A Review Paper On Challenges Of Internet Of Things in Power System

Mrs. Harini Vaikund[2], *Sneha Hosagoudar*[1] , *Miss Lata K Jadhav*[3]

[1]Student, Department of EEE, Dr. Ambedkar Institute of Engineering and Technology, Bengaluru, India
[2]Assistant Professor, Dr. Ambedkar Institute of Engineering and Technology, Bengaluru, India
[3]Assistant Professor, Sri Taralabalu Jagadguru Institute Of Technology, Ranebennur,India

Abstract: The main aim of electrical power system is to provide clean distributed energy for the global economic growth. For this purpose Internet Of Things (IOT) had been introduced in the power system. IOT has capability such as real time monitoring, intelligence, power control managing distributed generation along with eliminating energy wastage and energy saving is possible. Along with all the merits there are some risks and challenges associated with Internet of things (IOT). This paper provides brief information about the internet of things, working, benefits and challenges of IOT.

Keywords: *Connectivity, Data Processing, Sensors ,User Interface, Internet of things.*

INTRODUCTION

Electrical power systems are actual time energy provider systems. Actual time means that the power is generated, transferred and distributed to the consumers. These power systems are not storing energy which have been generated, supplied to the consumers as per the demand. As per the demand goes on , generators generate power according to the demand. The major drives of economic development are power and energy system. The main aim is to provide clean and affordable power .

An Electrical power System has three major components they are- generation, transmission and distribution. In generation power is generated by generators and supplied. In transmission, generated power is transmitted through transmission lines to the respective load centers. In distribution, power is fed to the nearby industries and domestic areas. Usually for large scale power transmission three phase AC power is used.

For providing flawless power supply, the advanced technology have been emerged that is Internet of things which is most emerging technology nowadays. The term Internet of Things was coined by Kevin ashton of procter & gamble. At that point , he thought internet of things is needed in emerging fields such as power systems, military, healthcare.

Internet of things can be defined as “Connecting day to day things immersed with electronics software and sensors to the internet for computing them to gather and interchange the information”.

Internet of things is needed to develop interdependence of humans to interrelate furnish and collaborate to things. It connects systems, sensors and actuator instruments to the broader internet. . Internet of things is now a reality. As more of us are using personal electronic devices. This is similar to humans talk to each other through media’s such as skype, duo or some other applications which is very common in today’s life. By continuously communicating IOT upgrade safety and reliability of the power system.

The utilization of internet of things in electrical sector has made dramtic change in the system. The internet of things has improved utilization of wireless technology to interconnect things or objects and also by this power consumption is reduced hence overall cost of the system is dropped. The IOT has unwrapped paths in many areas from military to healthcare. Every new emerging technology has both benefits and challenges likewise Internet of things has advantages and challenges.

Figure 1 Internet of Things

Internet of Things is evolved from machine-to-machine (M2M) communication, i.e., machines associating with one another via a network without human interaction.M2M alludes to interfacing a gadget to the cloud, administering it and gathering information. M2M is taken to next dimension, IOT is a sensor network of various smart gadgets that unite systems, peoples and other applications to accumulate and split data. As its base, M2M recommend interconnection that permits internet of things.

The internet of things is likewise characteristic expansion or addition to SCADA(Supervisory Control And Data Acquisition), for the control of process, for collecting of data in actual period from far away places to control devices and conditions, a sort of programming application program is included. Supervisory Control and Data Acquisition(SCADA) systems have hardware and software elements. The hardware collects and sends collected information into computer that has SCADA software installed, where it is then operated and submitted in well timed way. Application of IOT in power systems include management and monitoring of power consumption in smart grid and performance.

Working of IOT

The mechanism of IOT is highly technical. The working of IOT system is quite confusing to understand however it has major four components such as sensors or devices, availability, information integrity and user interface. Let us know brief about the components.

1) Sensors/devices

To begin with, sensors or gadgets help in gathering social affair careful minute information picked through encompassing atmosphere. Majority of this gathered information may have different level of difficulties going through a basic temperature observing sensing element or a mind bogging full video feed.

A gadget can have different sensors that can package together to accomplish something other than sense things. For instance,our telephone is a gadget that has different sensors for example GPS, accelerometer, camera.

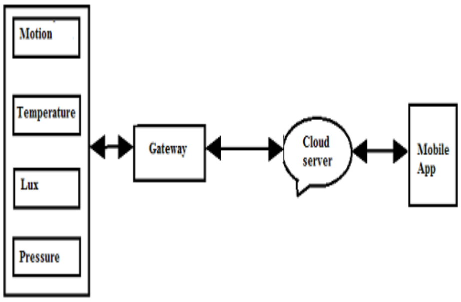

Figure 2 : Sensors/devices

2) Connectivity

At the point when the data is acquired/gathered, then transferred to a cloud foundation although needs a vehicle for transport. The sensors can be associated with the cloud through contradictory instruments of resemblance and transports for example satellite systems, phone systems, Bluetooth, Wi-Fi, low power wide zone organize, wide-zone systems (WAN) so on. Each choice we pluck have a few determinations and trade offs linking power utilization, level and information transmission. Along these lines, plucking the good availability choice in the iot framework is significant.

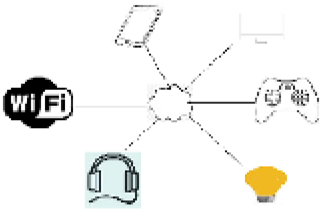

Figure 3: Connectivity

3) Data Processing

At the point when the information is gathered and it gets to the cloud, the thing executes preparing for the got up information.

To continue from undetermined straightforward, for example observing that the temperature scrutinizing on gadgets for example AC or radiators is inside a satisfactory level. It can at occasion additionally be unusual for an example recognizing things (interlopers in cottage) utilizing PC vision on record. Anyway there may be circumstance when a client communication is required, precedent imagine a scenario where when the temperature is excessively high or if there is an interloper in cottage.

4) User Interface

The data made open to the end-buyer some way or other. This may be accomplished by enacting cautions on their cell phones or exhorting by compositions or email .The last step involves notifying the end client about the activity through an email, text, notification or alert sound triggered on their IOT application. Contingent on the complexity of the IOT system, the user can then either leave performed action intact, proactively check in on their IOT system or manually perform an action to backfire or affect the system.

Benefits of Internet of Things

- By the adoption of IOT, generation can be made flexible thus it can bolster effective task at different limit factors rather than continually working in baseload mode.
- The advanced analytics of IOT can predict solar and wind generation so emission of power sectors is reduced.
- IOT has empowered a change where substantially more than supervision and control of the procedure related with production and distribution of power is practiced**.**
- IOT can achieve adaptability in generation and distribution in this way decrease the measure of abbreviation of clean power sources like wind and solar oriented, along these lines increment the capacity to completely acknowledge decrease in ozone depleting substance outflows from higher entrance of variable generation
- IOT can essentially improve the effective utilization of power while upgrading the comfort level of the consumers.
- Real time monitoring, maintenance assist, fault location detection for the generation transmission, substation, distribution of power and other aspects of power grid can be effectively provided by the IOT technology.
- IOT can adequately help in the infrastructure supply in electrical power system and improve the usage effectiveness of the system.
- IOT blocks a system from getting overloaded.

Data Tempering: - large measure of information is produced by many iot devices. This information can be utilized to control wearable medicinal equipments, traffic rules and so on[7], [8]. There are chances of attacks on data tempering, such attacks have potential to cause damage to the system. Objective of such assaults is to change the iot data in such a way as to interrupt the working of the system and create defective decisions. Also by the assaults, considerable financial loss, human harm. This attack leads to more power consumption hence the system is overloaded. Hence consolidated approach or new technology based on randomized way to deal with give low power information trustworthiness in high data rate applications for iot is suggested.

Complexity:- IOT associates smart gadgets to internet also may be connected to cloud computing platforms for analytics and data processing[11]. Scaling of such massive connection introduces complexity around device support, configuration. The answer to this issue is to simplify that means simplifying execution of secure device designs and structure.

Identity spoofing:- also called as personality parodying assault. This attacks are easy to commence in iot access network. By using faked identity such as MAC (media access control) or IP (Internet Protocol) address of the authorized user. The attacker can gain illegal access to the iot network and commence more attacks such as man-in-the-middle attacks and denial-of-service attacks[9].hence virtual channel in mm wave MIMO 5G communication, a two-step detection scheme was proposed.[10]

Eavesdropping:- This is also called as sniffing or snapping attack in which someone tries to steal information that smartphones or other devices transmit over a network. This attack takes benefit of unsecured network communications in order to get the information about sent and received data. Such attacks are quite difficult to detect as they doesn't commence network transmissions to look like abnormally. Hence to avoid or prevent this eavesdropping attacks use updated antivirus software, essential private networks , personal firewalls and avoiding public networks specially for sensitive transactions[12].

Authorization and access control issues:- The rules should be provided around what that user can access this is called authorization and faulty authorization can cause security defects that are difficult to track down. Hence capability based access control approach is proposed that individually or enterprises can utilize to handle their own access control operation to assistance and information[13]
Robustness:-The system has to be maintained stable in fault or disturbances periods for example voltage dips may cause uncertainty in the power system. Voltage dips can be defined as "reduction in the supply voltage to value between 90% and 1% of declared voltage followed by the voltage recovery after short period of time [14]. So two methods for analysis of voltage dips is proposed [15]they are i) critical distance method. 2) fault position method support analysis for electrical power system performance[15].

Identification of things on the Internet:- Various of things are associated to web rises, object or thing distinguishing proof becomes a challenge. Every real object or thing ought to be recognized as virtual object. A genuine item can have several essential proofs speaking to essential services. Hence IPv4, IPv6 identification method[16] is used to solve this issue.

Supplying energy to the sensors:- In iot each item bung and gets data to various articles or cloud of data. For this reason, sensors are used to identify data for every individual item and also energy should be supplied to each sensors. So large amount of energy is required hence this is challenge in iot in upcoming days. Hence a new hierarchical architecture containing 3 surfaces like hardware, middleware and application surface is planned to spare the vitality devoured by the sensors in iot-based system. Here sensors are turned off for specific conditions such as whenever sensors are not used, whenever using sensors affects their battery life and at the point when battery vitality is lower than threshold. A new framework has also been proposed to reduce human interactions and reduce energy consumption, self-organized system is introduced. This system optimizes energy efficiency so that prompts to large sparing of energy consumed by the sensors. There are also methods to provide efficient energy to the sensors. Wireless energy harvesting is the best way to provide vitality to numerous sensors. Hence energy reaped from environment sources like sun oriented energy is utilized to provide for sensors.

Big Data (BD) Processing:- As the measure of data turns into big in iot based framework. Information dealing turns into complex. This is one of the challenge in iot framework, as framework must reserve, analyze information and plan for future dependent on past and instant information. System security gets affected by heavy data. In 2004 google presented dependent on google record framework to manage information. In 2012 Hadoop with license permit acquainted new method to handle the big data, here sparkle SQL as data base framework behind this method progressed towards becoming dominant [17].

Standards:- IOT covers enormous innovations and use cases that go from solitary gadget to massive platforms following various different standards. The criss-cross or confound among iot gadgets utilizing various principles and conventions is a noteworthy issue or challenge. Assuming some data sent by apple iPhone to other cell through Bluetooth but this is not convincible as apple phones only associated to apple phone through Bluetooth. For iot several companies have given different definitions. Based on definitions related measures or standards must be tended to for data processing, communication systems, web conventions, services and applications. Suppose for communication, IEEE 802.15.4 based (ZigBee) is most received standards for low rated wireless networks. In light of such standard information is moved at 800/900 MHz and 2.4GHz. Different gauges like IEEE 802.11p moreover additionally created for remote communication systems.

Security and Privacy issues:- Presenting information on or exchanging information by means of the web is by all accounts the wellspring of numerous data innovation (IT) office bad dreams, and which is all well and good. Hacking is a global industry delivering continuous declares of security breaks. Putting information on the web especially information identified with basic hardware may appear to be risky. Numerous IOT stages think about security as a center component and work to guarantee that any potential breaks are halted before programmers discover them. When the security of the system turns lower, the framework would be progressively undermined by unapproved control. Thereby privacy of the system is also affected. IOT security analysis considers from various features such as given below

Data at rest:- Information housed in applications and databases on-premises or in the Cloud is said to be "very still." Most associations depend on ordinary edge based boundaries, for example, firewalls and hostile to infection programs, to secure information very still. Be that as it may, programmers discover these troves of information overpowering; henceforth, the Broadband Internet Technical Advisory Group and Cloud Security Alliance suggest utilizing a blend of equipment and programming encryption methods to ensure the security and decency of information exceptionally still.

Data in use:- Information "being used" by an application or entryway must be open to clients and gadgets, making it the hardest type of information to verify. With being used information, security relies upon the quality of verification methodology and the quantity of clients and gadgets getting to the information.

Data in flight:- When the data is travelling from device to cloud is it secure? Well Entrenched Internet correspondence conventions equipped with present day cryptography calculations make it for all intents and purposes inconceivable for programmers to unravel information in transmission. While numerous IOT gadgets bolster various security conventions, few empower them as a major aspect of their underlying setup. At any rate, IOT gadgets that associate with versatile applications or remote doors should utilize HTTPS, transport layer security (TLS), secure document exchange convention (SFTP), DNS security augmentations, and other encryption conventions.

Decoupling data just information from activity information- utilizing encoded, single direction outbound interchanges limits defenselessness should the information be blocked while in flight. Wherever conceivable, set IOT gadgets to "flame and overlook." Instead of sitting tight for a ping mentioning an estimation-demonstrative of a two-way channel-the gadget naturally will create estimation, push the estimation to the door or to the cloud on a pre-built up interim or upon an activating occasion, and after that dispose of the estimation information.

The enormous data is accessible on iot stage several specialist organizations like open and privately owned businesses can get variety of data so that client’s information can be imparted with some outsiders thus turns into issue concerned with privacy of the end users. Every information is accessible when the end user permission is there .hence without the permission of user the information is not accessible to the service providers. So adaptive scenario is proposed.

For the most part, there are two kinds of data identified with security of an IOT framework. The primary sort of data is that individuals would prefer not to share it for their security, for example, the situation of their electric vehicle around day. The secondary kind of data is that consumers are stressed about the safety of the data, this may endure money related misfortune if explicit outsiders are educated about it, similar to their ledger or the month to month vitality utilization. Hence users are intended to use their information for particular reason or else not to share their information with third party.

Generally, there are three fundamental classifications of security challenges: individual privacy, privacy saving information mining and hidden advancements protection. Privacy and lawful guidelines are comprehensively acknowledged by government which is firmly needed. Also human rights ought to be considered. The restrictions in iot sensors capacity make difficulties in protection and security issues. This implies that they can’t deal confounded security conventions. To overcome this issue, little cryptographic key size is proposed for iot protection.

Communication Infrastructure:- Utilizing a phone cellular gateway to associate IOT instruments sounds extraordinary, yet user don't get telephone gathering at some remote destinations. Building a framework would be excessively exorbitant. In spite of the fact that LTE-M and LTE-NB utilize existing cell towers, these low-controlled, wide-region systems give a lot more extensive inclusion. Regardless of whether the user doesn't get a sufficient sign for voice calls or 4G-LTE information, the person may in any case have the option to get to LTE-M.

Conclusion: In this paper discussed about the electrical power system in brief then the new technology that is internet of things(IOT) its brief introduction, working advantages and challenges such as security and privacy issues associated with iot are been discussed in this paper. Also solutions to the challenges which are proposed are presented briefly in this paper.

Acknowledgement: I’m grateful to thank my lecturers Mrs. Harini Vaikund and Miss Lata K Jadhav Assistant Professor who have supported and guided to make this paper.

References

1. *Definitions and applications of dynamic average models for analysis of power systems s chiniforoosh J. Jatskevich ; A. Yazdani ; V. Sood ; V. Dinavahi ; J. A. Martinez ; A. Ramirez.*
2. *Study on wide area measurement based transient stability control for power system F.F. song; T.S. Bi Q.X. Yang.*
3. *Systems and load points reliability evalution for electrical power system Ching Tzung Su; Ji Jon Wong; Chi-Jen Fan.*
4. *Analysis of vulnerability of the Latvian electrical power system Aleksejs Sobolevskis ; Inga Zicmane*
5. *Integration of premium power supply on electrical power system Jin Woo Park; ll-Yop chung Byung Moon Han 2005.*
6. *S. Li and L. Xu, “Securing the Internet of Things.” syngress, Elsevier 2017.*
7. *Y. Yang et al., “A Survey on Security and Privacy Issues in Internet-of Things,” in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017*
8. H. Yan, “An Emerging Technology-Wearable Wireless Sensor Networks with Applications in Human Health Condition Monitoring.” J. Manage. Analytics, vol. 2, no. 2, pp. 121-137, 2015.
9. *K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks],” IEEE Wireless Communications, vol. 17, no. 5, 2010*
10. *Efficient Identity Spoofing Ning Wang ; Long Jiao ; Pu Wang ; Monireh Dabaghchian ; Kai Zeng 2018 IEEE Global Communications Conference (GLOBECOM).*
11. *Tutorial 1: IOT big (input) data and learning complexity 2017 Third International Conference on Mobile and Secure Services*

(MobiSecServ)

12. Eavesdropping attack reviewed by jake frankenfield
13. IOT Access Control Issues: A Capability based Approach S. Gusmeroli ; S. Piccione ; D. Rotondi 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing
14. Voltage Characteristics of Electric Supplied by Public Distribution System, CENELEC EN 50160, CENELEC, 1994
15. Methods for Assessing the Robustness of Electrical Power Systems Against Voltage Dips Guido Carpinelli, Member, IEEE, Cosmo Di Perna, Member, IEEE, Pierluigi Caramia, Member, IEEE, Pietro Varilone, Member, IEEE, and Paola Verde, Member, IEEE
16. Savolainen, T.; Soininen, J Silverajan, B. IPv6 addressing strategies for IOT. IEEE Sens. J, 13, 3511–3519,
17. Meng, X.; Bradley, J.; Yavuz, B.; Sparks, E.; Venkataraman, S Liu, D; Freeman, J; Tsai, D; Amde, M; Owen, S.; et al. MLlib: Machine Learning in Apache Spark. CoRR.

JETIR