Chapter 8

Intrusion Detection Systems for Internet of Things

Gayathri K. S.
https://orcid.org/0000-0002-4029-3165
Mar Baselios College of Engineering and Technology, India

Tony Thomas
Indian Institute of Information Technology and Management, Kerala, India

ABSTRACT

Internet of things (IoT) is revolutionizing this world with its evolving applications in various aspects of life such as sensing, healthcare, remote monitoring, and so on. These systems improve the comfort and efficiency of human life, but the inherent vulnerabilities in these IoT devices create a backdoor for intruders to enter and attack the entire system. Hence, there is a need for intrusion detection systems (IDSs) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities. Due to the limited computing and storage capabilities of IoT devices and the specific protocols used, conventional IDSs may not be an option for IoT environments. Since the security of IoT systems is critical, this chapter presents recent research in intrusion detection systems in IoT systems.

1. INTRODUCTION

Today the whole world is digitized. Internet has revolutionized the life of people around the world. Just as how human-to-human communication happened from remote location, we are entering into an era of device-to-device communication. The Internet of Things (IoT) is an interconnection of computing devices that can communicate with each other requiring minimum human-to-human or human-to-computer interaction. IoT market is growing at a breathtaking pace, starting with two billion objects in the year 2006 to a projected 200 billion by 2020; a rise of 200% is observed (Chaabouni, 2018). Owing to the intelligent nature of IoT devices, they are used in almost all fields like finance, health care, education, energy distribution, smart cities etc., The Padova Smart City in Italy is an example of IoT based smart city.

DOI: 10.4018/978-1-7998-2242-4.ch008
High access to Internet makes network security a necessity in IoT networks. Internet usage has given rise to cyber critical threats ranging from a malware to a network intrusion, thereby causing business losses. An intrusion is any unauthorized activity on a device or a network with some malicious intention. The aim of intruder ranges from modifying system logs, making resources engaged; to threaten the security of data and resources in the network. The security loopholes of IoT systems create various security threats to the different IoT layers. Attacks on critical applications like medical and power plants may cause severe consequences in controlling a person or bringing down power supply. Attacks on household appliances cause loss of properties or can be threatening to the security and privacy of families.

IoT networks are vulnerable to a variety of different attacks towards disrupting the network. There are several built-in vulnerabilities of IoT devices through which a hacker can invade the system. Some of these vulnerabilities published by OWASP are weak or guessable passwords, insecure network services, insecure cloud, mobile or backend API services, lack of secure updates, use of insecure or outdated components, insufficient privacy protection, insecure data transfer and storage, insecure default settings etc. Also millions of services are using obsolete protocols like FTP and Telnet, through which majority of attackers invade the system. Moreover, the protocols used for communication lacks security as neither they check the data they transport nor they encrypt the data. So attackers try to use any of these loopholes to evade the system and cause various attacks of their choice. Mostly, malwares focus on low-level vulnerabilities to infect the system. The need for an Intrusion Detection System (IDS) is critical for IoT applications.

IoT devices are restricted with computation, memory, bandwidth and energy and hence cannot execute computationally intensive and latency-sensitive security solutions. This makes most of the existing security solutions involving heavy computation, communication overhead inapplicable to IoT networks. Many companies are investing in research using intelligent techniques to design lightweight IDS for IoT networks. This chapter is organized as follows: Section 2 covers the IoT networks and Architectures. Section 3 focuses on the Intrusion Detection System in IoT. Section 4 discusses the intrusion attacks in IoT. Section 5 focuses on some of the existing research works on IDS in IoT. Finally, the Section 6 provides the future research directions and challenges of implementing IDS in IoT.

2. IOT NETWORK AND ARCHITECTURE

IoT is not a single technology, rather a collection of various technologies that work together in a collaborative manner. IoT devices are embedded with sensors, actuators, processors and transceivers. Sensors are devices that collect data from the physical environment. Common sensors are temperature, camera, pressure, UV etc. Data from sensors are stored and processed either on the edge of the network or in remote servers. Actuators are devices used to effect a change in the environment based on the processed information. IoT devices are installed at geographically dispersed location and so uses wireless communication medium. Devices, local network (gateway), Internet and back-end services form the core infrastructure of IoT architecture.

The most basic architecture of IoT is a three-layered architecture. The three layers are perception layer, network layer and application layer as shown in Fig 1.

The perception layer resembles the physical layer equipped with sensors. Perception layer is responsible for the data coming from the physical environment. The network layer is responsible for connecting other devices, network devices and servers for processing and transmitting data. The application layer is
Related Content

Information System Integrated Security
www.igi-global.com/chapter/information-system-integrated-security/63088?camid=4v1a

Personalized Key Drivers for Individual Responses in Regression Modeling
www.igi-global.com/article/personalized-key-drivers-for-individual-responses-in-regression-modeling/252179?camid=4v1a

Privacy Preservation Based on Separation Sensitive Attributes for Cloud Computing
www.igi-global.com/article/privacy-preservation-based-on-separation-sensitive-attributes-for-cloud-computing/226952?camid=4v1a

Association Rule Hiding in Privacy Preserving Data Mining
www.igi-global.com/article/association-rule-hiding-in-privacy-preserving-data-mining/208130?camid=4v1a