IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

Challenges in Wireless Network for IOT

Onkar Gatir[1], Pranay Kokare[2]

U.G. Student, Department of Information Technology, B.K.Birla College of Arts, Science and Commerce, Kalyan, Maharashtra, India[1]

U.G. Student, Department of Information Technology, B.K.Birla College of Arts, Science and Commerce, Kalyan, Maharashtra, India[2]

ABSTRACT:The Very Promising paradigm and extensively faster adoption rate in the market, Internet Of Things(IoT) With specifically Wireless mobile network, Cloud Computing with advance infrastructure, power-efficient solutions surging ahead rapidly with some crucial significant challenges. IoT Networks representing the future of networking, automation, transferring sensitive data to the cloud database through the number of complex nodes,hostile-tricky environment, Data analysis, and of course with facing the number of security attacks on the network. In moving years user's widespread confidential/private/important data protection will be a major challenge for all types of networks.
IoT is revolutionizing the way humans lives by entering in the sector like health, transportation, automation, entertainment, automobile, etc. The purpose of this paper is to explore the challenges of the wireless network through the perspective of the Internet Of Things(IoT) such as user privacy, cloud storage, sustainable power solutions, hardware disposal, biological safety, accurate extraction of data in irregular conditions/environment. Precise classification of challenges with co-relation with each other. In the end, an overall discussion of the impact of IoT that may occur in the future

KEYWORDS: Internet Of Things, Wireless Network,data privacy and security in Iot, challenges in wireless Iot network

I. INTRODUCTION

The Internet Of Things (IoT) is a set of interconnected physical devices/objects/things that are embedded with sensors, power supply, software or code script, and related technologies to collect, transfer,
Exchanging,transferring and sharing data with other devices and systems over the internet. these devices vary from small sensors to count temperature in the room to the complex industrial automation tools. The expected number of these devices is 22 billion by 2025.

Internet of things is cheaper low-cost computing devices for low-level computing, data extraction for big data, cloud, machine learning, analytics with Smart devices such as smartwatch to automobile automation. The primary goal of the internet of things is low-cost computing with minimal or no human intervention. this
The hyper-connected world provides so many facilities at a low cost. But with as such so many advantages there are some disadvantages or being selective challenges. from user's sensitive data to biological safety(smartwatch to nanorobots), complex infrastructure to connectivity, sustainable power solution to hardware disposal and storage, cloud data storage to environmental concerns such as global temperature issue.

The paper is organized as follows. Section II describes the related work done on the Internet of Thing sector. in section III fundamentally important challenges are discussed in detail. analysis of each challenge with relevant information done in section III. After detection of challenges and analysis of all facts, figures, tables, statistics, justification of the analysis done in paper IV. Finally, Section V presents the conclusion.

II. RELATED WORK

The concept of connected devices has a long history of 70s.that time idea of connected devices called embedded systems or pervasive computing what we now call IoT. The surprising fact is the term internet is just 16 years old logically younger than embedded systems. the actual name Internet Of Thing was given by Kevin Ashton in 1999 during their work of Procter&Gambel. M2M, Web Of Things, Industry 4.0, smart Systems are some similar terms. there is some dangerous outcome of the IoT expansion, specifically in terms of data privacy and security. The basic concept of smart device connectivity was discussed in early 1982, with the Coca-Cola commercial machine

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

converted at Carnegie Mellon University into the first ARPANET connected, that machine system was able to report its list and whether freshly loaded drinks are cold. Mark Weiser's 1991 paper, which was widely distributed, "The Computer of the 21st Century", and educational institutions such as UbiComp and PerCom presented a modern IoT concept In 1994, Between 1993 and 1997, several companies proposed solutions such as Microsoft at Work or NEST's Novell. The camp gained momentum when Bill Joy considered metal communication as part of his "Six Web Web" framework, which was launched at the World Economic Forum in Davos in 1999. nowadays IoT is a vital part of day-to-day life from fire sensors to auto-driving car machines now become so smart with the Internet of things. the future of IoT is leading the direction of advanced biology tools to save or make better human life.

III. METHODOLOGY

Challenges in Wireless Network in IoT:

A) User Privacy Violation:

The vast availability of wireless networks in today's life leads to create more and more usage of IoT in day-to-day life. this routine creates the cycle of data transfer in the wireless network. those are like smartwatches, pulse meters, fire sensors, infrared sensors, and so on. these interconnected nodes create a very good network of the device for transmitting information but it becomes easy to do cybersecurity attacks. the vulnerability is obvious because the interconnectivity of the network brings along accessibility to an unauthorized person. majority of the time people are not aware of the fact and eventually open a door to bad guys. there are some small points mentioned below

1) Update time-generally in IoT manufacturers update the software quarterly which gives hackers plenty enough time to crack security protocol and access sensitive data.

2) Remote Access- IoT devices utilize various protocols for remote access like WiFi, ZigBee, etc. in that protocols some restrictions are not mentioned so hackers get back door to get into the system.

3) Malicious third-party application-ordinary user may not be aware of the difference between technical aspects of the software system. so it can be possible to fool them with malicious third party app which creates some vulnerability in the system

B) Security Attacks:

1)The Term Security attack is an attacking means to break the security of IoT Networks. the goal of those security attacks vary from destroying data packets or corrupt them, steal users data/privacy, destroy networks, prevent or stop data transmission, etc

2)Let's take an example of most fitness trackers to remain visible at the first pairing of BlueTooth connection. This is a Lack of one Global IoT Security standard, For cheaper Prices and manufacturing convenience companies stick to manufacture IoT products with Poor Security. because they don't have a security element at first place in their vision. some obvious security threats are as follows

a)Weak Password b)Hardware issue c)lack of frequent security attacks d)Insecure data transmission protocols or storage. e)Lack of Security awareness in users f)poor security update support

3)Types of attack on IoT Devices are as follows

a)BotNet Attack- A single infected IoT device can't make big difference in IoT Network but a group of devices.to make this attack hackers create an army of bots by infecting IoT devices. all IoT devices will attack the target by making thousands of requests from the target and bring the target device down. An example of this kind of attack is Mirai Bot Attack in 2016. multiple DDoS(Distributed Denial of Service) attacks from hundreds of thousands of IP cameras, NAS, and DNS Server that service to big platforms like Github, Twitter, Reddit, NetFlix.
What is more dangerous is these types of attacks can create fluctuations in power grids, manufacture Plants, Transporation systems, Water Filter systems which can target a big group of people.

b)Industrial Espionage & Eavesdropping -invading privacy is one of the serious issues in IoT.infected devices can't just spy on people but using that attacker can demand the money or some valuable demand. this does not just remain on the perspective of spying but devices like a smartwatch, smart toys, Wearable collect user data. attack on industrial level company's sensitive business data can be a leak.

c)other attacks- in some other attacks attackers hijack the devices and can gain access to the medical IoT devices, Gaining control of it, and being able to alter the data and change the medical signals. which can eventually damage the health of the patient.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

C) Connectivity Standards-Internet of Things is covering a wide sector of the world. like smart homes, industrial area, research, and development, automobile area, data science, etc. there are almost 14 standards used in IoT networking to enable the technologies like RFID, Li-Fi, Optical tags and quick response codes, Bluetooth low energy, Low energy wireless IP Networks, ZigBee, Thread, LTE Advance, wifi Direct, HalLow, Homeplug, Ethernet, MoCA are some commonly used technologies. Interoperability of those devices is a major challenge in IoT as from the customer perspective it has to be easy to connect and faster.the topmost interoperability quality is achieved by the efficient communication of software, application, services, and devices in the most predictable predefined style. which may not always become true. the reliability of any IoT wireless devices depend on their bidirectional signaling and routing data between devices, In smart home devices should contact to servers, the server should generate predictable action plan depends on data and after communication certain action should take place. This entire phenomenon should be performed in expected time span which defines the standards of Connectivity which is not so easy to Handel

D)Power Consumption-IoT Technologies need a Continuous power supply stream where only battery power is the option. that is not always economical. the expanding capabilities of the IoT devices and increased interest in artificial intelligence processing demand the better and sustainable power supply. Combining several methods of power consumption and harvesting energy or somehow reusable energy devices is a big challenge in front of the IoT world. One of the biggest obstacles to IoT technology is the implementation of continuous, efficient use. Most Internet of Things (IoT) functionality comes at a cost of power. The World is aware the traditional battery power is the most fitting solution for such applications and services, it is not always money First, the battery capacity may not be enough for emerging IoT devices with the capacity to connect and connect to a network. In addition, there are concerns about the cost of new batteries and the hours a person needs to service devices.

On that note, even renewable batteries made for reuse, which need to be replaced, have a negative impact on our environment. As businesses around the world become more aware of the environment, this has been seriously considered. Finally, continuous power access from the power grid does not always happen. Whether it's the type of deployment, or the cost of connecting devices to the grid, accessing unlimited power is a recurring challenge for many IoT systems.

E)Data Storage - IoT is a combination of the devices which create, share and transmit data over the IoT network. data sharing, as well as data storage, is primary or one of the most important factors to take into consideration. the distributed environment has distributed storage with one and more servers. server heat generation is one of the future concerns for the green earth revolution. generally, data get stored in the cloud nowadays which is a favorite option of the business owners and eventually for customers. being so many devices connected to the edge it is a major challenge not to transmit it and move to a data center in a timely fashion.in many instances, the value of data is not completely served or justified in the storage. For example, if we need a car number from a CCTV camera we have to go through with the entire video, storing the entire video is not ideal for data storage as well as for transmission. the video may need in the future for tracking some activity or most of the time it gets discarded. All major cloud providers offer affordable storage systems based on object storage technology. With very fast and cost-effective networks with data entry, the public cloud is a great place to opt for IoT data volumes generated by businesses and research.

Cloud service providers have expanded their product offerings to add great data analytics tools that include and process large volumes of unstructured content. This allows businesses to develop more sophisticated machine learning / Artificial Intelligence programs to process data more efficiently than would otherwise be available in a private location.

F)E-Waste Disposal -in the year 2016 CEO of Softbank predicted that in the next 20 years there will be a trillion devices connected on the planet and some of them are in the orbit of the planet. as we adding more and more computing power to each and every possible device we are also increasing the problem of the e-waste. the united nations research found that humans have generated approx 44.7 million metric tons of e-waste globally in just 2016, and it is expected to grow bigger to 52.2 million metric tons by the end of 2021. We are aware that many small connected devices such as smartwatches, IoT devices, or wearables are designed to fail intentionally if their battery stopped working. At that point, sailing and purchasing turn on a big scale. the challenge of making and installing sustainable batteries is huge challenge in front of engineer

G)Business Adoption-as we know the worldwide adoption of IoT is growing so fast with the demand. with data and analytic company, global data projecting the global market for IoT and related will hit 318 Billion Dollars in 2023.those numbers saying the better future of IoT and expansion of related products and services. but in fact, 90% of the almost 1000 Forbes Global 2000 enterprises surveyed and said that they are experiencing very significant barriers

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

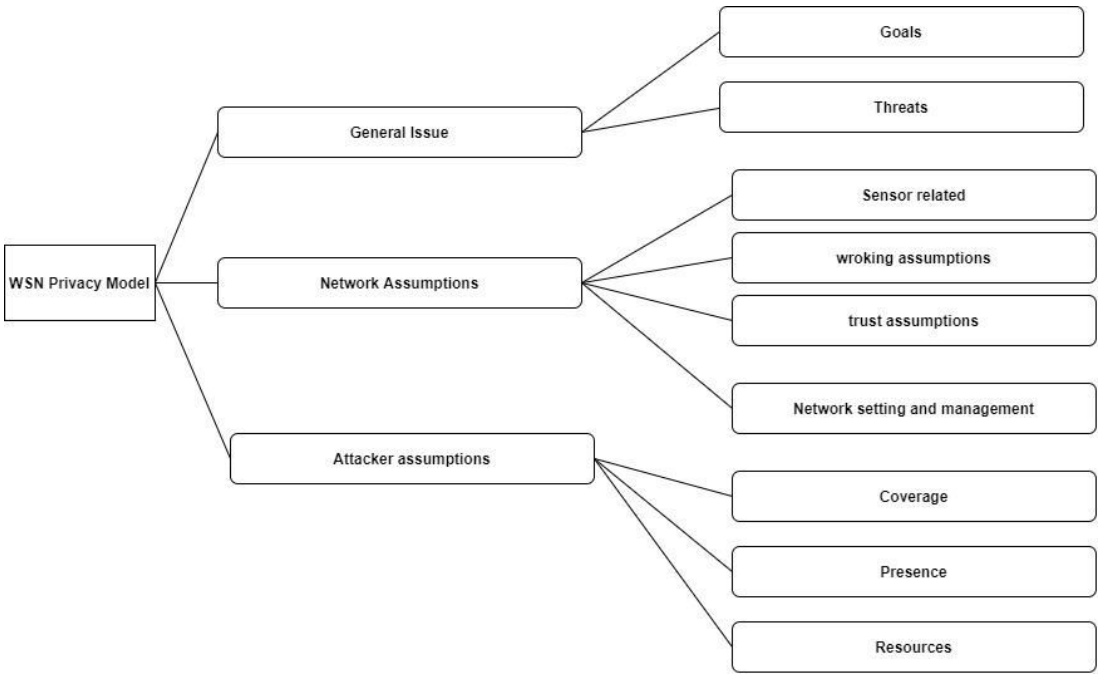
|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

to accept the IoT and changes related to that. some of the major reasons for that are the lack of In-House skills to Security concerns as said in A and B parts. which is also justified but in moving year big businesses which depend on client data so much they have to face a great challenge to adopt it and related resources/skills.

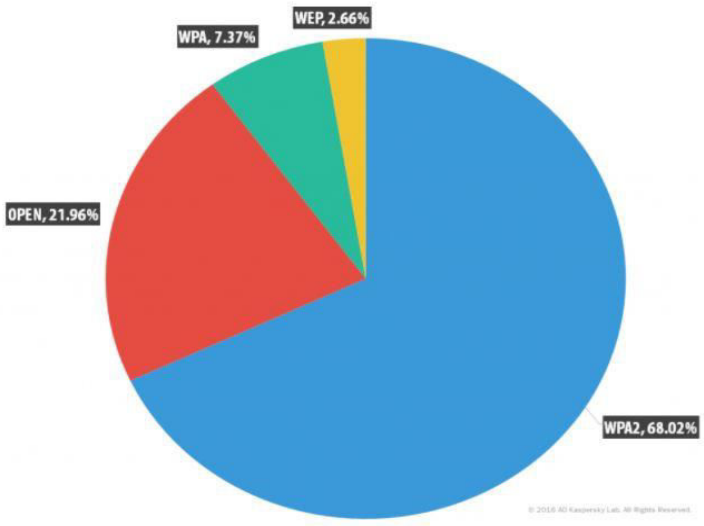
IV. EXPERIMENTAL RESULTS

Figures shows the general privacy model of the wireless networks related to interconnected device of IoT



(a)Privacy model in Wireless network

Following Figures (b) shows the Encryption type Used in Public WiFI hotspot across the world which is interconnected devices of IoT



(b) **Encryption type used in public Wi-Fi hotspots across the world**

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

Following Figures (c) shows the Encryption type Used in Public WiFI hotspot across the world which is interconnected devices of IoT

Communication Technologies
NFC, RFID, Bluetooth, ZigBee, ZWave, IEEE802.15.4, WiFi, 3G/ 4G, LTE, , WiMAX, Weightless, DASH7, PLC, QR Code, Ethernet
Prototype Hardware
Raspberry Pi, Hackberry, Arduino Yun, Arduino Uno, PCDuino, the Rascal, Cubie Board, BeagleBone Black,
Identification Techniques
IPv6, AIDC, RFID, QR Code, barcode etc.
IoT Architectures
3-Layer, 5-th layer, IoT-A, BeTaaS, OpenIoT, IoT@Work, IOT-I etc.
Operating System
Tiny OS, Contiki, Mantis, Nano-RK, LiteOS, FreeRTOS,
Protocol
IPV6, 6LOWPAN, UDP, Chirp, DTLS, XMPP-IoT, SSI, NanoIP , MQTT

(c) Layers of Internet of Things

Following Figures (d) shows the relative power Consumption Details of devices

	Bluetooth (BLE)	ZigBee	Wi-Fi	Wi-Max	LoRa	LTE	Z-Wave
Standards	IEEE 802.15.1 IoT Interconnect	IEEE 802.15.4	IEEE 802.11 ah	IEEE 802.16	IEEE 802.15g	3GPP	Z-Wave alliance
Network Type	P2P	Mesh	WLAN	MAN	LPWAN	GERAN /UTRAN	Mesh
Power Consumption	10 mW	30mA TX1, Standby 3# 956; A (low)	400+mA TX1 Standby 20mA (High)	N/A	Very low power	5W / 1 W	Very low power
Data rate (Mbps)	1	0.25	Min 150 kbps	70	250 kbps	0.1-1 Gb/s	0.1
Range	35 m	10-100 m	1 Km	50 km	100 Km	28 Km/ 10 Km	30 m
Spectrum	2.4 GHz	2.4 GHz	2.4-5 GHz	2 – 11 GHz	868-915 MHz	700-2600 MHz	908.42 MHz

(d) Power Consumption Details of Internet of Things devices

V. CONCLUSION

We have seen the Internet of Things as a paradigm of the future with the perspective of technologies and development.

Internet of things is cheaper low-cost computing devices for low-level computing, which is surrounding wide sectors in the world. The primary goal of the internet of things is low-cost computing with minimal or no human intervention. But with this, there are some crucial challenges that need to face such as User Privacy Violation, Security

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008178|

Attacks, E-waste management, data storage with the heating issue, energy consumption, Business adoption. we have to think with the perspective of the future and face these challenges and solve the respective Problem.

REFERENCES

[1] M. A. Burhanuddin1in,Ali Abdul-Jabbar Mohammed1 , Ronizam Ismail2 , Mustafa Emad Hameed3 , Ali Noori kareem4 and halizah Barisron1,"A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective",,e-ISSN: 2289-8131 Vol. 10 No. 1-7

[2] S.Pradeep1, T.Kousalya2, K.M.Aarsha Suresh3, Jebin Edwin4 "IoT AND ITS CONNECTIVITY CHALLENGES IN SMART HOME" e-ISSN: 2395 -0056 Volume: 03 p-ISSN: 2395-0072

[3] https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536?scroll=top&needAccess=true

[4] https://www.researchgate.net/profile/Soumyalatha-Naveen/publication/330501274_Study_of_IoT_Understanding_IoT_Architecture_Applications_Issues_and_Challenges/links/5c434fea458515a4c731d4bb/Study-of-IoT-Understanding-IoT-Architecture-Applications-Issues-and-Challenges.pdf

[5] https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/

[6] https://www.intellectsoft.net/blog/biggest-iot-security-issues/

[7] https://internetofthingsagenda.techtarget.com/feature/Top-challenges-of-IoT-adoption-in-the-enterprise

[8] https://spectrum.ieee.org/the-internet-of-trash-iot-has-a-looming-ewaste-problem

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details