IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

IoT Security: Ongoing Challenges and Security Enhancement

Chaurasia Sagardayal and Prasad Chandan
Student, Master of Computer Application
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *The Internet of Things (IoT) opens open doors for wearable gadgets, home machines, and programming to share and impart data on the Internet. Given that the mutual information contains a lot of private data, saving data security on the common information is a significant issue that can't be ignored. Here, we will start with general functioning of IoT and continue with data security related difficulties that IoT will experience. At long last, we will likewise call attention to explore bearings that could be the future work for the answers for the security challenges that IoT experiences.*

Keywords: IoT Security, IoT Security enhancement, IoT challenges, IoT Devices

I. INTRODUCTION

The Internet of Things (IoT) is an innovation used to consistently associate any electronic segment gadgets through web and won't just interface with PCs and cell phones, however it will likewise interconnect keen structures, homes, and urban areas, just as electrical matrices, gas, and water systems, vehicles, planes, and so on. IoT will prompt the improvement of a wide scope of cutting-edge data benefits that should be prepared progressively and require server farms with huge capacity and processing power. The incorporation of IoT with Cloud and Fog Computing can bring not just the necessary computational force and capacity limit which coordinates an assortment of gadgets into systems to offer progressed and shrewd types of assistance, needs to ensure client security and address assaults, for example, ridiculing assaults, disavowal of administration (DoS) assaults, sticking, and listening in.

The Internet of things (IoT) gives a joining of different sensors and items that can discuss straightforwardly with each other without human intercession. The "things" in the IoT incorporate physical gadgets, for example, sensor gadgets, which screen and accumulate a wide range of information on machines and human public activity. The appearance of the IoT has prompted the consistent general association of individuals, articles, sensors, and administrations. The primary goal of the IoT is to furnish a system foundation with interoperable correspondence conventions and programming to permit the association and joining of physical/virtual sensors, (PCs), brilliant gadgets, cars, and things, for example, cooler, dishwasher, microwave, food, and d rugs, whenever and on any system. The improvement of cell phone innovation permits incalculable items to be an aspect of the IoT through various cell phone sensors. Nonetheless, the prerequisites for the huge scope sending of the IoT are quickly expanding, which at that point brings about a significant security concern. Security issues, for example, protection, approval, check, access control, framework setup, data stockpiling, and the board, are the primary difficulties in an IoT situation. For example, IoT applications, for example, cell phone and inserted gadgets, help give an advanced domain to worldwide network that rearranges lives by being delicate, versatile, and receptive to human.

II. OVERVIEW

The IoT encourages coordination between the physical world and PC correspondence systems, and (applications, for example, foundation the executives and natural observing make protection and security strategies basic for future IoT frameworks. Comprising of remote-frequency IDs (RFIDs), wireless sensor networks (WSNs), and distributed computing [4], IoT frameworks need to ensure information protection and address security issues, for example,

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

satirizing assaults, interruptions, DoS attacks, distributed DoS (DDoS) attacks, jamming, eavesdropping, and malware. For example, wearable gadgets that gather and send the client wellbeing information to an associated cell phone need to stay away from protection data spillage. Nonetheless, most existing security arrangements create a weighty calculation and correspondence load for IoT gadgets, and outside IoT gadgets, for example, modest sensors with lightweight security assurances are typically more powerless against assaults than PC frameworks. As appeared in Figure 1, we research IoT validation, access control, secure offloading, and malware are discovery.

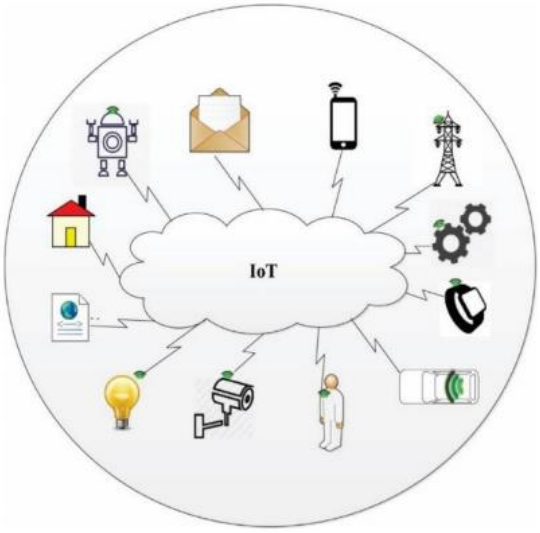
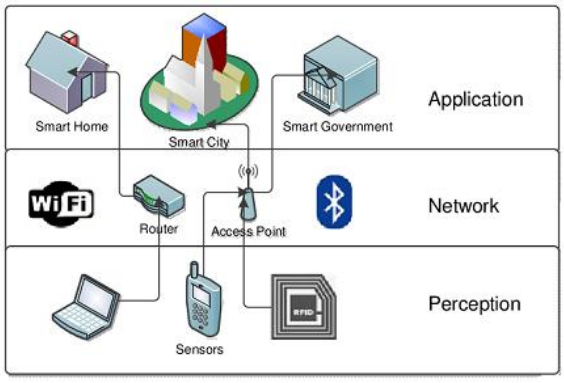


Figure 1: [3] Landscape of IoT (Demonstration of cloud IoT architecture)

III. SECURITY LEVELS



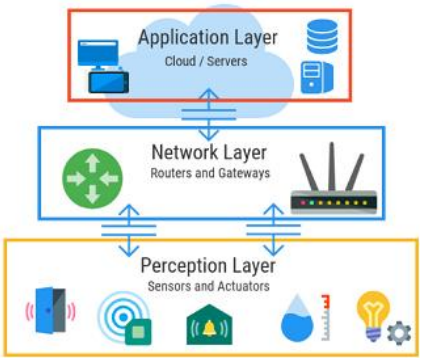


Figure 2 and 3: Three layers of IoT Architecture [5]

A) Three Layer of IoT Architecture

A. The perception Layer is also called as "sensors" layer in IoT. This layer collects the data from its environment by the help of sensors and actuators. It also processes the data and transmits to the next layer i.e. network layer. This layer connects the IoT node in a short-range network [5].

B. This network layer of IoT handles the function of data routing and transmission to other IoT hubs and devices over the local network (internet) basically. This layer, internet gateways, switching, cloud computing platforms, and routing devices etc. this operate by using latest technologies such as Wi-Fi, LTE, Bluetooth, 3G, etc. this network layers act as a mediocre between different nodes and sharing of sensor data [5]

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

C. Application Layer gives the authentication, integrity, and confidentiality of data. This creates a smart environment which fulfills the purpose of IoT [5]

IV. CHALLENGES IN IOT SECURITY

A) IoT Security Versus Normal Security

There are various key differences in the security concern. for example, in IoT setup is different as compared to normal internet. These IoT devices are setup on LLNs. whereas others have different topologies based on their application. they are stressed by dynamism, memory, and processing power and all these are not considered for the standard internet there is a great data loss to the node impersonation. So, there is a venerable system for e.g. attacker can authenticate with the network with its connected and active node. data can be manipulated by the attacker such as man-in-the-middle attack and counterfeit attacks over the network layer.[3]

As it shares the low IoT perception layer, sensors nodes also have less computational power so it is impossible for frequency hopping communication application and public key encryption. As the sharing of the data is the main key feature of the application layer this keeps the authentication, key arrangement. problem of data sharing makes security issue of user privacy across heterogeneous networks. as it is impossible to get secure over heterogeneous networks.[3]

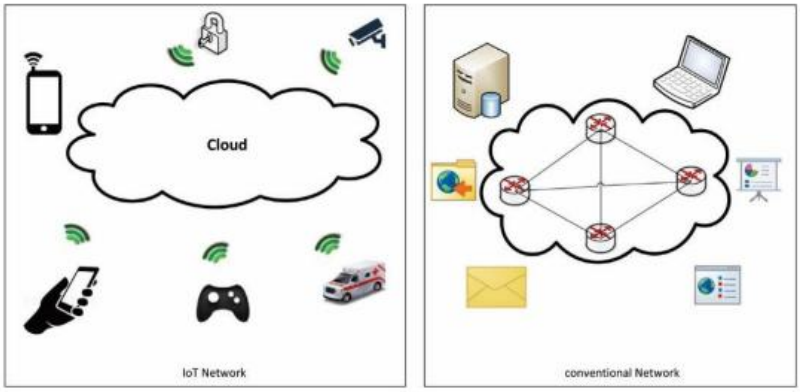


Figure 4: [3] IoT Network vs. Convectional Network [3]

B) IoT attack model

IoT attack model Consisting of things, services, and networks, IoT systems are vulnerable to network, physical, and software attacks as well as privacy leakage.

1. **DoS attackers:** The attackers flood the target server with superfluous requests to prevent IoT devices from obtaining services. One of the most dangerous types of a DoS attack is when DDoS attackers use thousands of Internet protocol addresses to request IoT services, making it difficult for the server to distinguish the legitimate IoT devices from attackers. Distributed IoT devices with lightweight security protocols are especially vulnerable to DDoS attacks [1].
2. **Jamming:** Attackers send dummy signals to disturb the ongoing radio transmissions of IoT devices and further drop the bandwidth, energy, central processing units (CPUs), and memory resources of IoT devices or sensors during their failed communication attempts [1].
3. **Spoofing:** A spoofing node impersonates a legal IoT device with its identity such as the medium access control (MAC) address and RFID tag to gain illegal access to the IoT system and can further launch attacks such as DoS and man in the-middle attacks [1].
4. **Man-in-the-middle attack:** A man-in-the-middle attacker sends jamming and spoofing signals with the goal of secretly monitoring, eavesdropping, and altering the private communication between IoT devices [1].
5. **Software attacks:** Many Mobile malware such as Trojans, worms, and viruses can result in privacy leakage, economic loss, power depletion, and network performance degradation of IoT systems [1].

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

6. **Privacy leakage:** IoT systems have to protect user privacy during data caching and exchange. Some caching owners are curious about the data content stored on their devices and analyze and sell such IoT privacy information. Wearable devices that collect user's personal information such as location and health information have witnessed an increased risk of personal privacy leakage [1]

C) IoT security issues

1. **Confidentiality:** It is one of the crucial things that the data must be shared with only available and authorized users. In IoT a user can be defined as humans, machines and services, and internal objects (network parts) and outside objects (not the part of the network). e.g. it's important that data must don't reveal the information to its neighboring nodes. So, the person should be responsible for data management in IoT and the applied process henceforth the data should be protected in the whole process [5].
2. **Integrity:** The IoT depends on exchanging information between a wide range of gadgets, which is the reason it is imperative to guarantee the precision of the information; that it is originating from the correct sen der just as to guarantee that the information isn't altered during the cycle of transmission because of proposed or unintended impedance. The honesty highlight can be forced by keeping up start to finish security in IoT correspondence. The information traffic is overseen by the utilization of firewalls and conventions, yet it doesn't ensure the security at endpoints in light of the trademark idea of low computational force at IoT hubs.
3. **Availability:** The vision of IoT is to interface however many keen gadgets as could be allowed. The clients of the IoT ought to have all the information accessible at whatever point they need it. Anyway, information isn't the main segment that is utilized in the IoT; gadgets and administrations should likewise be reachable and accessible when required in a convenient manner so as to accomplish the desires for IoT [5].
4. **Authentication:** Each entity in the IoT must be able to clearly identify and authenticate other objects. Actually, to achieve this it is difficult to authenticate many entity (devices, people, services, service providers and processing units) and other hand many times objects needs to authenticate for the first time. For this reason, we need such systems to be build that must authenticate each other when needed [5].
5. **Lightweight Solutions:** these are a unique type of security feature that is been added to the objects. For this reason, computational and power capabilities of the objects or the devices are included in the IoT. The objective is to work the protocols and authentication of the devices so this must be considered while designing the IoT devices. Since these algorithms are meant to be run on IoT devices with limited capabilities, so they ought to be compatible with the device capabilities [5].
6. **Heterogeneity:** The IoT is having full capabilities of connecting with other objects despite having compatibility issues, complexity, other brands(vendors). The devices even work with different firmware, algorithm, versions, bitrates, interfaces, and they are made for different f unctions, to solve this heterogeneity problem there must be a solution a protocol must be designed to work with other devices in any situation and environment. The main aim is to connecting device to device, human to device, and human to human, hence to provide connection between heterogenous things and network. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols [5].
7. **Policies:** Policies must be made and standard must be set to ensure that the data will be handled, protected and transmitted in a very authentic and proper(standard) way, but for this we need to make sure that every entity are following the policies and standards. Service Level Agreements (SLAs) needed to clarify that each service is involved in it i.e. computer and network current policies may not be applicable for IoT. The enforcement of such policies will introduce trust by human users in the IoT paradigm which will eventually result in its growth and scalability [5].
8. **Key Management Systems:** In IoT, the devices and its sensors exchange the information which is encrypted for the confidentiality of the data. For this reason, there must me some lightweight key management algorithm or a management system for all types for frameworks that can build the confidence in exchanging the information, can distribute the keys by consuming devices' minimum capabilities [5].

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

V. IoT SECURITY METHODOLOGY

Ali Dorri, [2] Has described a blockchain securities method we will get a glimpse of that methodology. They have described that every IoT home has local blockchain system which every smart home will have that and it will get the public key encryption and shared services to authorized the device.

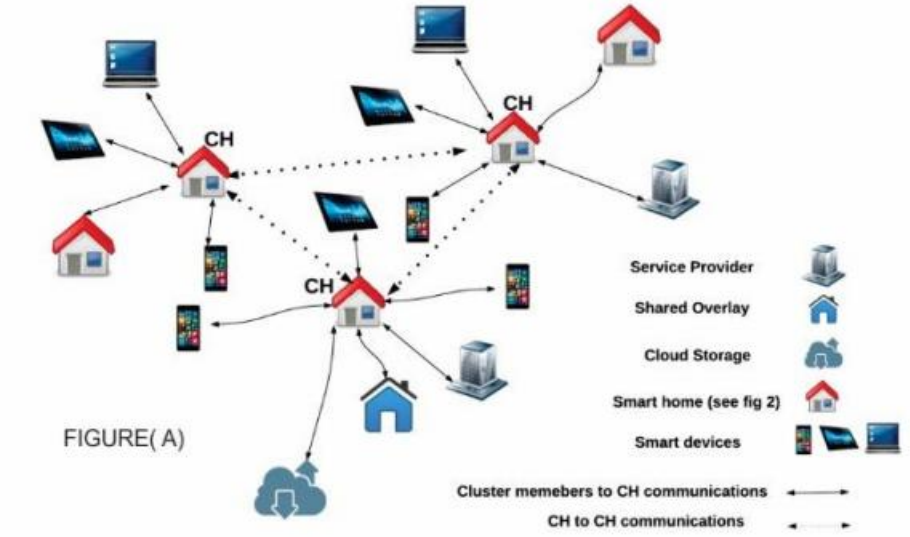


Figure 5: [2] proposed BC-based architecture [2]

Here in the figure (A) they have a topology smart provider, shared overlay, cloud storage, smart homes and a smart device that communicate with each other and build the stronger system. This Local block chain concept will eliminate the DDOS attack at certain level.

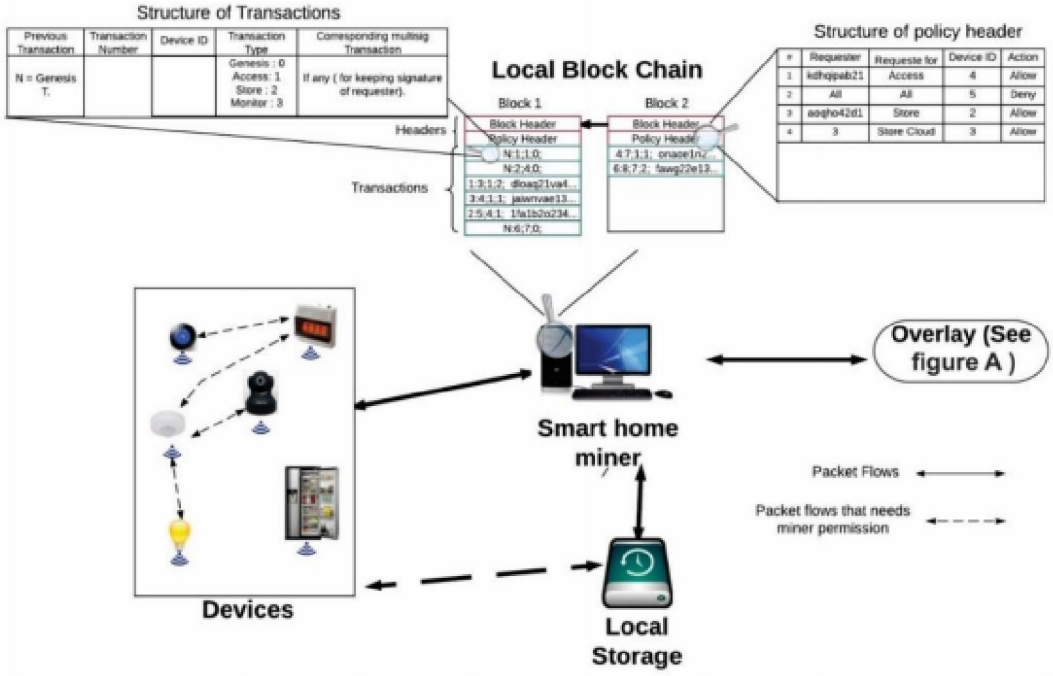


Figure 6: [2] The smart home consists of IoT devices, local storage the miner and the local BC

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

A) The Block Chain Based Smart Home

1. **Initialization:** here they have discussed the process of adding the device to the policy header to the local blockchain [2]. For adding the device miner will generates the genesis transaction by sharing the key with device using generalized Diffie-Hellman. The shared key will be between the miner and the stored device in the genesis transaction. As for defining policy header, the home owner generates its own policies according to our proposed policy structure in Figure 2 and adds the policy header to the first block. The m iner will use the policy header in the latest block of block chain hence forth for updating the policy the owner will update the latest block's policy header.[2]
2. **Transaction Handling:** The smart devices may may discuss straightforwardly with one another or with the other objects in the smart home. Every device inside the home may demand(request) some information from another internal devices to give some services, e.g., the light demands information from the movement sensor to turn on the lights naturally when somebody enters the home. To accomplish client power control on smart home exchanges, a shared key should be allocated by the miner to devices which need to directly communicate with each other [2]. To assign the key the miner checks the policy header and asks for the permission from the owner and then give them to the devices when received, then the devices can exchange the data till when their keys are valid. To stop the permission the miner invalids the key by sending the message to the devices that share data, and on the other, the communications between devices are secured with a shared key [2].
3. **Shared Overlay:** when the user has more than one home then he needs to setup separate miner and storage for each home. So, to overcome the cost of the managing overheads they have shared overlay which will be consist of maximum two smart home and manage that centrally as a one home because of shared miner in the picture. The shared overlay is similar to that smart home. Just the structure of shared block chain is different to that of smart home. Here in block chain each home has genesis transaction and all devices are chained to their home genesis transaction by shared overlay miner. The home which uses VPN (virtual private network) the connection is established by the internet gateway in every home and the miner will handles overlay that routes the packets to the shared miner [2].

B) Machine Learning Based IoT Security Model

Xiao, [1] They have described machine learning based IoT model which gets security improvement on its learning based environment.

1. **Learning based access control:** It is challenging to design access control for IoT systems in heterogeneous networks with multiple types of nodes and multisource data. ML techniques such as SVMs, K-NNs, and NNs have been used for intrusion detection. For instance, the DoS attack detection as proposed in uses multivariate correlation analysis to extract the geometrical correlations between network traffic features. This method increases the detection accuracy by 3.05% to 95.2% compared with the triangle-area-based nearest-neighbors approach using the KDD Cup 99 data set [1].
2. **Learning-based IoT malware detection:** IoT devices can apply supervised learning techniques to evaluate the runtime behaviors of the apps in malware detection. In the malware detection scheme as developed in [14], an IoT device uses K-NNs and random forest classifiers to build the malware-detection model. As illustrated in Figure 5, the IoT device filters the TCP packets and selects the features among various network features including the frame number and length, labels them, and stores these features in the database. The K-NN-based malware detection assigns the network traffic to the class with the largest number of objects among its K -NNs. The random forest classifier builds the decision trees with the labeled network traffic to distinguish malware. According to the experiments in [14], the true positive rates of the K-NN-based malware detection and random forest-based scheme with the MalGenome data set are 99.7% and 99.9%, respectively. IoT has fulfilled with supervised learning techniques to evaluate the runtime behaviors of the apps in malware.

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

C) IoT Security via Android Application

Android platform, the most renounced mobile operating system, and one of the fastest growing in the mobile and other market segment it has highly taken the mobile market share. Based on Android, more and more smart devices have been developed as personal assistants that surely headlined the IoT [8] the Android platform attracted IoT developers' attention in many aspects. Many features of Android have been adopted in IoT devices, such as power saving, near-field communication, multi-sensors, voice control. Namely, Android already has been part of IoT. Although there are other competitors such as Apple iOS, Windows phone, and Mozilla Firefox OS, Android is supported by a large development community bootstrapping IoT toward many possible directions [8]. Here in the big community the android plays important role in continuous development in security at application level and with the availability of machine learning and cloud computing it has provided higher security and all the possible improvement.

VI. FUTURE WORK

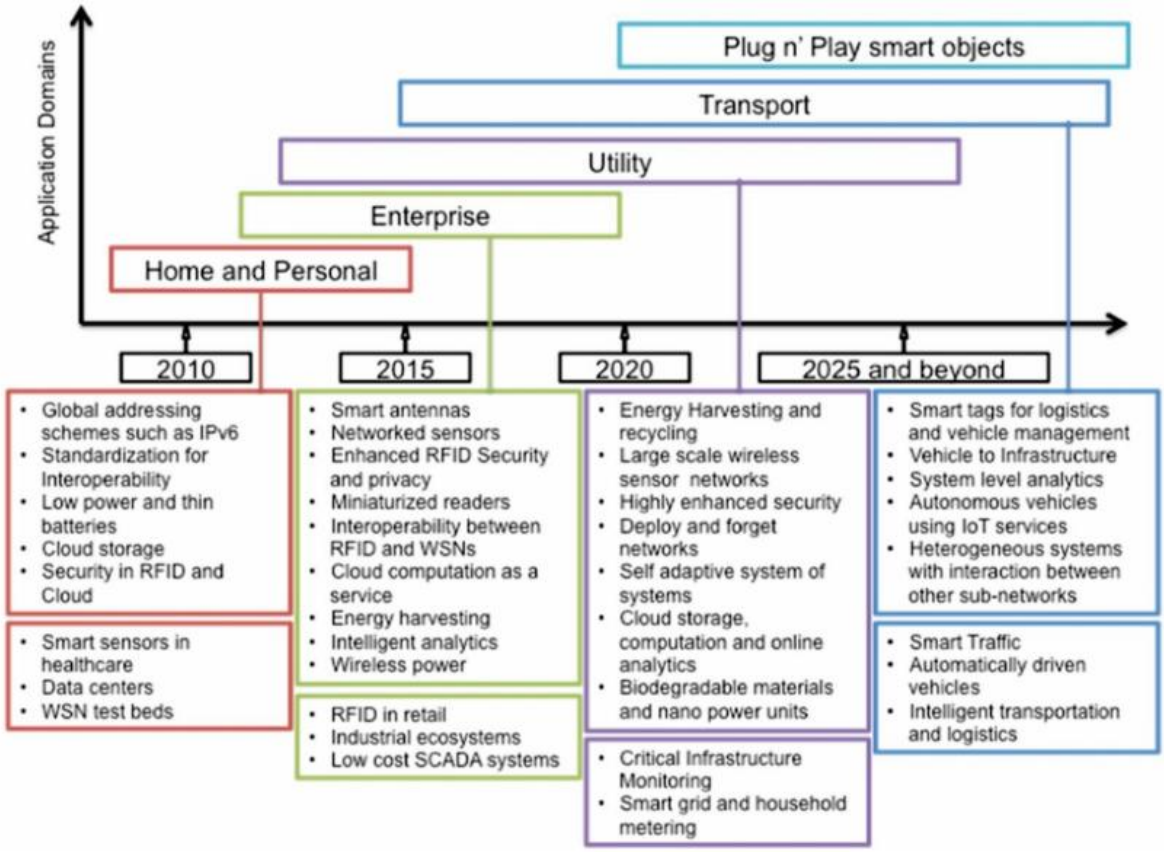


Figure 7: Roadmap of key technological developments in the context of IoT application domains envisioned [8]

Gubbi [8] has described some future work development in IoT in this fig 7 what newer and improvements in the future works will be like this in the above diagram (fig 7) they have segmented some future work each 5 years gap e.g. 2010, 2015, 2020, 2025 and further In near future we will be having more and more ease and high security in IoT platforms due to continuous improvements.

VII. CONCLUSION

The main features that differentiate IoT security issues from the traditional ones are the heterogeneous and large scale objects and networks. These two factors, heterogeneity and complexity, make IoT security much more difficult to deal

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) ABCD-PQRS
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 9, Issue 5, September 2020

with. This article addressed ongoing challenges and research opportunities in IoT security. New research topics and their possible solutions are also discussed.

ACKNOWLEDGEMENT

We would like to acknowledge the University of Mumbai, Mumbai, India to give us the opportunity to do the research work under the title "**IoT Security: Ongoing Challenges & Security Enhancement**". Also, we would like to acknowledge the college L.B.H.S.S. T's ICA Bandra East, Mumbai, India to support us during the research process. Last but not the least, I would like to express my sincere gratitude to my advisor **Prof. Vikram Patal Bansi** for his patience, motivation and continuous support. Her immense knowledge and guidance helped me all the time.

REFERENCES

[1]. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT devices Uses AI to Enhance Security? IEEE Signal Processing Magazine, 35(5), 41-49.

[2]. Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram , P. (2017). Blockchain for IoT security and privacy: The Case study of a smart home, 2017 IEEE international Conference on Pervasive Computing and Communicatons Workshops (perCom Workshops).

[3]. Alaba, F.A., Othman, M., Hashem, I.A.T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[4]. Pacheo, J., & Hariri, S. (2016). IoT security Framework for Smart Cyber Infrastructures. 2016 IEEE 1st International Workshops on Foundations and Applications of self* Systems (FAS*W).

[5]. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things and Prospective measures. 2015 10th international Conference for Internet Technology and Secured Transactions (ICITST).

[6]. Xu, T., Wendt, J.B., & Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD).

[7]. Zang, Z, -K., Cho, M. C. Y., Wang, C.-W., Hsu, C, -W., Chen, C, -K., & Shieh, S. (2014). IoT Security: Ongoing Challenges and Research Opportunies. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications.

[8]. Gubbi, j., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer systems, 29(7),

[9]. Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013). A Systemic Approach for IoT Security. 2013 IEEE international Conference on Distributed Compu ting on Distributed Computing in Sensor Systems.