IoT security improvement based on SDN Controller

Abdulrasool A. Abdulsamad Northern Technical University
abdulrasool.abduladheem@ntu.edu.iq

Thair A. Salih Northern Technical University
thairali59@ntu.edu.iq

ABSTRACT

The Internet of Things (IoT) is a promising and modern technology in which devices and things around us are connected to a remotely controlled network. A large number of IoT devices produce large amounts of data, which have a significant impact on the elements of the network and its security. As the various attacks on IoT networks are a source of great concern, mitigating these attacks has become necessary. Because traditional networks do not meet the purpose, it has become essential to search for other techniques to improve the network's ability to deal with these challenges. Hence the role of Software Defined Networking (SDN), a technology that has recently emerged to support the growth of large organizations and offer benefits that may be challenging to obtain in conventional networks, allows for the expansion and updating of network resources by appropriate needs, makes it easier to keep up with the ongoing development of the network structure, and lowers numerous expenses and costs

In this study, we discuss the concepts of the IoTs, then explain SDN technology, explain the mechanism of SDN networks, and discuss security problems and ways to solve them using SDN technology. We present a practical scheme that we have implemented in reality using OpenVswitch with Raspberry Pi and RYU SDN Controller In addition to NodeMCU.

The IoT Network is designed and then implemented in reality. A DDOS attack execution test is applied to these devices, and the attack is prevented and stopped using SDN technology.

The Raspberry Pi 4B is used with the USB to Ethernet Adapter in addition to the OVS as a switch that supports the OpenFlow protocol, and the NodeMCU with ESP is used as an IoT device

Keywords: Internet of Things (IoT), Software-Defined-Network (SDN), Security, Distributed Denial of Service (DDoS), OpenFlow, OpenVswitche (OVS).

Introduction

The term "IoTs" only emerged in the last few years. It represents a significant step forward in developing new information technologies and communication systems and has had important economic implications. There is no agreed-upon definition of the IoT. However, it is typically understood to be an expansion of the current internet to incorporate any inanimate object capable of two-way communication with Internet-connected electrical devices. IoTs are "a worldwide infrastructure for the information

society, which allows improved services by joining things (physical or virtual) with current or developing interoperable information and communication technologies," according to the International Telecommunication Union (ITU). In a smart environment, internet-connected IoT devices are frequently wireless communication, RFID (Radio Frequency Identification) tags, and sensor nodes. These gadgets' proliferation in daily life is a testament to their versatility (phone, watch, fridge, etc.) [1].

The IoT boosts and enhances human life and work efficiency in various disciplines. Smart buildings, smart cars, and multiple uses of IoT devices are expanding very quickly. The IoT is a network of physical items that can communicate with one another and with humans. These objects are sensors, software, and electronics[2].

In the coming years, IoT will have rapidly expanded. This new technology area will expand horizons and service options, bettering consumers' lives and boosting corporate productivity. Consumers can benefit from IoT's many application areas, which include healthcare, security, energy savings, comfort, and more. The IoT has the potential to significantly enhance such business processes as productivity, storage management, product and item tracking, agriculture, and decision-making. Smart environments, including smart cities, smart grids, smart buildings, etc., have been the focus of many IoT-related studies in recent years [2].

By 2025, it's expected that every gadget will have an Internet connection, which will drive up the total number of online gadgets. Cisco predicts that by 2030, there will be 500 billion IoT-connected devices. In addition, Telefonica (a Spanish multinational telecommunications company headquartered in Madrid) believes that by 2030, 90% of automobiles will be connected to the IoT and that by then, each person will have an average of 15 connected devices [3].

Because of the variety of IoT devices, underlying communication infrastructure, and protocols, IoT infrastructure is complicated and vulnerable to security attacks. Many IoT devices are already live but lack any security mechanism. Security in such IoT infrastructures is an enormous obstacle. These devices can be easy prey for hackers who can exploit vulnerabilities in these devices by sending fraudulent requests or intercepting sensor data. Most attacks on IoT devices involve either DoS denial of service or device battery drain. Traditional protection is often applied to these devices, but it is useless.[4].

Related Work

In 2016, Mehdi Nobakht et al. proposed an IoT-IDM intrusion detection and prevention system that use SDN architecture to offer network-level security for the IoT [8]. In 2016, Fatma AL Shuhaimi et al. analyzed the difficulties linked with IoT technology. They have reviewed and examined an integrated model of IoT and SDN. They have presented an algorithm or model based on SDN that can prevent various threats in an environment with IoTs.Then recommended, a procedure for selecting the Cluster head [9]. In 2016, Peter Bull et al. gave an overview of the necessity for a flexible and dynamic approach to IoT security. A discussion of the possibility of an SDN-based gateway to handle this issue has been offered to them. A Pox controller was used [10]. In 2017, Suman Sankar Bhunia et al. invented SoftThings, a secure IoT architecture built on SDN, to identify aberrant behavior and attacks as early as possible and mitigate them as necessary. This architecture relies on machine learning to track and learn from the behaviors of IoT devices over time [11]. In 2017, Mert Ozcelik et al. presented an edge-oriented detection and prevention solution against DDoS in the IoT utilizing SDN and Fog methods using Mirai as a case study. By utilizing SDN and fog computing as they approach the edge, they can lessen the hazards posed by a distributed denial of servicze in the IoT. In 2017, Pradip Kumar Sharma et al. proposed coupling SDN and blockchain technology to create the notion. They discovered that DistBlockNet satisfies the architectural requirements for the future IoT network and can identify attacks in real time with negligible performance overheads [13]. In 2018, Narmadha Sambandam et al. presented a study to create a system that could detect DDoS attacks early on using a measure of entropy. The project has been implemented using Raspberry Pis as OpenVswitches [14]. In 2018, Bhavika Pande et

al. offered a plan to identify all DDoS assaults by recording network traffic entering the SDN plane and filtering it through multiple modules, allowing them to detect DDoS attacks [15]. In 2020 Abdullah Al Hayajneh et al. They presented a solution for mitigating man-in-the-middle attacks against IoT, and then they implemented the proposed system model using Raspberry Pi, Kodi Media Center, and Openflow Protocol [16].

Software-Defined Networking (SDN)

SDN is a modern and promising way to connect computers. In this technology, the control plane and the data plane are fragmented. The control plane is prepared with a program called SDN Controller. The data plane consists of a Switch device. Standard protocols are used in these devices, and the control plane speaks to the Data plane via the OpenFlow protocol. SDN technology makes networks more visible and improves the network's ability to evolve and keep pace with various changes in the network structure. It also has many advantages, such as monitoring and managing traffic. SDN can also be used to find strange patterns in traffic. [5].

A range of services and programs in SDN technology, including Deep Packet Inspector (DPI), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and monitoring, are included in the application plane. In various applications, including traffic engineering, quality of service (QoS) differentiation, monitoring, and routing, these applications can help with decision-making.

The responsibility for managing and forwarding data is one of the main tasks of the Controller, which makes decisions based on information and knowledge of the entire network, connects to the data plane that contains switches and different network devices, and forwards the packets based on the flow table that is populated by the application level (SDN Controller) .as shown in Figure 1[6]

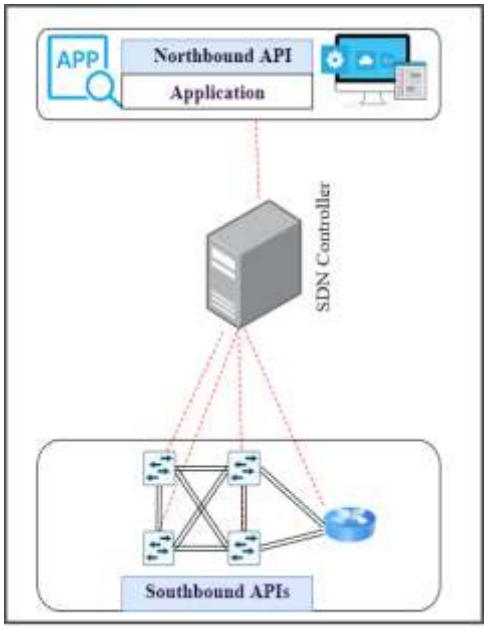

Figure 1 Software Defined Networking (SDN) Architecture

One of the most important advantages of separating the control plane from the data plane is that network management is improved, costs are reduced, and implementation and operation time is shortened while giving greater dynamics to the network due to programming skills [7].

SDN Communications Interfaces

The SDN comprises layers and communication interfaces, as shown in Figure 2. There are six main types of coatings and communication interfaces.

1. Application layer: also called the "management plane" It is represented by programs and applications that the

network administrator creates and that control data traffic in the network, such as (traffic engineering applications, quality of service, security, etc., and the "northbound API" interface is used to create these applications.

2. Control layer: also called the "control plane," consists of one or more SDN Controllers connected on one side to the Northbound APIs and on the other to the Southbound APIs via the OpenFlow protocol.
3. Transmission layer: also called the "data plane," This layer contains the devices and equipment of the network, such as (switches, routers, and Access Points) and its primary role is to connect the devices and transfer data.
4. Southbound APIs: This interface connects the SDN controllers with the network infrastructure (Switches and Routers). OpenFlow protocol is used in this connection process.
5. Northbound API: This interface is used to program and execute applications on the SDN console side
6. East/West communication interfaces enable controllers in a multi-controller architecture to communicate with one another and synchronize the network state [1].

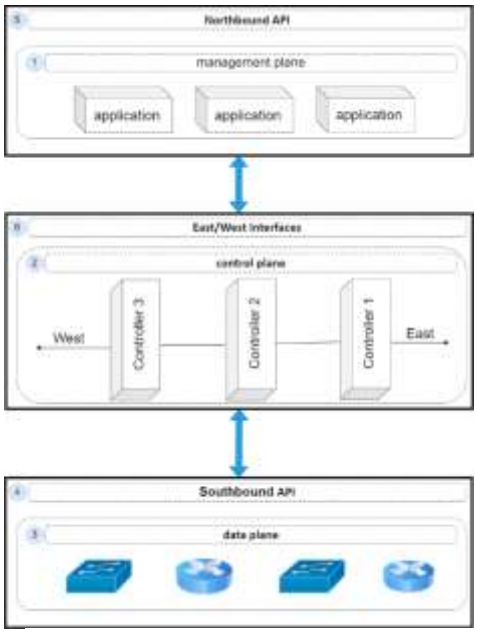

Figure 2 SDN's architectur

OpenFlow

It is considered the most important and widely used protocol between the data plane and the SDN Controller, as this protocol facilitates the work of devices in the data plane. The protocol is constantly being developed and now includes new features that meet the challenges posed by SDN technology. The OpenFlow protocol provides a physical communication channel, such as a TCP connection between controllers and switches [17].

SDN for IoT

Researchers have been looking into alternative methods, like SDN, to boost the bandwidth and flexibility of the IoT because of its scalability and heterogeneity challenges. The decoupling of the data and control planes in networking devices is the primary feature of SDN. Traditional networks use routers to implement sophisticated algorithms. While switches are in charge of data forwarding in SDN, the SDN controller controls the decision-making process. Instead of using more advanced routers, simpler networking gear can be used because decision algorithms do not execute on network devices. As a result, two of the most alluring SDN features for network operators are the central management and simplicity of network components. We can benefit from a significant

decrease in their costs because there are many network devices. Unlike previous networks, each device would manage all upgrades [18].

Methodology

This research aims to combine SDN and IoT technology to improve the performance of IoT devices, develop their capabilities, and enhance the security mechanism of IoT devices based on SDN technology. Peripheral devices and sensors were connected to the Node MCU, the famous ESP controller, and the OVS switch that supports the OpenFlow protocol and the Ryu SDN Controller.

IoT-SDN Test Architecture and Setup

We implement a DDOS attack on IoT devices and then block it using the Ryu SDN Controller. A firewall application was used to prevent this attack. The illustrative diagram is shown in Figure 3.

1. In the SDN networks, the network's backbone is the Switch which must support the OpenFlow protocol. Because these devices are expensive and not widely available, an OVS was installed as a virtual and open-source switch on a Raspberry Pi B4 device. The Raspberry Pi contains one Ethernet port with 4 USB ports in its original condition. To get more Ethernet ports, a USB to Ethernet adapter has been used to get a switch that supports OpenFlow protocol and contains 5 Ethernet ports.
2. To connect the rest of the devices that do not have Ethernet ports or contain Wi-Fi communication technologies, the Access Point device was used to bridge the peripheral devices and the OVS Switch.
3. IoT platform: tools that can connect things and let the Wi-Fi protocol transfer data. For this purpose, we used NodeMCU, an open-source platform based on ESP8266.
4. A Linux Ubuntu operating system was used with RYU as the SDN controller. It is the most reliable and secure operating system, as it is the primary operating system for computers and servers, it is included in most modern applications, such as IoTs applications, and it manages most network devices.

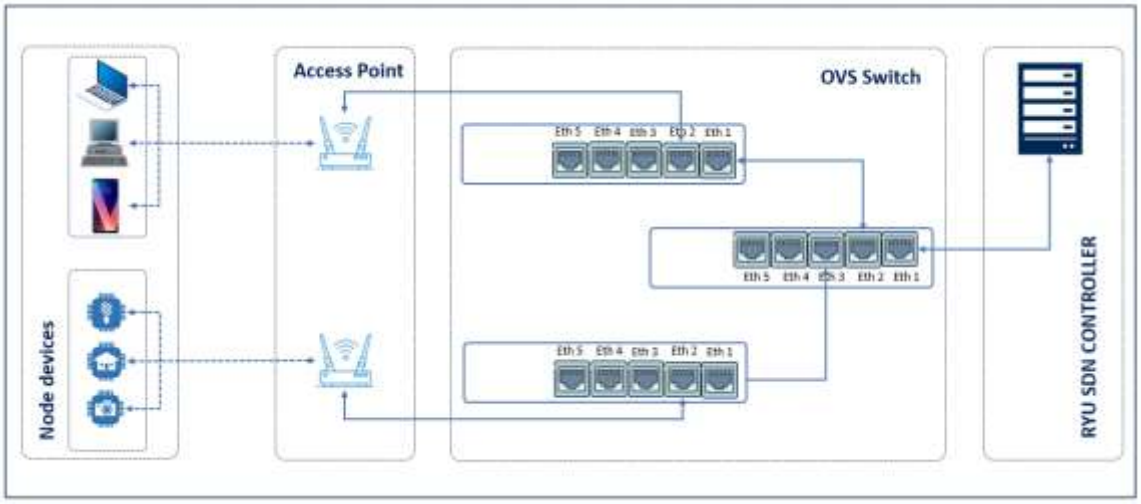

Figure 3 Physical Layout of the System Environment.

5. According to our review of previous works, the RYU SDN controller is better than the rest of the types of SDN Controllers in terms of use in many aspects, such as (ease of programming because it is based on the Python language and it is light and easy and does not require server resources).
6. A low-strength DDOS attack is performed for testing on Node MCU devices using the DDOS Ripper tool.

The attack is carried out on IoT devices represented by Node MCU using the DDoS-Ripper tool. Figure 4 shows the effect of the attack on the processing unit in IoT devices.

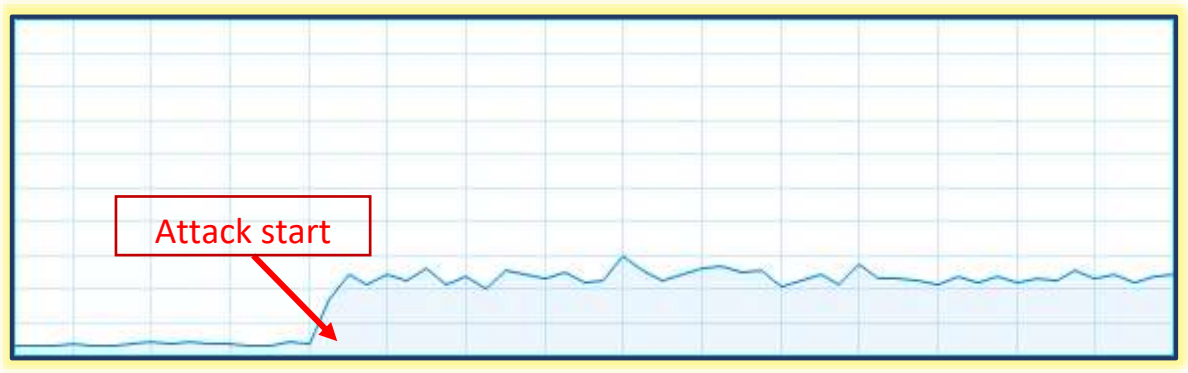

Figure 4 Utilization Diagram of CPU Performance Before and After the Attack.

In order to rid the IoT devices of the effect of the attack, the firewall is implemented on the network, and the RYU Controller detects and reads the information of the SDN Switch, as shown in Figure 5.

Figure 5 Firewall Application When Executing.

Through the rules of allowing and preventing in the (firewall) application, the IP addresses of trusted devices are allowed, and the addresses of untrusted devices are blocked.

Where the permission is given to allow the devices connected to the network proposed by us, and at the same time, the SDN Controller prevents and blocks the attacking device from affecting the IoT devices, as shown in Figure 6

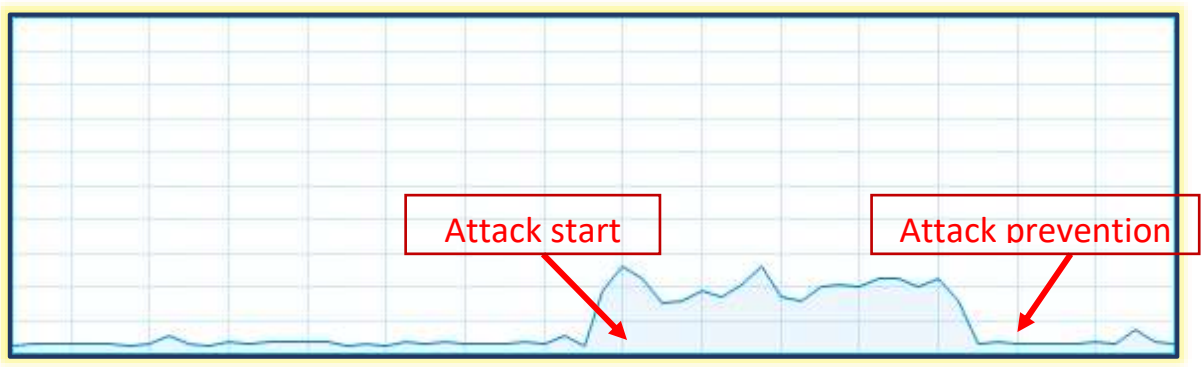

Figure 6 Utilization Diagram of CPU Performance After Implementing an SDN Firewall Application.

Conclusion

Recently, there has been interesting in IoT technologies, which may develop to include all aspects of our daily lives. For this purpose, this technology requires effective ways to manage data forwarding and security in these different devices by design and structure, and to regulate the passage of the huge amount of data produced by these devices. In addition, these devices contain few resources. They cannot implement complex security algorithms. They need effective methods to protect these devices from cyber attacks and ensure that the data reaches its destination, which is sensitive and important.

In this paper, the two techniques mentioned are combined. A proposal for the IoT devices based on SDN technology was implemented using Ryu SDN Controller and OVS as Switch (Installed on Raspberry Pi) with nodes (IoT device, smartphone, laptops, etc.)

In this work, a DDOS attack is carried out on the IoT devices connected to the network. In this attack, the devices are destroyed, rendered inoperable, and disabled. Then the firewall application is implemented by the Ryu SDN Controller on the network, where the attack is prevented, and its impact on these devices is stopped. Thus The devices are back to functioning well and without any problems.

Researchers in the field of IoT and SDN benefits from the work presented. According to the tests above, the protection of IoT devices using SDN technology is carried out easily, regularly, without any complexity, and at lower costs. The RYU SDN controller may also be regarded as one of the most potent security controllers

References

1. Y. Abbassi and H. Benlahmer, "BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain," *International Journal of Electrical and Computer Engineering Systems*, vol. 13, no. 2, 2022, doi: 10.32985/IJECES.13.2.8.
2. S. Jamal Rashid, A. Maamoon Alkababji, and A. Mohammed Khidhir, "Communication and Network Technologies of IoT in Smart Building: A Survey," *NTU JOURNAL OF ENGINEERING AND TECHNOLOGY NTU Journal of Engineering and Technology E*, vol. 1, no. 1, pp. 1–18, 2021.
3. Y. bin Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-generation internet of things (IoT): Opportunities, challenges, and solutions," *Sensors (Switzerland)*, vol. 21, no. 4. 2021. doi: 10.3390/s21041174.
4. K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, "SDN-Enabled Secure IoT Architecture," *IEEE Internet Things J*, vol. 8, no. 8, pp. 6549–6564, Apr. 2021, doi: 10.1109/JIOT.2020.3043740.
5. M. Nobakht, V. Sivaraman, and R. Boreli, "A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Aug. 2016, pp. 147–156. doi: 10.1109/ARES.2016.64.
6. J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp.

155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

7. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput Secur*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101629.
8. M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, Dec. 2016, pp. 147–156. doi: 10.1109/ARES.2016.64.
9. F. al Shuhaimi, M. Jose, and A. V. Singh, "Software defined network as solution to overcome security challenges in IoT," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Sep. 2016, pp. 491–496. doi: 10.1109/ICRITO.2016.7785005.
10. P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow Based Security for IoT Devices Using an SDN Gateway," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2016, pp. 157–163. doi: 10.1109/FiCloud.2016.30.
11. [S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2017, pp. 1–6. doi: 10.1109/ATNAC.2017.8215418.
12. M. Ozcelik, N. Chalabianloo, and G. Gur, "Software-Defined Edge Defense Against IoT-Based DDoS," in *2017 IEEE International Conference on Computer and Information Technology (CIT)*, Aug. 2017, pp. 308–313. doi: 10.1109/CIT.2017.61.
13. P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017, doi: 10.1109/MCOM.2017.1700041.
14. N. Sambandam, M. Hussein, N. Siddiqi, and C.-H. Lung, "Network Security for IoT Using SDN: Timely DDoS Detection," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, Dec. 2018, pp. 1–2. doi: 10.1109/DESEC.2018.8625119.
15. B. Pande, G. Bhagat, S. Priya, and H. Agrawal, "Detection and Mitigation of DDoS in SDN," in *2018 Eleventh International Conference on Contemporary Computing (IC3)*, Aug. 2018, pp. 1–3. doi: 10.1109/IC3.2018.8530551.
16. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving internet of things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, 2020, doi: 10.3390/computers9010008.
17. J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 159. 2020. doi: 10.1016/j.jnca.2020.102595.
18. K. Kalkan and S. Zeadally, "Securing Internet of Things with Software Defined Networking," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 186–192, Sep. 2018, doi: 10.1109/MCOM.2017.1700714.