Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

Classifications on IoT Attacks

Ninad Gadkar
M.E Student,
Electronics and Telecommunication Department
Sinhgad College of Engineering
Vadgaon-Pune, India

Dr. Achala Deshmukh
Associate Professor,
Electronics and Telecommunication Department
Sinhgad College of Engineering
Vadgaon-Pune, India

***Abstract*— Internet of Things is an emerging technology having the ability to change the way we live. In IoT vision, each and every 'thing' has the ability of talking to each other that brings the idea of Internet of Everything in reality. Numerous IoT services can make our daily life easier, smarter, and even safer.**

Automated object detection algorithm is an important research challenge in intelligent urban surveillance systems for IoT and smart cities applications. In particular, smart vehicle license plate recognition (VLPR) and vehicle detection (using RFID) are recognized as core research issues of these IoT-driven intelligent urban surveillance systems. They are key techniques in most of the traffic related IoT applications, such as road traffic real-time monitoring, security control, searching stolen vehicles, etc.Our proposed method can not only help to detect object vehicles rapidly and accurately, but also can be used to reduce big data volume needed to be stored in urban surveillance systems.

I. INTRODUCTION

Right now we are living in the era of Internet and rapidly moving towards a smart planet where every device will be connected to each other. Internet of Things (IoT) [1] is the technology helping us to achieve the goal of a smart world. IoT [2] have the ability to change the vision of our way of living. All developing countries are aiming to transform their cities into Smart City [3] by taking several projects. For example, the government of India has taken an initiative called Digital India and Smart City [4] to connect the nation to Internet.

In a smart city every device or better to say every 'thing' is connected 24 × 7 to the Ubiquitous network [5]. They can communicate to each other regardless of their communication protocols and hardware or software infrastructure. In this paper, we have used the concept of a smart city to provide a life saviour system for a smart vehicle in any kind of emergency situation occurred on road. And vehicle detection also.

II. BASIC IOT CONCEPT

A. Comprehensive awareness:
It is because of sensors and RFID. The advantage of this Sensor is to collect the information of the object.
B. Reliable transmission:
Reliable transmission provides real time and high accuracy.
C. Intelligent processing:
Intelligent processing does the analyses and couples the intrinsic information as per the user speculation.

III. CLASSIFICATIONS OF ATTACKS

Andrea et al. [10] come up with a new classification of IoT devices attacks presented in four distinct types:

A. Physical.

B.Network,

C.Software,

D.Encryption attacks.

Each one covers a layer of the IoT structure (physical, network, and application), in addition to the IoT protocols for data encryption. The physical attack is performed when the attacker is in a close distance of the device. The network attacks consist of manipulating the IoT network system to cause damage. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system.

Encryption attacks consist of breaking the system encryption. This kind of attacks can be done by side channel, cryptanalysis, and man-in-the-middle attacks. They also presented a multi-layered security approaches to address the IoT structure layers and encryption system vulnerabilities and security issues. Based on the study, to countermeasure the security problems at the physical layer, the device has to use secure booting by applying a cryptographic hash algorithms and digital signature to verify its authentication and the integrity of the software. Also, a new device must authenticate itself to the network before any transmission or reception of data. In addition to that, a device should carry an error detection system, and all of its information has to be encrypted to maintain data integrity and confidentiality.

At the network layer, authentication mechanisms and point-to-point encryption can be used to ensure data privacy and rooting security. The application layer can also provide security by means of authentication, encryption, and integrity verification, which allows only the authorized users to access data through control lists and firewalls, in addition to the use of anti-virus software. The physical attack is performed when the attacker is in a close distance of the device. The network attacks consist of manipulating the IoT network system to cause damage.

Ronen et al. [11] introduced a new taxonomy classification for IoT attacks based on how the attacker features deviates from the legitimate IoT devices. The categories are presented in: ignoring, reducing, misusing, and extending the system functionality. The study focused on the functionality extension

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

attacks on smart lights. The paper presented two attacks: the first one consisted of creating a covert channel to capture confidential information from an organization building that implemented smart lights which are connected to the internal sensitive network.

The work is done by using an optical receiver that could read the data from a distance of over 100 meters by measuring the exact duration and frequency of the small changes in the lights intensity. The second attack showed that an attacker can use those lights to create strobes in the sensitive light frequencies, which can lead to a risk of epileptic seizures. The experiments showed that it is necessary to focus on security issues during the different phases of designing, implementing and integrating of the IoT devices.

IV. IOT DEVICE LIMITATION

Why is it difficult to secure and apply security features to IoT as those used in traditional Internet? Trappe et al. [9] presented the issue of IoT constraints, and their effects on using current cryptographic tools as the ones utilized in traditional Internet. The two main limitations are the battery capacity and computing power.

A. Battery Life Extension

Because some IoT devices are deployed in environments where charging is not available, they only have a limited energy to execute the designed functionality and heavy security instructions can drain the devices' resources. Three possible approaches can be used to mitigate this issue. The first is to use the minimum security requirements on the device, which is not recommended especially when dealing with sensitive data. The second approach is to increase the battery capacity.

V. CONCLUSION

In this paper we have discussed about the present state of Internet of things, also we have examined the different attacks in IoT. We discussed the various layered in IoT architecture and applications of IoT.We have also discussed about the solutions to improve the robustness in various service level and systems for global navigation satellite system. In future, detection of Denial of Service (DoS) attack in IoT will put forward and effectiveness will be calculated.

ACKNOWLEDGEMENT

Authors express his sincere thanks to our research guide Dr.Achala Deshmukh, Department of Electronics & Telecommunication Engineering, for their valuable guidance and continuous support. Also Author takes this opportunity to thank Dr. M.B.Mali, Head of Department of Electronics & Telecommunication Engineering and our PG Co-coordinator Dr. Achala Deshmukh for their helpful suggestions.

REFERENCES

[1] IoT Analytics, "Why the internet of things is called internet of things:Definition,history,disambiguation,"https://iotanalytics.com/internetof-things-definition/, 2014.

[2] Irfan Saif and Sean Peasley and Arun Perinkolam, "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connectedage,"https://dupress.deloitte.com/dup-en/deloittereview/issue-17/internet-of-things-data-security-and-privacy.html, 2015.

[3] Margaret Rouse, "Iot security (internet of things security)," [8] http://internetofthingsagenda.techtarget.com/definition/IoT-securityInternet-of-Things-security, 2013.

[4] Brian Lam and Cynthia Larose, "How did the internet of things allow thelatestattackontheinternet?" https://www.privacyandsecuritymatters.com/2016/10/how-did-theinternet-of-things-allow-the-latest-attack-on-the-internet/, 2016.

[5] Talkin Cloud, "Iot past and present: The history of iot, and where it's headed today," http://talkincloud.com/cloud-computing/iot-past-andpresent-history-iot-and-where-its-headed-today?page=2, 2016.

[6] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for ipv6 enabled wireless sensor networks," in 2010 IFIP Wireless Days, Oct 2010, pp. 1–6.

[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146 – 164, 2015.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266 – 2279, 2013, towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet.

[9] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in 2016 11th International Conference on Availability, Reliability and Security (ARES), Aug 2016, pp. 382–388.

[10] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180–187.

[11] E. Ronen and A. Shamir, "Extended functionality attacks on iot devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P), March 2016, pp. 3–12.