

SECURITY COMMUNICATION AND PROTOCOLS TOWARDS INTERNET OF THINGS

Yeshwanth Valaboju¹

¹Technical Manager, Rigved Technologies Pvt. Ltd, India

Abstract:- IoT gadgets are made use of in a lot of treatment fields that make the users' daily life much comfier. These tools are utilized to pick up temperature, blood pressure, as well as sugar degree etc., which are utilized to examine the health and wellness disorder of the patient. Communicating the collected relevant information to the medical professional, making an exact choice on the data collected as well as alerting the person is the challenging duty in the IoT. In this particular job, An IoT located Individual Wellness Tracking Body making use of Arduino is suggested to accumulate the demanded criteria and also assess the data secured coming from the sensing unit devices. PHMS with Arduino also gives the notifications to the client along with achievable preventative solutions to become performed through all of them. This device proposes the patient with medical care as well as the following step to becoming observed if of essential condition. The mix of IoT along with Arduino is the new means of offering Internet of Things in the Healthcare Surveillance body of people. Arduino Uno board picks up data from the sensing units and also move wirelessly to the IoT site.

Keywords: Internet of Things, security communication, protocols.

I. INTRODUCTION

Smart devices. Mobile phone. Smart cars. Smart homes. Smart metropolitan area areas. A brilliant whole world. These thoughts have been truly allowed for several years. Achieving these intendeds invites reality been examined, to time, through many various along with frequently disjoint study neighbourhoods. 5 such visible review locations are actually: Internet of Things, Mobile Pc, Pervasive Handling, Wireless Sensing Device Networks, in addition to quite most lately, Cyber-Physical Units. Having indicated that, as technology in addition to solutions progression in each of these locations there remains in truth a bring up the overlap and also merging of suggestions and also additionally research study concerns. Slim significances of each of these regions are truly no more proper. Moreover, a study in IoT, PERSONAL COMPUTER DEVICE, MC, WSN and additionally CPS often trust funds embedding technologies like real-time pc, artificial intelligence, security, personal privacy, clue handling, major records, as well as similarly others. Ultimately, the creative eyesight of the planet requires a significant volume of computer science, pc system style, and

also power design. Greater interactions among these regions are heading to accelerate enhancement.

Internet of Things (IoT) has surfaced safely as a so much more prospering place to share this sort of brand-new present-day innovation. It resides not the quite very first present-day innovation in this particular market, however, additionally, the cloud computing technology invites fact been made use of to stand for the anywhere computer planet. In the 7th in the set of ITU Internet Highlights initially, it was in truth delivered in 1997 under the tag "Challenges to the System" [1], and also it was first coined with Kevin Ashton in the RFID publication 1999 [2], In 2005 this headline was come to be "Internet of things". The sight of IoT relying on Kevin's mindset was actually to make it achievable for on-line devices to proliferate their information concerning real-world objects via the internet. Over the last handful of years, some most of the IoT suggested styles are capitalized on, internet semantic to upload details through the social networks; as a case, the Apple iPhone has given service is Nike + iPod to tape information and likewise submitted it on the socials media as well as the social networking sites unit friends

[3] Among the absolute most detectable and also reliable on the web device remains, in reality, the Internet of Things. It connects to the Internet together with various picking up units in addition to similarly operators, also, to assist to get direct communication in between individuals and also things. The key future of the Internet looks that. The quantity and also likewise range of devices have enhanced quickly, Together with the durability of the IoT market, particularly in previous opportunities. The IoT devices discuss a comparable structure kind. Under this construct, each appearance (side, middleware, along with use) provides its own incredibly own selection of security dangers that need to be taken into account. Moreover, Sizable combos in development sources produce IoT security a challenging concern to take care of. As a result, it will support their nourishing as well as also potential product versions to grow a distinctive security variety for IoT devices. IoT, like a lot more level of sensitivities and also additionally security hazards, gives driving security challenges. It additionally needs new and also additionally smarter IoT security procedures, primarily methods capable of handling complex, random as well as additionally usually misaligned threats on an array. On top of that, linked devices possess an upright impact on the way of livings of people, brand innovations along with protocols demand a unique category of security threats as well as an ideal security structure that might minimize security challenges in connection with individual privacy, files integrity, as well as IoT source. Cyber-attacks targeting it are cultivating as IoT devices end up being popular. In addition to these assaults, each in the home and also around the entire world, create remedy and also function problems, intelligence voids, and also additionally affordable harm, interrupting monetary progression and also likewise the protection and also security alongside the security of normal jobs. Cyber-attacks on IoT devices result in economic in addition to a social problem, social understanding besides the demand for IoT device security is heading to a lot more widen. A massive quantity of info builds as a result of the Internet of Things remains in truth the main issue to be taken care of, different other challenge includes the law of the existing unit design that is incapable to manage real-time at risk therapies utilizing IoT, subsequently, Program treatment Described Media is depended on ahead to be an essential system construct for such techniques. This paper's products are mosting likely to be teamed up as

adhering to part 2 offers easy information concerning security components, region 3 discloses IoT quantities and likewise, security cinemas, section 4 Security mechanisms for IoT services, region 4 clarifies IoT protocols as well as communication, as well as additionally lastly, location 5 supplies a recap and also likewise suggestions for achievable standards for an evaluation relating to IoT protocols.

Truly, the study of IoT contrasts based upon that you chat, but officially, may be defined as a lively worldwide body system industrial locations together with self-configuration and likewise interoperable communication. Just, IoT indicates the ability to create whatever around our supplier beginning along with (i.e. Devices, Devices, Cellular telephone and also Autos) also (Cities as well as additionally Roadways) are anticipated to be linked to the Internet in addition to intelligent actions and also thinking about the visibility of the type of liberty and also individual personal privacy. Alternatively, the IoT setting contains a sizable significant amount of the different objects/things that may be identified in to set of kinds only; i) Things chargeable electric batteries things: the total most of all of them are mobiles (e.g. Notebook, tablets along with cellular phone), as well as furthermore ii) Things are non-rechargeable things: these things are corrected originating from the adaptability aspect of view [4] Commonly, IoT components 3 significant essential needs are in fact: the initial, a communal understanding of the scenario of its individuals and also add their uses. The second thing is of all, software type as well as furthermore widespread communication systems to cope with and also operation contextual appropriate facts, and also finally, the analytics details in IoT that choose personal as well as also smart actions [5] Considerably, might be presented the pointer idea of IoT is making certain the communication in between everything stemming from anywhere at any time making use of context-aware treatments. As needed to have, IoT has depended upon RFID along with picking up system modern innovations in the asks for. As an instance, IBM carrier used IoT in Norwegian Ocean oil systems, using releasing sensing units at seabed that reside in truth utilized to pick up legit applicable information to decide on a strategy in the ocean [3] Conversely, the IoT specifying like a significant quantity of devices having to deal with the assortment of challenges which substantially determine their performance a variety of each one of each of them dominate

and also others, are in simple fact distinct; the paper divides these challenges right into pair of kinds, especially, i) General challenges: that feature prominent challenges in between IoT and additionally conventional device like communication, variety, QoS, scalability, virtualization, info expedition as well as likewise security; and ii) Special challenges: like RFID along with WSN.

II. LITERATURE SURVEY

[1]: This paper examines the present evaluation of IoT, essential making it viable for modern technologies, key IoT makes use of in industries and also identifies research study trends as well as additional challenges. A key add-on of the evaluation paper is in fact that it recaps the existing stylish IoT in industries methodically.

[2]: This paper provides the framework for realizing electric energy reliable intelligent online on cordless picking up device physical bodies and also individual task discovery. Their task is based on the tip that many of the personal tasks in your house associated with a selection of electric property appliances that are truly essential to perform these work. Consequently, they display exactly just how it is feasible to realize the buyer's existing activity using checking his rough device- amount energy application. This link in between obligations and also energy residence appliances makes it practical to realize devices that can be discarding energy in the house. Our unit is dealt with in 2 parts. On one palm, the task outlook framework is responsible for observing the consumer's located activity based on his power consumption.

[3]: This paper checks out the existing concentrate on occupancy security in addition to likewise multi-modal records combo approaches for brilliant office domestic or even commercial buildings. The aim is in fact to prepare a platform for a feasibility study to utilize the Spatio-temporal reports got coming from many of a variety of IoT devices like heat level observing units, security digital camera, as well as RFID tags that may reside presently reliable in the styles.

[4]: This paper centres particularly on an affable IoT device that, while still being instead of a considerable design, are found out through their certain app domain name. Urban IoTs are created to assist the Smart Location dream. This targets making use of

the most ideal state-of-the-art communication developments to assist added-value services for the management of the area as well as for the consumers. This paper subsequently utilizes a comprehensive poll of the making it possible for current time innovations, protocols, as well as additionally developing for an affable IoT.

[5]: This paper delivers a summary of the Internet of Things (IoT) along with convenience on allowing developments, protocols, in addition to also functionality issues The IoT is made it possible due to the very most updated progressions in RFID, clever getting devices, communication modern-day modern technologies, and additionally Internet protocols. The vital facility is really to have brilliant sensing units team upright without particular engagement to provide an all-new training of functions. The existing change in the Internet, smartphone, as well as machine-to- manufacturer innovations might be thought about as the incredibly first phase of the IoT. In the taking place years, the IoT is expected to link unique present-day technologies to make it possible for new functions using linking considerable items along with each other on behalf of fantastic decision making. This paper gives a matching resource of the IoT. Then supply a recap of some focused particulars that panic the IoT enabling modern innovations, protocols, and also likewise makes use of. Examined to other study data in your service, our goal is truly to provide an added comprehensive rundown of the downright most suitable protocols as well as likewise therapy conditions.

III. ARCHITECTURES AND DESIGN

A scaleable and respectable concept is heading to develop the groundwork for the prospective advancement of IoT. The style requires to deal with the new standards of IoT and also show the challenges specified in Location II. This Area covers the layout endorsement style IoT-A, besides 2 fledged designs developed in the work BETaaS as well as OPENIoT.

A.IoT-A

The IoT Design Promotion Design is not an IoT design by definition, but a set of finest practices, manual- pipelines, as well as additionally a starting bring about generate certain IoT layouts. It provides a building endorsement style marketing the interoperability of IoT devices. It additionally supplies the

information, including resolution, looks for, in addition to looking for things, for the actual assimilation right into the remedy level.

The LIMB Improve illustrates the actions to make concrete IoT designs coming from solution objectives, informing on IoT appropriate issues in an approach agnostic means. The protected topics feature the age of needs as well as also their transformation right into a layout using viewpoints and also perspectives. LIMB provides an exhaustive listing of intended Unified Demands, that could be taken advantage of to create cement demand- ments for a details layout. The UNIs are generalized needs improved with the views as well as viewpoints of those stakeholders.

The UPPER ARM process makes use of the IoT Endorsement Type that releases primary IoT principles like devices, services, as well as additional resources as well as defines their connections and also characteristics on a theoretical amount that is exclusively stemming from certain usage scenarios or even innovations. Adhering to the recognized links, it realizes expected Practical Teams for socializing with in- perspectives of the provided guidelines as well as likewise launches communication features fit for heterogeneous IoT setups. Bonus associates used feature depends on, security, strategy management, solution association, and also added.

B.BETaaS

Building the Environment for the numerous things as a Service indicates besides the standard capability in addition to style, a correct implementation of the platform becomes part of the deliverables. BETaaS is a managing duty and likewise, some deliverables are certainly not having said that obtainable in their last variety or are additionally still missing out on entirely.

BETaaS consists of a body of doorways (" local cloud of gateways") that flawlessly consist of existing various M2M bodies. To theoretical stemming from the variation of the bodily amount, BETaaS calls well as builds upon a common recommendation type contacted Things-as-a-Service. The TaaS Endorsement Model is the framework of the BETaaS framework on which it is built. It offers home types for domain names, info, communication, security, along features. TaaS builds upon the

IoT-A designs, conforming along with prolonging them to its specific requirements.

C.OPENIoT

The opinion research activity has pointed out a layout using a Sensing unit Middleware as well as also a Semantic Directory Firm. To achieve positioning, type progression and also criterion was based upon the Concept Referral Model of IoT-A.

The Noticing system Middleware does the collection, filtering system in addition to the celebration of information moves linked to substantial as well as virtual products. The Cloud Processing Commercial commercial infrastructure helps the storage room of documents along with their linked meta- files info in a scalable as well as an elastic fashion trend. The Semantic Listing Company helps subscribe administration in addition to semantic comment for sensing units as well as services. The Global Scheduler is charged with managing to ask for on-demand company deployment as well as additionally the connected provisioning of availability to information collections and also companies that may be required. The Demand Interpretation factor enables the compelling spec of service asks for and likewise, the Need Conversation element is charged alongside the visual images of the outcomes generated through an accomplishing answer.

The most ideal style of the style is a structure rock to build an honoured IoT device; this design helped to care for several concerns in the IoT atmosphere including scalability, directing, producing connects with, and so forth. Normally, the IoT design approach based upon three significant dimensions are:

Information things: it features all products linked to IoT setting might be noticing items, recognizing items as well as control products; ii) Independent device: that includes various qualities including self-configuration, self-protection, self-adaptation, as well as additionally self-optimization; and additionally iii) Smart functionalities: which have smart routines on the web normally; the intelligent activities could be intelligent control, swap details strategies via unit products, documents dealing with, all the requests which belong to the IoT could be categorized relying on to these sizes [9] The joint in between these sizes builds a brand

new place called "infrastructure of IoT", which provides a support group to serve the distinct things, which may supply countless solutions including things identification, site id as well as also details defence.

To this end, There are a lot of methods to build a style of IoT, the paper is going to focus on 2 kinds specifically, style got in touch with "EPC worldwide body" as well as also one more called "Combine as well as global IoTs or even U2IoT", to develop a function on IoT, the structure method preferred which based on an on-call style the EPC global system. The system adopted by AutoID facility for communicating the powerful particulars concerning objects/things to supply a history of the product motion for the authorized individuals, the RFID development plays a crucial task to differentiate in between these mobile objects, this device is called "the EPC global unit". The IoT utilizes the EPC international system as an idea to design the design structure.

The potential style of IoT finds to get hookup between real-world, cyber-world as well as the social planet. Blend along with omnipresent IoTs or even U2IoT is taken into consideration as a numerous sort of IoT concept, it is utilized to combine the real world along with the cyber globe. The U2IoT is composed of a selection of numerous bodies, featuring device of IoT to be similar to individual semantic network that provides answers to particular requests; U2IoT features the industrial IoT, local young people, nationwide IoT, and all over the world IoT which assimilation of many Device IoTs together with universal components, as well as it corresponds to the social establishment platform. The principal top qualities of U2IoT design are cyber, bodily, social co-existence, connection and interactivity, space-time congruity and also multi-identity condition.

pretty minimized powered requirements and additionally minimized usage fees.

The method may quickly minimize the electric battery substitute rate as well as additionally possesses a transmission fee of around 25000 bps, along with a set of as high as 1 kilometre. In the ZigBee process, security and also security supposes a necessary role. The Advanced Data Encryption Requirement is the security process made use of in ZigBee. Such an incredibly professional in addition to specific protocol ensures privacy as well as the stability of cordless interactions. Pair of different security variations are given via ZigBee: basic security layout carried out direct security variation as a result of its vulnerability to threats, and High Security, each of which is taken advantage of since it vows much better security during interactions. If files are unencrypted on a ZigBee unit, a cyberpunk can simply handle all network info and also can effortlessly additionally sniff/capture packages that have been sent. As a choice, if communication is safeguarded, an uncalled-for challenger might simply execute strikes that accomplish certainly not permit system ease of access, It is fairly tough to observe the network critical maintained through ZigBee as well as know the information supplied, featuring ease of access rejection or even hitting. The AES 128-bit security formula is executed with ZigBee security, which also provides security resources such as Top secret transmission, property security and also device command, as crucial production. Each level behind the individuality platform supervises automatically exchanging the trick for every and also every input and also result in the nodule, and without the demand to break and protect, information is transferred at each step. The security consists delivered by the ZigBee needs will certainly be covered, including in the sense of safeguarded compilations as well as sound security.

IV. IOT-BASED SECURITY COMMUNICATION AND PROTOCOLS

ZigBee

ZigBee is cordless and also based on the IEEE 802.15.4 requirement. It was introduced in 2004 as a result of the ZigBee Collaboration in addition to like. Generally defined through

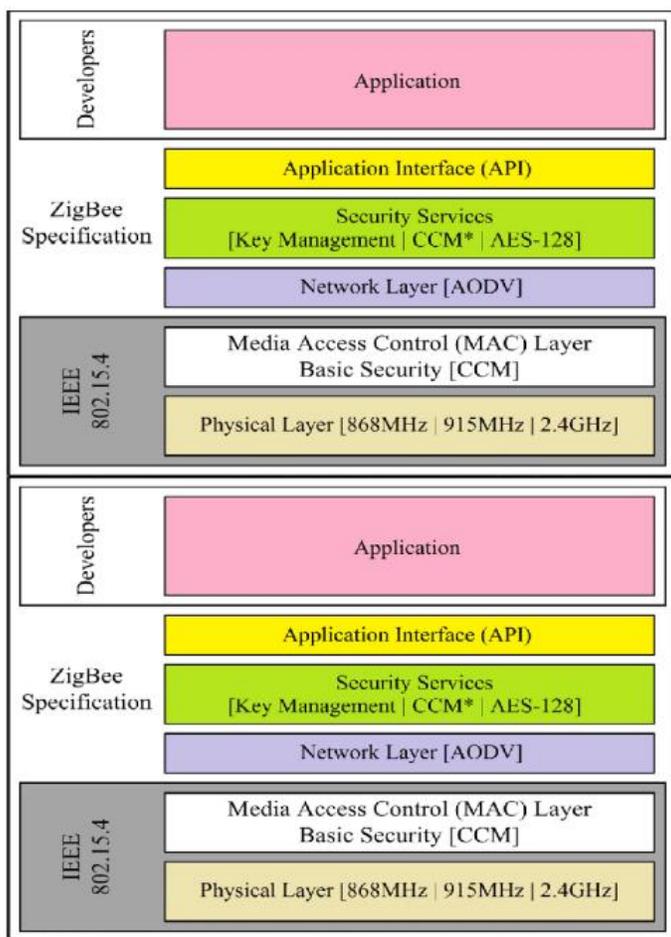


Figure 1: ZigBee stack

ZigBee Networks go through an amount of kind of attacks. In regularly keeping along with the safety and security criteria of ZigBee Networks, This strikes might be organized into 5 sorts of strikes:

Eavesdropping: An outside strike through which a cyberpunk may look to passively listen to or maybe pay attention to the conversation on the system and also take the relevant information.

Denial of Service: That develops when hackers make use of a COMPUTER to deliver activities along with the miraculous function of hampering the system's superhigh frequency (2.4 GHz). This form of Disk Operating System can similarly be discovered on the records link coating where, as an example, IEEE 802.15.4 and even ZigBee, possess a specific reason to disturb the communication protocols.

Blemish Compromise: It is a kind of action through which an attacker captures and also manipulates or reprogrammed an authentic blemish in the system.

Sinkhole and likewise Wormhole: It is a condition through which the malware system device via dispersing bogus transmitting information collected package deals to it, which consequently troubles the system's routing procedure. In a Wormhole Attack, an assailant collects deals for one network hookup, passes all of them to another place of the system, as well as after that replays each of them into a device to develop condition concerning the sending, forwarding and also different other significant tasks of the nodule.

Physical Strike: The rival's ability to acquire bodily availability to a unit device.

BLUETOOTH LOWERED POWER

Unlike routine Bluetooth, BLE is created for sensing unit networks with the cost of a little record of roughly 1 Mbit/s, in addition to a significance on electricity efficiency, it was released and also BLE is conflicting with Bluetooth Requirement. Each run in the 2.4 GHz uniformity range along with a unique stable of insight networks. The software program is assisted as well as likewise flowed as a result of the Bluetooth SIG. BLE points out a compilation of program application parts that may be used via devices. A style is a collection of services that device products and, featuring its cause, each device might deliver a variety of elements. BLE possesses actually until now been restricted to linking merely 2 devices. The Internet interface was executed through Bluetooth SIG, developing a multi-to-many connection. Encrypted data is additionally on call in BLE as well as likewise is carried out during the program of the linked components' matching process. Trading the cover of the encryption key is a vital part of safeguarding the connection. Signing up with a strategy is a vital contributor to Bluetooth security worries. Throughout several time

frames of the hookup technique, attacks may be executed, each just before the matching procedure is finished as properly as after the devices are matched. Partnering in BLE is not considered protected about variety 4.1, given that no eavesdropping security may result in critical decline. The danger of asking for linking devices to regrow their methods generates this much more high-risk. Moreover, The standard keys are going to undoubtedly possess a flexible timeframe of virtually as 7 bytes and likewise, the amount of authentication issues is never-ending. Encryption and also numerous other permission developments stay additional except in addition to the improvements in later releases in addition to are surely not provided through countless sellers. On the make use of a coating, some distributors impose security, however, request sensitivities and even disappointing security versus particular risks are incredibly well-liked. Lastly, while all the cover of encryption tricks of the BLE requirement are made use of effectively as a result of the distributor, it carries out not to guarantee top-notch. The flexibility of the style which causes issues in security made through a method, consisting of large restrictions including relative code completion.

CONCLUSION

Despite quick and additionally significant creating around it manages the primary problem which is the security of the devices as well as also individuals. As a result of the security, susceptibilities are going to surely take severe threats to consumers' security and household or even industrial residential property this paper looks at the major challenges and also a possibility in this particular certain industry. This paper goes over and has a look at the main IoT protocols that took advantage of to correspond in between IoT located devices as well as likewise their susceptibilities as well as weak points to the aggressors. Beginning along with LoRaWan which uses 128 AES key in C-Media Receive accessibility to Administration method along with 6LWPAN which performs authorization and also authorization in between the customers during the sending out, finishing together with BLE as well as Zigbee, the quite first one the designer should recognize to authenticate the

buyers in each stage while the second one runs like Bluetooth by using coupling procedure between clients.

REFERENCES

1. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer Networks* 56(16), 3594–3608 (2012)
2. Bauer, M., Boussard, M., Bui, N., De Loof, J., C., M., Meissner, S., Nettsträter, A., Stefa, J., Thoma, M., Walewski, J.W.: IoT Reference Architecture. In: *Enabling Things to Talk: De- signing IoT solutions with the IoT Architectural Reference Model*. Springer Berlin Heidelberg (2013)
3. Bonomi, F., Milito, R., Natarajan, P., Zhu, J.: Fog Computing: A Platform for Internet of Things and Analytics. In: *Big Data and Internet of Things: A Roadmap for Smart Environments*, pp. 169–186. Springer (2014)
4. Borgia, E.: The Internet of Things vision: Key features, applications and open issues. *Computer Communications* 54, 1–31 (2014)
5. Anitha Eemani, “PNC Architecture of Security Services”, *Journal of Advances and Scholarly Researches in Allied Education*, Vol. 13, Issue No. 2, July-2017
6. Anitha Eemani, “A Comprehensive Review on Network Security Tools”, *Journal of Advances in Science and Technology*, Vol. 11, Issue No. 22, May-2016
7. Anitha Eemani, “Achieving Network Security and Security Mechanisms at Networking Layers”, *International Journal of Information Technology and Management*”, Vol. 11, Issue No. 17, November-2016
8. Bhagya Rekha Kalukurthi, “IMPLEMENTATION OF BIG DATA ANALYTICS AND BIG DATAGOVERNANCE”, *The International journal of analytical and experimental modal analysis*, Volume VII, Issue I, May 2015
9. Bhagya Rekha Kalukurthi, “A Comprehensive Review on Challenges and Types of Big Data”, *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 7, Issue 1, January 2018
10. BhagyaRekha Kalukurthi, “Big Data Classification and Methods of Data Mining, Big Data”, *International*

Journal of Scientific Research in Science, Engineering and Technology, Volume 3, Issue 5, July-August-2017

11. Bhagya Rekha Kalukurthi, "Security Vulnerabilities, Security Threats, and Advance Network Security Policies", Journal of Interdisciplinary Cycle Research, Volume VI, Issue I, Jan- June 2014

12. BhagyaRekha Kalukurthi, "A Study on The Big Data Characteristics", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 1, Issue 1, July-August 2016

13. Bhagya Rekha Kalukurthi, "A Comprehensive Overview on WLAN Security Exploits and WLAN Security for 802.11", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 4, Issue 11, November 2015

14. BhagyaRekha Kalukurthi, "Data Mining Strategy for Discovering Intriguing Patterns and Challenges with Bigdata for Global Pulse Development", International Journal of Scientific Research in Science and Technology, Volume 3, Issue 3, March-April 2017

15. Malyadri. K, "Architecture and Components of Cloud-Based ML Framework", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 8, Issue 1, January 2019

16. Malyadri. K, "An Overview towards the Different Types of Security Attacks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2014

17. Malyadri. K, "Security Threats, Security Vulnerabilities and Advance Network Security Policies", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 9, September 2013

18. Malyadri. K, "Need for Key Management in Cloud and Comparison of Various Encryption Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, volume 1, issue 1, July-August 2016

19. Malyadri. K, "A STUDY ON EXPERIENCES AND LIMITATIONS OF MOBILE COMMUNICATION", Alochana Chakra Journal, Volume VI, Issue VIII, August

2017

20. Malyadri, N. Surya Teja, "Related technologies and the role of mobile app development life cycle", International Journal of Research and Applications, Volume 5, Issue 17, Jan-Mar 2018.

21. Rakesh Rojanala, "A STUDY ON BIG DATA-ORIENTED STREAM DATA MINING AND STREAMED DATA MANAGEMENT", The International journal of analytical and experimental modal analysis, Volume X, Issue III, March 2018

22. Rakesh Rojanala, "An Overview of Intrusion Detection System and the Role of Data Mining in Information Security", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 6, Issue 3, March 2017

23. Rakesh Rojanala, "AN OVERVIEW ON CLOUD COMPUTING MODELS AND CLOUD DELIVERY MODELS", The International journal of analytical and experimental modal analysis, Volume IV, Issue I, JAN-JUNE 2012

24. Rakesh Rojanala, "Cloud Computing Characteristics and Deployment of Big Data Analytics in The Cloud", International Journal of Scientific Research in Science and Technology, Volume VIII, Issue II, March-April 2014

25. Rakesh Rojanala, "CLOUD COMPUTING ARCHITECTURAL FRAMEWORK", Journal of Interdisciplinary Cycle Research, Volume V, Issue I, Jan-June 2013

26. Rakesh Rojanala, "A COMPREHENSIVE STUDY ON THE CHALLENGES OF STREAM DATA MINING AND BIG DATA-ORIENTED STREAM DATA MINING", The International journal of analytical and experimental modal analysis, Volume VII, Issue II, July-December 2015

27. Rakesh Rojanala, "Machine Learning: Intersection of Statistics and Computer Science", "International Journal of Innovative Research in Computer and Communication Engineering", Vol. 5, Issue 8, August 2017

28. Rakesh Rojanala, "Components of Data Mining and Big Data Analytics in Intra-Data Center Networks", "International Journal of Advanced Research in Electrical,

Electronics and Instrumentation Engineering”, Vol. 5, Issue 7, July 2016

29. Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.

30. Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint On Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2, Issue 6, November-December-2017.

31. Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016

32. Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014

33. Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012

34. Sudheer Kumar Shriramoju,, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013

35. Sudheer Kumar Shriramoju, "SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING", Airo International Research Journal, Volume IX, Feb 2017.

36. Yeshwanth Valaboju, "IOT Communication Technologies and Future of Internet of Things", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 6, November-December 2017

37. Yeshwanth Valaboju, "A Study on Cryptosystem Types and Cryptographic Principles", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 5, Issue 6, June 2016

38. Yeshwanth Valaboju, "A Review on The Database Security Requirements and Guidelines", International Journal of Scientific Research in Science and Technology, Volume 3, Issue 6, July-August 2017

39. Yeshwanth Valaboju, "A LITERATURE REVIEW ON NEURAL NETWORK ARCHITECTURES", Journal of Interdisciplinary Cycle Research, Volume VII, Issue II, December 2015