Challenges and Ongoing Researches for IOT (Internet of Things): A Review

[1]Anurag Tiwari, [2]Harishchandra Maurya
M.Tech. Scholar[1], Assistant Professor[2]
[1]Computer Science and Engineering Department
[1]Bhagwant University, Ajmer(Rajasthan), India.

***Abstract*- Internet of Thing is the emerging technology in the field of Information technology especially in networking field. Where networking may consist of the internal or external network. The Internet is the backbone of the IOT. And IOT is the technology where electrical, mechanical objects may be connected to the internet to control them remotely from anywhere of the world. Useful data and information will be swapped by billions of devices and services and these services and devices will be powered by Internet of Things. As IOT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. And the things which are connected to the internet may have many security concerns. Due to security and privacy related concerns, IOT could not set himself as a reliable technology. Because of these two issues, wide adoption of Internet of Things could not be occurred. As we know that IOT is still in its maturing state so security is the main concerns of this emerging technology. This is a review paper where we discuss on ongoing security researches in the field of Internet of the things as well as aspects of security.**

***Keywords*- IOT, Security**

I. INTRODUCTION

We are living in information revolution era. Now the ordinary devices like mobile phones, televisions, cars etc are rapidly transforming into smart phones, smart television and smart cars etc. And internet is playing an important role to making things smart. The concept of internet of things is basically based on internet and things means where things are connected to the internet. Now a days the concept of smart cities, smart hospital, wireless sensing network, home automation are coming into existence where IOT is the backbone of these application. All these application are somewhere based on the IOT and these applications must make a communication path to transmission of the data which may lead many security concerns. Internet of Things basically used internet to connect all devices to control them by users so risks factors may have increased during communication of devices and users because they transmit lot of data to establish a proper connection.

II. CHALLENGES IN IOT-

Energy Efficiency And Robustness-

Internet of Things shows a new way in computing where the devices are connected to the internet and having communication with each other. Because these devices are generally thought to be wireless, small and cheap, in other words not very reliable, so it is necessary to address the robustness problems in IOT. Fault tolerance is almost not possible in IOT.

The IOT devices may be desperate, and different devices have completely different capabilities and serve completely different functions (they have different sensors). Because of these difference in IOT devices it is difficult to measure energy consumption of devices.

IOT devices are works over the internet and these are wireless that is why IOT systems need to be energy efficient and because these devices are generally cheap so IOT systems need to be robust. [1]

Standardization of IOT devices-

As we know that IOT will have countless interconnected devices. And these devices will exchange information, communicate with each other over the internet and perform coordinated task. And IOT devices may be manufactured by multiple manufactures from all across the globe with variety of categories of these devices. So it is necessary to provide a common communication technology and standard for all IOT devices. [2][3][4]

Data collection, protection and privacy-

The main principle of IOT is to make individual’s life convenient and enhance the efficiency of employees of corporate world. The collection of data of individuals and corporate world’s will improve the our decision taking power and will help us make smarter decisions. But convenience bring some bad impact so data collection will have some security and privacy concerns. If data collected by connected devices is compromised it will undermine trust in the IOT.

And Apart from above when everything will be connected to the internet, everyday household items could potentially be exploited by cybercriminals to gain access to these devices. Sensors send data to the multiple information processing subsystem over the internet where definite implementation of encryption mechanism is required to maintain the data integrity at the layer of information processing. Also, security mechanisms must be devised and applied to ensure the secure transfer of the transmitted data and guard against unauthorized interference or misuse of the data being transmitted across the network.
[5][6][7].

Big Data-

We have to address some of the more unpleasant aspects of the Internet of Things, mainly that of data security. The more connected we become, the more intrusion we're likely to see. And as far as the IOT is concerned, it may already be too late to provide a secure environment. This may be seen as a pessimistic view by some, but one thing most people can agree on is that the IOT has some major security problems to address. All the more pressing is the fact that we're looking at the number of IOT devices to reach up to 50 billion by the end of the decade. All of these devices use data — massive amounts of data that can detail some very private information. That means tremendously personal data is at risk of theft or leaking. Those industries that manufacture IOT devices may want to ensure that information is kept private, but for now, it appears they view security and big data problems as a secondary issue. [8][9]

III. WHY SECURITY FOR IOT?

- In total, there will be 34 billion devices connected to the internet by 2020, up from 10 billion in 2015. IOT devices will account for 24 billion, while traditional computing devices (e.g. smartphones, tablets, smartwatches, etc.) will comprise 10 billion.
- Nearly $6 trillion will be spent on IOT solutions over the next five years.
- Businesses will be the top adopter of IOT solutions. They see three ways the IOT can improve their bottom line by 1) lowering operating costs; 2) increasing productivity; and 3) expanding to new markets or developing new product offerings.
- Governments are focused on increasing productivity, decreasing costs, and improving their citizens' quality of life. We forecast they will be the second-largest adopters of IOT ecosystems.
- Consumers will lag behind businesses and governments in IOT adoption. Still, they will purchase a massive number of devices and invest a significant amount of money in IOT ecosystems. [10]

IV. ONGOING RESEARCHES ON IOT SECURITY-

Secure Protocols for IOT and IOT secure Layers-

As per the author of this research "Building interconnected and interoperable smart objects requires the adoption of standard communication protocols. At network layer, an IOT node can secure data exchange in a standard way by using the Internet Protocol Security (IPsec) IPSec can provide confidentiality, integrity, data-origin authentication and protection against replay attacks, for each IP packet (it works at network layer). These security services are implemented via two IPSec protocols: Authentication Header (AH) and Encapsulated Security Payload (ESP). The AH is responsible for providing integrity, data-origin authentication and anti-replay capabilities, while ESP is responsible for providing confidentiality, authentication and integrity." [11] [12]

Enhancing Security in lOT based Home Automation using Reed Solomon Codes-

The proposed Home automation system based on lOT uses Reed Solomon codes where authors mitigate risks and thus enhancing security by providing error correction scheme both in the communication channel as well as the data store. A Reed-Solomon (RS) code is an error-correcting code first described in a paper by Reed and Solomon in 1960. Since that time they've been applied in CD-ROMs, wireless communications, space communications, DSL, DVD, and digital TV. RS encoding data is relatively straightforward, but decoding is time consuming, despite major efficiency improvements made by Berlekamp and other during the 1960's. Only in the past few years has it become computationally possible to send high-bandwidth data using RS. [13] [14]

Privacy Preservation In Cloud-Based IOT Applications

In this research the author has contributions take the form of a *conceptual Reference Architecture* for building a security, privacy, and trust management protocol (SPTP) that is capable of protecting private data at the time of disclosure or collection, in-transit, at-rest and for the life of a private data element even when it crosses the boundaries of the original system to be consumed by another system. In addition, we propose a *logical Reference Architecture* for building cloud-enabled IOT applications.
The authors also propose a Secure, Private and Trustworthy Protocol (SPTP) with an associated seal that will be readily recognizable by end-users in various online and ubiquitous computing settings. The standard seal is to be used in all systems (including cloud services, mobile devices and applications, sensors, gadgets, web sites, and more) that wish to identify themselves as being secure, private and trustworthy to end-users and other entities. [15] [16]

Authentication and Authorization for Internet of Things-

The author identifies significant resource requirements for the DTLS handshake when employing public-key cryptography for peer authentication and key agreement purposes. These overheads particularly hamper secure communication for memory-constrained devices. To alleviate these limitations, we propose a delegation architecture that offloads the expensive DTLS connection establishment to a delegation server. By handing over the established security context to the constrained device, our delegation architecture significantly reduces the resource requirements of DTLS-protected communication for constrained devices. Additionally, our delegation architecture naturally provides authorization functionality when leveraging the central role of the delegation server in the initial connection establishment. Hence, in this paper, author present a comprehensive, yet compact solution for authentication, authorization, and secure data transmission in the IP-based IOT. The evaluation results show that compared to a public-key-based DTLS handshake our delegation architecture reduces the memory overhead by 64 % computations by 97 %, network transmissions by 68 %. [17] [18]

Data Encryption for Internet of Things-

The author has given an excellent way of encryption for IOT which is used FPGA for the implementation because of several reasons. FPGA is cheap, easy to implement, reprogrammed, has high speed and has a good level of security. This research is focused on performances and implementation of blowfish algorithm. The performance measure of encryption algorithm schemes conducted changing round fiestel and changing key size. The performances parameters that were discussed are encryption time, FPGA implementation resource used, avalanche effect, and throughput. [19]

Wireless Sensor Networks-

Wireless sensor network plays an important role in IOT, the issue causing in wireless sensor networks are false node, node modification, DDOs attacks, node malfunction, message corruption, traffic analysis, spoofed attacks, skin hole attacks, Sybil attacks, worm hole attacks in wireless sensor networks. Authentication, cryptographic algorithms can’t be implemented on wireless networks because of constrained resources, low computational power. There are many security approaches which are providing security for wireless sensor networks. [20]

V. CONCLUSION-

So by this paper we discuss the present IOT challenges and issues on IOT security. We will also discuss the design guidelines to be considered while designing any solution for the IOT.

VI. ACKNOWLEDGMENT-

I would like to pay my respect and thanks to all authors and researchers whose references I have been used in this survey paper. Without studying and using references of mentioned research papers, it was impossible for me to prepare this survey paper. Thanks again to all researchers.

REFERENCES-

[1] Cristian Chilipirea, Andrei Ursache, Dan Octavian Popa, Florin PopEnergy efficiency and robustness for IOT:
building a smart home security system 2016 IEEE pp.43-48

[2] Shrivastava Vandana Jaiprakash,” IOT: Challenges in the standardization of IOT communication”, 2015 IJEDR,pp.1283-1289

[3] https://datafloq.com/read/internet-of-things-IOT-myths-and-facts/1042

[4] https://www.iso.org/news/2016/09/Ref2112.html

[5] https://securingtomorrow.mcafee.com/business/3-key-security-challenges-internet-things/

[6] Ratnam Dodda, Dr. J. Rajendra Prasad, Venugopal Gaddam, Dr.B.V. Subba Rao,” The Evolution of Internet of Things (IOT) and its Impact on Existing Technology” ”IJSTE January 2016,pp. 96-103

[7] Sathish Alampalayam Kumar 1 Tyler Vealey1 Harshit Srivastava,” Security in Internet of Things: Challenges, Solutions and Future Directions” 2016 49th Hawaii International Conference on System Sciences pp.5772-5781

[8] http://www.dataversity.net/internet-things-big-data-data-security-problems

[9] K.R.Kundhavai1, S.Sridevi2 IOT and Big Data- The Current and Future Technologies: A Review International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, January- 2016, pg. 10-14

[10] http://www.businessinsider.com/IOT-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2?IR=T

[11] Secure Layers Based Architecture for Internet of Things Dhananjay Singh, Gaurav Tripathi, Antonio Jara 2015 IEEE

[12] Jan Henrik Ziegeldorf1∗ , Oscar Garcia Morchon2 , and Klaus Wehrle Privacy in the Internet of Things: Threats and Challenges Security Comm. Networks 2013

[13] Idris Afzal Shah,Faizan Amin Malik, Syed Arshid Ahmad," Enhancing Security in loT based Home Automation using Reed Solomon Codes" 2016 IEEE, pp.1639-1642

[14] https://www.cs.duke.edu/courses/spring10/cps296.3/rs_scribe.pdf

[15] Ivor D. Addo, Sheikh I. Ahamed, Stephen S. Yau, Arun Buduru," REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD-BASED IOT APPLICATIONS" International Journal of Services Computing, Oct.-Dec. 2014 pp.65-78

[16] Syed Abdul Muqtader Razvi, Abdullah Al-Dhelaan, Mznah Al-Rodhaan and Riman A. Bin Sulaiman IOT Cloud-Sensor Secure Architecture for Smart Home *Int'l Conf. Security and Management | SAM'15 Pp243-249*

[17] Sanaz Rahimi Moosavi∗, Tuan Nguyen Gia1, Amir-Mohammad Rahmani , Ethiopia Nigussie1 , Seppo Virtanen , Jouni Isoaho , Hannu Tenhunen SEA: A Secure and Efficient Authentication and Authorization Architecture for IOT-Based Healthcare Using Smart Gateways ANT 2015 pp.452 – 459

[18] Ren´e Hummen_, Hossein Shafagh{, Shahid Razaz, Thiemo Voigtzx, Klaus Wehrle_," Delegation-based Authentication and Authorization for the IP-based Internet of Things"2014 IEEE pp.284-292

[19] Kurniawan Nur Prasetyo,Yudha Purwanto, Denny Darlis," An Implementation of Data Encryption for internet Of Things Using Blowfish Algorithm On FPGA" 2014 IEEE, pp.75-79

[20] Rodrigo Roman and Javier Lopez Integrating wireless sensor networks and the internet: a security analysis Internet Research Vol. 19 No. 2, 2009pp. 246-259

BIOGRAPHIES

1. Anurag Tiwari is a M.Tech. student at Bhagwant University, Ajmer, Rajasthan(India). Anurag's research interests are focused on security and privacy issues in IOT.

2. Harishchandra Maurya is an Assistant Professor at Bhagwant University, Ajmer, Rajasthan(India). He has a numbered of published papers on various conferences as well as journals.