International Journal of Knowledge and Systems Science
Volume 11 • Issue 4 • October-December 2020

SDN-Based Secure Architecture for IoT

Shailendra Mishra, Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Saudi Arabia

ABSTRACT

Internet of things (IoT) means connecting things through the internet. The growing market for IoT also attracts malicious individuals trying to gain access to the marketplace. Security issues are among the most significant worries in companies that rely on the cloud of things to do business. SDN-based architecture has improved the security of IoT networks. The centralized controller is responsible for managing the critical network's operations, and growing the network size increases the network load in the controller. Controllers in SDN-based architecture are still facing security challenges such as unauthorized access, configuration issues, distributed denial of service (DDoS) attacks, and a man-in-the-middle (MITM) attacks. The attack scenario and security of SDN-based IoT networks are evaluated in this research. The simulation results show that the proposed approach and security solutions are fast and effective in mitigating the attacks.

KEYWORDS

Attack Mitigation, CVSS Score, DDoS attack, Internet of Things (IoT), MITM Attacks, Software-Defined Networking (SDN)

1. INTRODUCTION

The internet of things is developed from the concept of connection created by cloud computing and leads to the empowering of physical resources. The ability to connect one computer to the next irrespective of distance and control processes remotely leads to the IoT. An embedded system consisting of sensors and actuators connected through cloud computing is a remarkable discovery in the current century (Khan et al.,2017). Nevertheless, some security concerns continue to derail the expansion of cloud computing-based IoT systems in all parts of human life. Irrespective of how wonderful the technology continues to become with matters of application intelligence and data analytics, the query of how to protect information sufficiently emerges most of the time (De Donno et al.,2019). Companies and even government stores, enormous amounts of data in clouds for ease of use, and the servers used in the processes are invaluable to many people. These factors attract malicious parties to attack and extract information.

Security issues are among the most significant worries in companies that rely on cloud computing to do business; the businesses' management states that unauthorized activities affect business flow. Moreover, the risk increases when the company outsources these cloud storage services through a vendor (Marotta et al., 2019). Third-party vendors in cloud computing are standard practice in the

DOI: 10.4018/IJKSS.2020100101

corporate world (Stergiou et al., 2019). All these companies are at least if the vendor suffers from security breaches.

IoT technology comes with difficulties in protecting the privacy and safety of data. Organizations with interest in IoT technology should train their staff about safety measures and ways of detecting cyber-attacks. The organization should ensure they use robust protection measures while installing and operating their servers and other connected systems (Conti et al.,2019). Information and network security systems help protect the confidentiality of people's lives that employ it during communication; these systems protect the network and the database (Deng et al.,2019). SDN a new network paradigm that improves security in IoT networks. (Muthanna et al., 2019). The basic idea behind SDN is the separation of the network control plane and data plane. It decouples the network control and network forwarding elements. Software systems controlling the hardware must centralize network control on standard servers (Kreutz et al.,2019). SDN is expected to grow with the latest technology, and integration with cloud and IoT is secure and cost-effective (Dey & Yuksel, 2019). Google is one of the major companies which has deployed SDN to manage its data centers (Casado et al., 2019). Scalability and security have become a primary concern now a day in the SDN based IoT network (Al-Hayajneh, & McAndrew,2020).

SDN platform enables load balancing, virtualization, energy-efficient, and secure networking (Priyadarsini et al., 2019). The main security challenges in SDN are central control, virtualization, trust, and IT organizational changes (Wang et al.,2018; Alam et al.,2020). SDN deals with DDoS attacks due to the separation of network control planes and data planes with well-defined Open flow API (Hameed& Ahmed,2018). Researchers (Hameed& Ahmed, 2018; Yao et al.,2019; Abdulqadder et al.,2000) proposed multiple SDN controllers' architectures to address the challenges with a single point failure. The Control plane remains the main component in the networks, and attacking the control will compromise the system. It also suffers from attacks such as the denial of service (DDoS), IP spoofing, man in the middle (MITM), and information modification attacks. Therefore, the security of IoT networks based on multiple SDN controllers' system is evaluated in this work. This work focuses on attack surfaces: denial of service (DDoS) attack, IP spoofing, and man in the middle (MITM). An attacker can exploit SDN vulnerabilities that are located mostly in the control plane, such as control services and messages.

This research aims to discuss present security challenges, attack mitigation, and countermeasures in SDN based IoT network. In this paper, we proposed and simulated a secure SDN based IoT network architecture that protects the SDN based IoT network from attacks and efficiently mitigates the attacks. The attack model scoring system based on common vulnerability scoring system (CVSS) scores (S Mishra et al.,2020; CSV 3.0, 2020) is used to calculate the transition rate and probability of an attack. Calculated transition rates are used to investigate the relationship between attack probability and disconnection rate.

The contributions of this work are organized as Section 1 discussed the internet of thing, software defined networking, opportunities, and challenges of SDN based IoT network. Section 2 provides the background and systematic literature review on IoT and SDN security attacks in the SDN based network. Proposed SDN based IoT network, attack scenario, and attack model scoring are discussed in Section 3. Simulation setup, result analysis, and major findings are discussed in Section 4, and paper is concluded in Section 5.

2. BACKGROUND

The internet of things (IoT) developed about a decade ago with people wanting to use the internet to automate processes in different environments. The connection of the internet with an embedded computer system coupled with sensors and actuators brought about the notion of the IoT. However, the name 'Internet of Things' developed from a presentation in the Procter & Gamble corporation. The presenter showed that the company could use the internet to gather information about clients without

Run-Time Compositional Software Platform for Autonomous NXT Robots

Ning Gui, Vincenzo De Florio and Chris Blondia (2011). *International Journal of Adaptive, Resilient and Autonomic Systems (pp. 37-50).*

www.igi-global.com/article/run-time-compositional-software-platform/53465?camid=4v1a

Efficient Training Algorithm for Neuro-Fuzzy Network and its Application to Nonlinear Sensor Characteristic Linearization

Ajoy K. Palit and Walter Anheier (2010). *Intelligent Systems for Automated Learning and Adaptation: Emerging Trends and Applications (pp. 72-90).*

www.igi-global.com/chapter/efficient-training-algorithm-neuro-fuzzy/38451?camid=4v1a