Concerns of Modern IoT: Exploration over Attainments of Past Observational Challenges in IoT

Vikram Narayandas, Maruthavanan Archana, D. Raman

Abstract*: In the previous past times internet of things (IoT) constructed up the different parts of life to improve usefulness by reducing human work including only a pair of sensors. In the previous there were frequently the absolute greatest obstacles which IoT as of now prompts achievement are not automatic. Just a few percent of organizations were fruitful with their IoT activities be that as it can, given a considerable number of which are simply operational or authoritative. Albeit numerous issues related with IoT arrangements are not mechanical, they are similarly agonizing and hard to survive. Furthermore, if each association needs to beat these difficulties in a void, a 74 percent 3 dissatisfaction rate is probably going to proceed. Be that as it may, by transparently sharing the information and bits of knowledge increased through broad experience encouraged IoT to push ahead all in all intensifying our human potential. The achievement of IoT over the past impediments puts more prominence on its capacity to conquer the future difficulties. IoT is an innovation that should be known as an aid. In any case, since it interfaces all the things to 4 the Internet, the things become defenseless against a type of security dangers. Huge organizations and cyber security analysts are giving their best to make things ideal for the purchasers, yet there is still a ton to be finished.

Keywords: IoT, IWOT, Security.

I. INTRODUCTION

The Internet of Things is a powerful worldwide infrastructure network [1] with self-arranging abilities dependent with interoperable protocols resolutions where physical and virtual things are consistently incorporated and communicate with smarter objects and consistently integrated into the data organization. Internet of Things is observing for its own shape, its belongings have just made worldwide answers making extraordinary steps as an all-inclusive arrangement for the associated situation. And in Shrewd cultivating [2] Internet of Things (IoT) innovations have become the significant way ahead towards novel cultivating rehearses. The ability of information collection and the executives offered by IoT depends on a few elements of the fundamental correspondence network innovation among IoT hubs, doors, and application servers offers a state-of-the-art review of examination endeavors on the IoT application layer conventions, concentrating on their vital qualities, their presentation just as their ongoing use in rural applications.

The Internet of Things (IoT) was at first called the "Web of Everything"[3] and IoT objects have identifiers which are distinctive and they can direct the data over a system interrelating physical and practical things without expecting human-to-human or human-to-framework and communication among network associated gadgets that incorporate sensors, actuators, administrations and other web accompanying objects. The IoT is involved by various improvements [4] in RFID, smart sensors, correspondence advances, and Internet communications. In the upcoming years IoT is relied upon to be unique of the primary centers between different innovations by associating smart physical objects together and permit various applications and dynamic communications. Unique advancements [5] in wired and remote sensor and actuator structures, improved correspondence conventions i.e. conveyed to the Successive Generation Internet, and dispersed knowledge for brilliant items are only the most applicable. The range of IoT application areas is enormous together with bright homes, shrewd urban communities, wearables and so on. Such gadgets will have intense abilities to gather, break down and even settle on choices with no human cooperation. [6][7].Since IoT frameworks are developed with heterogeneous equipment and systems administration progressions [8], interfacing them to the product side and a portion of data is a perplexing undertaking with diverse engineering and conventions in IoT frameworks. The Internet of things (IoT) shaped [9] in the late twentieth century, highlighting various applications like new radio interfaces, communication resolutions, and strong information-based models. From Model to Truth—How Companies Are Leveraging IoT to Move Their Businesses Forward [10] of all the developing advancements, and have the best effect on the industrial family. To realize the present status of the IoT more readily, Forbes Insights joined forces with Hitachi Vantara to study senior administrators around the globe who are driving IoT activities inside their organizations. The information in this examination is obtained from a 2017 Forbes Insights review of 502 administrators who recognized themselves as liable for, or acquainted with, the current or arranged IoT exercises of their organizations. Respondents were situated in Europe, the Americas and Asia-Pacific, and spoke to a scope of businesses with not one including over 25% of the aggregate.

Manuscript received on March 09, 2021.
Revised Manuscript received on March 14, 2021.
Manuscript published on 30 March 2021.
* Correspondence Author
Vikram Narayandas*, Research Scholar, Department of Information Technology, Annamalai University Chidambaram, Tamil Nadu, India. Email: narayandas.vikram@gmail.com
M.Archana, Department of Information Technology, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India. Email:archana.aucse@gmail.com
D.Raman, Department of Computer Science and Engineering, Varadaman College of Engineering, Hyderabad, India. Email: raman.vsd@gmail.com

The Economist Intelligence Unit's (EIU) IoT Business Index[11] overview has built up itself as the most definitive inside and out investigation of IoT development with most recent Index report shows a the new Roaring '20s decade sees boundaries bringing down over all parts with simply over portion of all organizations studied now in right on time or broad arrangement of inner and outer IoT systems .Gartner Survey Reveals Block chain Adoption [12] Combined with IoT Adoption Is Booming in the U.S. And with 75% of IoT Expertise Adopters in the U.S "The Gartner IoT Implementation Trends Survey was led by means of an online overview from May through June 2019 with in excess of 500 respondents from the U.S. Defendants were required to be at chief level or above and must to have an essential contribution and obligation regarding settling on choices in IoT execution. Seventy-five percent of IoT innovation adopters in the U.S. have just embraced block chain or are wanting to receive it before the finish of 2020. Among the block chain adopters, 86% are actualizing the two advancements together in different activities. "In the long haul, we expect the mix of IoT and block chain to empower inventive gadgets and plans of action, however the important development in both block chain and IoT will take five to 10 years to accomplish development," said Ms. Litan.

II. PAST OBSERVATIONAL CHALLENGES: AN OVERVIEW

In the 2014 report "The Devices are coming!" Shared first perceptions on the curiosity recognized as the Internet of Things (IoT) and how its appearance influences IT conditions. Presently that IoT is even more completely improved into our way of life. Progressively bringing IoT gadgets into the workplace and interfacing them to corporate systems directly close to their PCs, cell phones, and tablets.

"BYOD, IOT… YOU'RE AS OPEN TO THREATS AS YOU LET YOURSELF BE." – MARK H., IT PRO 440 IT geniuses in North America (NA) and Europe, the Middle East and Africa (EMEA) to disclose to us how the developing number of IoT gadgets is influencing the operational situation and in what way genuinely they think about the danger. Security presently starts [13] to lead the pack over inadequate transmission capacity as the main concern with regards to keeping clients connected. Indeed, about 90% of IT masters state IoT presents security and protection that should concerns in the way that IoT gadgets make more attentive into the system (84%). Around 75% of IT experts are additionally stressed that IoT producers aren't executing suitable safety efforts. A key innovation in the acknowledgment of IoT frameworks is middleware[14], which is typically represented as a product framework intended to be the intermediary between IoT gadgets and applications, primarily the requirement for an IoT middleware through an IoT application intended for constant forecast utilizing of smart watch sensor information., Microsoft review finds [15]:Over 80% of huge organizations around the globe are receiving IoT arrangements, that enlarging business grasp of the Internet of Things is happening even as 97% of business and tech pioneers recognize they have security worries about their IoT usage, Microsoft's examination found. "IoT is regularly a entry for organizations experiencing computerized change – it's not the end yet rather simply the start," says Sam George, chief of Azure IoT at Microsoft. "IoT is turning out to be standard." The overview crossed about 2,500 business and IT leaders – just as 737 designers – working at organizations of 1,000 representatives or bigger in the U.S., Germany, Japan, China, France and U.K. Customers progressively depend on IoT-empowered items to streamline their lives and tidy their homes, from lighting and temperature to security, cooking and cleaning. The developing Internet of Things can possibly realize major traditional difficulties [16] related with medicinal services arrangement. Low-power remote conventions for private Health Internet of Things applications are described by high unwavering quality prerequisites, the requirement for vitality proficient activity, and the need to work vigorously in differing conditions within the sight of outer impedance.

The Internet of Things and Mobile Development Survey [17] is directed two times per year, in the spring and fall. This far reaching report dependent on essential examination with designers effectively producing for associated gadgets and the Internet of Things. These days Internet of Things succeeds an incredible consideration [18] from examiners, after all it turns into a major automation that agrees a shrewd body being life, by permitting methods between articles, machines and everything consistent with people. The larger part of buyers anticipate that makers should give security to associated items before they hit the market, as per another review led by Karamba Security [19]. The overview, entitled "Buyer Attitude towards IoT Security" found that 74% of respondents expected their customer "Internet of Things" gadgets to be made sure about by makers, and as much as 87% trust it is the duty of producers to do as such. The study was done by Market Sight and surveyed 1,000 individuals between the ages of 18 and 65+ over the whole United States. Half of the defendants were male and half female, and they spoke to an assortment of ethnicities and pay levels running from under $25,000 every year to more than $200,000. All things considered, while about half of respondents said they wanted to buy an associated gadget in the coming year, just 23% will explore the security foundation of the item before making a buy. Likewise, while 42% said they do not consider gadgets that get on-air updates to be secure, just 35% said they play out the update when they get a warning.. IoT innovation has added another vision to this procedure by empowering associations between keen items and people. IoT is viewed as the future web, which is fundamentally not relatively the similar as the Internet we use today. [20]. Microsoft scored [21] most elevated, with other normal suspects of AWS, IBM and Nokia and frameworks integrators including Tata Consulting Services. The other most normally picked were proficient systems, sites and fora, and investigators. The Eclipse Foundation [22], one of the world's biggest open source establishments concentrated on the Internet of Things (IoT), today declared the arrival of its first yearly IoT Commercial Adoption outline. The Figure 1 is composition of IOT personnel for a business requirement analysis.

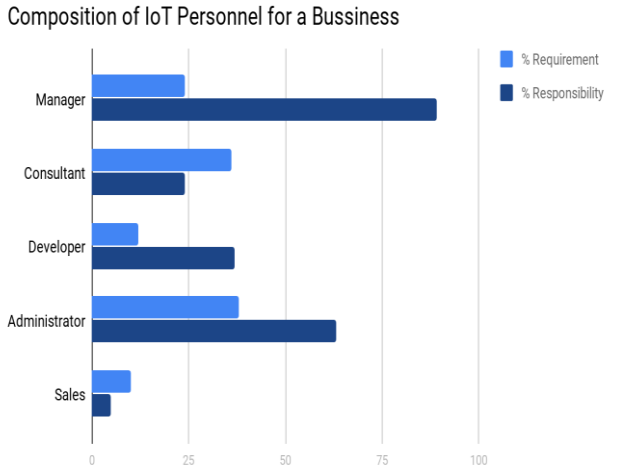

Fig 1 composition of IOT personnel for a business

To enlarge the base for direction in this field, the technology Group asked supplementary than 2,000 clients to share their perspectives on 38 distinctive IoT stages. Bosch's IoT Suite was one of the stages remembered for this overview to share a serving of the structures of how clients appraised us in the classifications security, execution fulfillment, client suggestion, and timeline.[23].Digicert as of late appointed a worldwide investigation of more than 700 organizations over a wide assortment of enterprises to perceive how associations are drawing closer IoT security. To even more prospective understand what is a powerful accomplishment aimed at the persons who are progressing nicely, DigiCert[24] partitioned out overview results into levels to contrast those doing great with those that are battling with security. Connected with worldwide client base with an IoT review between September 2019 and December 2019, got 2,015 finished surveys, essentially from architects of IoT arrangements, in 67 countries[25] As solutions for these difficulties, respondents[26] looked to least security principles and authorizing compulsory item reviews, updates, or orders as the two finest approaches for improving IoT item security. Furthermore, 83% accept that open divulgence of weaknesses all alone is not sufficient, and that some type of administrative activity would be further effective.

III. CURRENT IOT FUNDAMENTALS

An IoT framework is included various practical measures to encourage different utilities to the framework, for example, detecting, distinguishable evidence, incitation, communication, and the executives An IoT framework depends on gadgets that give detecting, activation, control, and observing movements. An IoT gadget may comprise a few interfaces for interchanges to different gadgets, both wired and remote. These incorporate (I) I/O interfaces for sensors, (ii) interfaces for Internet accessibility, (iii) memory and bulk interfaces, and (iv) sound/video interfaces. IoT gadgets can be of different types, for example, wearable sensors, smart watches, LED lights, vehicles, and modern machines. The communication plays major role among gadgets and remote servers. IoT correspondence conventions for the utmost portion of work in information edge layer, transport layer, and application layer. An IoT framework serves different kinds of abilities, for sample, administrations for gadget displaying, gadget control, information distributing, information investigation, and gadget exposure. Administration part gives various capacities to administer an IoT framework to look for the essential direction of IoT framework. The figure 2 shows utilization of IOT in different segments.

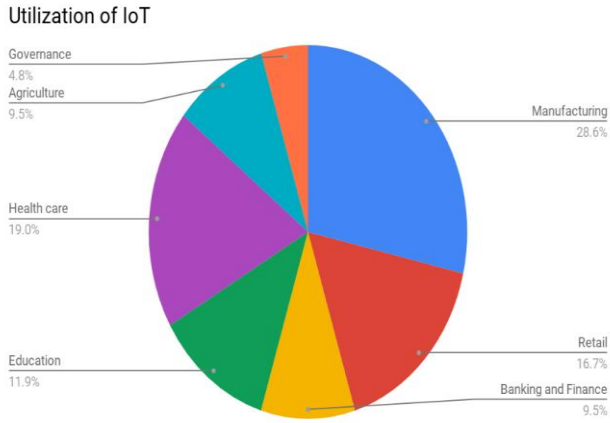

Fig.2. Utilization of IOT

A.Ongoing Utilities of IoT

IoT gadgets and frameworks ought to have dynamic and self-adjusting capability to adjust with the varying situations and take activities dependent on their working conditions, customer's unique condition, or detected condition. The reconnaissance cameras can adjust their modes dependent on whether it is day or night. Cameras could change from lower goals to higher goals modes when any movement is identified and alert close by cameras to do likewise. IoT gadgets may make Self-arranging their design capacity, permitting numerous gadgets to cooperate to give certain usefulness, (for example, climate checking). These gadgets could design themselves (in relationship with IoT foundation), set up the systems administration, and bring most recent programming updates with negligible manual or client mediation. IoT gadgets may support a few interoperable correspondence conventions and can speak with different gadgets and furthermore with the framework. Each IoT gadget has a special character and one of a kind identifier, for example, IP address or URI. IoT frameworks may have wise interfaces which adjust depending on the unique situation, permit speaking with clients and natural settings. IoT gadget interfaces permit clients to inquiry the gadgets, monitor their status, and control them remotely, in, in relationship with the control, arrangement and the board foundation. IoT devices are ordinarily planned into the information association that grants them to bestow and exchange data with various contraptions and structures. IoT contraptions can be effectively found in the framework, by various devices and masterminds, and can depict themselves (and their characteristics) to various devices or customer applications Based on the detected data about the physical and natural boundaries, the sensor hubs gain information about the covering situation. The choices that the sensor hubs take from there on are setting mindful IoT multi-jump in nature as Wise dynamic capacity. in an enormous zone, this component improves the vitality effectiveness of the general system, and henceforth, the system lifetime increments.

Utilizing this element, various sensor hubs work together among themselves, and all things considered take an official conclusion. The figure 3 shows rising conditions of current IoT drivers.

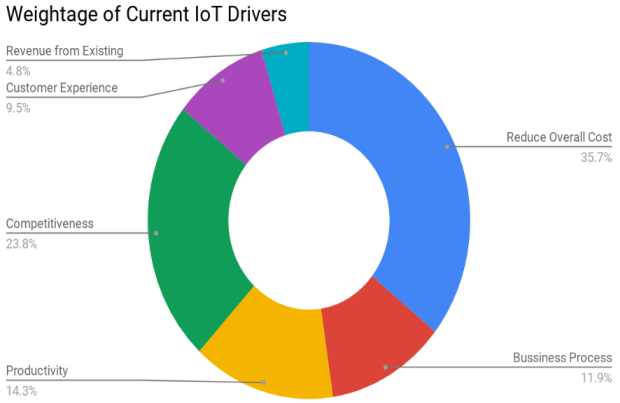

Fig 3 Weightage of current IoT drivers

B. Threats and Challenges for IoT

Anything that is associated with the Cyberspace is available to danger. Since IoT gadgets are employed and managed by people, a trespasser might need to increase spontaneous gain access to the human. By listening stealthily on the remote IoT gadgets, the trespasser might need to grasp classified data. IoT gadgets run on low force and less figuring asset ability. Because of this, they cannot bear to have complex security conventions. Henceforth, it turns into an obvious objective for interlopers. The most basic principal issues examined by the IoT is Vulnerability, Easy Exposure, human hazard, or a distinctive hazard. Today, IoT arrangements have developed after certain time. Gadgets, today, have developed to be water-resistant. It is a long excursion before IoT arrangement providers create something that is flame resistant or quake evidence. The numerous categories of threats in IoT were discussed in table 1.

Table 1: different categories of threats

Level	Category of Threat	Alleviation
Physical	Tampering	Tamper-resistant wrapping
	Eavesdropping	Encryption techniques
	Denial of Service	Spread-spectrum methods
Networking	Exhaustion	Dynamic firewalls Investigative monitoring Transportation governance Two way link certification
	Collision	
	Unfairness	
	Spoofing	
	Selective forwarding	
	Sinkhole	
	Wormhole	
	Sybil	
	Flooding	
Data processing	Exhaustion	Traffic flow checking
	Malware	Malware discovery
Application	Client app.	Anti-virus straining
	Communication	Traffic flow checking
	Integrity	Auditing
	Modifications	Endorsement
	Multi-user access	Process planning and design
	Data access	Authorization

C. Predicting IoT addiction beyond 2020

1)IoWT: Internet of Wearable Things: Internet of Things (IoT) future shaped by wearables-74 percent believe multiple wearable's and sensors will help them interrelate with further devices and physical things around them, whilst 1 in 3 smartphone users believes they will wear at least 5 wearable's beyond 2020. Thus, a setback in wearable's adoption might delay the overall adoption of the IoT among consumers

2) Quantitative study: In March 2016, Ericsson Consumer Lab carried out an online survey of 5,000 i Phone and Android smartphone users, aged between 15 and 65, of whom 2,500 were also existing wearable technology owners. The participants were based in Brazil, China, South Korea, the UK and the US. Their views are representative of the opinion of 280 million smartphone users across these 5 markets.

3) Wearable future: However, the wearable's market is still in the early phases of expansion, and currently dominated by health, wellness, and activity tracking devices – despite industry developments pointing to an increasing number of use cases. This report explores consumer views on if, how and when wearables might break beyond health and wellness scenarios and cover more diverse needs.

4) Authoritative substance limitations: Clients of IoT are bound to impart their information to makers than with specialists, insurance agencies and web firms, with 70 percent seeing wearable's producers to be intense in ensuring their information. This receptiveness can be credited to two factors: a conviction that the bits of knowledge and administrations gave are of worth..

5) Outmaneuvering the cell phone: The current age of IoT is only the start of an earth-shattering change. Clients consent that IoT revolution will grow in more various and effective manners than cell phones have in the previous 10 years. They trust IoT could in the long run supplant existing methods for access that IoT have gotten coordinated in each part of our lives, making it difficult to visualize a future without them.

6)Assembly of advanced and physical universes: Bringing individuals into IoT: While customers are certain that innovation will assist them with cooperating with objects in their environmental factors, they likewise state that this innovation may not really be gadgets, yet sensors that could be ingestible. Truth be told, ingestible pills and chips under the skin will be normally utilized in the coming years – not exclusively to follow indispensable wellbeing data, however in addition to open entryways, validate exchanges and character, and to controller objects. The figure 4 represents concentration of future IoT challenges.

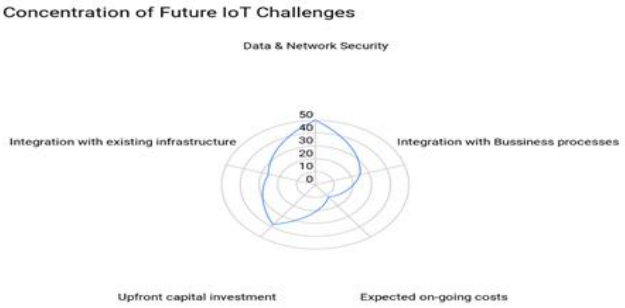

Fig 4 future IoT challengers

IV. CONCLUSION

Security Issues and administrations in IoT need most extreme significance as the utilization of interfacing objects in regular individuals' lives can make them dangerous. The shrewdness incorporated into homes, vehicles, and electric lattices can be redirected into unsafe situations when abused by programmers.

Diverse surviving situations introduced in the previous year's outline the grade of impairment that possibly will consequence from a protection dissemination, particularly along with the turn of events and enormous appropriation of IoT uses managing touchy data. The primary IoT security worries to be taken into consideration are verification, approval, respectability, secrecy, non-disavowal, availability, and protection. The way towards affirming and safeguarding the character of articles in IoT setting should be able to identify and verify every other item in the framework. The method about allowing a substance to do or have something in the direction of preserving up the uniformity, accuracy, and reliability of data over its entire progression in IoT leads to the modification of fundamental data or even the implantation of invalid data provoking significant issues. The path toward ensuring that the data is just gotten to be approved by individuals ought to be considered with respect to secrecy in IoT to assure that the element getting the information will not move this information to different things. Assuring non-availability to private data by open or noxious items examine the safety measures matters, assaults, and safety necessities at every level of the planning. System Layer Security Issues and Requirements should diffuse information as of the observation level to the application level wherever information directing happens just as the essential information examination. These possible assaults next to the system level (wired up or remote) should prompt the meaning of the accompanying protection necessities with a key understanding. The board security steering should also involve managing IoT Big Data which makes an overhead on the application investigating this information and affects the accessibility of the services opted through various applications.

REFERENCES

1. P.P. Ray"A survey on Internet of Things architectures", Journal of King Saud University - Computer and InformationSciences, Volume30, Issue3,2018,Pages291-319,ISSN1319-1578,https://doi.org/10.1016/j.jksuci.2016.10.003.(http://www.sciencedirect.com/science/article/pii/S1319157816300799).
2. Dimitrios Glaroudis, Athanasios Iossifides, Periklis Chatzimisios,"Survey, comparison and research challenges of IoT application protocols for smart farming"Computer Networks,Volume 168,2020,107037,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2019.107037.(http://www.sciencedirect.com/science/article/pii/S1389128619306942).
3. R. M. Gomathi, G. H. S. Krishna, E. Brumancia and Y. M. Dhas, "A Survey on IoT Technologies, Evolution and Architecture," 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), Chennai, 2018, pp. 1-5, doi: 10.1109/ICCCSP.2018.8452820.
4. .S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," 2016 IEEE Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2016, pp. 381-385, doi: 10.1109/SEGE.2016.7589556.
5. .Luigi Atzori, Antonio Iera, Giacomo Morabito,"The Internet of Things: A survey",Computer Networks,Volume 54, Issue 15,2010,Pages 2787-2805,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2010.05.010. (http://www.sciencedirect.com/science/article/pii/S1389128610001568)
6. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey
7. of Internet of Things (IoT) Authentication Schemes. Sensors 2019, 19, 1141.
8. Balaji, S., Nathani, K. & Santhakumar, R. IoT Technology, Applications and Challenges: A Contemporary Survey. Wireless Pers Commun 108, 363–388 (2019). https://doi.org/10.1007/s11277-019-06407-w.
9. Sobin, C.C. A Survey on Architecture, Protocols and Challenges in IoT. Wireless Pers Commun 112, 1383–1429 (2020). https://doi.org/10.1007/s11277-020-07108-5.
10. Giovanni Perrone ; Massimo Vecchio ; Javier Del Ser ; Fabio Antonelli ; Vivart Kapoor "The Internet of things: a survey and outlook"Sensors in the Age of the Internet of Things: Technologies and applications,2019.
11. Hitachi is a trademark or registered trademark of hitachi, ltd | copyright © 2017 forbes insights https://www.forbes.com/forbes-insights/our-work/internet-of-things/
12. The Arm-sponsored Economist Intelligence Unit IoT Business Index reports from 2013, 2017 and 2020 Copyright © 2020 Arm Limited.https://www.arm.com/blogs/blueprint/economist-2020-iot-investment
13. STAMFORD, Conn., December 12, 2019 Gartner Survey Reveals Blockchain Adoption Combined With IoT AdoptionIsBoomingintheU.S.https://www.gartner.com/en/newsroom/press-releases/2019-12-12-gartner-survey-reveals-blockchain-adoption-combined-with-iot-adoption-is-booming-in-the-us.
14. 2016 "IoT Trends: The Devices have Landed How IT and IoT are learning to peacefully coexist",https://www.spiceworks.com/marketing/reports/iot-trends/
15. A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," in IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1-20, Feb. 2017, doi: 10.1109/JIOT.2016.2615180.
16. "The Internet of Things is going mainstream, Microsoft survey finds" https://news.microsoft.com/transform/the-internet-of-things-is-going-mainstream-microsoft-survey-finds/
17. Atis Elsts, Xenofon Fafoutis, George Oikonomou, Robert Piechocki, and Ian Craddock. 2020. TSCH Networks for Health IoT: Design, Evaluation, and Trials in the Wild. ACM Trans. Internet Things 1, 2, Article 9 (April 2020), 27 pages. https://doi.org/10.1145/3366617
18. IoT and Mobile Development Survey "2019 Vol 2 https://evansdata.com/reports/viewRelease.php?reportID=43
19. Saini R. K, Dahiya A. K, Dahiya P. A Survey on Internet of Things (IoT) Applications and Challenges for Smart Healthcare and Farming. Biosci.Biotech.Res.Comm. 2019;12(4).
20. Survey: Consumer IoT Customers Expect Manufacturers to Embed Security in Devices Karamba Security | December 8th, 2019
21. Shammar, E.A. and Zahary, A.T. (2019), "The Internet of Things (IoT): a survey of techniques, operating systems, and trends", Library Hi Tech, Vol. 38 No. 1, pp. 5-66. https://doi.org/10.1108/LHT-12-2018-0200.
22. .2020EnterpriseIoTMarketResearchSurvey-,https://internetofbusiness.com/2020-enterprise-iot-market-research-survey/
23. TheEclipseFoundationReleasesIoT.-https://www.eclipse.org/org/press-release/20200310-iot-commercial-adoption-survey-2019.php
24. TheIoT User Survey 2019-https://bosch.io/resources/report/the-iot-user-survey-2019/
25. [.https://www.digicert.com/state-of-iot-security-survey/
26. IoT Survey 2019 – Date Published: February 2020-https://in.element14.com/global-iot-survey-2019
27. [26]IoTSecurityFoundation2015-2020-https://www.iotsecurityfoundation.org/survey-less-than-10-of-iot-devices-keep-data-secure/

AUTHORS PROFILE

Vikram Narayandas Research Scholar in Department of Information Technology, Annamalai University, Chidambaram, Tamil Nadu, India. And Member of CSI, IAENG and published 9 international journals.

Dr. Maruthavanan Archana, presently working as Assistant Professor in Department of Information Technology, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India. And Member of CSI, IAENG and published 12 international journals.

Dr.D.Raman, working as Professor in Department of Computer Science and Engineering, Varadaman College of Engineering, Hyderabad, India.And member of CSI,,IAENG and senior member of IEEE, published 19 international journals .