Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 02, February -2018

Security assaults on IoT and pageant a synopsis of conversant safekeeping elucidations

Gayathri . B,

Assistant Professor, Department of Computer Science,
Valliammal College for Women, E-9 Anna Nagar East, Chennai – 600 102.

Abstract-*Internet of things (IoT) is seen as a pervasive network of networks; which consists of numerous heterogeneous entities both physical and virtual networks interconnected with another entity through unique addressing schemes. IoT applications are expected to affect many aspects of peoples living. This survey focuses on the various security aspect of IoT&DDoS.*

Keywords *:Internet of things (IoT), Distributed Denial of Service (DDoS)*

I .Introduction :

In recent years, smart devices, smart cars, smart cities and smart homes have received great interest from various research communities. This concept is considered as the future of internet and it is called the Internet of Things [1,2,3]. Recent advancement in electronics have enabled the development of all kinds of small size devices with various degrees of sensing computing, storage and power capabilities which leads to the opportunity of utilizing almost any objects as a smart and communicating device rather than an isolated entity for the purpose of unlimited number of applications providing security and confidentiality requirements [4,5].On technical aspect, IoT encompasses both static and dynamic objects of the physical world. The essential features of IoT include : (i) Interconnectivity (ii) things-related service such as privacy and semantic consistency (iii) heterogeneity (iv) support of dynamic changes in the number of devices. (v) enormous scale.

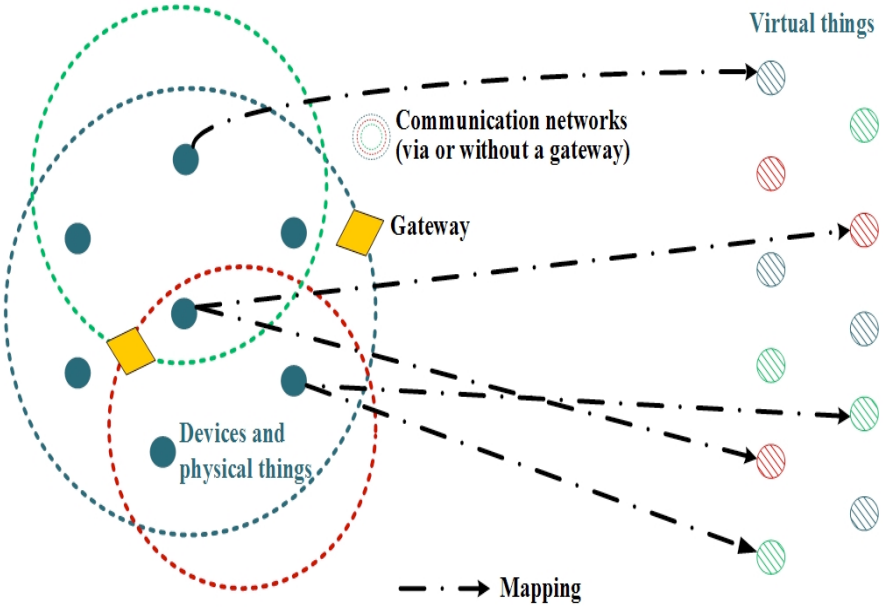

Fig 1 :Technical perspective of the Internet of Things

The goal of this paper is to examine the security attacks on IoT and present an overview of up-to-date security solutions. The rest of this paper is organized as follows : Section – II describes Security attacks on IoT, Section III –related work in the field of IoT security, Section IV – protection and preventive measures in DDoS attack. Section V – Future enhancement.

II . Security Attacks on IoT

The biggest challenge is IoT is ensuring data privacy and protection. Since it is an integration of multiple heterogeneous networks it is difficult to achieve a reliable connection between the individual nodes in IoT. The most basic architecture is a three-layer architecture. It has three layers, namely, the perception, network, and application layers.(i)The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.(ii)The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.(iii)The application layer is responsible for delivering application specific services to the user.[6] It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.
DDoS attack on IoT based at different layers are as follows: [6]

DDoS on Perception Layer:

- RFID: The RFID devices are wireless microchips used for tagging object for automated verification. It may be used for identifying objects wirelessly. It is used for reading data from sensors without human interaction.
- Using the Kill Command any command can be easily disabled. Using brute force attacks these commands may be disabled even if they are password protected.

DDoS on Network Layer:

- Flooding attacks: An attacker tries to disrupt the service by flooding the victims system with large amount of traffic. eg : UDP Flood
- Reflection based flooding attacks : An attacker sends fake replicated request to the Network amplifier with the return address, addressed to the victims' address. eg : Smurf Attack
- Protocol Exploitation flooding : An attacker tries to exploit specific resources to make system unresponsive to the data traffic.
- Amplification based flooding attacks: An attacker tries to generate continuous messages to the amplifier (to broadcast messages) so that the traffic to the system increases. A Botnet may be used for this purpose.

DDoS on Application Layer: In this layer two types of attack can happen:

1) Reprogramming attack: In this attack, the attacker modifies the source code in such a way that it goes to an infinite loop so that the resource becomes inaccessible.
2) Path based DDoS : The attacker burdens the sensor nodes by flooding multi hop end-to-end communication path by injecting spurious packets.

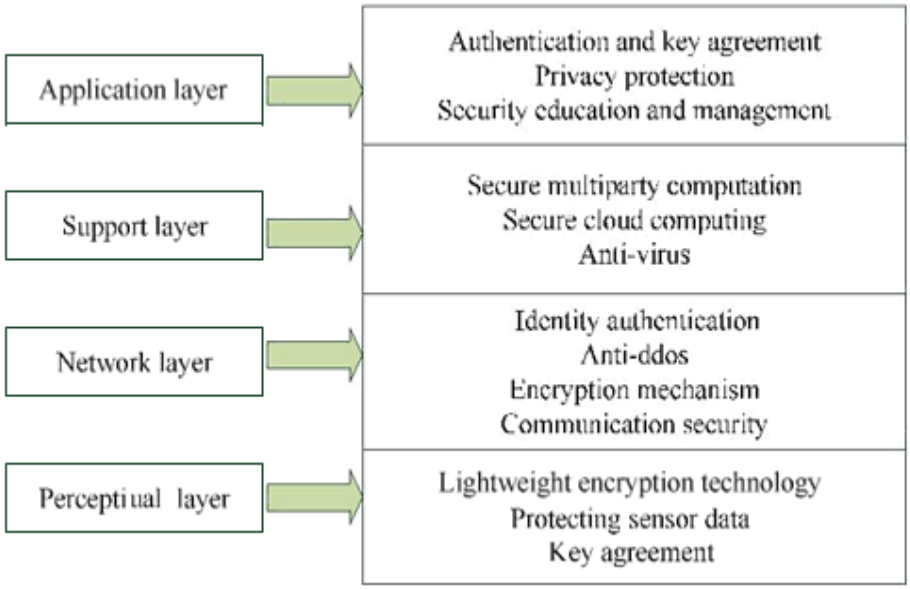

Figure 2. Security requirements in each level *Security Requirements*

According to the above analysis, we can summarize the security requirements for each level in the following, as shown in Fig. 3.

a) Perceptual Layer: At first node authentication is necessary to prevent illegal node access; secondly to protect the confidentiality of information transmission between the nodes, data encryption is absolute necessity; and before the data encryption key agreement is an important process in advance; the stronger are the safety measures, the more is consumption of resources, to solve this problem, lightweight encryption technology becomes important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol. At the same time the integrity and authenticity of sensor data is becoming research focus, we will discuss this question more in-depth in the next section.

b) Network Layer: In this layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, and it is the premise of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrality mechanism. Besides distributed denial of service attack (DDoS) is a common attack method in the network and is particularly severe in the internet of thing, so to prevent the DDOS attack for the vulnerable node is another problem to be solved in this layer.

c) Support Layer: Support layer needs a lot of the application security architecture such as cloud computing and secure multiparty computation, almost all of the strong encryption algorithm and encryption protocol, stronger system security technology and anti-virus.

IoT Layer	Security issues
Application Layer	Information availability, User authentication, Information Privacy Data Integration
Transport layer	DoS / DDoS attack, forgery/ middle attack, WLAN Application conflicts
Perception Layer	Interruption, interception modification, fabrication uniform coding for RFID

d)Application Layer: To solve the security problem of application layer, we need two aspects. One is the authentication and key agreement across the heterogeneous network, the other is user's privacy protection. In addition, education and management are very important to information security, especially password management [4,10].

In summary security technology in the IoT is very important and full of challenges. In other hands laws and regulations issues are also significant, we will discuss this problem in the following.

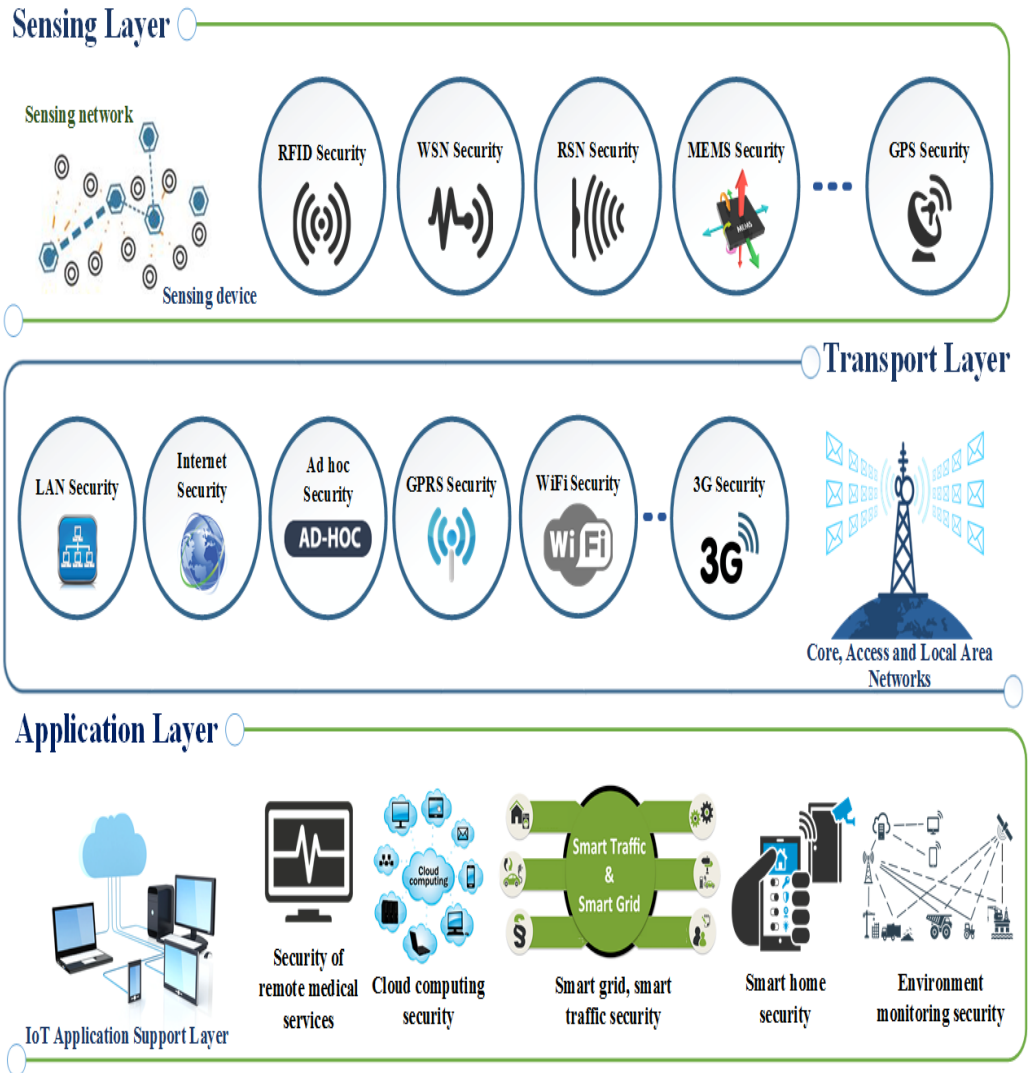

Fig 2: Security architecture of 3 layers in IoT

III . Related work in the field of IoT Security

In the transport layer of the IoT the DDoS attack is very common.A denial of service (DoS) attack happens when a service that would usually work is unavailable. There can be many reasons for unavailability, but it usually refers to infrastructure that cannot cope due to capacity overload. In a Distributed Denial of Service (DDoS) attack, a large number of systems maliciously attack one target. This is often done through a botnet, where many devices are programmed to request a service at the same time. When such types of attack occur from various compromised malicious nodes at the same time then it is called Distributed Denial Of Service (DDoS).

IV. Protection and Preventive Measures in DDoS attack.

Increase the Bandwidth to mitigate DDoS attacks
Attackers just flood the website with requests and the website gets blocked. If the bandwidth is expandable, it can handle attacks of any size. Having bandwidth redundancy can fix DDoS attacks at the initial stage.

Use of CDN for DDoS protection :
CDN – is a network that is geographically distributed network of proxy servers and their centers. If the requests are processed in a distributed then it may help in DDoS prevention. The goal is to distribute service across end users to provide high performance. CDN's serve a very good way for DDoS prevention.

Use of DDoS Mitigation :
ADDO Smitigationappliance uses ahardware server to help mitigate and DDOS prevention.

Key features of a DDOS mitigation appliance:
A DDOS mitigation appliance is good at blocking limited DDOS threats, but it has several limitations.
Key features of DDoS mitigation appliance :
1. It offers a hybrid and network based service.
2. It delivers DDoS protection network as well as third party network providers.
3. It is used for robust reporting
4. Security for threats, for layers 3 to 7.

Cloud Based Services to block and fix DDoS attacks :
A cloud based DDoS protection service is needed to block DDos Attack. Multiple servers with high bandwidth ensures that DDoS flood attack can be controlled.

Human collaboration during an DDOS attack :
Here we can learn that how a DDoS attack can be fixed. Human Collaboration for multiple ISP's and security is important during a massive DDoS attack. It will be great when a particular IT security expert can find a way to block a DDoS attack.

V. Future Enhancement

IoT is expected to integrate advanced technologies of communication, networking, cloud computing which paves the way for ground breaking applications in various areas. This survey focuses on the security attacks of IoT and DDoS attacks which provides an overview of up-to-date IoT security solutions and enhances others to work on any one of the security measures to overcome the drawbacks as mentioned earlier in this paper.

References:

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), "The Internet ofThings," Springer, 2010. ISBN: 978-1-4419-1673-0.J.
[2] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey,"Computer Networks (2010),doi:10.1016/j.comnet.2010.05.010
[3] J. A. Stankovic, "Research Directions for the Internet of Things",IEEEInternet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.
[4] A. Mohsen Nia, and N. K. Jha, "A Comprehensive Study of Security ofInternet-of-Things," in IEEE Transactions on Emerging Topics inComputing , vol. PP, no. 99, pp. 1-1, 2016.
[5] International Telecommunication Union TelecommunicationStandardization Sector Study Groups (ITU-T), "Y.4000/Y.2060 (06/2012) Recommendation,"
[6] Krushang Sonar and HardikUpadhyay "A survey :DDoS attack on Internet of Things" in International Journal of Engineering Research and Development,Volume10,Issue 11(November 2014)
[7]Richard H, Shivakant M Jing D(2005, Nov) "Defending against path based DoS attacks in wireless sensor networks"
[8] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.
[9]T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[10]C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

