International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 02, February 2022
www.ijates.com
ijates
ISSN 2348 - 7550

SECURITY AND PRIVACY CONCERNS IN IOT DEVICES

[1]Mrs.M.Angelin Rosy, [2]Dr M Felix Xavier Muthu, [3]Ms.S.Elamathi,

[1]Assistant Professor, [2]Associate Professor, [3]I MCA,

[1, 3]Master of Computer Application, [2]Mechanical Engineering

[1,3]Er Perumal Manimekalai College of Engineering, [2]St Xavier's Caholic college of Engineering

[1]angel_rosym@yahoo.co.in, [2]umilfelix@gmail.com, [3]Mathishanmugam.pem@gmail.com

ABSTRACT

Internet of Things (IoT) is a global network of substantial and virtual 'things' connected to the internet. Each object has special ID which is used for identification. IoT is the developing technology which will change the mode of interaction with devices. In future almost every electronic device will be a smart device which can calculate and commune with hand-held and other infrastructure devices. As most of the devices may be battery functioned due to less processing power the security and privacy is a major issue in IoT. Authentication, Identification and device diversity are the major security and privacy concerns in IoT. Major challenges include assimilation, expanding, moral principles commune mechanism, business models and surveillance. In this paper major issues related to security and privacy of IoT are concentrated.

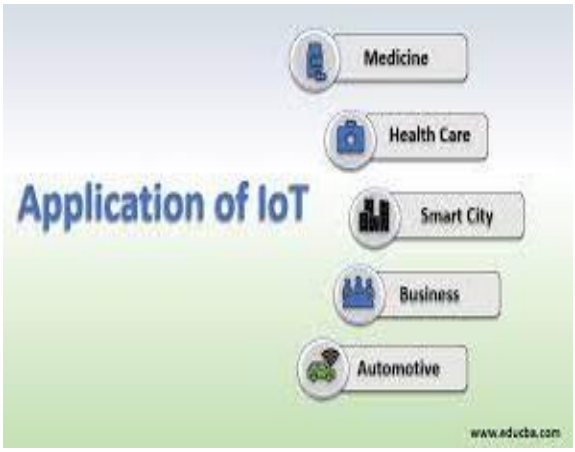
Keywords: *Security, Privacy, IoT, Authentication, Access control, Identification*.

INTRODUCTION:

Internet of Things (IoT) is a conspicuous part of internet future. IoT has a infrastructure of network that is global where any object that is bodily connected to internet has an identity and can commune with the other devices on the internet. The devices like systems, mobile phones, tablets, washing machines etc are a few to name. IoT is a large network of interrelated 'things'. The devices contain micro chip that interrelated with all the devices. These micro chips track the environments and report the same in the network as well as to the humans. The best part of IoT is that each and every bodily entity can be commune and is reliable through the internet. As a result of the low cost internet, large number of devices is connected to the internet. The number of devices joined to the internet in 2008 was more than the people on the earth. According to a research concern there were 4.48 billion devices connected to the internet and the development in 2016 is expected to be 30%. By 2020 it is awaited to attain 50 billion. These devices result as a surface for hackers

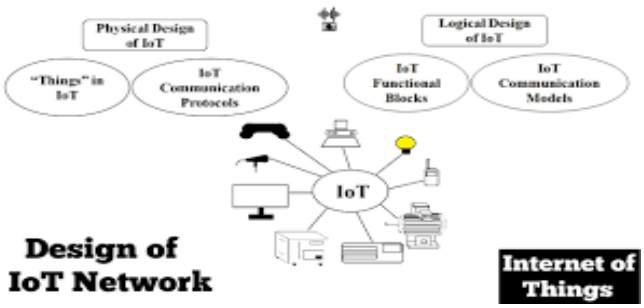
APPLICATIONS OF IOT:

Environmental Monitoring: The environmental protection is made by using sensors and by observing the atmospheric conditions like air and water quality. The wildlife is also observed to know their habitats. The results of the observing are used to develop ways to save our environment.



- **Infrastructure management:** One of the important applications is the process to observe and control the functions of infrastructure like roads, bridges and railway tracks etc. The change in structural conditions can negotiate safety and increases risk, hence it can be observed by IoT infrastructure management. The quality of service are often enhanced
- **Manufacturing:** The real time enhancement of manufacturing can be accomplished. The production and supply can be controlled by using sensors and control systems. This also leads to quick manufacturing of new products.
- **Home Automation:** The information about the gas, water and power can be sent to their convienient company by an automated system. This process can develop the efficiency of the resources. The home automation process can operate the devices like washing machine, air conditioner, windows, doors, lighting and refrigerator to achieve enhancement.
- **Transportation:** IoT technologies were used first in this sector. It uses the assimilation of light sensors, GPS and GSM. The vehicle can act as an entity and commune with each other as well as road side infrastructure. The sensors in the automobiles can be used to avoid collision, traffic management and to provide space for parking.
- **Medical and Health care system:** It is one of the optimistic areas of IoT technology. The patient's vital parameters can be transmitted by medical devices to a platform like safe cloud where it is stored and examined. A particular care can be provided to the aged and chronic disease patients.

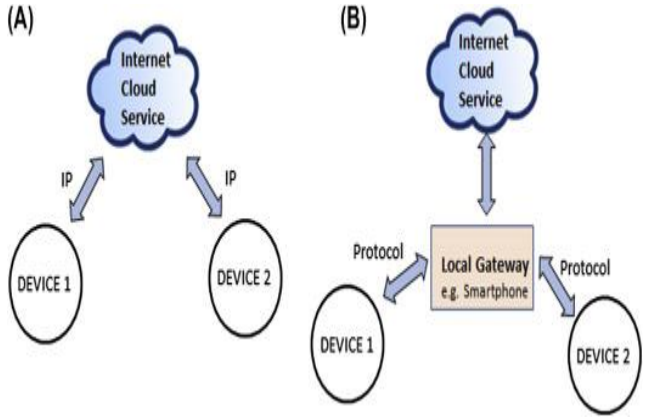
DESIGN OF IOT NETWORK:



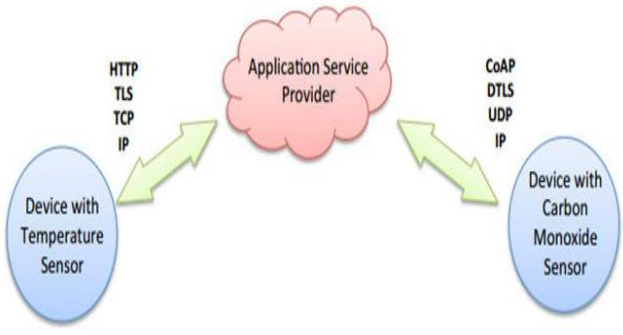
COMMUNICATION MODELS OF IoT:

The functional perspective of IoT devices is prominent as how these devices connect and commune. The communication models are classified into four models as follows:-

- **Device to Device Communication:** In this model, two or more devices connect directly and a commune is established. No emissary application server is used. IoT devices are capable to commune in different types of networks. Usually these devices set up connection using technologies like Bluetooth, Zigbee etc. In device to device network, all the devices follow a protocol to commune and interchange messages. The applications like home automation system interchange data over a low bandwidth. IoT devices like door locks, light switches, light bulbs frequently commune on a low bandwidth in a home automation system.

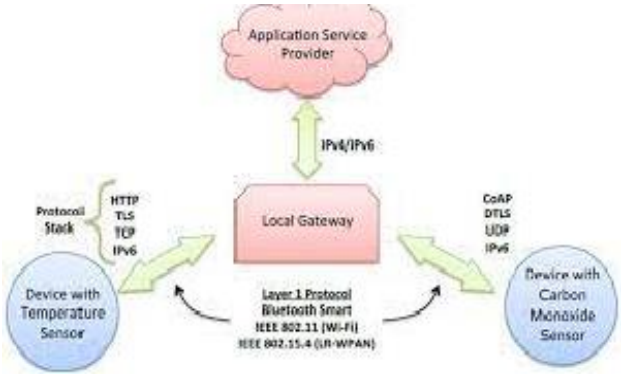


- **Device to cloud Communication:** In this model, an internet cloud service like application service provider is used to commune and interchange the data. The connection is entrenched between the device and the IP network by using Wi-Fi or Ethernet. This type of commune model is used by big companies like Samsung SmartTV. Here the Internet connection is used to transfer user viewing data to Samsung for analysis. This model gives value to the end user by improving the capabilities of the device.

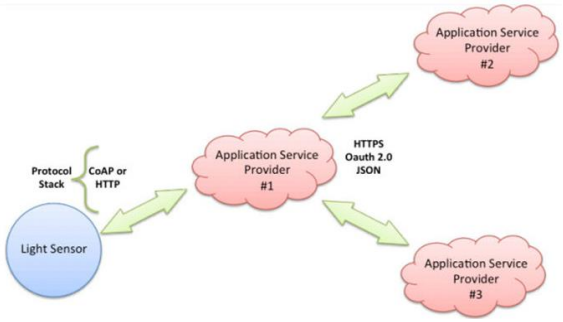


- **Device to Gateway model:** In this model, an application layer gateway (ALG) service is used to interconnect the IoT devices to the cloud service. Here the application software acts as an negotiator

between device and cloud service and functions on a local gateway device to provide security and data translation. In most of the cases, the smart phone with an app to commune with a device acts as a local gateway and transfers data to a cloud service. The devices like Fitness tracker are not capable of communing directly with the cloud service. Hence, they rely on smart phone apps to transfer the data to the cloud.



- **Back-End Data sharing model:** In this model, the commune architecture helps users to export data and also examine smart object data from various sources including cloud service. The data is then loaded to different application service providers. The architecture also helps to collect the data and examine it. An industrialist will be interested in examining the energy consumption of the factory by collecting the data produced by the IoT sensors and the utility systems. The back-end data sharing allows us to access the data and examine it.



SECURITY REQUIREMENTS :

The Technologies are developing rapidly and so are the machines. This development in the technology leads to threats and privacy issues. The smart devices will commune with each other and interchange data in a network. If any device gets crooked then the whole infrastructure is at risk. For example, if a machine is cracked, the production can be at stake along with the critical data involved.

Some of the main security concerns are:-

- **Integrity of Data:** The accuracy of the data transfers between two nodes is an prominent issue. Hence, the correctness of the data should be maintained. For example, in a manufacturing firm, if the hacker gives instruction for the production to stop then it is a very critical issue.
- **Confidentiality of Data:** The data that is transfer between two nodes should be privy. There should be no access to the data apart from the contributor and acceptor. For example, if the infrastructure data is hacked, then there can be destruction to the roads and bridges, moreover the security can be on trouble.
- **Authenticity of Data:** The method of authentication assures that the information received is original and may be trusted. For example, in the medical and health care system, the patient's variable are sent across to different medical centers. If this data is modified by a hacker and then received, the treatment of the patient can be on danger
- **Availability of Data:** Availability of data to the users is always a major unease of IoT. If the user is 'nt ready to access the information, then it is a enormous issue. It should be corrected as soon as possible.

SECURITY THREATS AND CHALLENGES IN IOT :

To design and implement complete security solutions for IoT pattern, identification of threats and challenges of IoT networks, IoT devices, IoT applications and IoT is significant. Internet Engineering Task Force (IETF) has identified several IoT security threats [54]: (1) cloning of IoT devices by suspicious manufacturer, (2) substitution of things with malicious lower quality things, (3) man-in middle hack during commissioning and due to lack of proper authentication and authorization mechanisms in place, (4) firmware replacement with malicious code by an hacker, (5) privacy threat against sensitive data, (6) denial-of-service attack, (7) routing hack, (8) eavesdropping hack on poorly configured IoT network, and (9) extraction of security variable from the bodily unprotected IoT devices.

The following key IoT Security challenges need to be communicated in future

- **IoT security research Device identity:** A singular identity of IoT devices is crucial. Domain Name Servers (DNS) assign names to the interconnected IoT devices. But DNSs are also suspectible of different hacks, i.e. man-in-middle hack, DNS cache positioning attack and so on. hackers may reuse a stolen/hijacked device identity and perform a different kind of malicious activity within the network.
- **Firmware issue:** Firmware refreshing and installation of security patches to IoT devices could be challenging. Everyday new security exposure are introducing to the Internet. Users of IoT devices may need to monitor of the updates installed on the devices. All IoT devices don't support live update. Users may need to remove the device to install firmware and/or updates. A new device administration system could be introduced to reduce the issues interrelated to a firmware update. An automatic refresh may help but as discussed many of the devices don't support over-the-air update, so challenges exist.
- **Authentication and authorization:** IoT networks consist of a enormous number of devices. These devices need to be able to feasible to interconnect the network at any time. As IoT devices produce and/or process sensitive data, it must authenticate itself to accept and transfer data to the gateway. Security suspectabilities improve by the use of default passwords, set by the manufacturers without changing it also by the use of weak passwords on any device. Authorization is equally prominent as

authentication. IoT devices goto be ready to read and write to a selected area of database and not the others. hackers may get read/write access to sensitive data environment if the device is compromised.

- **Management of giant IoT devices:** Because the number of devices in IoT networks are increasing day by day, the management of those devices is becoming more and more complicated. A enormous number of devices introduces new security suspectabilities. Still, now, no common organization scheme has initiated.
- **Implementation of security algorithms:** IoT devices are almost small with restricted power, processing, and memory capabilities. Implementation of complex cryptographic algorithms during this limited capability devices is sort of impossible. Even encryption and deception might be hard thanks to device capabilities. These devices could also the victim of side channel attacks. Hackers may apply reverse engineering to restripe plain data transmitted over the network. Implementation of lightweight encryption algorithms on these devices may reduce the likelihood of eavesdropping. Research opportunities exist for the planning, implement, and test of latest lightweight algorithms which can protect the information in IoT networks.
- **Communication security:** Secure communication is very important for the transfer of sensitive IoT data in realtime over the Internet. As discussed earlier many IoT devices don't encrypt data before transfers over the internet. Secure private networking can reduce the suspectabilities but as IoT data needs to be sent and accepted over a enormous network in many cases secure private network couldn't be a proper solution. The packaging of IoT data at an intermediate level like, at an foothold network can also reduce the challenges. Future research opportunities exist to deal with this challenge.
- **Application security:** Users information from the IoT nodes are stored in cloud, web and/or mobile devices. User data could include checking account information, health data, location information and more. Even secure communication will not protect the user data if the hacker gets access to the data from the web, cloud or mobile devices. So, the safety of the IoT data stored in cloud web and mobile devices is additionally also challenging.
- **Digester recovery and incident management:** IoT devices might be placed in anything. Failure in an IoT node may introduce a enormous problem. Proper digester recovery plan and event management are very reduced for realtime IoT devices where sensitive information is handled by the IoT sensors.
- **Vulnerability detection and management:** Detection and management of various security vulnerabilities of IoT nodes are challenging. As IoT networks contains of many IoT devices it It's not very easy to detect an affected node. Further research possibility exists to introduce new frameworks to deal with this challenge.
- **Availability and repair disruption:** IoT devices should always available to monitor/gather data. IoT devices could also be compromised, physically damaged or stolen which can cause service interruption. High availability of IoT devices is extremely important for real-time monitoring systems.
- **Data privacy and integrity:** Privacy and implementation protection is challenging. Only permitted user should have access to users' personal data. Proper permission from the user is required before access to the information by somebody else. Data must be securely disposed of when it's is no more needed.

- **Human factors:** Handling of inactive users of IoT devices are challenging. For example, if a user of a car doesn't change a damaged device it might be a life threat for him or anybody else.

OPEN ISSUES AND DISCUSSION:

Any security solution should consider three basic properties: confidentiality, implementation, and availability. Confidentiality of knowledge or information means that the access to the information is restricted for the unauthorized persons. Integrity assures the originality of data. It means that the information is n't changed by any unauthorized person. Availability refers to the presence of knowledge for access at any time. It means the information is accessible at any time [51]. Internet of Things is not any more a group of few connected nodes. IoT is moving forward every day with its rapid implementation in all most all sectors including smart city, smart agriculture, intelligent traffic management, self-driven car, intelligent logistics, smart buildings, intelligent power network, smart GPS navigation, environmental management, industrial monitoring, remote medical treatment then on [6]. Secure IoT systems need to ensure confidentiality, integrity, and availability of sensitive data produced from all these smart systems.

- **Open issues :** Based on the IoT security challenges pointed above we have identified the following open issues for future research: • IoT end device identity for proper authentication and authorization • Trust between different components in IoT paradigm • Privacy of user data generated by IoT end devices • End to end IoT data security with proper security enforcement and standardization
- **Discussion :** To achieve security in IoT, it 's vital to possess a simplified generic presentation of any IoT system. We have suggested a generic six layers simplified presentation of the Internet of Things (IoT) paradigm and security requirements at each layer in Local communication security Gateway objects layer Gateway data security Internet Communication layer Internet security Cloud storage and data analysis layer Cloud data security IoT application layer Application security

CONCLUSION:

In this paper, we first examine and consider the IoT security and privacy issues from a new perspective - IoT properties. We display the security threats, the available solutions, and research challenges yet to be solved related with these IoT properties. We also indicate what new security technologies are required to promote study. Finally, based on examining lots of exquisite research, we demonstrate the growth of recent IoT security research and how IoT properties follow on the existing research. Through deeply examining the effect of IoT new properties on security and privacy, we can better understand the future research plague spot and growth of the IoT security.

REFERRENCES:

1. The Statistics Portal. (2017). Internet of Things (IoT) interconnected devices installed base from worldwide 2015 to 2025 (in billions). [Online]. Available: https: //www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/
2. IDC. (2016). Internet of Things Market Statistics. [Online]. Available http://www.ironpaper.com/webintel/articles/internet-of-things-marketstatistics/

3. crimes/hacking-the-human-heart
4. Envista Forensics. (2015).The Most Hackable Cars on the Road. [Online]. Available: http://www.envistaforensics.com/news/the-mosthackable-cars-on-the-road-1
5. Khvoynitskaya, S. The Past and Future of the Internet of Things. 2021. Available online: https: //www.itransition.com/:https://www.itransition.com/blog/iot-history (accessed on 25 March 2020).
6. Contit, M.; Dehghantangha, A.; Franklein, K.; Whathson, S. web of Things security and pathological: Challenges and opportunities. Future Generation. Computer. System. 2018, 78, 544–546. [CrossRef]
7. Manther, A.A.; Tawalbeh, L. Security tools and methods for intelligence junk sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.
8. Makhdhoom, I.; Abolohasan, M.; Lipmane, J.; Liu, R.P.; Ni, W. Anatomy of threats to the web of things. IEEE Commune. Surv. Tutor. 2018, 21, 1636–1675. [CrossRef]
9. Gartner‘s Hype Cycle Unique Report for 2011, Gartner Inc. http://www.gartner.com/technology/research/hype-cycles/ (2012)
10. Variations between the IoT and Conventional Internet by Dr. Opher https://www.rtinsights.com/differences-between-theiot-and-traditional-internet/
11. E. Welbourne, L. Battle, G. Cole, K. Gould, K N. Rector, S. Raymeer, Building the web of Things Using RFID The RFID Ecosystem Knowledge, Internet Computing. 13 (2009) 48–55.12.A. Jouels, RFID security and privacy: A search , R Sel Area Commune. (2006) 381–394.
12. Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S., &Sadeghi, S. (2012). A Novel Algorithm for checking Sinkhole Hacks in WSNs. IJCTE, 4(3), 418-421.
13. Balte, A., Kashid, A., &Patil, B. (2015). Security Issues in Internet of Things (IoT): A Survey.National Journal of Research in Computer Science 5(4), 450-455. ISSN: 2277 128X.
14. Betta , A., de Denato, W., Pernsico, V. and Pescape, A., “ Integration of Cloud computing and Internet of things: A Survey”, Foreseen Generation Computer Systems, Volume 56, March 2016, pp. 684700.