IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102033 |

A Review Paper on IOT's Research Issues and New Challenges

Yogendra Kushwaha[1], Neha Maurya[2], Awadhesh Kumar Maurya[3]

Guest Faculty, Department of Computer Science & Engineering, MCAET, Ambedkar Nagar U.P., India [1]

B.Tech. Student, Department of Computer Science & Engineering, MCAET, Ambedkar Nagar U.P., India [2]

Assistant Professor, Department of Information Technology, IET, DR. RML Avadh University, Ayodhya U.P., India [3]

ABSTRACT: Internet of Thing is the come up technology in the field of Information technology mainly in networking field where networking may consist of two types of networks i.e. the internal or external network. The Internet is the spinal cord of the IOT. And IOT gives a technology where electrical, mechanical objects may be connected to the internet and anyone can control them from anywhere of the world. All useful data and information will be swapped by billions of devices and devices will be powered by Internet of Things. As IOT systems will be pervasive, different types of security and privacy issues will arise. Those things which are in connection with the internet may have different security concerns. Due to different security and privacy related concerns, IOT could not set itself as a reliable technology. Because of these basic two issues, wide adoption of Internet of Things could not be occurred. As we can see that IOT is still in its evolving state so security is the main point of this emerging technology. This is a review paper where we are trying to discuss on ongoing security and research challenges in the field of Internet of the things.

KEYWORDS: IOT, IOT Security.

I. INTRODUCTION

Nowadays as we can see we are 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 a crucial role to making all electric gadgets smart. The basic concept behind the internet of things is that on the basis of internet and things means where different things are connected to the internet. Currently the concepts of smart cities, smart hospital, wireless sensing network, Home automation are coming into existence where IOT is the spinal cord of these application. Different application are somewhere based on the IOT and their applications must make a communication path of transmission of the data which may lead many security issues. Internet of Things basically used internet to connect all devices to control them by users. 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 world where many devices are connected to the internet and having communication with each other with the help of particular application. 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 lacking, 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 different manufacturers from all across the globe with variety of different categories of these devices. Hence it is necessary and crucial to provide a common communication technology and standard for all IOT devices [2][3][4].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102033 |

Data collection and privacy-

The main aim of IOT is to make individual's life comfortable 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 comfort bring some bad impact so data collection will have some efficient ways to reduce security and privacy concerns. If data collected by different connected devices is compromised then it will undermine trust in the IOT.

Apart from above when everything will be connected to the internet, everyday household items could potentially be utilized by cybercriminals to gain access to these devices. Sensors send data to the multiple information processing sub system 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 formulate and applied to ensure the secure transfer of the transmitted data and protect against unauthorized interference or any misuse of the data being transmitted across the network.
[5][6][7].

Data-

We have to understand and work with the security aspects of the Internet of Things. The more connected we become, the more encroachment we're likely to see. As far as the IOT is concerned, it is very necessary to provide a secure environment. This may be seen as a pessimistic view by some, but one thing most users can agree is that the IOT has some major security issues which needs to address very efficiently. It creates a remote environment for accessing the data and it has been used in many real-time applications such as smart cities, smart homes, smart energy, smart agriculture, smart industry, and smart living. IoT has its characteristics which provide and enhanced interconnectivity, safety, heterogeneity, enormous scale, dynamic changes, and connectivity. Different IoT devices use data — massive amounts of data that may have some very private information. That means broadly personal data of any user is at risk of theft or leaking. Different industries that manufacture IOT devices may want to ensure that information is kept private, but for now it seems they face security and big data problems as a secondary issue.[8][9].

III. WHY SECURITY IS A CONCERN FOR IOT?

- As we have seen, about 34 billion devices connected to the internet by 2020, up from 10 billion in 2015. IOT devices will account for 44 billion, while traditional computing devices (e.g. smart phones, tablets, smart watches, etc.) will comprise 10 billion [10].
- Nearly $10 trillion or may be more than that will be spent on IOT solutions over the next five years.
- Businesses are the top adopter of IOT solutions and it will continuously increase in future because of e-marketing etc. There are three ways the IOT can improve their bottom line by1) lowering operating costs;2) increasing productivity; and 3) expanding to new markets and provide security to the users.
- Governments are continuously focusing on increasing productivity, decreasing costs, and enhancing their citizen quality of life. We predict they will be the second-largest adopters of IOT ecosystems.

IV. UNDERWAY RESEARCHES ON IOT SECURITY

Secure Protocols for IOT -

According to the author of this research "Building interconnected and interoperable smart objects needs the adoption of a standard communication protocols. At network layer phase , an IOT node can secure data interchange in a standard way by using the Internet Protocol Security (IP sec) IPSec can provide confidentiality, integrity, data-origin authentication and protection against different attacks, for each IP packet (it works at network layer).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 Applications-

The proposed Home automation system based on lOT uses Reed Solomon codes where authors reduce risks and thus enhancing security by providing error correction scheme both in the communication channel as well as the data store.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102033 |

A Reed-Solomon(RS) code is an error-correcting code and was first described in a paper by Reed and Solomon in 1960. Since that time they've been highly applied in CD-ROMs, wireless communications, space communications, DSL, DVD, and digital TV.RS encoding data is relatively straight forward, 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]

Cloud-Based IOT Applications Privacy-

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 trust worthy to end-users and other entities[15][16].

Authentication and Authorization in IoT-

Here it identifies significant resource requirements for the DTLS handshake when applying public-key cryptography for peer authentication and key agreement purposes. These overheads hamper secure communication for memory-inhibited devices. To ease these limitations, we propose a envoys architecture that discharge the expensive DTLS connection establishment to a delegation server. By handing over the established security context to the strained device, our delegation architecture significantly reduces the resource requirements of DTLS-protected communication for constrained devices. In addition to that, 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 solid 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 bring down the memory overhead by 64% computations by 97%, network transmissions by 68%[17][18].

Data Encryption for IoTs-

The author has given a better way of encryption for IOT which is used FPGA for the implementation because of different reasons. FPGA is very cheap, easily implemented, reprogrammed, has high speed and has also a good level of security. This research is basically focused on performances and methodologies of blowfish algorithm. The performance measure of encryption algorithm schemes conducted changing round festal 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 a crucial 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.Cryptographic algorithms can't be implemented on wireless networks because of its constrained resources, low computational power. There are many security approaches which are providing security for wireless sensor networks [20].

V. CONCLUSION

IoT has been gradually bringing a sea of technological change in our daily lives, which in turns helps in improving our life simpler and comfortable, through various technologies and applications. There are different applications of IoT into all the domain including medical, transportations, educations etc.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102033 |

REFERENCES

1. Cristian Chilipirea, Andrei Ursache, Dan Octavian Popa, Florin PopEnergy efficiency and robustness for IOT:buildingasmarthome securitysystem2016IEEEpp.43-48
2. ShrivastavaVandanaJaiprakash," IOT:ChallengesinthestandardizationofIOTcommunication",2015IJEDR,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. RatnamDodda,Dr.J.RajendraPrasad,VenugopalGaddam,Dr.B.V.SubbaRao,"TheEvolutionofInternetofThings(IOT)and itsImpactonExistingTechnology""IJSTEJanuary2016,pp.96-103
7. SathishAlampalayamKumar1TylerVealey1HarshitSrivastava,"SecurityinInternetofThings:Challenges,SolutionsandFutureDirections" 2016 49thHawaiiInternationalConference onSystemSciencespp.5772-5781
8. http://www.dataversity.net/internet-things-big-data-data-security-problems
9. K.R.Kundhavai1,S.Sridevi2IOTandBigData-TheCurrentandFutureTechnologies:AReviewInternationalJournalofComputer Science andMobile 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. SecureLayersBasedArchitectureforInternetofThingsDhananjaySingh,GauravTripathi,AntonioJara2015IEEE
12. JanHenrikZiegeldorf1∗,OscarGarciaMorchon2,andKlausWehrlePrivacyintheInternetofThings:ThreatsandChallengesSecurityComm. Networks2013
13. IdrisAfzalShah,FaizanAminMalik,SyedArshidAhmad,"EnhancingSecurity in loTbasedHomeAutomationusingReedSolomonCodes" 2016IEEE,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, ArunBuduru,"REFERENCE ARCHITECTURES FOR PRIVACYPRESERVATION IN CLOUD-BASED IOT APPLICATIONS"International Journal of Services Computing, Oct.-Dec. 2014pp.65-78
16. Syed Abdul MuqtaderRazvi, Abdullah Al-Dhelaan, Mznah Al-Rodhaan and Riman A. Bin Sulaiman IOT Cloud-SensorSecureArchitectureforSmartHome*Int'lConf.Security andManagement|SAM'15Pp243-249*
17. SanazRahimiMoosavi∗, Tuan Nguyen Gia1, Amir-Mohammad Rahmani , Ethiopia Nigussie1 , Seppo Virtanen , JouniIsoaho , HannuTenhunen SEA: A Secure and Efficient Authentication and Authorization Architecture for IOT-Based HealthcareUsingSmartGatewaysANT2015pp.452–459
18. Ren´eHummen_, Hossein Shafagh{, ShahidRazaz, Thiemo Voigtzx, Klaus Wehrle_," Delegation-based Authentication andAuthorizationfor the IP-basedInternet ofThings"2014IEEE pp.284-292
19. KurniawanNurPrasetyo,YudhaPurwanto, Denny Darlis," An Implementation of Data Encryption for internet Of ThingsUsingBlowfishAlgorithmOnFPGA" 2014IEEE,pp.75-79
20. Rodrigo Roman and Javier Lopez Integrating wireless sensor networks and the internet: a security analysis Internet ResearchVol. 19No.2, 2009pp.246-259

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details