International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Enhancing Security, Authentication and Traceability for Non Standard Internet of Things (IOT) Enabled Devices by Implementing Mandatory IOT Enabled Devices Having Hardware and Software Authentication Cum Registration Mechanism Before their Usage to Every IOT Enabled Devices Manufacturer Cum Supplier as Well as User

Er. Mukesh Chauhan

Head of Department Faculty of Engineering Department of Electronics and Communication Engineering Govt. Polytechnic Rohru Distt. Shimla H.P. India

Abstract:
Internet of things (IoT) [1] has emerged a new field of huge numbers of interconnect devices in term of connecting various gadgets with devices together for sharing data between them as well as working together to form a cluster of sensors with actuators for better monitoring and controlling of various processes of agriculture and industrial automation. A differential non standard approach by various vendors and developers of IoT based application has led to impose great challenge and threat in terms of data security and integrity as well as cost on traceability for Government agencies.

Keywords: Internet of Things (IoT), Data Security, cost on data security and traceability

Introduction

The fast emerging world of IoT based technologies today has generated vast opportunities in every processes or products from consumer goods, process automation, agriculture automation, industrial automation everything has demand of IoT enabled devices. The data are shared using various channels on the internet using GSM[31] mobile, RFID[19], WI-Fi[18], Wi-Max[20], Bluetooth[21] or standard internet based Apps[2] as user interface or programming the available IoT cloud channels to store the data for further reading and manipulating etc. So the volumes of data of such devices are processed through cloud networks many times on internet in every minutes or some case on Intranet method of local collection and fetching or sending the data later using FTP [3] or data transfer protocol etc. Cloud computing and accessibility on Internet has various other key players that may use or misuse such data easily for their self gain like data miners or hacker etc. Developers are making profit by implementing

IoT solution to the manual problems. Most of them are following their own approach on their own IoT devices interfaces as well as protocols as a kind of non standard differential approach that has no vision of long term problems or difficulty to maintain data security on cyber network.

II Past related research works

The approach of multimedia based data processing in IoT devices was also suggested to offer much robust architecture behind the concept of Block chain technologies [4], their research results on proposed methods has shown little increase in percentage of product drop but some gain in terms of less delay in authentication as well as less number of authentications..

The IoT results an efficient as well as accurate blockchain based data collection digital technologies.[5] which further results in efficient machine learning with reliable data and that help in better decision making.

In order to achieve IoT high data security can be an implemented using Ethereum blockchain technology [6] that makes effective technologies in term of data security.

In order to enhance IoT security of data blockchain technologies has been found to most safe and reliable as well as transparent solution and accepted by industry also. [7]

IoT devices are more prone to cyber attacks and unable to protect themselves and also suggested to ID based IoT devices. [8]

The security of IoT devices are big concern in the current scenario and much research is needed to identify potential threat to IoT devices. [9] Microsoft also suggests in his white paper much reliable public blockchain network are required that uses optimization techniques to reduce power consumption and cost too.

Integrating blockchain with IoT can improve or overcome many challenges faced by Iot and also suggests that current architecture of IoT is client/server based and has many issues yet to solve in term of data security and integrity. [10]

Decentralized IoMT (Internet of medical things)[30] based smart healthcare system novel approach to solve the problem related to data security has been suggested and in future much research is needed [11]

Intenet of Medical things (IoMT)[30] healthcare data can be protected by the building security features of blockchain such as heterogeneous encrypted communications methods and digital signatures. Alternatively using authorization and access control provided by proposed Blockchain integrated cyber security based on artificial Intelligence BICS-AI[30]) proposed model [12]

Research Methodology

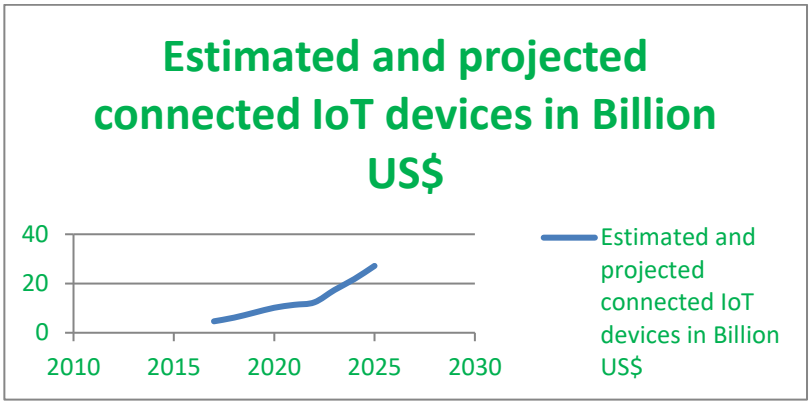
The various research methods will be used to support the proposed system for every IoT enabled devices having standard dynamic user interface implementation guideless.

(a) Comparative Research Method

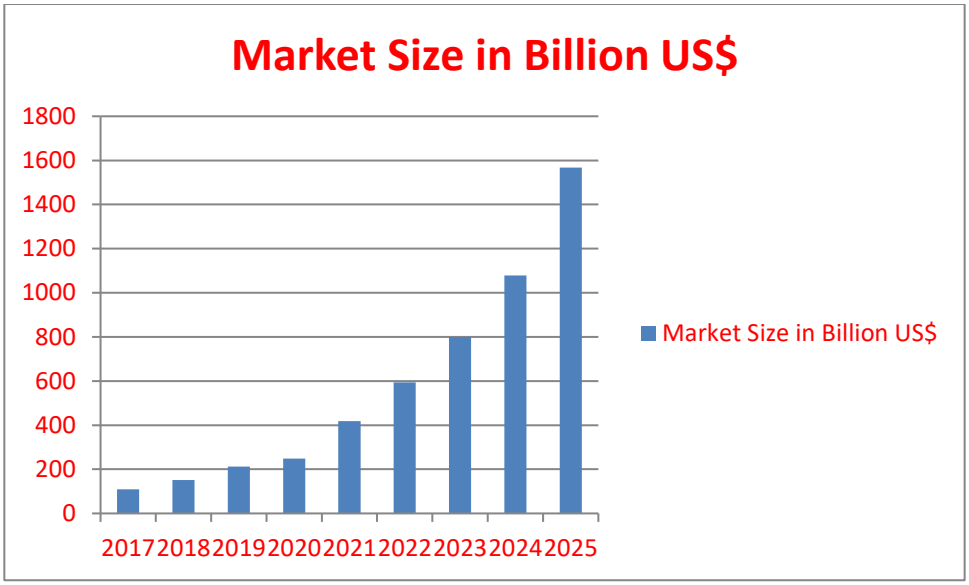
Comparative method is a kind of research method which looks the matter of research of study in relation to another available research. The purpose of research of study is compared across time to time volumes of research. This will help finding comparison of existing methods for IoT user Interface protocols to proposed method.

The global market for industrial Internet of Things (IIoT)[22] was sized at over 544 billion U.S. dollars in 2022. The market is expected to grow in size in the coming years, reaching some 3.3 trillion U.S. do-

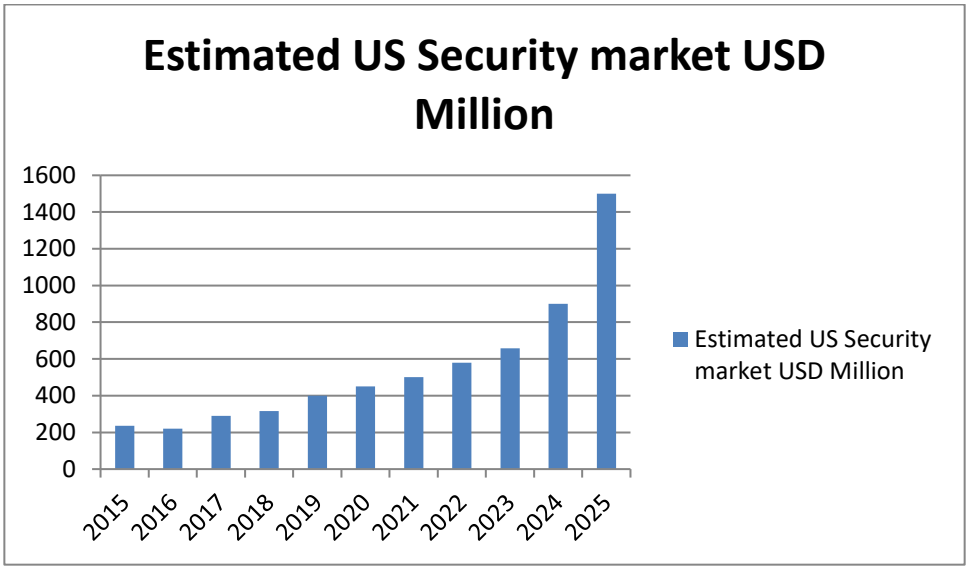
llars by 2030.[13]



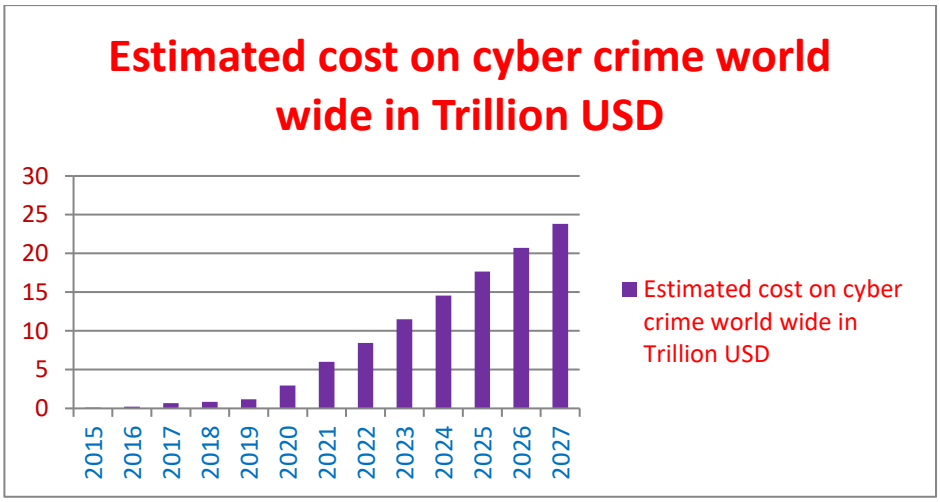
Global IOT market forecast [13]



Industrial IOT market Research [14]



US IoT security market {15}



Estimated cost of Cybercrime worldwide [16]

Based on the data available word wide above it is analysed as below

Sr. No	Expected IOT market in 2025	Expected Security Market 2025	Expected cost on cybercrimes 2025	Comparative Research Analysis
01	US$27.1 Billion	US$30 Billion	US$17.65 Trillion	• The overall global Internet of Things (IoT) security based market size was estimated valued at USD 1.24 billion in 2017. It is likely to rise at 29.7% during the forecast period. • The professional service segment is anticipated to lead the IoT security services market through 2025, registering a 28.3% over the forecast period. • According to estimates from Statista's Cybersecurity Outlook, the global cost of cybercrime is expected to surge in the next five years, rising from $8.44 trillion in 2022 to $17.65 trillion by 2025.

The cost on increasing security threats issues are increasing many time than providing business solution using IoT devices to various sectors.

(b) Theoretical Research Method

Theoretical research a kind of systematic evaluation and examination of hypothesis attributes and assumptions. It will justify more about proposed method and help to understand better way. The data

and information collected in such a manner that it is not used for anything as its aim is to learn or understand research more theoretical for IoT standard dynamic user interface

$IoT\{a, b,c,d\}=a^n x^n +b^n y^n+c^n z^n+a^n d^n+ b^n d^n+ c^n d^n$.....

Where x is hardware dependent parameters

y is software dependent parameter

z is networking protocol related parameter

d is security related parameter

a,b,c, are various solution and manufacturer on the globe working and supply IoT

On the basis of current scenario of IoT market, it is not possible to provide common security solution to all IoT devices as they are non standard devices having multiple attributes dependency complexities. So the cost of finding solution on security will be much more that volume of business solution provided by IoT devices as theoretically it has many non optimal solution.

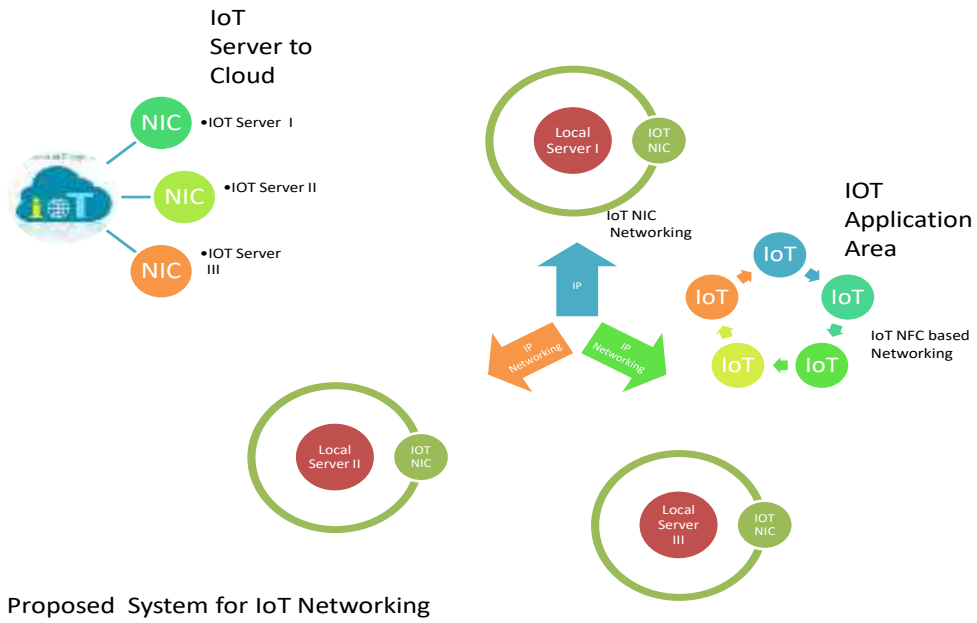
(c) Scientific Research Method

Scientific research methods is a kind of research which involves drawing from various observations to form hypothesis or prediction then conducting an practical experiment and justifying or analyze the results. Standard dynamic IOT user common user interface with be more tested and justified will the help of data and results as secure and better way of connecting IoT devices and processing their data using common data processing methods.

Proposed System

Enhancing Security, authentication and traceability in non standard Internet of Things (IoT) devices by implementing mandatory IoT devices having hardware address(Mac/RFID/IMI code etc) followed by registration of user to common randomization algorithm protocols cum database using dynamic user interface as well as intelligent authenticated Block chain technologies for data communication. Common dynamic user Interface cum data processing methods for every IoT device to convert it as standard smart IoT device.

Having many forms IoT device specific communication protocol is very difficult to build common security system as well as difficulty in data transfer between IoT to IoT as device to device or device (IoT) to Server, local server to main server, Server to cloud, one cloud to another cloud and vice versa also in case of sending data to IoT devices from remote. Till date several solutions have been proposed which make use of sending data in the form of channel to cloud but still IoT devices are using own interface methods. Dynamic user Interface let the device be connected to common type of interface and common security features which is like Network Interface standard followed by various NIC[23] cards at present. The system scans for Wi-Fi[18] packets and identifies the origin and destination MAC[24] addresses as mandatory given to every IoT devices of the devices communicating. The system then checks for the MAC[24] address of the owner's phone to know his/her presence. Then it decides to notify the owner as IoT device to grant accessed permission and Instance of intrusion will also be logged in a common database such as open SQL[25] database etc and the data will be processed by any of the data processing methods depends upon need and volume of data in the form of as asymmetrical data.



Proposed System for IoT Networking

Standard IoTs Networking techniques

Most of the tiny Iot Devices having no user interface in such cases dynamic user interface will be installed at local and cloud server . The IOT device having two types of RF tags for auto networking configuration. RF tag I having NFC tag is used for IoT to IoT device and RF tag II for IoT to local or remote server networking using Mac addressing scheme of virtual IP[29] address scheme of OSI[26] standard. To establish IOTs Local as well as cloud network connectivity there are various methods various using traditional networking techniques such as RF Tag on IoT devices, NFC Tag on IoT Devices, QR Code on IoT devices and BLUETOOTH type IoT devices .

RFID[19] Tag on IoT Devices

RFID[19] is the Radio frequency Tag which uses electromagnetic waves to identify and connect/ attached to cloud database local servers. Other parts are using radio waves, RFID[19] based device require a tag as well as reader mechanism and an antenna. RFID[19] tags a memory data chip which stores information as data, and in order to see that data, you need an RFID[19] reader to identify or attached the device. Passive RFID[19] tags are used in IOT devices, although RF tag do not have own power source, have small read range up to 25-30 meters but in active RFID[19] tags have own power supply, that have higher range up to 100 meters.

NFC[27] Tag on IoT Devices

Alternatively Near Field Communication (NFC)[27] can also be used for the communication among one IoT device to another IoT device having short distance less than 4 CM in-between them.Most of the tiny IoT Devices having no user interface in such cases dynamic user interface will be installed at local and cloud server . The IOT device having two types of RF tags for auto networking configuration. RF tag I having NFC tag is used for IoT to IoT device and RF tag II for IoT to local or remote server networking using Mac addressing scheme of virtual IP address scheme of OSI[26] standard. Near Field Communication key enable IoT devices to unpowered various objects with its ability to establish

connection to the unconnected object by easy-to-use with its "scan -and-go" functionality and provides a number of security options too. The smart home automation can be done using NFC[27] which simplify IoTs as Connecting , implementing and Controlling with Near Field Communication technologies. Other many other benefits of NFC provide major capabilities that will make IoT to wide-scale adoption.

QR Code[28] on IoT devices

QR means Quick Response type of special code that helps in fast scanning from any scanned camera gadgets. Nowadays QR codes are use to link to particular app of URL too on website on internet using mobile or computer. It has wide range of application from merchant store to online payment etc as contact less payment means.

If IoT devices are assigned QR code[28] that it is easy to link all device to local host or thru common app to form small cluster too

BLUETOOTH[21] on IoT devices

Bluetooth is a kind of small open wireless standard for making communication between various electronics gadgets for about 10 to 100 metres range as it can also support lots of product fictions. Products with Bluetooth tag if made part of IoT devices than it can provide an IoT device additional sensing information of nearest network. Bluetooth tag based technologies are quite simple to use and it interact direct with users and accept their authentication prior to make network connection.

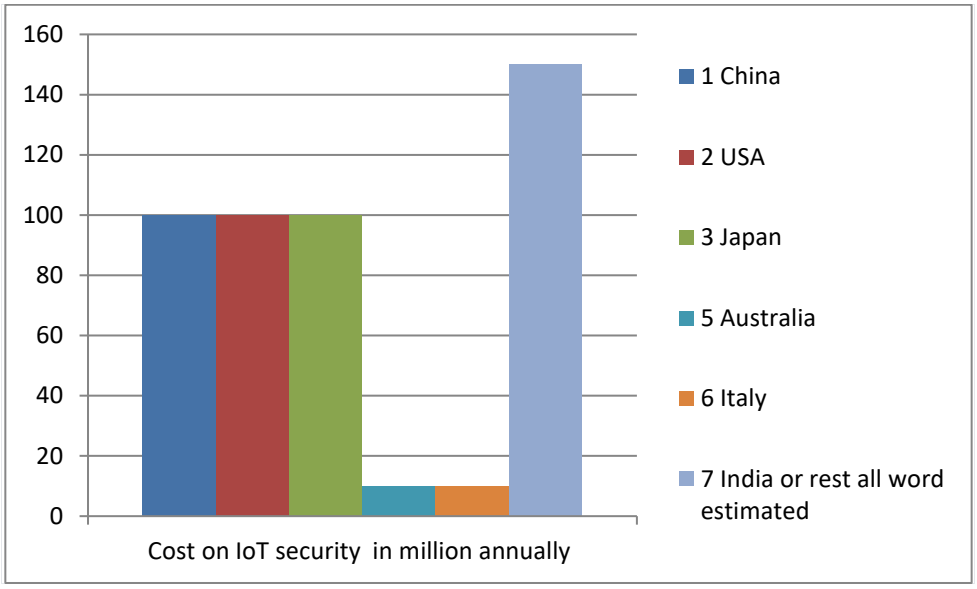
Based on the comparison of all the above available Iot network technologies such as QR, NFC or Bluetooth etc all depends on the objectives and requirement of network based on various IoT enabled products. Every time regardless of method or technology, all must be uniquely coded to have proper data communication and accurate networking between IoT devices.

Result & Discussions

Based on the current trends in IoT enabled devices in the market the following is the projected scenario of the country based IoT enable devices in use and risk investment based on the project data by company through their websites

Sr. No	Major Key players Country	Total number of IoT enabled products up to 2025 (in Million)	Total number of non standard IoT enabled products up to 2025 in Million	Security Risk	Cost on IoT security
01	China	3 Million [17]	2.8 Million	High	More than 100 Million US$ annually [17]
02	USA	1 Million [17]	0.5 Million	Medium	More than 10 MUS$ [17]
03	Japan	2 Million	1.5 million	Medium	More than 10 MUS$ [17]

04	UK	0.5 Million [17]	030Million	Medium	More than 10 MUS$ [17]
05	Australia	05 Million [17]	0.35 Million	Medium	More than 10 MUS$ [17]
06	Italy	1 Million [17]	0.80 Million	Highest	More than 10 MUS$ [17]
07	India or rest all word	2 Million [17]	1.9 million	High	Still many country's Govt. has not yet enforced security for IoT enabled devices.



Cost as well security Comparison of IoTs Networking techniques by implementing mandatory IoT devices having hardware address (Mac/RFID/IMI etc) followed by registration of users/Manufacturer or reseller to common randomization algorithm protocols cum Cloud database . Which means by making IoT enabled products as standard registered products and removal of all not standard IoT Enabled products from market will not only improve the country revenue on detecting the fraud as well secure the customer interest and usage of IoT enabled devices. As per project market for IoT enabled devices to 2035 is around 50 billionUS$ (50 million IoT enabled devices and cost on IoT enabled devices security . So enhancing security at the beginning is by removing all the non standard IoT enabled devices usage will not only saves cost on IoT security but also use of excising technology software and hardware networking protocol usage, So making standard IoT hardware and software protocol will be much useful in detecting security issue building customer faith as well as enhancing Iot enabled devices business in many sectors worldwide.

Conclusion

Establishing country based national as well as International standard for IoT enabled devices at earlier stage of the launch or product growth period of this huge market of IoT enabled devices and automation in almost all sectors will be highly beneficial to cut the adjacent cost that Every country Government has to bear to provide or resolve security related issues faced due to non standard IoT

enabled devices functional in the market. Although there are available some standard related an internet network model that has to be implement mandatory and modified IoT enabled devices to have permanent identification address such as Mac or IMI or RFID[19] etc assigned to them. Every IoT device need to be first register to common data with the help of dynamic user interface common to all IoT devices and non standard IoT devices should be banned to be used and sold in the market. Non standard IoT ebnabled devices are more vulnerable to face security issues as compared to standard Iot enabled devices as they are supported with high standard of security protocol from data security to network security as well block chain technologies protection in case of cloud computing on distributed database.

Declaration

The author declares that he has not any known financial interest or any other relationship to influence the work published in this research paper.

Acknowledgement

The author would thanks all the higher authorities and faculty members of Government Polytechnic Rohru Distt. Shimla India for their immense support and encouragement.

References

1. M kim, “IoT devices grow 2.5x in 2022, expecting half the world’s networking devices, “Science times ,2019.
2. Ahmed I. Taloba ‘et al’, A Block chain based hybrid platform for multimedia data processing in Iot-Healthcare Alexandra Engineering Journal (2023) 65 263-274.
3. Hui Hu ‘et al’, “Vaccine supply chain management : An intelligent system utilizing blockchain, Iot and Machine learning” , Journal of Business Research 156(2023 113480
4. Sharda Tiwari ‘et al’, “A real time secured medical management system based on blockchain and internet of things.” Elsevier Measurement Sensor 25(2023) 100630
5. Siti Rubaeah ‘et al’ “A Review of Internet of Things (IoT) and Blockchain in Healthcare : Chronic disease detection and Data security .”
6. Abid Sultan ‘et al’ “IoT security issues via blockchain: A review Paper” DOI:https://dio.org/10.1145/3320154.3320163
7. Mandrita Banerjee ‘et al’ “ A blockchain future for Internet of things security: a positional paper.” Digital Communications and networks 4(2018)149-160
8. Henry F. Atlam ‘et al’ “ Blockchain with Internet of things : Benefits, challenges and Future Directions.” I J. Intelligent system and applications 2018 6.40-48
9. Bhaskara S. Egala ‘et al’ “ Fortified Chain: A Blockchain Based Framework for security and privacy assured Internet of Medical Things with effective Access Control” Journal of Internet of things (IOT) Vol.No xxx 2020
10. Mohammed Alshehri, “ Blockchain-assisted cyber security in medical things using artificial intelligence” AIMS Press DIO 10.39.34/era.2023035 published 22 November 2022.
11. gi Djuraskovic Blog Internet of Things stats, facts and trends 2023 “https://firstsiteguide.com/internet-of-things-stats/” published in Oct. 2023

12. Lionel Sujay Vailshery research " https://www.statista.com/aboutus/our-research-commitment/2816/lionel-sujay-vailshery " published on Jul 26, 2023
13. Grand view Research Report https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market "published in 2017
14. Statista research report " https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027 " published in November 2022
15. Kumar et al. J Big Data (2019) 6:111 https://doi.org/10.1186/s40537-019-0268-2" Internet of Things is a revolutionary approach for future technology enhancement: a review" Survey paper
16. Selvaraja Angaswamy Et al. "USE OF WI-FI CONNECTION BY THE RESEARCH SCHOLARS OF UNIVERSITY OF MYSORE, KARNATAKA: A STUDY" published in January 2014 vide 2(10):150-157 DOI:10.14662/IJALIS2014.041
17. Davinder Parkash Chechi Et. al. "THE RFID TECHNOLOGY AND ITS APPLICATIONS: A REVIEW" published in September 2012 vide 2(3):109-120 Research Gate
18. Gyan Prakash & Sadhana Pal "WIMAX TECHNOLOGY AND ITS APPLICATIONS" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 2, pp.327-336
19. Madavi Verma & Satbir Singh "An Overview of Bluetooth Technology and its Communication Applications" published in May 2015 5(3):1588-1592 ResearchGate
20. Shams Forruque Ahmed et.al. "Industrial Internet of Things enabled technologies, challenges, and future directions", published in Computers and Electrical Engineering, Volume 110, September 2023, 108847ELSVIER
21. Stuart Ferguson and Rodney Hebels in Computers for Librarians (Third Edition), 2003 ScienceDirect
22. Jeremy Martin et. al. "A Study of MAC Address Randomization in Mobile Devices and When it Fails Proceedings on Privacy Enhancing Technologies ; 2017 (4):268–286
23. Yasin N. Silva Et.al. "SQL: From Traditional Databases to Big Data" published in February 2016 DOI:10.1145/2839509.2844560 Conference: the 47th ACM Technical Symposium
24. John D Day et. al. "The OSI reference model" January 1984 Proceedings of the IEEE 71(12):1334 – 1340 71(12):1334 – 1340 DOI:10.1109/PROC.1983.12775 Source IEEE Xplore
25. Hussein al ofeishat "Near Field Communication (NFC)",February 2012 12(2):93-99 ResearchGate
26. Abbash AI-Ghalli "QR code based authentication method for IoT applications using three security layers" August 2020 TELKOMNIKA (Telecommunication Computing Electronics and Control) 18(4):2004 18(4):2004
27. Bhaskra et al " Fortified Chain : A blockchain based framework for security and privacy assured internet of medical thing with effective access control" Journal of Internet of things (IOT) Vol. No XXX.2020
28. Mohd. Alshehri " Block chain-assisted cyber security in medical things using artificial Intelligence" Electroni Reacher Archive published on 22 Nov. 2022.
29. Zia Ur Rahman "GSM Technology: Architecture, Security and Future Challenges". February 2017 5(1):70-