International Journal of Advanced and Innovative Research (2278-7844) /
Volume 7 Issue 1

# A Survey: Power Consumption monitoring and IoT techniques for electric equipments

Surbhi Mohnani, Mrs Priyanka saxena

SIRT, Bhopal

Email -surbhi.mohnani@gmail.com

**Abstract:**

***IoT is a trending topic over the several articles and portals which deal with the recent trends. IoT is the technique which helps in component communication over the network. A network analysis for the component connected over the internet is required concept in any area. IoT use IPv6 protocol which help identifying the connected component as unique. Further the IPv6 utilize as network traffic analysis for any component connected in a network. Home automation is one of the trend which help in automate electronic equipments used in any public or private house. Each component consume some energy, hence a monitoring and controlling the wastage of electricity is always required. Human interaction with the device is not possible all the time, thus an automation to handle the request is required. In this paper a discussion on IoT and IoT enabled technique is discussed. This paper discuss about , how IoT technique can help in real time for power consumption and other real time fields for public or private utilization.***

***Keywords: IoT, Power Consumption, IPv6, Network Monitoring, Home Automation, Internet Analysis over IoT.***

## I. INTRODUCTION

Computer and the Industry related to the internet devices are increasing day by day. IoT is an emerging field which deals with the data devices and communication entity. There are different manner of communication in between the devices are increasing. Security concern in the communication and passing message from the particular network is one of the barrier challenges to save data from the intruder. Data communication needs to pass in such a way to save it from the attacker activity [9].

IoT makes it enable to communication multiple devices over the IP. IP addressing system is becoming strong to communicate between the given components. IP address assignment to the component participant is an important task thus an identical knowledge and finding the proper communication to every single identity is derived in the concept of IoT. IPv4 and IPv6 is the range of IP address which works with the IP addressing system scenario , thus which help in building a wide range of unique Ip addressing system and mechanism communication entity [10].

IoT is an emerging technology which is aiming to connect every device with the internet and providing control of the technique with each device operation. IPv6 is an enhancement of previous IPv4 which help in communication unique IP assignment and finding best out of given input [11].

As per the discussion associated with the IoT and motivation which make us working towards is given. There is still some more requirement area which is required to get focused working assignment. In order to provide a better and efficient communication, a security is the major factor. It gives the idea of key generation, better key exchange mechanism and communication system.

## II. Literature Review

IoT is an helpful technique for network monitoring and communication. Any request can get handle with the help of internet commands. Human interaction skill can be avoided using the IoT technique. IPv6 is the key for communication which can have a wide range of internet protocol address and unique IP can get assign to N number of components, equipments etc.
Thus the following section discuss about the IoT enabled atmosphere, technique , authors which works with the IoT enabled algorithms.

1. Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers **[01]**

To understand the expansive vision of inescapable figuring, supported by the "Web of Things" (IoT),

it is fundamental to separate application and innovation based storehouses and bolster wide network and information sharing; the cloud being a characteristic empowering agent. Work in IoT tends towards the subsystem, frequently concentrating on specific specialized concerns or application areas, before offloading information to the cloud. Accordingly, there has been little respect given to the security, protection and individual dangers that emerge past these subsystems; that is, from the wide-scale, cross stage receptiveness that cloud administrations convey to IoT. In this paper we concentrate on security contemplations for IoT from the viewpoints of cloud inhabitants, end-clients and cloud suppliers, with regards to wide-scale IoT multiplication, working over the scope of IoT advances (be they things or whole IoT subsystems). Our commitment is to examine the present condition of cloud-bolstered IoT to make unequivocal the security contemplations that require additionally work.

2. Flauzac Olivier, Gonzalez Carlos, Nolot Florent, "New Security Architecture for IoT Network"
In this paper, we have given a review of another SDN-based system structures with circulated controllers. Additionally, our answer can be utilized as a part of the setting of Ad-Hoc systems and IoT. To start with, we gave another design numerous SDN controllers in level with connection. Second, we proposed a design which is versatile with numerous SDN areas. In every space we can have systems with or without framework and every controller is dependable just for its area. The correspondences between areas is made with exceptional controllers called Border Controllers. These edge Controllers need to work in another conveyed association so as to ensure the autonomy of every area if there should be an occurrence of disappointment. We receive a design to ensure the security of the whole system with the idea of network of security installed in every controller to counteract assaults. As future work, we will additionally ponder the attributes of the broadened SDN-Domain, research greater security systems and investigate the potential outcomes of utilizing them with regards to SDN. What's more, we intend to take better favorable position of the building structure of Open sunlight and test our framework at a much bigger scale so as to improve our framework plan.

3. "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues" IEEE communications surveys & tutorials **2015**

The Internet of Things (IoT) presents a dream of a future Internet where clients, figuring frameworks, and regular articles having detecting and inciting abilities collaborate with uncommon comfort and monetary advantages. Similarly as with the present Internet engineering, IP-based correspondence conventions will assume a key part in empowering the universal availability of gadgets with regards to IoT applications. Such correspondence advancements are being created in accordance with the limitations of the detecting stages prone to be utilized by IoT applications, shaping an interchanges stack ready to give the required power—effectiveness, dependability, and Internet availability. As security will be a principal empowering element of most IoT applications, systems should likewise be intended to ensure correspondences empowered by such advances. This review breaks down existing conventions and systems to secure correspondences in the IoT, and additionally open research issues. We break down how existing methodologies guarantee basic security necessities and ensure interchanges on the IoT, together with the open difficulties and systems for future research work in the territory. This is, the extent that our insight goes, the principal study with such objectives.

4. "SecKit: A Model-based Security Toolkit for the Internet of Things". Computers & security · **2014**

The control and assurance of client information is a critical angle in the plan and arrangement of the Internet of Things (IoT). The heterogeneity of the IoT innovations, the quantity of the taking an interest gadgets and frameworks, and the distinctive sorts of clients and parts make critical difficulties in the IoT setting. Specifically, necessities of versatility, interoperability and security are hard to address even with the impressive measure of existing work both in the exploration and institutionalization group. In this paper we propose a Model-based Security Toolkit, which is incorporated in an administration structure for IoT gadgets, and backings determination and proficient assessment of security strategies to empower the assurance of client information. Our system is connected to a Smart City situation keeping in mind the end goal to exhibit its plausibility and performance. [04]

5. John A. Stankovic, "Research Directions for the Internet of Things", National Science Foundation under grants **2014 IEEE.**
Numerous specialized groups are energetically seeking after research themes that add to the Internet of Things (IoT). Today, as detecting, activation, correspondence, and control turn out to be always refined and universal, there is huge cover in these groups, some of the time from somewhat alternate points of view. A key issue that is unavoidable in the Internet today that must be unraveled is managing security assaults. Security

assaults are dangerous for the IoT due to the negligible limit "things" (gadgets) being utilized, the physical availability to sensors, actuators and objects, and the receptiveness of the frameworks, including the way that most gadgets will impart remotely.

6. Design and Implementation of a Simple User Interface of a Smartphone for the Elderly **2014**

In this paper we introduce a straightforward and helpful UI for the elderly with an open source framework stage utilized as a part of cell phones. This plan gives an improved interface, a huge textual style, a major catch and a straightforward UI starter for simple operation, and offers the elderly a technique for the individuals who are more usual to dial telephones. Our outline incorporates an enhanced specific answer instant message work, prescription updates, return arrangements and a logbook with a rundown of the straightforward errands of day by day living, and a simple to work program for offering photographs to relatives and companions. [06]

7. Securing the IP-based internet of things with HIP and DTLS **2013**

The IP-based Internet of Things (IoT) alludes to the inescapable cooperation of savvy gadgets and individuals empowering new applications by methods for new IP conventions, for example, 6LoWPANand CoAP. Security is an absolute necessity, and for that we require a safe design in which all gadget cooperations are shielded from joining an IoT system to the safe administration of keying materials. Nonetheless, this is testing in light of the fact that current IP security conventions don't offer all required capacity a lilies and commonplace Internet arrangements don't prompt the best execution. We propose and analyze two security designs giving secure system get to, key administration and secure correspondence. The main arrangement depends on another variation of the Host Identity Protocol (HIP) in light of pre-shared keys (PSK), while the second arrangement depends on the standard Datagram Transport Layer Security (DTLS).

**8.** Research Directions for the Internet of Things 2014 IEEE

Numerous specialized groups are overwhelmingly seeking after research subjects that add to the Internet of Things (IoT). Today, as detecting, activation, correspondence, and control turn out to be always modern and pervasive, there is huge cover in these groups, some of the time from marginally alternate points of view. More collaboration between groups is supported. To give a premise to talking about open research issues in IoT, a dream for how IoT could change the world in the inaccessible future is first exhibited. At that point, eight key research subjects are counted and investigate issues inside those themes are talked about. [08]

The complete section discuss about the IoT enabled techniques and the application area, where IoT is implemented. It is being observed that IoT help in communication with devices by assigning a unique IP address to each device. Our further work is going to provide an algorithm which help in data communication and finding electronic component usage using IPv6 protocol.

## III. CONCLUSION

IoT is an important sector in current digital world, which deals in communication between components using some automated algorithms. IPv6 is the key concept which helps in assigning a unique value to the devices available in a network. Using unique IP address a device can identify and processing can be done. In this paper a discussion is made through the IoT enabled technique, usage of IoT and challenges face during any IoT enabled communication network. This paper contains the literature review, platform which works with the IoT and home automation technique. There are algorithm and concept which deals in automation, communication while working with IoT network. A further work is finding an algorithm, which can classify the data of given communication, performing decision based on the communication obtained data.

## REFERENCES

[1] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, “Twenty security considerations for cloud-supported Internet of Things”, Internet Of Things Journal, IEEE 2015.

[2] Flauzac Olivier, Gonzalez Carlos, Nolot Florent, “New Security Architecture for IoT Network”, International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems (BigD2M 2015), s. Published by Elsevier, Science Direct, Procedia Computer Science 52 (2015)

[3] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, IEEE

communications surveys & tutorials July 2015.

[4] Ricardo Neisse, Igor Nai Fovino, Gianmarco Baldini, Vera Stavroulakiy, Panagiotis Vlacheasy and Raffaele Giaffreda "Sec Kit: A Model-based Security Toolkit for the Internet of Things". Computers & Security · September 2014.

[5] John A. Stankovic, "Research Directions for the Internet of Things", National Science Foundation under grants CNS-1239483, CNS-1017363, and CNS-1319302. Copyright (c) 2014 IEEE

[6] Design and Implementation of a Simple User Interface of a Smartphone for the Elderly 2014 IEEE 3rd global conferences on consumer electrionces(GCCE)

[7] Securing the IP-based internet of things with HIP and DTLS, April 2013

[8] Research Directions for the Internet of Things 2014 IEEE

[9] Omar Said, "Development of an Innovative Internet of Things Security System", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013

[10] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig, Georg Carle, "DTLS based Security and Two-Way Authentication for the Internet of Things", Elsevier Journal of AdHoc Networks in May 2013.

**[11]** Z. Shelby, K. Hartke, C. Bormann, B. Frank, Constrained Application Protocol (CoAP), IETF draft, RFC Editor (March 2013).