International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Study on Tailor-made Security Schemes to defend IoT's

M N Rajaprabha[1], P Jayalakshmi[2], R Vijay Anand[3]

[1,2,3] *School of Information Technology & Engineering, VIT (India)*

ABSTRACT

The Internet of Things refers to the internet enabled systems and the network of physical devices, and the communication that occur between them. Therefore this IoT requires security solutions that are tailor-made. The security attacks from the outsiders are being handled by various methods, but the attacks from the insiders are not handled. The legacy solutions does not consider about the peculiarities of the attacks. Our idea is to study the security solutions for tackling attacks in the IoT's. Our proposal projects the vulnerabilities by verifying the data between the nodes of communication. Thus, we compare the existing solutions with ours and find the efficient mechanism to handle the described attacks.

Keywords: Attacks, Denial of Service,Internet of Things, Security.

I. INTRODUCTION

Internet of Things (IoT) is a global network with configuration abilitiesthat are automaticallyconfigured with virtual and physical things of their own identities and personalities. These "things" use interfaces that are integrated into the internet. It also provides connectivity for the people irrespective of the time and place.

Due to the technology advancements we are in a world where everyone is connected with each other [2]. The "things" in IoT are active objects that take part in the social and business processes. They are capable of interacting and exchange information between the objects with or without human intervention. But there exists a great concern on the areas of security and privacy [1][3]. In order to protect the Internet of things, many layers of security are required to protect the failure of code through manipulations. This leads to the idea of developing tailor-made security solutions for protecting the IoT's. Because, the IoT devices possess special characteristics like collaborative tasks, low processing power and memory etc. The ultimate aim of our paper is to develop a code as a security solution to help the IoT's to defend their devices from internal attacks from the network and also finding the vulnerabilities in the distributed systems. For this, we have reviewed a lot of methodologies to provide security solutions to the IoT's and surveyed in terms of their performance and efficiency thereby determining the best mechanism to defend the Internet of things from network attacks especially that are internal. The IoT's basic scenario has been pictured in the Fig. 1. Here it describes how internet is smartly connecting the real world objects and entrenchingthe intelligence within it. This stretches that IoT's can introduce several applications with all enhanced technologies.

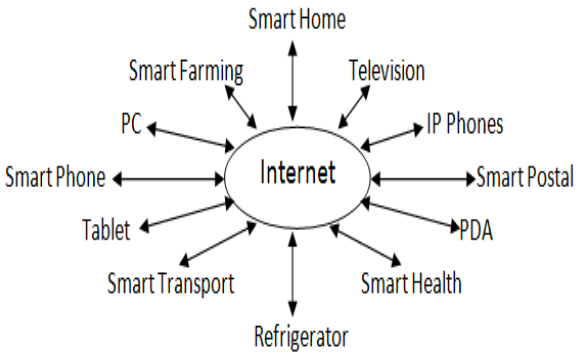

Fig. 1.IoT's scenario

II. LITERATURE SURVEY

Mohsen HallajAsghar et al. have proposed a paper on the principle of applications and visualization of Internet of Things on future. Here they have explained about IoT used over various applications in different domains to increase its efficiency and making things as easier as it can by automating and also making smarter. And also this paper addresses how IoT is related with pursuing of technologies like actuators and wireless sensors in integrating and identifying objects for communication. IoT's over six applications has evidenced that somehow it works effectively for optimizing and saving the energy. Here things like EPC (Electronic Product Code) and RFID (Radio Frequency Identification) are considered as the key factor of IoT for identifying or labelling unique objects and transferring or sharing it throughout the network. By discussing these things to explain the connectivity bridge between the virtual and real world they also have envisioned the future vision of IoT'sfor fulfilling "anything, anytime, anywhere and any media" communication in the physical world [4].

Michael J. Covington et al. has suggested an impact of threat consequence over Internet of Things and its security measurement at each tier [5]. From their view IoT is interaction between various objects interconnected through a sophisticated network and as of the interconnected systems increases then the attackers with different anticipation increases. Here the author have devised three tiers and at each tier the surface characteristics like population, heterogeneity, complexity, mobility, interoperability and distribution is discussed to expand the security that meet all the challenges. And also they have discussed about the applegate objective for cyber-attack effects that is to capture or disrupt or manipulate resources. Here context information is the one which must be kept secured to say that thespecific application has achieved privacy. Privacy is concerned more in now days where the hackers keep on introducing many tools just to break it. When IoT keep on bringing together new things the security must be concernedby ensuring privacy and safety.

Louis Coetzee et.al has proposed a work on introducing "Internet of Things [6]. This paper is completely focused about explaining the application of IoT's and its potential benefits. The authors have discussed the evolution and a component of IoT's which helps in enhancing the connectivity for any-where, any-time and any-thing. Also the paper includes a 7 application drives which are used for machine to machine language

communication and for user integration. The author mainly defines two categories of application; 1. Information and Analysis meant for decision making services. 2. Automation and Control deals with an output of the data which is being processed. The challenges like privacy, security issues and data deluge are discussed. The multinationals like IBM, Microsoft and HP are active in updating IoT are explained with their infrastructure. Framework developed by internet of things group at South Africa consist of various protocols with sensor and devices and applications within it helps to serve as a knowledge repository linked with the cultural events of impact that are living in cyberspace is discussed.

Rolf H. Weber has proposed a work on internet of things security and privacy challenges [7]. The author discuss the architecture of IoT's impact on security of stakeholders. Some privacy requirements like data authentication, access control, client privacy, resilience to attacks to govern the business activities are discussed. In order to fulfill the requirements the author has focused on Privacy Enabling Technologies called PET. Some of the PETs discussed are: 1.Virtual Private Networks (VPN) ensures reputable close group of business partners. 2. Transport Layer Security (TLS), global structure which attains confidentiality and integrity of IoT. 3. DNS Security Extensions make use of Public Key cryptography to guarantee authenticity. 4. Onion Routing mixes internet traffic and increases waiting time .5.Private Information Retrieval (PIR) systems, which is a global accessing system but leads to performance issues. Also the data protection principles are discussed with legal course of action. The legal framework when binding the participants of IoT, there are four main challenges towards regulations explained are Globality, Verticality, Ubiquity and Technicity. And these regulations can be helpful in making the framework "global".

III. IoT ARCHITECTURE

As IoT connects billions of objects, issues like storage and traffic will increase. So the development of IoT depends on the design of vary business application and models [16][17]. The general architecture of IoT in Fig.1 works with following layers:

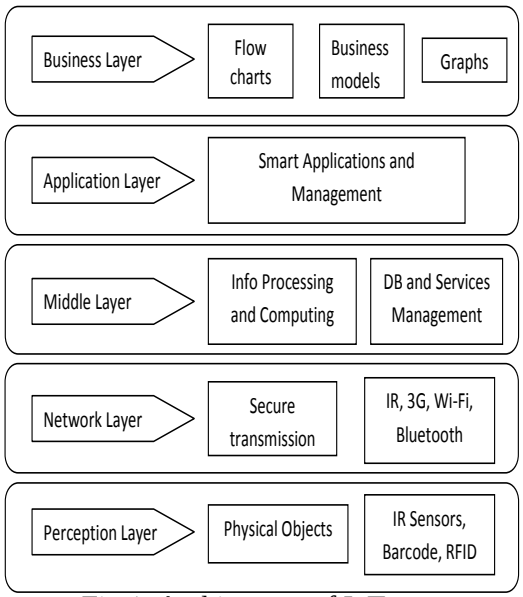

Fig.1. Architecture of IoT

A. Perception Layer

Also called as device layer, consists of sensor devices like RFID, 2d-Barcode or infrared sensors which deals with the process of identifying and collecting the objects with the specific information via sensor devices. Then the collected information is transmitted to network layer for further processing.

B. Network Layer

Also called as transmission layer and it helps in transferring the data from previous layer to information processing system. With the help of transmission medium like Wi-Fi, 3G, Bluetooth, depending on the sensor devices the transmission is done to next layer.

C. Middle Layer

It receives the information from previous layer and helps in storing it into the database. It is responsible for providing the service management and it performs computation with all the received data and takes decision to move on.

D. Application Layer

It is whole responsible for all the applications globally based on the objects received from the middle layer. It deals with all kind of smart applications.

E. Business Layer

Good business layers can lead to a successive IoT. This layer deals with overall management of the applications and services of IoT system. It helps in developing graphs, business models, flow charts depending on the content received from previous layers. Also determines the future business strategies based on the results obtained.

IV. TYPES OF ATTACKS ON IoT

The major challenges faced by IoT's are mostly concerned with the technological and security challenges. When security is taken as the subject of concern, authentication could be the area of toll as other loopholes will gain strength if this is not being addressed. On strengthening the authentication level we naturally could cascade solutions to other loopholes as well. The sources of threats are categorized into four domains which are explained below.

A. Application Based Attacks

As there are large amount data to be processed the application environments of the IoT are complex. The issues could be either internal or external. An example for external threat could be physical insecurity that is interferences from people compromising the actual results and generating biased information. The environments

being constrained for certain objects results in security threats being elongated. For instance, when the environment's capacity of processing and storing the security software is small it will not be able to function properly leading to vulnerable objects prone to attacks and intrusions. This requires lightweight security application software. Sometimes, the application environments may not be compatible with the inborn gadgets, thereby paving the way for vulnerability of the entire environment. This stresses on the fact that both the environment and the objects need reliable security considerations. Also it is important to have privacy protection for heterogeneous data and data processing which requires detailed study on privacy protection methods. In [8] it is been noted that the privacy protection is achieved through algorithms with respect to data processing methods, however these yet remain weak for entire security packages. Therefore, this dimension requires further expansion. These environments chip in a lot of metadata files that paves a way for attacks. One best example could be a phone being hacked.

B. Connection Based Attacks

The privacy of the object is at stake due to the presence of data flow paths between objects which are being connected to a sensor indirectly. In order to achieve a good representation of application domain, other hidden objects are revealed. A good example could be a device that is location aware, which contribute to unsuspected and unsecured devices to be attacked, since they are connected to a device that broadcasts information. Things that are resource constrained are connected to un-trusted internet through IPv6 and so on. The work in [9] briefs how the connections pave way for vulnerabilities in IoT. Internet itself is insecure, so when an IoT device is added it leads to a lot of attacks in the entire web of networks. In [10] RFID obstacles are explained where if we assume the internal problems of integrations wit old systems, there are two cases possible. Either the existing systems are vulnerable or the RFID connections weaken the setup. In both cases, the links established is available for attacks. The work by [11] has emphasized the abilities of hardware that is heterogeneous causes complicated network because of the security issues that depends on each manufacturer. Also such critical problems need to be resolved to make future internetapplications reasonable and acknowledged by users.

C. Platform BasedAttacks

There are various platforms and each as its own challenges. Few of them possess unsolved security issues. As described in [12], the evolutions of recent technologies like cloud computing with privacy issues that persist to spate the market lowering their growth rates. But IoT applications have invested on such platforms for many reasons. So, the platform security issues have to be addressed. Due to the growth of connections in IoT, the security concerns have to be addressed; there must be a secure connection path between the communicating objects as they transfer data from one end to another.

D. Other Forms of Attacks

The above mentioned may not be the only forms of attacks imposed on IoT's and so are the nature of these attacks be defined. Such issues occur due to improper standards during application development and

deployment. This enforces the development of rigid security measures; however the assurance to security is still questionable. A group of the mentioned threats also breed another combination of threats to IoT. On encapsulating the platform and application based threats leads to multiple issues lowering the security grounds, thereby endangering the IoTapplications. A combination application and connection based threats endangers the entire application. This raises a question as to how IoT will bloom in other deployment areas.

V. NEED OF SECURITYOF PRIVACY

A. Security

As of now security is concerned more in all the new technologies, in IoT security must be attained to ensure characteristics like reliability, confidentiality, availability, etc. By implementing Intrusion Detection System (IDS), secure routing protocol and SVELTE we cannot achieve security as it is limited to a level [7][13]. And since IoT's is multi-layered, security cannot be achieved by implementing single add-on device it can be achieved only by addressing security issues throughout the framework [14]. By achieving security throughout the application system as followed, will increases performance of the system rapidly.

*1) Secure Start-up:*When the power introduced, the system starts booting-up cryptographically by verifying all digital signatures issued for authenticity and then integrating the required software. The trust basis is achieved, but still the system is not protective it might go through many run-time attacks and threats.

*2) Access Governor:*The standard minimal-access privilege is followed; hence any credentials accessed will not be sufficient for making any changes. Access control can be provided of either of these role-based, device-based or network-based accesses to limit the privilege given to do their job.

*3) Authentication:*In network, authentication plays a major role in giving right of entry. Device authentication and client authentication must be made for inputting and outputting the required credentials.

*4) Prevention and Firewall:*Intrusion Prevention Detection is a safe guard from malicious attacks and Firewall is used to control the device from high-level traffic and threats. Both the safe guards undergo deep inspection of data and filter the data that are ordained to let go the device.

*5) Updates:*After getting into the operations the device starts receiving updates and patches. Before delivering, these must be crisscrossed with certain constraints. The patches must be trailed out if it goes beyond the limited bandwidth. The secure functional operations must be executed through these patches and updates.

B. Privacy

Privacy is another key feature enrolls throughout the IoT's applications. The main issue in the IoT is information leakage which can be maintained by privacy management. Among the information location is the sensitive context which is automatically track the user and make available of the information to everyone. IoT is not only interaction between the humans but also with the real world, so that adopting privacy plays a major role [14]. Making use of some privacy enabling technologies like onion routing, VPN, Private Information Retrieval, DNS Security Extensions, etc. privacy is achieved but still there is another method known as Peer-to-Peer with hash table increases the performance of achieving fulfilled privacy.

VI. PERFORMANCE ANALYSIS OF ATTACKS

As the number of connection increases, the attacks on IoT increases in its complexity among the heterogeneous platform. Iot application platforms of Virtual level and physical layer lead to face a complex security challenges. Unlike networked and other platforms, this results in threats in IoT which is particular in wireless system along with sensor technologies. Platform like Cloud computing, quantum computing and many other technologies leading to high processing capabilities are also the factors of increase in attack challenges.

To ensure secure communication, authentication and access control are the basic factors need to be considered in IoT. In IoT, Three pillars of security package namely, confidentiality, integrity and authenticity are very important. But it is a challenge to attain the security for IoT by using light weighted, distributed and attack resistant environment. IoT attack sources should be looked over to achieve these three security packages. But it is difficult to identify one common solution for realizing the security goals. So the application model discussed in this paper as it interacts with the middleware which monitors and enforces the security measures. Attacks and malfunctions in IoT will be more when these security features are not strengthened. In order to support the magnitude of such challenges and issues, protection mechanisms like privacy assurance, secured protocols and cryptographic algorithms. Even then it doesn't help with higher security applications of IoT. Advance digital signatures were introduced to solve the problem of spamming in IoTwhich helped one stop gap measure but it doesn't create any practical solution because of various IoT platforms [15]. Still there are needs to address these problems in focusing IoT applications with different platforms.

VII. CONCLUSION

The IoT demands security solutions created solely for their circumstance. IoT being heterogeneous in nature demands a flexible and one of a kind structure or framework to handle the attacks. When the IoT devices are considered in terms of security, it is noted that the interactions between them are not limited to homogeneous. But it extends both in horizontal and vertical horizons. From our above study we have inferred that a holistic approach can be identified which can further be modified based on the nature and class of attacks. But a single approach cannot efficiently solve the issues.

VIII. REFERENCES

[1] Attlee M. Gamundani, "An impact review on internet of things attacks," 2015 International Conference, Emerging Trends in Networks and Computer Communications (ETNCC), ISBN: 978-1-4799-7706-2, May 2015.

[2] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. Mouftah, "The Internet of Things," IEEE Communications Magazine, vol.49, no. 11, pp. 30-31, 2011.

[3] Wangham, MS, Domenech, MC, and de Mello, "Authentication And Authorization Infrastructure for the Internet of Things," 13th Brazilian Symposium on Information and Computer System Security (SBSeg'13), vol. 1.

[4] Mohsen HallajAsghar, AtulNegi and NasibehMohammadzadeh, "Principle Application and Vision in Internet of Things (IoT)," International Conference on Computing, Communication and Automation (ICCCA), ISBN:978-1-4799-8890-7, 2015.

[5] Michael J. Covington and Rush Carskadden, "Threat Implications of the Internet of Things," 5th International Conference on Cyber Conflict, 2013.

[6] Louis Coetzee and Johan Eksteen, "The Internet of Things – Promise for the Future?An Introduction", IST-Conference Proceedings Paul Cunningham and Miriam Cunningham, International Information Management Corporation (IIMC), ISBN: 978-1-905824-26-7, Africa, 2011.

[7] Rolf H. Weber, "Internet of Things – New Security and Privacy Challenges", Science Direct, computer law & security review no.26, pp. 23-30, 2010.

[8] D.C. ZHU Shunbing, "Research On Urban Public Safety Emergency Management Early Warning System Based On Technologes for the Internet Of Things," International symposium on safety science and technology, Procedia Engineering, vol. 45, pp. 748-754, 2012.

[9]S.Raza, L.Wallgren and T. Voigt, "SVELTE:Real-Time Intrusion Detection in the Internet of Things," Elsevier, Ad Hoc Networks, vol. 11, pp. 2661-2674, 2013.

[10]M.Aharan, "Critical Success Factors And Challenges of Implementing RFID in Supply Chain Management," Journal of supply chain and operations management,vol. 10, no.1,pp. 144-167, 2012.

[11]P.Jappinen, R. Guarneri and L. M.Correia, "An Applications Perspective into the Future Internet," Journal of network and computer applications, Elsevier, vol. 36, pp. 249-254, 2013.

[12] S. Subashini and V.Kavitha, "A Survey On Security Issues In Service Delivery Models Of Cloud Computing," Journal of network and computer applications, Elsevier, vol. 34, pp. 1-11, 2011.

[13] M.U. Farooq, Muhammad Waseem, AnjumKhairiandSadiaMazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, February 2015.

[14] Security In The Internet Of Things. Windriver. Retrieved October 16, 2015, Fromhttp://www.windriver.com/whitepapers/security-in-the-internet-of-things/.

[15] M. Aharan, "Critical Success Factors And Challenges of Implementing RFID in Supply Chain Management," Journal of supply chain and operations management, vol.10, no.1, pp144-167, 2012.

[16] M.U. Farooq, Muhammad Waseem,SadiaMazhar,AnjumKhairiandTalha Kamal, "A Review on Internet of Things (IoT),"International Journal of Computer Applications, vol. 113, no.1, March 2015.

[17] Rafiullah Khan, SarmadUllah Khan, RifaqatZaheer and ShahidKhan,"Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges," 10th International Conference on Frontiers of Information Technology, ISBN: 978-0-7695-4927-9, 2015.