime these smart devices may become out of power if they are battery enabled devices. In that case the they cause an issue that is denial of service. We can use power saving modes to save the energy. A sleep deprivation attack is enough to prevent the device to go into the proper sleep mode and lead to DoS attack.
- Hardware failure: Theses smart compact
  devices act as the lifeline to any user of it. And they become so dependent on these devices so it is very important that there not occurs any hardware failure. An attacker can send incorrect data and can lead to the failure of some hardware that can lead to serious issues in user's daily life.
- Physical tampering: The embedded chipsets and board are available without any physical covering so it is important to provide physical covering so that can be prevented from the physical tempering of the devices.
- also vulnerable to many security threats no special mechanism for encryption is used by the vendors while creating the IoT solutions. IoT using the existing various solutions combined with the sensors network. So IoT has many security threats as they are existing from long time for the currently used internet.

Layer/Method	Issues it addresses	Solution	Limitation
Perception Layer / Ambient Assisted Living [1]	Safe and secured life style for the elderly people	Keep in Touch (KIT) through smart objects and methodologies like RFID, NFC and CLH (Closed Loop Hierarchy)	This method fails to address security and privacy issues, even though it identifies security, privacy and reliability as the major needs of intended users
Perception layer / Cyber Sensors [2]	Lack of real time data/output from physical objects	Cyber sensors capturing the data from physical objects can be used later to perform actions or real time event response	Few technologies for the sensors do not yet exist
Perception Layer / ASM [3]	Security threats are identified in data integrity and adapts to environmental and censored changes that it identifies by using the security metrics	ASM method has 4 steps, I. Continuous monitoring of Node ii. Analytics and predictive function. iii.Making decision on predicted values iv. Adaptive security models on metrics based. Sensors are analyzed to gather information about devices surrounding and environment	Major limitation is sensors can fall subject to interference from other electronic devices. Another limitation is it do not provide details on the security metrics
Network Layer / Security Middleware [9]	To provide security to intelligent home systems and communication devices	It uses entity identification, secure storage, security audit, data encryption/decryption	Middleware is an upcoming trend; it is not yet widely integrated or widely in use

Network Layer / Authentication and access control [4]	Fixes loop holes in device security and data integrity	A user requests authentication to access a device, things ask for permission to do so from a "RA-Registration Authority" RA approves/denies the request.	Systems are still very vulnerable to the man-in-middle attacks and eavesdropping attacks.
Application layer / DSM [5]	Security metrics for Ehealth information systems	Five elements are proposed that deals with security analysis and policies	It fails to give solution for the identification , collection, computation issues
Application layer / Game Theory [6]	Attacks of various varying in complex devices	Method of attacking systems to develop better security methods	Prototyping is not yet available. So how the system will handle varying complex devices.

So there some issue arises in IoT devices as follows: -

Application Layer / Adaptive Security and Trust Management [7]	A smart system that can a react with the environmental changes	Adaptive learning technique by changing the internal parameters and dynamic change to its architecture	ASTM model has to be validated against dynamic scenarios of application domain and unknown threats
Application Layer / CCM [8]	A security metric model based on risk assessment approach	In this model the security is quantified in terms of incident asset loss	Availability and attainability of the data is a big issue to detect all the security metrics

VI. Conclusion and Future Scope

IoT is going to play a major role in future and its application is everywhere and it using in every area of daily life to make our life easier and comfort. With this comfort there some threats are also exist for this device and we already discussed about various threats at different layers of the IoT. So a standard protocols need to be design by the official bodies. The standard architecture should be defined to avoid the various threats related to the open source design.

The IoT is the future of automation and it is going to change our daily life from morning to night its giving so much comfort. This includes many security threats and privacy issues and this need to be address.

So, in future the IoT may include such devices which can actively participate with users and can make their work with ease.

we believe this survey will give some contribution current going threats for IoT, by documenting the various issues and security attacks in various layers and it will motivate the researchers in developing new protocols and design or architecture to address security issues present Internet of Things (IoT).

REFERENCES

[1] A.Dohr ., R.Modre-opsrian ., M.Drobics, D.Hayn.,G.Schreier : The Internet of Things for ambient assisted living , Seventh International Conference on Information Technology ,pp.804-809 (2010).

[2] Huansheng Ning and Hong Liu.,Laurenct T Yang , Cyberentity security in the internet of Things, Vol 46,No.4 pp.46-53 (April 2013).

[3] Reijo M Savola., Habtamu Abie ., Markus Sihvonen:Towards metrics driven adaptive security management in e-health IoT applications, Proc of the 7th International Conference on Body Area Networks, pp.276-281 (2012).

[4] .Lui., Xiao., Chen : Authentication and access control in the Internet of Things ,32nd International Conference on distributed computing systems workshop (ICDCSW) ,pp.588-592 ,(2012).

[5] Kozlo et al: Security and Privacy Threats in IoT architectures, Proc of the 7th International Conference on Body Area Networks, pp.256-262 (2012).

[6] Abie H., and Balasingham :RISK based adaptive security for smart IoT in e-health , Proc of the 7th International Conference on Body Area Networks, pp.269-275 (2012).

[7] Abie H., and Balasingham I.: Adaptive security and trust management for autonomic message oriented middleware, IEEE 6th Intl conference on mobile Adhoc and Sensor Networks (MASS'09) pp.810-817 (2009).

[8] Wei B Weissmann O ., and Dressler F., : Comprehensive and comparative metric for information security , in Proc of IFIP – International Conference on Telecommunication security ,modelling and analysis ,pp 1-10 (2005).

[9] Li You Guo., Jiang Ming Fu: The reinforcement of communication security of internet of things , International Symposium on information science and Engineering , pp531-534 (2010).

[10] Taj Uddin Sheikh, Tapan Kumar Hazra, Hasina Rahman "Countermeasure of Attack Vectors using Signature-Based IDS in IoT Environments", (2019)

[11] Chao Lin , Debiao He , Neeraj Kumar , Member, IEEE, Xinyi Huang , Pandi Vijayakumar , and Kim-Kwang Raymond Choo "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes", IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 2, FEBRUARY 2020

[12] Muneer Bani Yassein, Ismail Hmeidi, Omar Meqdadi, Fatimah Alghazo Bayan Odat , Omar AlZoubi, Ayat Smaira "Challenges and Techniques of Constrained Application Protocol (CoAP) for Efficient Energy Consumption", 2020 11th International Conference on Information and Communication Systems (ICICS)

[13] Rahul Shokeen, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Sami Azam, Mirjam Jonkman, Mamoun Alazab, "Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things", 2019 Cybersecurity and Cyberforensics Conference (CCC)

[14] Calebe Micael de Oliveira Conceic ,ao, Ricardo Augusto da Luz Reis, " Security Issues in the Design of Chips for IoT", 978-1-7281-5503-6/20/$31.00 ©2020 IEEE

[15] Riddhi A. Joshi, Hiral K. Thakar, Ashwin Dobariya, "Internet of Things : Application and Challenges", 6th International Conference on Computing for Sustainable Global Development (INDIACom), 978-93-80544-34-2$31.00 c 2019 IEEE

[16] Mahesh Kavre, Aditya Gadekar, Yash Gadhade, " Internet of Things (IoT): A Survey", 2019 IEEE Pune Section International Conference (PuneCon)

[17] Sachin A. Goswami Bhargav P. Padhya Dr. Ketan D. Patel Research Scholar,"Internet Of Things: Applications, Challenges And Research Issues", Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019) IEEE Xplore Part Number:CFP19OSV-ART; ISBN:978-1-7281-4365-1

[18] Nickson M. Karie, Nor Masri Sahri, Paul Haskell-Dowland, " IoT Threat Detection Advances, Challenges and Future Directions", 2020 IEEE Workshop on Emerging Technologies for Security in IoT (ETSecIoT)

[19] Syed Rizvi, Joseph Pfeffer, Andrew Kurtz, Mohammad Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering

[20] Wattana Viriyasitavat, Zhuming Bi, "Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective", IEEE Internet Of Things Journal, vol. 6, no. 5, 2019