Asian Journal of Applied Science and Technology (AJAST)
(Quarterly International Journal) Volume 4, Issue 1, Pages 01-05, January-March 2020

A Survey on 3-Tier Architecture of IOT-Challenges and Remedies

D.John Pragasam[1], P.Selvaprasanth[2] & A.Manoj Prabaharan[3]

[1,2,3]*Assistant Professor, Department of ECE, Sethu Institute of Technology, Tamil Nadu, India.*

Article Received: 13 October 2019 Article Accepted: 14 December 2019 Article Published: 10 January 2020

ABSTRACT

Internet of things (IoT) is a new revolution that uses Internet services to connect to the entire world anywhere, at any time without restricting geographic location. It provides a platform for communication between objects, self-regulation and identification by radiofrequency identification (RFID), the ZigBee network, the wireless network, etc. for efficient communication. The unique features of this technology provide the dynamic nature, connectivity, massive scale, heterogeneity, sensor power, etc., which have the ability to improve various innovative applications and services. However, the IoT structure provides a complex environment that has many difficult problems such as connectivity, power, power and other security, which must be resolved. The success of the Internet of things depends on a security problem that protects users' personal data from threats in real time. But many of the security mechanisms already used in the traditional network are no longer enough to protect the next generation of the Internet from things. This article reviews several security attacks and their countermeasures on the three levels of the Internet of things. Initially, we provide an overview of each level of the Internet of things with applications and challenges. After that, we discuss different attacks and countermeasures for each layer. Finally, we analyze network routing attacks, which are more powerful attacks that can degrade the Internet performance of things.

Keywords: Perception layer, Security and challenges, Internet of Things.

1. INTRODUCTION

Internet of Things (IoT) is a new revolution that uses Internet services to connect to the entire world anywhere, anytime without restricting geographic location. It provides a platform for interconnecting things, self-organizing, identifying themselves using radio frequency identification (RFID), ZigBee network, wireless network, etc. for effective communication. The unique characteristics of this technology provide the dynamic nature, connectivity, large size, heterogeneity, sensed energy, etc., which have the ability to promote various innovative applications and services such as smart supply chain, smart city, industrial internet, cars and smart connected health networks, smart home, agriculture Smart, smart retail, etc., which are more suitable for today's needs. Internet of Things provides a three-tiered architecture - perception, network, and layer application.

In the perception layer, Internet of Things is deployed with different types of sensors - RFID, temperature sensor, proximity sensor, etc. Each sensor is an information source that captures the contents. The second is the network layer, which is the core of the Internet of Things that integrates various wireless and wired networks for accurate transmission of information that is collected regularly from the sensor nodes. Another layer is the application layer that collects, processes and analyzes the necessary data. However, the structure of the Internet of Things provides a complex environment that contains many difficult problems like connectivity, energy, energy and security, which need to be solved. The success of IoT depends on a security issue that protects personal user data from real-time threats. However, the different security mechanism already used in the traditional network is no longer sufficient to protect the next generation of Internet of Things. This paper reviews several security attacks and countermeasures at the three levels of the Internet of Things.

2. RELATED WORK

In this section, we presents related work on various attacks and their countermeasures in the Internet of Things, proposed by various researchers. In [1],[2],[3] Manish Gupta et.al developed an ontological framework to differentiate the existing countermeasures under three categories namely prevent, detect and respond. They also proposed a different classification method for DDoS prevention depending upon the location of components placed.

Swathigavaishnavi et.al in [4],[5],[6] has proposed a two-phase malicious code detection mechanism, in which phase 1 detects the malicious code that exhibits obfuscated behavior by performing static analysis on the instruction sequence. In phase 2, the opcode is extracted from the dataset and is used in the construction of a classification model. Finally, it is compared with the results of phase 1 to decide if it's malicious or not.

Mauro Conti et.al reviewed various literatures the Middle Attack and grouped the existing prevention mechanisms into various categories in [7],[8]. They also suggested few direction for research in future.In [9], a new protocol namely, Secure Data Exchange Protocol(SDEP) is proposed by Yaping which takes advantage of both sequence encryption algorithm and Hash algorithm and helps in maintaining user privacy and preventing leakage of information. Focused on reviewing existing counter measures against sinkhole attack. George W. Ki[10],[11],[12] classified the existing solutions based on their advantages and limitations. The IoT architecture represented in the figure 1.

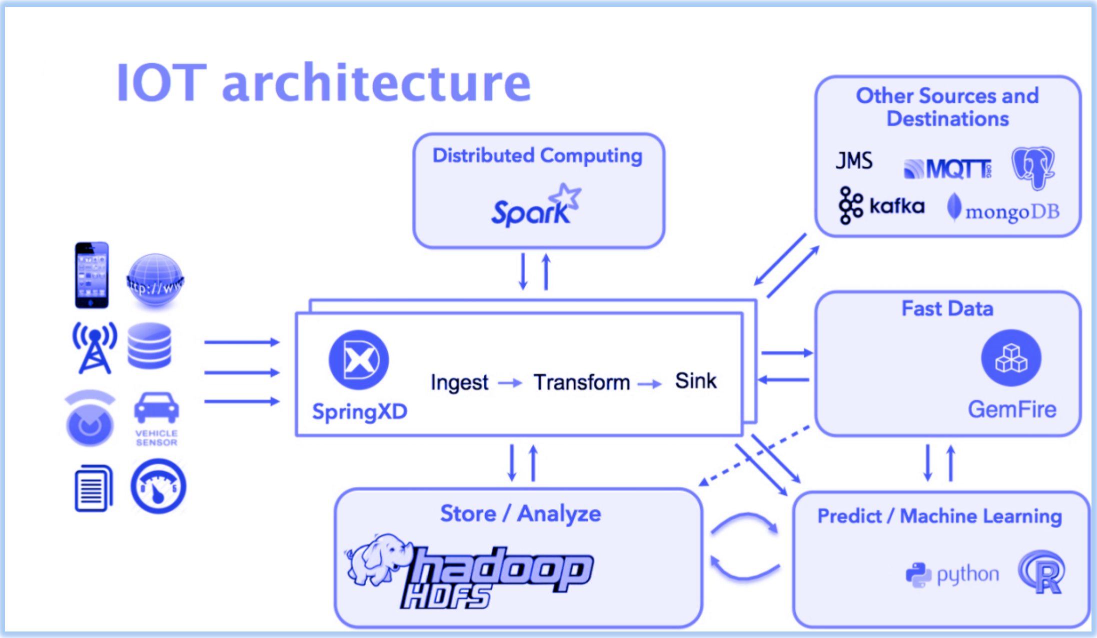


Figure 1: Architecture of IoT

3. NETWORK LAYER

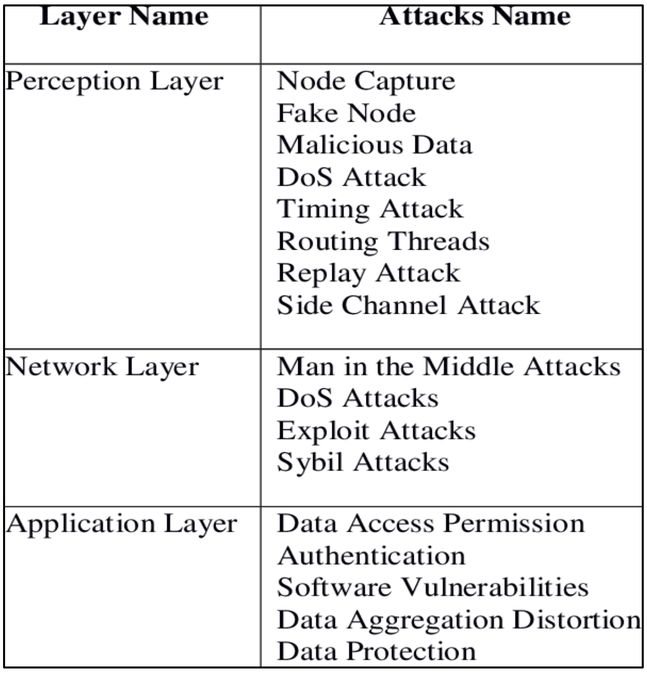
The network layer is the second layer of IoT that communicates with existing networks to transfer the data that has received from the perception layer. The entire process of this layer can be carried communication networks such as Ad hoc, GPRS, WiFi, or Mobile Internet. To achieve effective communication between the constrained devices, there is a need of efficient routing protocol. Some of these protocols in this layer are listed below[13],[14],[15].

Routing Protocol for Low-Power and Loss Networks (RPL)-RPL refers to Routing Protocol for Low-Power and Loss Networks, which is a distance vector protocol that supports different varieties of data link protocols. This protocol builds a Destination oriented directed acyclic graph that has only one route between every leaf node and root. In order to build the DODAG, each leaf node individually sends a (DODAG Information Object) DIO which advertises itself as root. This advertised message is transmitted back to the network. While communicating, a node sends Destination advertisement object (DAO) to their own parents and it will be propagated directly to the root.

Later, the root will decide where to send it depending upon the destination. Suppose, when fresh node wants to join the network then it will send a DIS (DODAG Information solicitation) request to join the network and the root replies with a DAO-ACK (DAO Acknowledgment) by approving the request. The RPL nodes can be either stateless (or) state full. In this stateless, node keeps track of their own parents and the only root has the entire (Destination-oriented directed acyclic graph) DODAG knowledge.so that all the communications go through the root. While, in state full, node keeps track of their own children as well as parents also, because it is a sub-tree communication of the DODAG that does not have to refer the root.

Cognitive Routing Protocol for Low-Power and Loss Networks(CORPL)-The extension of RPL is CORPL named as Cognitive RPL that is designed for cognitive networks and uses (Destination-oriented directed acyclic graph) DODAG topology with two new changes to RPL. This utilizes the opportunistic forwarding while forwarding all the packets with multiple forwarders and chooses the best next hop to forward the packets. Each node maintains its own forwarding set and updates its neighbors with the changes occurred via DIO (DODAG Information Object) messages.

With this updated information, each node continuously updates its neighbor's priorities so as to construct the new forwarding set. Channel-Aware Routing Protocol(CARP)-CARP refers to Channel-Aware Routing Protocol. It is a distributed routing protocol that is designed for underwater communications and can be used because of its lightweight packets. It also studies the link quality, which is computed depending upon old data transmissions (successful) that are collected from neighbouring sensors, to select



Layer Name	Attacks Name
Perception Layer	Node Capture Fake Node Malicious Data DoS Attack Timing Attack Routing Threads Replay Attack Side Channel Attack
Network Layer	Man in the Middle Attacks DoS Attacks Exploit Attacks Sybil Attacks
Application Layer	Data Access Permission Authentication Software Vulnerabilities Data Aggregation Distortion Data Protection

Figure 2: Attacks on Layers

4. PERCEPTION LAYER

Attacks on Perception layer: The collected information from the sensor devices may be highly sensitive in nature, as these nodes are deployed in inaccessible and hostile area in which attackers can physically captured and later destroy the information. Moreover, the attacker may be of hardware or software that significant damages the networks. Therefore security in such networks is crucial concern and poses severe challenges. Some of the attacks in this layer is shown in figure 2. Each of the attacks and its count measure are discussed below. Finally summary of attacks and its countermeasures in depicted in table.

5. CONCLUSION

This paper reviews various security attacks and its countermeasures in the three tiers of IoT. Initially, we presented overview of each tier of IoT with application and challenges. Next, we discussed the various attacks and countermeasures of each tier. Finally, we analysed the network routing attacks, which are more powerful attacks that can degrade the performance of the IoT.

REFERENCES

1. P. Meenalochini and S. P. Umayal ,Comparison of Current Controllers on Photo Voltaic Inverters Operating as VAR Compensators, Journal of Electrical Engineering The Institution of Engineers, Bangladesh Vol. EE 38, No. I, June, 2012.

2. Karthick, R and Sundararajan, M: “A Reconfigurable Method for TimeCorrelatedMimo Channels with a Decision Feedback Receiver,” International Journal of Applied Engineering Research 12 (2017) 5234.

3. Karthick, R and Sundararajan, M: “PSO based out-of-order (ooo) execution scheme for HT-MPSOC”Journal of Advanced Research in Dynamical and Control Systems 9 (2017) 1969.

4. Karthick, R and Sundararajan, M: “Design and Implementation of Low Power Testing Using Advanced Razor Based Processor,” International Journal of Applied Engineering Research 12 (2017) 6384.

5. Karthick, R and Sundararajan, M: “A novel 3-D-IC test architecture-a review,” International Journal of Engineering and Technology (UAE)7 (2018) 582.

6. R.Karthick, P Selvaprasanth, A ManojPrabaharan, “Integrated System For Regional Navigator And Seasons Management,” Journal of Global Research in Computer Science 9(4),2018(11-15).

7. Karthick, R and Prabaharan, A.Manoj and Selvaprasanth, P. and Sathiyanathan, N. and Nagaraj, A., High Resolution Image Scaling Using Fuzzy Based FPGA Implementation (March 15, 2019). Asian Journal of Applied Science and Technology (AJAST), Volume 3, Issue 1, Pages 215-221, Jan-March 2019 . Available at SSRN: https://ssrn.com/abstract=3353627

8. Karthick, R and Sundararajan, M., Hardware Evaluation of Second Round SHA-3 Candidates Using FPGA (April 2, 2014). International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2, Issue 2, Ver. 3 (April - June 2014). Available at SSRN: https://ssrn.com/abstract=3345417.

9. Karthick, R and and Prabaharan, A.Manoj and Selvaprasanth, P.,Internet of Things based High Security Border Surveillance Strategy (May 24, 2019). Asian Journal of Applied Science and Technology (AJAST), Volume 3, Issue 2, Pages 94-100, Apr-June 2019. Available at SSRN: https://ssrn.com/abstract= 3394082.

10. Karthick, R and Sundararajan, M: “SPIDER based out-of-order (ooo) execution scheme for HT-MPSOC” International Journal of Advanced Intelligence paradigms, In Press.

11. Karthick, R and John Pragasam, D “Design of Low Power MPSoC Architecture using DR Method” Asian Journal of Applied Science and Technology (AJAST) Volume 3, Issue 2, Pages 101-104, April -June 2019.

12. Karthick, R and Sundararajan, M., Optimization of MIMO Channels Using an Adaptive LPC Method (February 2, 2018). International Journal of Pure and Applied Mathematics, Volume 118 No. 10 2018, 131-135. Available at SSRN: https://ssrn.com/abstract=3392104

13. Karthick, R and Rinoj, B. Micheal Vinoline and Kumar, T. Venish and Prabaharan, A.Manoj and Selvaprasanth, P., Automated Health Monitoring System for Premature Fetus (July 27, 2019). Asian Journal of Applied Science and Technology (AJAST) (Peer Reviewed Quarterly International Journal) Volume 3, Issue 3, Pages 17-23, July -September 2019. Available at SSRN: https://ssrn.com/abstract=3427756

14. Karthick, R.,Deep Learning For Age Group Classification System, International Journal Of Advances In Signal And Image Sciences. Volume 4, Issue 2, Pages 16-22, 2018.

15. R. Karthick, N.Sathiyanathan, "Medical Image Compression Using View Compensated Wavelet Transform" Journal of Global Research in Computer Science 9(9), 2018(1-4).