International Journal of Engineering, Science and Mathematics
Vol. 10 Issue 4, April 2021,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

SECURITY MANAGEMENT AND ENHANCEMENTS FOR UPCOMING INTERNET OF THINGS (IOT) APPLICATIONS

ANJU BALA[1], DR. PRASADU PEDDI[2]

[1]Research Scholar, Department of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

[2]Assistant Professor, Department of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

ABSTRACT

The emerging patterns in the Internet and embedded innovations have enabled objects surrounding us to be interconnected with one another. The security gives nice the speed of the advancement of IoT on the grounds that the IoT is a rich wellspring of information it will consistently is helpless against refined attacks. The layers of the IOT are presented to various threats like unapproved access, eavesdropping and spoofing. Security is highly critical in practically all IoT applications that have effectively been conveyed or are currently deployment. The applications of IoT are increasing quickly and penetrating the vast majority of the existing industries. We can say that IoT network is formed with asset constrained and low-power low-performing objects. Considering the IoT reference model, each layer will have its own security difficulties and issues.

KEYWORDS: security management, internet of things, application, threat, attack, etc.

1. INTRODUCTION

The emerging patterns in the Internet and embedded innovations have enabled objects surrounding us to be interconnected with one another. We envision a future where IoT gear will be invisibly embedded in the earth around us and would deliver an overwhelming measure of information. This information should be saved and refined to make it valuable and understandable. An IoT model requires various entertainers which include portable administrators, software engineers, access innovation suppliers, and so on. The application domains of IoT are moreover incredibly wide and such networks might be utilized in healthcare, agriculture, utility management, and manufacturing. IoT can be seen as the group of people yet to come interconnection worldview which is going to empower connectivity among individuals' gear and models enabling conduct to occur with no human intervention. IoT overcome any issues between the physical and cyber world by considering things to take an interest and share information with other substances in the cyber world, be that as it may, in the new years, numerous researchers and organizations attempted to explain the definition of IoT.

2. SECURITY MANAGEMENT OF THE INTERNET OF THINGS

IoT is a network system in both wired and wireless connection that consists of numerous software and equipment elements like manufacturing management, energy management, agriculture irrigation, electronic commerce, logistic management, medical and healthcare system, aerospace survey, building and home automation, infrastructure management, large scale deployments and transportation. The reason for IoT is to transform traditional items into connected items by taking benefit of exchanging information and communicating with one another in request to monitor and control the destinations. As the IoT advances, cyberattacks are really becoming actual dangers. The security gives nice the speed of the advancement of IoT on the grounds that the IoT is a rich wellspring of information it will consistently is helpless against refined attacks. There has been research works distributed on the IoT security necessities. Nonetheless, there is an absence of a brought together way to deal with systematically addressing the difficulties arising from the integration and conversion of the IoT into the existing network environment. As a response to increasing concerns over security, the Internet of Things security Foundation (IoTSF) was dispatched on September 23, 2015. Its mission is to advance information and test rehearses for security of the IoT. There is a requirement for developing integrated security management system (SMS) to incorporate new applications to give a proficient, strong, and sustainable security in the IoT environment. In this paper, to fill this hole, we propose a layered functional architecture for an IoT security management system.

- **IOT layered architecture:**

The IoT reference model has been partitioned into four main layers. The layers from base up are component layer, network layer, administration layer and application layer, as demonstrated in Fig 1.

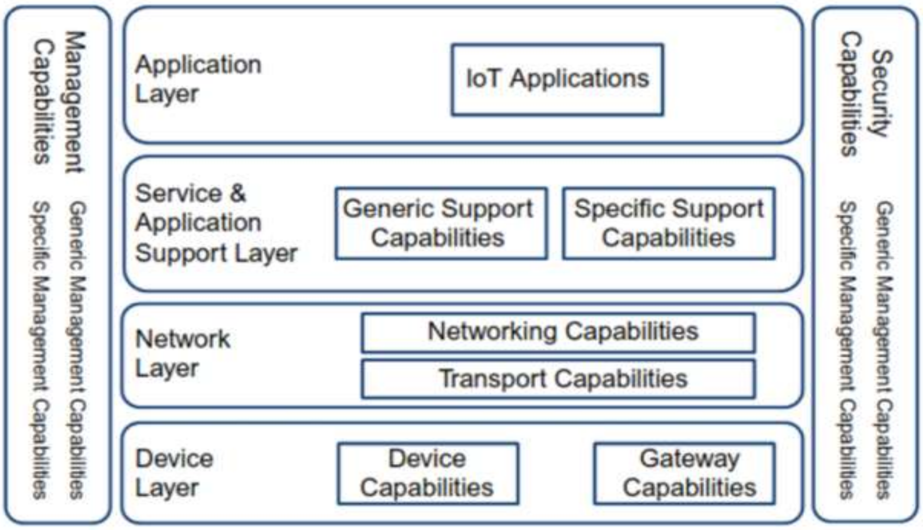
Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application Layer
IoT Applications
Service & Application Support Layer
Generic Support Capabilities
Specific Support Capabilities
Network Layer
Networking Capabilities
Transport Capabilities
Device Layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Management Capabilities
Specific Management Capabilities

Figure 1: The IoT layered reference model

Each layer has its own components, communication standards and protocols. The benefits of layered architecture are:

- The layered construction is effectively expandable, and the lower layers are providing services to upper layers.
- Allowing the new advancements for both equipment and software to be incorporated into the existing IoT network system, and the layered construction is not difficult to oversee just as configure in a down to earth implementation.
- Providing measured management of the IoT. Taking everything into account, the security services and security components at each layer can be executed to upgrade the general protection of the IoT network system.

a. **Device Layer:** This layer consists of the device layer and different kinds of nodes and sensors like RFID, barcode labels, actuators and intelligent detection devices. Sensors are utilized to distinguish the articles just as transport the gathered information to the following layer. Devices gather and transfer information to the network layer either straightforwardly or indirectly. It is normal that all devices will be IPv6-able later on.

b. **Network Layer:** The network layer sends the information through the existing communication strategies either wired or wireless network, Internet, cloud, versatile network, satellite network or military network. The IoT requires versatility in networking of large quantities of devices. In excess of a billion devices will be added to the system yearly. For this reason, IPv6 will assume a significant part in handling the network layer adaptability.

c. **Service Layer:** The service layer consists of functionalities that processing the gathered information and providing the links to the capacity for the obtained information from the element layer. This layer fills in as an interface between the various devices of IoT and gives communication techniques between the elements. Likewise, the service layer on top of the network layer gives connectivity between the sensors and application layer. Figure 2 shows the information passing through the service layer as an integration layer.

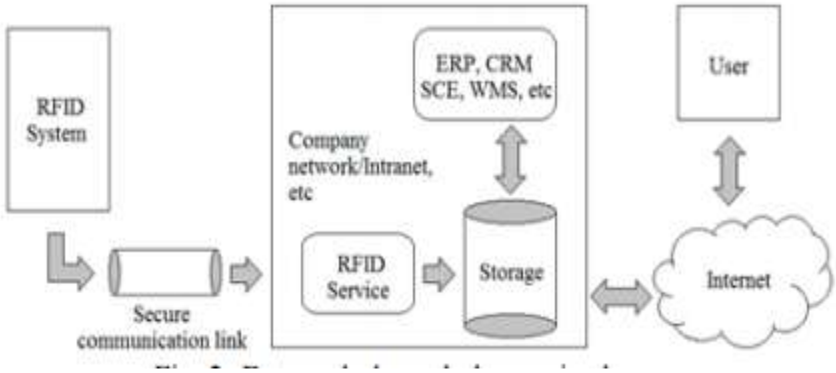

Figure 2: Data path through the service layer

d. **Application Layer:**The application layer consists of an assortment of pragmatic applications of IoT, based on the prerequisites of the clients. The application layer utilizes different quantities of various protocols, like the constrained application protocol (CoAP), the message queue telemetry transport (MQTT) protocol, the high level message queuing protocol (AMQP), and extensible messaging and presence protocol (XMPP).

3. THREATS AND ATTACKS ON IOT

The layers of the IOT are presented to various threats like unapproved access, eavesdropping and spoofing. The element layer utilized nodes and sensors like RFID, labels, barcode labels, actuators and intelligent detection devices to gather the information from the environment. Because of the shortfall of authentication services, unapproved gatherings can admittance to the information and adjust or even erase the information. The information gathered by the wireless components like RFID and labels can without much of a stretch is perused by the attackers. The information might be utilized by the attackers to hack any IoT system or track down the significant information like passwords or confidential information of the clients. Spoofing is the point at which the attackers send some phony information to the nodes and sensors pretending to act like the original disappointment, and then the attackers may have the full admittance to the system. Disavowal of-service attack is the point at which the attackers send loads of futile information to make the network traffic overflowed. By the enormous consumption of the system assets, the IoT network system will block the entrance of the approved clients. Man-in the-center attack is a kind of eavesdropping that the unapproved attackers can control the communication between the two gatherings. The attacker can get the valuable information through the communication channels.

For the situation of malicious code injection, the attacker bargains the weak nodes and sensors by injectioning malicious codes and attacking the entire IoT system. As a result, the network may closure, and the attackers could deal with the system. The malicious insider attacks happen from the inside of an IoT environment, where the information are utilized for personal purposes this is an unexpected danger in comparison to unapproved get to and require various components to counter the danger. Disseminated refusal of-service attacks in the application layer are complex these days. For this situation, the casualties will have no admittance to the services of the system and barely saw that the DDoS attacks happened in the IoT system. DDoS attacks at the element/network layer are dispatched from a wide range of connected devices; these connected devices are appropriated across the IoT system. The phishing attack on the IOT is a kind of email attack where the approved clients attracted to open the email and the attacker can hack into the IoT system to oversee the system.

4. SECURITY CRITICAL APPLICATION AREAS OF IOT

Security is highly critical in practically all IoT applications that have effectively been conveyed or are currently deployment. The applications of IoT are increasing quickly and penetrating the vast majority of the existing industries. Despite the fact that administrators support these IoT applications through existing networking advances, a few of these applications need more stringent security support from innovations they use. In this section different security critical IoT applications are examined.

- **Smart Cities:** Smart cities involve broad utilization of emerging computation and communication assets for increasing the general personal satisfaction of individuals. It includes smart homes, smart traffic management, smart debacle management, smart utilities, and so forth There is a push to make cities smarter, and governments overall are encouraging their advancement through different incentives. Albeit the utilization of smart applications is intended to improve the general personal satisfaction of the residents, it accompanies a danger to the protection of the residents. Smart card services will in general put the card subtleties and buy conduct of the residents in danger. Smart portability applications may release the location hints of the clients. There are applications using which guardians can monitor their kid. Nonetheless, on the off chance that such applications are hacked, the wellbeing of the youngster can come to chance.

- **Smart Environment:** Smart environment includes different IoT applications, for example, fire detection in forests, monitoring the level of snow in high elevation regions, preventing landslides, early detection of tremors, pollution monitoring, and so forth. Every one of these IoT applications is firmly identified with the existence of individuals and creatures in those areas. The public authority organizations involved in such fields will likewise be relying on the information from these IoT applications. Security breaks and weakness in any area identified with such IoT applications can have genuine consequences. In this context, both bogus negatives and bogus positives can prompt lamentable results for such IoT applications. For instance, on the off chance that the application begins detecting tremors erroneously, it will prompt monetary misfortunes for the public authority and businesses. On the other hand, on the off chance that the application can't foresee the seismic tremor, it will prompt the deficiency of both property and life. Therefore, smart environment applications must be highly exact, and security penetrates and information tampering should be stayed away from.

- **Smart Metering and Smart Grids:** Smart metering includes applications identified with different estimations, monitoring, and management. The most common application of smart metering is smart grids, where the power consumption is estimated and monitored. Smart metering may likewise be utilized to address the issue of power theft. Other applications of smart metering include monitoring of water, oil and gas levels away tanks and storages. Smart meters are additionally used to monitor and upgrade the performance of sun oriented energy plants by progressively changing the point of sun based boards to reap the greatest conceivable sun based energy. There likewise exist some IoT applications those utilization smart meters to quantify the water pressure in water transport systems or to gauge the heaviness of merchandise. Notwithstanding, smart metering systems are defenseless against both physical and cyber-attacks when contrasted with simple meters that can be altered only by physical attacks.

- **Security and Emergencies:**Security and crises is another significant area where different IoT applications are being sent. It includes applications, for example, allowing only approved individuals in limited areas and so on another application in this domain is the detection of spillage of unsafe gases in industrial areas or areas around substance production lines. Radiation levels can likewise be estimated in the areas around atomic force reactors or cell base stations and cautions can be produced when the radiation level is high. There are different buildings whose systems have delicate information or that house touchy products. Security applications can be sent to ensure delicate information and merchandise. IoT applications that recognize different fluids can likewise be utilized to forestall corrosion and break downs in such touchy buildings. Security penetrates in such applications can likewise have different genuine consequences. For instance, the criminals may attempt to enter the confined areas by attacking the weaknesses in such applications.

5. IMPROVEMENTS AND ENHANCEMENTS REQUIRED FOR UPCOMING IOT APPLICATIONS

Personal computers (PC) and smartphones have various security highlights incorporated into them, e.g., firewalls, antivirus software, address space randomization, and so on These security safeguards are, as a rule, missing in different IoT devices that are as of now on the lookout. There are different security challenges that the IoT applications are facing as of now. An all around defined system and standard for a start to finish IoT application isn't yet accessible. An IoT application isn't a standalone application, and it is a gathered item which includes work from numerous individuals and industries. At each layer starting from sensing to the application, a few different items and advancements are being utilized. These include countless sensors and actuators at the edge nodes. There are numerous communication standards like cell network, WiFi, IEEE 802.15.4, Insteon, dash7, Bluetooth; and so on A handshake system is required between every one of these standards. Aside from this, different connectivity advancements are being utilized at various levels in a similar IoT application like Zigbee, 6LOWPAN, wireless HART, Z-Wave, ISA100, Bluetooth, NFC, RFID, and so on Far beyond this, the nonexclusive HTTP protocol can't be utilized in the application layer.

HTTP isn't reasonable for asset constrained environments since it is significant burden and in this manner incurs a large parsing overhead. Therefore, at the application layer additionally there are many substitute protocols that have been sent for IoT environments. Some of them are MQTT, SMQTT, CoAP, XMPP, AMQP, M3DA, JavascriptIoT, and so on Because of the intense variety of protocols, advances, and devices in an IoT application, the critical compromises are between cost adequacy, security, dependability, protection, inclusion, inertness, and so forth In the event that one measurement for development is advanced, it might result in the degradation of other measurement. For instance, imposing such a large number of security checks and protocols in all information transactions in IoT applications may wind up increasing the cost and inactivity of the application, thereby, making it unacceptable for the clients. An ordinary IoT application consists of a big chain of connected devices, advances, domains, and geologies. Regardless of whether one of the device or innovation or their combination is left powerless, then that might be the reason for a security danger for the whole application. The chain is considered to be just about as strong as the most vulnerable link. There has been a large increase in the quantity of feeble links in IoT applications as of late. For instance, even fundamental IoT applications, for example, smart bulbs and smart entryway locks can be utilized as a powerless link in a smart home IoT application to remove the client's WiFi password.

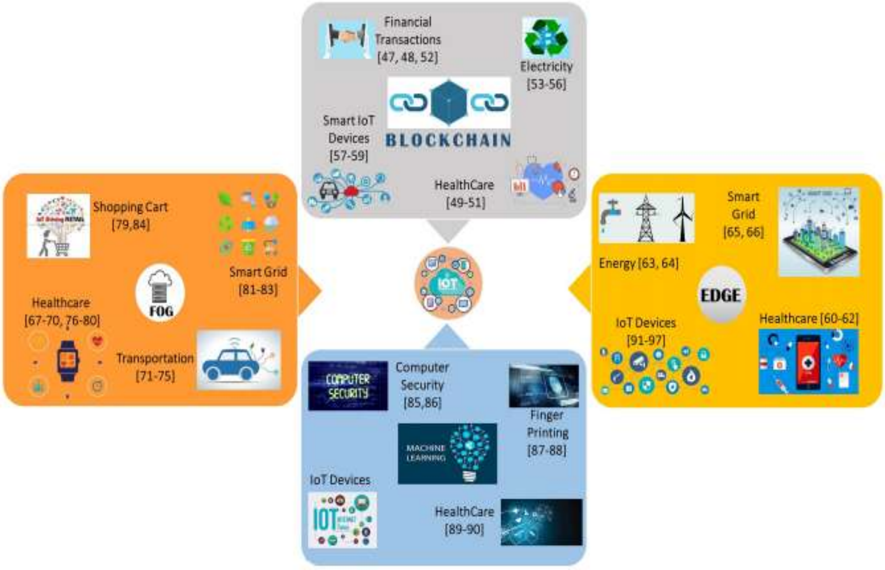

Figure 3: IoT security using various security techniques

IoT application construction and structure are required to make it dependable, secure and hearty. In such manner:

i. Thorough penetration testing for IoT devices is important to measure the level of hazard involved in deploying these devices in various applications.

ii. Encryption techniques are being utilized in IoT system at various layers and protocols. In any case, there are different levels of encrypt, decrypt, and re-encrypt cycles in the total system.

iii. Authenticate-consistently protocols should be executed. At whatever point a device needs to interact with another device, an authentication cycle ought to be executed. Computerized declarations can be a promising solution to give consistent authentication bound characters that are attached to cryptographic protocols.

iv. Any IoT security system being carried out ought to be tried and confirmed for versatility. The security protocols ought not to be working only for a restricted arrangement of clients. The genuine threats begin coming only when the application gets public and starts being utilized generally in the public domain. Therefore, legitimate methodology and planning are required.

6. CONCLUSION

We can say that IoT network is formed with asset constrained and low-power low-performing objects. Their asset limitations are considered regarding battery limit, computational force, and memory-footprint and bandwidth utilization. Considering the IoT reference model, each layer will have its own security difficulties and issues. Various threats may cause various consequences at each layer. Security is highly critical in practically all IoT applications that have effectively been conveyed or are currently deployment. The applications of IoT are increasing quickly and penetrating the vast majority of the existing industries. Diverse security services and distinctive security instruments should have been carried out for these four layers of the IoT reference model to counter the corresponding security threats. We have additionally talked about the existing and upcoming solutions to IoT security threats.

REFERENCES

1. Numair, Mohamed, Mansour, Diaa-Eldin & Mokryani, Geev. (2020). A Proposed IoT Architecture for Effective Energy Management in Smart Microgrids. 10.1109/NILES50944.2020.9257923.

2. Pundit Gupta, Jasmeet Chhabra, "IoT-based smart home design using power and security management," International Conf. on Innovation and Challenges in Cyber security, pp. 6-10, August 2016.

3. M U. Farroq, et al., "A critical analysis on the security of Internet of thing (IoT)," International Journal of computer Applications, vol. 111, p. 1-4, Feb. 2015.

4. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: vision, applications and research challenges," Ad Hoc Networks, vol. 10, pp.1497-1516, Sept. 2012.

5. R. Uttarkar and R. Kulkarni, "Internet of things: architecture and security," International Journal of Computer Applications, vol 3, pp. 12- 19, June 2014.

6. B. Khoo, "RFID as an enabler of the Internet of things: Issues of security and privacy," IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp. 709-712, Oct. 2011.

7. A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, "Classification of RFID attacks," Journal of Research and Innovation, vol. 12, pp. 491- 505, Nov. 2010.

8. G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol 4, pp. 2-7, Sept. 2009.

9. R. P. Padhy, M. R. Patra, S. C. Satapathy, "Cloud computing: security issues and research challenges," International Journal of Computer Science and Information Technology & Security, vol. 1, pp. 13-18, Dec. 2010.

10. Smarthomeblog, "How to make your smoke detecter smarter," https: //www.smarthomeblog.net/smart-smoke-detector///, online;accessed 10 Feburary 2019.

11. Tictecbell, "Sensor d'ultrasons," https://sites.google.com/site/tictecbell/ Arduino/ultrasons//, online;accessed 11 Feburary 2019.

12. S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. Mahapatra, “Security enhancements to system on chip devices for iot perception layer,” in 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS). IEEE, 2017, pp. 151–156.