Internet of Things security concerns using SDN: An overview of theory and research

Thair A. Salih[1*], Abdulrasul A. Samad[2]

Abstract

The International Telecommunication Union (ITU) defines the Internet of Things (IoT) as a collection of physical objects that may be integrated with and controlled by wireless communication networks. The IoT) is currently a popular technology due to its numerous applications. It consists of a large number of disparate devices that are linked together via the Internet, and it is difficult to regulate and protect these devices. SDN, short for Software Defined Network, is a new networking paradigm that simplifies network management and encourages network growth while also making it easier to create and introduce new abstractions in networking. One day, IoT will permeate every aspect of our life and be available everywhere, so security is more essential than ever. IoT devices must be able to react dynamically to various threats, requiring a new approach to security and protection. To achieve this, SDN will be a vital component in enabling IoT devices to be intelligent and secure.

This study aims to emphasize the literature focusing on the security issue in IoT, which gives a brief introduction to SDN technology and provides a taxonomy and survey of the current state of IoT security research based on SDN technology.

Key Words: Internet of Things (IoT), Software-Defined-Network (SDN), Security, OpenFlow, OpenVswitche (OVS), Mininet

DOI Number: 10.14704/nq.2022.20.8.NQ44785 **NeuroQuantology 2022; 20(8): 7606-7615**

1 Introduction

1.1 Internet of Things (IoT)

International Telecommunication Union defines the Internet of things (IoT) as a set of physical things that can be integrated with wireless communication networks and controlled by them.[1]IoT applications and services are intelligent networks, vehicles, sensors, smart cities, and smart homes to control agricultural technologies, factories, and others [2].

All devices are expected to be connected to the Internet by 2025, which will increase the number of connected devices. Cisco predicts that by 2030, there will be 500 billion IoT devices linked. In addition, Telefonica predicts that 90% of automobiles will be connected to the IoT by 2030 and that each person will have an average of 15 connected gadgets by then [3], [4]. morphology of the formed fibers. Many innovative

IoT refers to a variety of services that make our daily lives easier:

- Smart homes, Consumer Services, and intelligent objects
- Smart grids and smart meters for energy
- Smartphones and tablets
- Internet-controlled cars and self-driving cars
- Wearable technology includes watches, smart clothes, dogs' implanted "RFID": collars or other smart collars for tracking their health and fitness, as well as human implanted technology ("pacemakers")
- Data recording, environmental monitoring (earth sensing, water quality, air pollution monitoring, fire detection), weather measurement, healthcare monitoring, and industrial monitoring. [5]

Corresponding author: Thair A. Salih
Address: 1* Computer Technology Engineering Dep. Technical Engineering Collage of Mosul, Northern Technical University, Mosul, Iraq.
1*E-mail: thairali59@ntu.edu.iq
Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Concerns about these issues have increased after the development of IoT technology because users or network resources are likely to be exposed to many attacks through the use of IoT in simple home sensors such as cars, medical devices, or even nuclear reactors, which may pose a real danger to humans [3]

IoT deployment has been hampered by several issues, including processing capacity restrictions, storage volume constraints, low battery life, and radio range constraints. Every device has an IP address and can be accessed via the web, so security is an increasingly important consideration in IoT, as hackers and other intruders increasingly target IP addresses. [6]

An IoT device's security is critical. Many IoT devices collect personal information that must be protected. IoT's sensitive data could be an open invitation to attackers who could use them in various ways, including stealing and selling them. Because of this, preserving privacy in the IoT isn't as simple as it sounds for these reasons:

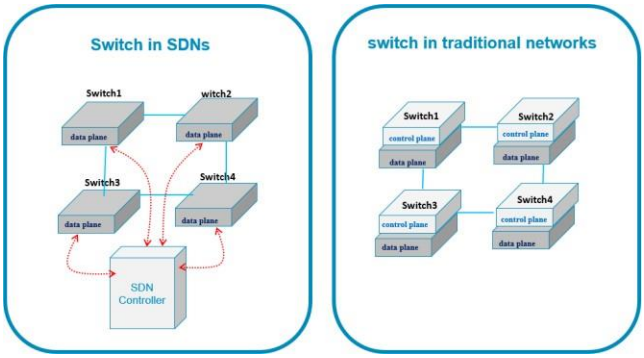
The first: in IoT devices, the CPU is severely constrained and unable to execute complicated commands. Second, because the battery powers most IoT devices, the security algorithm's power consumption must be extremely low. Third, the cost of implementing the security algorithm should be minimal so that as many devices as feasible can benefit from the protection provided by the algorithm. So, security algorithms such as ("3DES, RSA, Blowfish, AES, and ete1…") are not suited for IoT devices since they do not meet the requirements of IoT devices.[7]

1.2 Software Defined Networking

Software Defined Networking (SDN) is a technology that has emerged in recent years to expand the work of large organizations and provide advantages that may be difficult to obtain in traditional networks, which provides the ability to expand and update network resources according to the appropriate needs, facilitates keeping pace with the continuous development in the network structure, and reduces lots of expenses and costs.[8]

In traditional networks, every device (switch or router) contains two layers: the control plane and the data plane. In SDN technology, the control plane is separated from the network devices and is limited to the data plane. A controller is added to the network, who is responsible for the role of the control level for all devices in the network, as shown in (figure 1).[8]

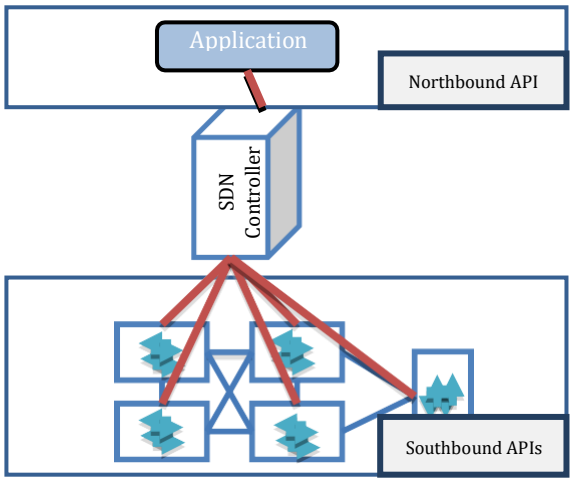
SDN provides various chances to safeguard the network more effectively and flexibly. In SDN architectures, network devices don't decide which path to take. Instead, network devices connect with a specific node known as the SDN controller, which allows them with the necessary forwarding decisions. The network devices can communicate with the Controller by employing several different protocols, and the most important protocol used in this communication process is the OpenFlow protocol.



(Figure 1: The difference between a traditional network and an SDN network)

The Controller is the network's brain in SDN networks since it is connected northbound and southbound on opposite sides, as shown in Figure 2.

1- Northbound API: Consists of one application or a number of network applications that communicate, interact and integrate with the Controller and are responsible for controlling the Southbound and full control of the network.
2- Control plane: This is an important part of this architecture. It allows the network (based on policies) to Manage all forwarding devices.
3- Southbound APIs: This section refers to network equipment such as switches and routers responsible for directing data to different paths.[9]



(Figure 2: SDN Network Parts network)

The southbound interface offers communication between controllers and network devices (switches and routers), while the northbound interface connects the SDN Controller to the network management plane applications.[10]

1.3 OpenFlow

OpenFlow is a network flow protocol that is the backbone of SDN networks. OpenFlow provides a unified method for managing traffic and describes how the control plan communicates with the network devices.[8]

The Open Networking Foundation (ONF) describes it as the initially shared communication interface between the control and infrastructure layers of an SDN architecture. Switches and routers, among other physical and virtual network devices, are given direct access to and control over the forwarding plane thanks to OpenFlow.[11]

This protocol often involves communication between the SDN controller and network devices. In addition, SDN technology provides a rapid response to security risks and granular traffic filtering, With the introduction of dynamic security measures.[12]

OpenFlow Switches contains three parts:

A Flow Table: Responsible for routing the switch around the flow process, informing the switch how the way to process the flow.

1. Secure channel: It allows packets and commands to be transferred between the switch and Controller via a remote-control procedure (referred to as the Controller).
2. The OpenFlow Protocol enables a controller and switches to communicate openly and uniformly. The OpenFlow Protocol specifies a common interface for externally defining entries in the Flow Table.[13]

1.4 SDN Controllers

The data plane is made up of networking elements such as routers, switches, and other devices. Based on the Controller's choice, the data is forwarded. The server or cluster of servers (Distributed SDN) that acts as the Controller makes up the control plane. The Controller is often referred to as the "network brain" because it contains all of the system's logic functions. When it comes to establishing flow entries in routing devices and keeping track of packet information (flow statistics), the Controller is in charge. It is possible to compare the flow entries in a table (referred to as the "flow table") to the routing table in traditional networking architecture.[14]

2 Security in IoT

The issue of security and data protection in the IoT is crucial. Most of the data collected through the Internet is considered personal data and needs protection. Attackers may exploit this data for destructive purposes because ensuring data privacy and security on the IoT is not easy for many reasons, the most important of which is that the central processing unit in the IoT is limited and cannot perform complex operations. In addition, energy expenditure must be taken into account because most IoT devices run on battery or low power sources, and also that most security and protection algorithms are unsuitable to work with the Internet or do not meet the IoT Standards.[7]

2.1 SDN assessment criteria in IoT

To achieve high efficiency and flexibility and obtain more accurate results, some basic criteria must be implemented to evaluate the application of the SDN system in IoT networks such that.[15]

- It connects securely with dozens, even hundreds, of heterogeneous IoT devices.
- To obtain awareness and operate in real-time, low latency security monitoring is required.
- Flexible architecture to expand the scope of work in the future.
- The possibility of developing or updating programming to impose policies and custom applications.

2.2 Bringing SDN to IoT Networks

Service providers and researchers have been looking into alternative methods like SDN to boost the IoT's flexibility and bandwidth because of its scalability and heterogeneity concerns. Data and control planes are separated in SDN, making it easier to manage networks. All of the high-level algorithms in traditional networks are applied by routers. The Controller handles the decision-making process on the SDN, while the switches handle the data transfer. Unlike more advanced routers, simpler networking hardware can be used because decision algorithms do not execute on network devices. One of the most appealing advantages of SDN for network operators is the central management and simplicity of network devices.

In SDN, all updates are controlled centrally, as opposed to previous networks, where each network device was responsible for its own updates. But because the (IoT) nature is so dynamic, the traditional networks can't meet its needs. As an alternative, SDN moves away from static networks and toward networks that can be programmed and changed.

SDN uses smart routing to prevent network bottlenecks.

This is possible because the SDN controller may divert traffic appropriately and has a broad network view. Integration of SDN makes it easier to analyze information and make decisions in IoT. Also, SDN provides various debugging tools that may be used in an IoT context to enhance the network's capacity to gather data for debugging.
Integration of SDN and IoT has also been seen to have benefits in a number of fields, like ("smart homes", "smart grid settings", and "smart transportation"). Integrating SDN and IoT is also a good way to make IoT safer because the properties of the SDN make setting up security methods simple.[16]

3 previous works

Since the emergence of IoT technology, many concerns have been raised about it, such as security and privacy threats and other concerns about how to organize or manage this vast number of terminal devices, protect them from various attacks and protect them from hackers. Recent research to resolve this issue is comprehensively reviewed in our literature study.
Younes ABBASSI and Habib Benlahmer [17], describe Blockchain SDN-IoT (BCSDN-IoT) architecture, and they presented BCSDN-IoT.
Muhammad A. Abid and others[18] comprehensively discussed the principles of traditional IoT, its shortcomings, and how they might be addressed through the use of SDN-based intelligent IoT networks.
Mimi M Cherian and Satishkumar L. Varma[19] they undertook a comprehensive analysis of security risks in IoT and upcoming countermeasures, and as a result, came to the conclusion that important security challenges in IoT networks include denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, and (Man in the Middle) assaults. Utilizing a conventional network as a defence mechanism and trying to stop this kind of assault will not provide the desired results. They compared the accuracy of detection provided by their BBSC algorithm to that of two DDOS methods that were more similar; as a consequence, the accuracy of detection provided by the BBSC security algorithm has been improved.

Ali Haider Shamsan and Arman Rasoul Faridi [20] suggested integrating software-defined networking and virtualization of network functions with the IoT to overcome the inadequacy of these networks built with limited capabilities. This paper presents a unique architecture to reduce IoT resource constraints by programming as it is combined with SDN and NFV. The results of the experiment revealed that the performance of the SDNFVIoT architecture was

Kamaran H. Manguri and Saman M. Omer [21], In this research, highlight numerous works that offer SDN-based solutions for the Internet of Things settings. In this analysis, optimizing network performance by using SDN has shown interesting solutions for modern IoT. The findings of this investigation indicate that the solutions are not completely incorporated into the SDN environments used by IoT. In addition, the majority of models are evaluated and verified based on simulation models rather than being put into action in an actual Internet of Things environment. In conclusion, despite the many efforts made to design frameworks that are based on SDN, academics are at a considerable disadvantage when it comes to establishing an all-encompassing architecture and framework.

Jazaeri, S. S. and others[22] explore the creation of a new cooperative framework that makes advantage of the synergies between software-defined networking and edge computing in IoT networks. In this study, an optimised platform for the Internet of Things (SDN-EC-IoT) is proposed. This platform makes use of network resource virtualization in order to provide resources for heterogeneous Internet of Things devices. Additionally, it enables the most efficient infrastructure configuration and maintenance possible.

Ali H. S.; Arman R. F. [23] offered an introduction to the IoT, SDN, and architectural models, as well as a study of the available IoT architectures based on SDN and architectural specifics of the suggested SDN-based IoT models.
Md. J. et al. [24], a Black (SDN)is presented as a highly secure SDN that improves network performance, security, and payload efficiency of distributed networks with NFV implementation for smart cities.
Bedhief Intidhar et al. [25] In this study on extremely dynamic Internet of Things networks, you will need to provide a self-adaptive management architecture of SDN controllers. In a situation that more closely resembles real life, the topology of the network is constantly changing. ODL and ONOS, which are currently the two most popular distributed SDN Controllers, both had their performance evaluated here.
Abbas Yazdinejad et al.[26], in their paper proposed an IoT network design based on two new emerging technologies: SDN and Blockchain, using a cluster structure with a new routing protocol.
Francesco Restuccia et al. [27] organized and summarised the pertinent state-of-the-art research in this report. They presented their unique take on IoT security based on a unique combination of security-by-design,
polymorphism, and software-defined networking

concepts.

Mustafa Abdulkadhim et al., in their paper [28], simulated the environment and how it interacts with the various sensors. The algorithm is modelled and coded for smart, efficient power sharing that is handled and monitored centrally with the help of an SDN controller.

Van Farris et al. [29] provided a broad overview of major security threats to IoT systems and traditional security countermeasures. Then a comprehensive analysis of security features introduced by Network Function Virtualization and Software Defined Networking describes the various strategies capable of monitoring, protecting, and responding to IoT security threats. The security characteristics given by SDN and NFV-based security mechanisms are thoroughly investigated in this study, which analyses the appropriate state-of-the-art solutions for IoT systems.

Suman Sankar Bhunia et al. in [30] introduced Soft Things, a safe internet of things architecture that is built on software defined networking, with the goal of detecting anomalous behaviours and assaults as early as feasible and mitigating them as required. Machine learning is used by the SDN controller in order to monitor and learn from the behaviour of IoT devices over the course of time. The mininet emulator served as the platform for the conduct of experiments. Initial findings indicate that this framework is capable of identifying risks posed by IoT devices with an accuracy of about 98 percent.

Abdullah Al Hayajneh et al. in [31] It is important to offer a system model for properly combining SDN with IoT networks as well as a solution for mitigating (man-in-the-middle attacks) against IoT devices that can only utilise HTTP. This kind of attack is tough to protect against since HTTP is such a crucial protocol. The Raspberry Pi, the Kodi Media Center, and the Open flow Protocol were used in the successful execution of the suggested system design. This solution that is being suggested makes use of machine learning on the SDN controller in order to monitor and analyse the normal behaviour that is now being seen on IoT devices in order to identify any potentially malicious actions that may occur in the future. According to the system installation and assessments, the method that has been presented has a higher level of resistance against cyberattacks.

ANICHUR RAHMAN et al. in [32], Present a revolutionary design for a smart building system, which includes a control system and autonomous techniques. An effective (cluster head selection algorithm. The development of an improved mix of IoT forwarding devices with Software-Defined Networking (SDN) technologies is progressing. Furthermore, the proposed "Dist Block Building" architecture is used to manage data transmission from one surface to another safely and securely. Additionally, Blockchain technology is used for data transmission within the smart building. Finally, the performance of secured networks based on IoT-SDN is assessed.

Ahmed Dawoud et al. in [33] suggest improving the security of SDN-based IoT architectures. This study offers a detection method based on recent breakthroughs in machine learning. The Restricted Boltzmann Machine is used in this technique to detect anomalies. The simulation results reveal that the accuracy rate is over 94 per cent. They concentrated on the installation and evaluation of theirs proposed detection system in this study. They developed a broad paradigm for IoT and SDN integration.

Farris et al. [34] present a revolutionary architecture that aims to take advantage of SDN/NFV-based security capabilities and provide new efficient integrations with existing IoT security approaches. Two case studies are used to validate the suggested framework's potential benefits. Finally, a feasibility study is provided, which considers potential interactions with open-source SDN/NFV initiatives and relevant standardization efforts.

Md. Jahidul Islam al et. [35] proposed an efficient and secure SDN-IoT architecture with NFV utilization. They created an "energy-efficient Cluster Head Selection (CHS) algorithm" to make use of theirs proposed architecture, as well as a highly protected SDN that gives improved network efficiency, protection, and privacy results. In comparison to the old network in the proposed architecture, the new network provides better protection for each network layer.

Bivash Kanti Mukherjee et al. in [36] suggest an SDN-based distributed IoT network with NFV implementation for smart cities to increase load balancing, scalability, availability, integrity, and security of the entire network.

Yaser Jararweh et al. in[37] proposed a software-defined based framework for the IoT (SDIoT). They talked about existing SDN, SDStore, and SDSec solutions, as well as a suggested SDIoT architectural model and how they used SDN, SDStore, and SDSec ideas to develop it.

They explained its primary components and demonstrated how they combine to give a comprehensive framework for controlling the IoT network.

Ammar Muthanna et al. in[38] suggested an Internet of IoT with distributed fog computing deployed and managed via a software-defined network. The traffic model was used to construct the data offloading algorithm for regulating and managing data offloading over the proposed system.

In [39], Kubra Kalkan and Sherali Zeadally Present a comprehensive examination of the ways in which SDN technology might offer security for the IoT

environment, as well as a study of many newly suggested SDN designs
and an evaluation of the pros and downsides of each of these architectures. In conclusion, they provide a categorization with the intention of assisting network security researchers and analysts in picking the most suitable security mechanism for their needs, depending on the criteria for that level of security. In addition to this, they propose a Rol-Sec, which is an acronym for role-based security controller architecture, for the SDN-IoT environment.

Kotaro Kataoka, et al. in [40], combining blockchains and Software-Defined Networking. This article offers a Trust List that depicts trust distribution across IoT-related stakeholders and provides autonomous enforcement of IoT traffic management at the edge networks (SDN).

Mehdi Nobakht et al. [41] present IoT-IDM intrusion detection and mitigation system that uses the SDN architecture to provide network-level protection for IoT. IoT-IDM keeps track of the network activities of intended smart devices in the home and looks for unusual or malicious activity. It is capable of prohibiting the attacker from accessing the victim's device on the fly once an incursion has been identified.

Mert Ozcelik et al. [42] use Mirai as a case study to present an edge-oriented detection and mitigation system against DDoS in IoT using SDN and Fog approaches. When they get close to the edge, they can reduce distributed denial of service threats from the IoT by employing software-defined networking and fog computing.

Sharifah H. S. [43] presents a number of IoT-based SDN architectures for enhancing network security.

Anchor Rahman et al. [44] proposed the Block-SDoTCloud architecture to improve security in the cloud storage network. Two major technologies, SDN and Blockchain, were used to provide the cloud storage environment with the necessary capabilities. Mininet-WiFi is utilized as an emulation platform and the OpenFlow protocol. The Wireshark platform is also used to analyze packets in an IoT-SDN network. To boost security in the cloud storage environment, this study presented the Block-SDoT Cloud architecture.

Nagarathna Ravi et al. [45] presented a new technique called learning-driven detection mitigation (LEDEM), which uses a semi-supervised machine-learning algorithm to detect DDoS and neutralize it. They put LEDEM through its paces in the testbed, simulating topology and comparing the results to state-of-the-art systems. In detecting DDoS attacks, they boosted their accuracy rate to 96.28 per cent.

Yaser Jararweh et al. [46], a full software-defined framework model was presented. By combining the software-defined network, software-defined storage, and software-defined security into a single software-based control model, it is possible to simplify the IoT management process and provide an essential solution for the challenges presented by traditional IoT architecture in terms of the ability to forward, store, and secure the data that is produced by IoT objects. They started out by emphasizing how software-defined systems overcome the limits of conventional system design by offering a method for system control that is centralized, programmable, flexible, user-friendly, and scalable. Additionally, they emphasized how simple it is to use. After then, other variations of SDSys, including SDN, SDStore, and SDSec, which are generally regarded as the most well-known SDSys, were shown and discussed.

Pradip Kumar Sharma et al. [47] combined two new technologies: software-defined networking (SDN) and blockchain technology. They found that DistBlockNet can detect assaults on the IoT network in real-time with low-performance overheads while meeting the architectural criteria required for the future IoT network.

Ahrish Khan Tayyaba et al. [48] study the existing IoT solutions leveraging SDN control and data plane programmability. Architectural details and contributions to a framework of SDN-based IoT are described in this work, followed by a summary of architectural details and their evolution, and finally, a report on some of the unsolved challenges in this merger. Finally, in the framework of SDN-based IoT, some forecasts for the world in 2020 are given.

Nikos Bizanis; Fernando A. Kuipers in [49] looked at how "Software Defined Networking, Network Virtualization, and IoT" came together. They look at the state of the art for SDN and NV in IoT. They are the first to describe every possible aspect of IoT implementation for the two technologies.

Narmadha Sambandam et al. in [50] present a study to create a system that could detect DDoS attacks early on using a measure of entropy. The Controller can counteract the attack by detecting it early and terminating the processing of these fraudulent packets, freeing up resources for genuine users. The Raspberry Pis were used as OpenVswitches.

Fatma AL Shuhaimi et al., in [51], discussed and analyzed a combined IoT and SDN paradigm in their article. They proposed an algorithm or model based on Software Defined Networks that can be utilized to prevent various threats in the IoT. The cluster head selection method is proposed, and the cluster head is enabled with SDN software to manage and regulate the domain's various security challenges.

Shaibal Chakrabarty et al. [52] describe Black SDN, an (SDN)(SDN) architecture for secure IoT networking and communications.

Olivier Flauzac, et al. [53] presented a novel SDN-based network design with distributed controllers in this article. Furthermore, they can be employed in Ad-Hoc networks and IoT scenarios.

Bhavika Pande et al. [54] plan to identify all types of DDoS assaults by recording network traffic entering the (SDN)plane and filtering it through multiple modules, allowing them to detect DDoS attacks and take appropriate preventive steps.

Mengmeng Ge et al. [55] offer two proactive protection methods that modify the IoT network architecture with the help of software-defined networking (SDN). They use a graphical security model and several simulation metrics to determine how security and performance change when the recommended remedies are implemented. According to the results, proactive security measures in the SD-IoT effectively increase attack effort while retaining the average shortest path length.

Carlos GONZALEZ, et al. [56], They describe a preliminary investigation in this paper that focuses on gaining a better understanding of how to design a cluster network using SDN. By generating virtual nodes utilizing network virtualization and OpenFlow technologies, a prototype system with over 500 devices managed by SDN can be simulated and resembles a cluster. The results reveal that network devices can only forward packets according to the Controller's specified rules. As a result, they propose employing Opflex within the SDN architecture to control the IP header at the application level to solve this problem. They offer a novel solution for a new form of IoT network in cluster contexts based on SDN.

Carlos Gonzalez et al. [57], In this research, provide a cluster management system that is based on OpenFlow. Within an SDN controller, an SDN cluster head is responsible for managing communication across the system's various clusters. An OpenFlow network has been simulated in real-time using a technology that is currently in the prototype stage of development. Experiments suggest that the solution can govern both physical and virtual networks, as well as topology, traffic, flow tables, and services in a network that is controlled by SDN.

Jie Li, Eitan Altman, and Corinne Touati [58] present a quick, up-to-date overview of the IoT architecture model, SDN, and NFV in this article. They research the features of these new technologies. They provide a general SDN-based IoT architecture with NFV deployment.

Cheng Li, Zhengrui Qin, Ed Novak, et al. [59] look at the potential hazards of Man-in-the-Middle attacks on the OpenFlow control channel in this article. They highlight the serious repercussions of such attacks by first introducing a plausible attack model in an IoT-Fog architecture and then implementing attack demos. They also offer Bloom filters as a lightweight countermeasure. They put together a prototype for this way of tracking stealthy packet alterations. According to the results of their evaluation, theirs Bloom filter monitoring system is efficient and uses few resources.

Rihab Fahd Al-Mutawa; Fathy Albouraey [60] described a distributed Blockchain-based security solution for industry 4.0 applications running in an SDN-IoT enabled environment where the Blockchain can lead to theirs desired system's robustness, privacy, and confidentiality. Furthermore, the SDN-IoT combines several industrial 4.0 services with increased security and flexibility. Furthermore, the authors propose an outstanding mix of technologies such as IoT, SDN, and Blockchain to adequately increase the security and privacy of Industry 4.0 services. Finally, the authors analyze performance and security in the provided architecture in various ways. This article provides the "DistB-SDo Industry" paradigm for Industry 4.0 applications, built on distributed Blockchain technology and the SDN-IoT architecture.

Anchor Rahman et al. [61], Put forth a Blockchain-based SDN-IoT architecture for smart cities that is safe, decentralised, and includes deployment of Network Function Virtualization (NFV). They have suggested a distributed blockchain-based SDN-IoT architecture with NFV execution for smart cities, as well as a unique cluster head selection mechanism that is dependent on the assumption that this is the case. Both of these ideas are geared toward the development of smart cities. This Controller has the potential to enhance the levels of privacy, availability, confidentiality, and integrity that are currently present within a decentralised blockchain network that has a large number of dynamic controllers. These improvements could be made possible by the decentralised nature of the network.

Peter Bull et al. [62], Created a Blockchain-based SDN-IoT architecture for smart cities that is decentralized, secure and involves the installation of Network Function Virtualization (NFV). They have suggested a distributed blockchain-based SDN-IoT architecture with NFV execution for smart cities, as well as a unique cluster head selection mechanism that is dependent on the assumption that this is the case. Both of these ideas are geared toward the development of smart cities. This Controller has the potential to improve the levels of privacy, availability, confidentiality, and integrity that are currently present in a decentralized blockchain network that has a large number of dynamic controllers. These improvements could be made possible by the increased number of dynamic controllers.

4 Discussion

SDN technology is considered one of the emerging technologies in the field of networks, and it is expected

to make a breakthrough in the field of networks because it shortens and facilitates many things and provides solutions to many network problems. IoT devices are usually simple devices with few resources of processors or memories, so it is difficult for them to implement complex encryption algorithms; for this purpose, it was proposed to protect data for this type of device using SDN technology, so a number of researchers put forward their ideas and theories in this field for the purpose of improving Security in IoT devices

5 Conclusion

The process of maintaining data in the IoT network is very complex, and the process can be simplified and shortened by using SDN technology. The researchers presented their different ideas as ways to protect data and design smart and secure IoT networks using SDN.

In this study, we presented a brief idea of a number of previous literatures in this field, in which we show many important aspects of the methods of protecting IoT data using SDN, where we clarified the proposed and used methods to solve such problems, and also clarified the field that the authors took and the results they reached.

We are also working on a new project that provides a solution to this type of problem, and we will present it later.

Resources

[1] Sector, I. T. S. (2012). Recommendation ITU-T Y. 2060: Overview of the Internet of things. *Series Y: Global information infrastructure, internet protocol aspects, and next-generation networks-Frameworks and functional architecture models*.

[2] Lee, W., Nam, K., Roh, H. G., & Kim, S. H. (2016, January). A gateway based fog computing architecture for wireless sensors and actuator networks. In *2016 18th International Conference on Advanced Communication Technology (ICACT)* (pp. 210-213). IEEE.

[3] Zikria, Y. B., Ali, R., Afzal, M. K., & Kim, S. W. (2021). Next-generation internet of things (iot): Opportunities, challenges, and solutions. Sensors, 21(4), 1174.

[4] At-a-Glance Connected Means Informed. (2016). www.cisco.com/go/iot.

[5] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.

[6] Al-Sarawi, S., Anbar, M., Abdullah, R., & Al Hawari, A. B. (2020, July). Internet of things market analysis forecasts, 2020–2030. In 2020 Fourth World Conference on smart trends in systems, security and sustainability (WorldS4) (pp. 449-453). IEEE.

[7] Hameed, A., & Alomary, A. (2019, September). Security issues in IoT: a survey. In 2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT) (pp. 1-5). IEEE.

[8] Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. Security and communication networks, 9(18), 5803-5833.

[9] Tioutiou, A., & Diouri, O. (2019, November). Improving IoT Security with Software Defined Networking (SDN). In International Conference on Advanced Communication Systems and Information Security (pp. 233-238). Springer, Cham.

[10] Paliwal, M., Shrimankar, D., & Tembhurne, O. (2018). Controllers in SDN: A review report. IEEE access, 6, 36256-36270.

[11] Li, W., Meng, W., & Kwok, L. F. (2016). A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. Journal of Network and Computer Applications, 68, 126-139.

[12] Flauzac, O., González, C., Hachani, A., & Nolot, F. (2015, March). SDN based architecture for IoT and improvement of the security. In 2015 IEEE 29th international conference on advanced information networking and applications workshops (pp. 688-693). IEEE.

[13] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. ACM SIGCOMM computer communication review, 38(2), 69-74.

[14] Paliwal, M., Shrimankar, D., & Tembhurne, O. (2018). Controllers in SDN: A review report. IEEE access, 6, 36256-36270.

[15] Krishnan, P., Najeem, J. S., & Achuthan, K. (2017, August). SDN framework for securing IoT networks. In International Conference on Ubiquitous Communications and Network Computing (pp. 116-129). Springer, Cham.

[16] Kalkan, K., & Zeadally, S. (2017). Securing internet of things with software defined networking. IEEE Communications Magazine, 56(9), 186-192.

[17] ABBASSI, Y., & Benlahmer, H. (2022). BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain. International journal of electrical and computer engineering systems, 13(2), 155-163.

[18] Abid, M. A., Afaqui, N., Khan, M. A., Akhtar, M. W., Malik, A. W., Munir, A., ... & Shabir, B. (2022). Evolution towards smart and software-defined internet of things. AI, 3(1), 100-123.

[19] Cherian, M. M., & Varma, S. L. (2022). Mitigation of DDOS and MiTM Attacks using Belief Based Secure Correlation Approach in SDN-Based IoT Networks. International Journal of Computer Network & Information Security, 14(1).

[20] Shamsan, A. H., & Faridi, A. R. A Novel SDNFV IoT Architecture Leveraging Softwarization Technology Services to Alleviate IoT Network Resource Restrictions.

[21] Manguri, K. H., & Omer, S. M. (2022). SDN for IoT Environment: A Survey and Research Challenges. In ITM Web of Conferences (Vol. 42, p. 01005). EDP Sciences.

[22] Jazaeri, S. S., Jabbehdari, S., Asghari, P., & Haj Seyyed

Javadi, H. (2021). Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions. Cluster Computing, 24(4), 3187-3228.

[23] Shamsan, A. H., & Faridi, A. R. (2018, December). SDN-assisted IoT architecture: a review. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-7). IEEE.

[24] Islam, M. J., Mahin, M., Roy, S., Debnath, B. C., & Khatun, A. (2019, February). Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-6). IEEE.

[25] Bedhief, I., Kassar, M., Aguili, T., Foschini, L., & Bellavista, P. (2019, June). Self-Adaptive Management of SDN Distributed Controllers for Highly Dynamic IoT Networks. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 2098-2104). IEEE.

[26] Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., & Choo, K. K. R. (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing, 13(4), 625-638.

[27] Restuccia, F., D'Oro, S., & Melodia, T. (2018). Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal, 5(6), 4829-4842.

[28] Abdulkadhim, M., Qusay, N., & Al-Kadhimi, A. M. (2022). Design and simulation of a software defined networking-enabled smart switch, for internet of things-based smart grid. Indonesian Journal of Electrical Engineering and Computer Science, 25(2), 780–787. https://doi.org/10.11591/ijeecs.v25.i2.pp780-787

[29] Farris, I., Taleb, T., Khettab, Y., & Song, J. (2018). A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Communications Surveys & Tutorials, 21(1), 812-837.

[30] Bhunia, S. S., & Gurusamy, M. (2017, November). Dynamic attack detection and mitigation in IoT using SDN. In 2017 27th International telecommunication networks and applications conference (ITNAC) (pp. 1-6). IEEE.

[31] Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). Improving Internet of Things (IoT) security with software-defined networking (SDN). Computers, 9(1), 8.

[32] Rahman, A., Nasir, M. K., Rahman, Z., Mosavi, A., Shahab, S., & Minaei-Bidgoli, B. (2020). Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management. IEEE Access, 8, 140008-140018.

[33] Dawoud, A., Shahristani, S., & Raun, C. (2018). Deep learning and software-defined networks: Towards secure IoT architecture. Internet of Things, 3, 82-89.

[34] Farris, I., Bernabé, J. B., Toumi, N., Garcia-Carrillo, D., Taleb, T., Skarmeta, A., & Sahlin, B. (2017, September). Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 169-174). IEEE.

[35] Islam, M. J., Rahman, A., Kabir, S., Khatun, A., Pritom, A. I., & Zaman, M. (2020). SDoT-NFV: Enhancing a distributed SDN-IoT architecture security with NFV implementation for smart city. Dept. Comput. Sci. Eng., Green Univ. Bangladesh, Dhaka, Bangladesh, Tech. Rep. 2020A3321.

[36] Mukherjee, B. K., Pappu, S. I., Islam, M., & Acharjee, U. K. (2020, February). An SDN based distributed IoT network with NFV implementation for smart cities. In International Conference on Cyber Security and Computer Science (pp. 539-552). Springer, Cham.

[37] Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., & Rindos, A. (2015). SDIoT: a software defined based internet of things framework. Journal of Ambient Intelligence and Humanized Computing, 6(4), 453-461.

[38] Muthanna, A., A. Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.

[39] Kalkan, K., & Zeadally, S. (2017). Securing internet of things with software defined networking. IEEE Communications Magazine, 56(9), 186-192.

[40] Kataoka, K., Gangwar, S., & Podili, P. (2018, February). Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 296-301). IEEE.

[41] Nobakht, M., Sivaraman, V., & Boreli, R. (2016, August). 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) (pp. 147-156). IEEE.

[42] Özçelik, M., Chalabianloo, N., & Gür, G. (2017, August). Software-defined edge defense against IoT-based DDoS. In 2017 IEEE international conference on computer and information technology (CIT) (pp. 308-313). IEEE.

[43] Ariffin, S. H. (2020, December). Securing Internet of Things System using Software Defined Network based Architecture. In 2020 IEEE International RF and Microwave Conference (RFM) (pp. 1-5). IEEE.

[44] Rahman, A., Islam, M. J., Khan, M. S. I., Kabir, S., Pritom, A. I., & Karim, M. R. (2020, December). Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network. In 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.

[45] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet of Things Journal, 7(4), 3559-3570.

[46] Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., & Rindos, A. (2015). SDIoT: a software defined based internet of things framework. Journal of Ambient

Intelligence and Humanized Computing, 6(4), 453-461.

[47] Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. IEEE Communications Magazine, 55(9), 78-85.

[48] Tayyaba, S. K., Shah, M. A., Khan, O. A., & Ahmed, A. W. (2017, July). Software defined network (sdn) based internet of things (iot) a road ahead. In Proceedings of the international conference on future networks and distributed systems (pp. 1-8).

[49] Bizanis, N., & Kuipers, F. A. (2016). SDN and virtualization solutions for the Internet of Things: A survey. IEEE Access, 4, 5591-5606.

[50] Sambandam, N., Hussein, M., Siddiqi, N., & Lung, C. H. (2018, December). Network security for iot using sdn: Timely ddos detection. In 2018 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-2). IEEE.

[51] Al Shuhaimi, F., Jose, M., & Singh, A. V. (2016, September). 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) (pp. 491-496). IEEE.

[52] Chakrabarty, S., Engels, D. W., & Thathapudi, S. (2015, October). Black SDN for the Internet of Things. In 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (pp. 190-198). IEEE.

[53] Flauzac, O., González, C., Hachani, A., & Nolot, F. (2015, March). SDN based architecture for IoT and improvement of the security. In 2015 IEEE 29th international conference on advanced information networking and applications workshops (pp. 688-693). IEEE.

[54] Pande, B., Bhagat, G., Priya, S., & Agrawal, H. (2018, August). Detection and mitigation of DDoS in SDN. In 2018 Eleventh International Conference on Contemporary Computing (IC3) (pp. 1-3). IEEE.

[55] Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. Future Generation Computer Systems, 78, 568-582.

[56] Gonzalez, C., Charfadine, S. M., Flauzac, O., & Nolot, F. (2016, July). SDN-based security framework for the IoT in distributed grid. In 2016 international multidisciplinary conference on computer and energy science (SpliTech)(pp. 1-5). IEEE.

[57] Gonzalez, C., Flauzac, O., Nolot, F., & Jara, A. (2016, May). A novel distributed SDN-secured architecture for the IoT. In 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 244-249). IEEE.

[58] Li, J., Altman, E., & Touati, C. (2015). A general SDN-based IoT framework with NVF implementation. ZTE communications, 13(3), 42-45.

[59] Li, C., Qin, Z., Novak, E., & Li, Q. (2017). Securing SDN infrastructure of IoT–fog networks from MitM attacks. IEEE Internet of Things Journal, 4(5), 1156-1164.

[60] Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M., Hasan, M., ... & Nasir, M. K. (2020). Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture. arXiv preprint arXiv:2012.10011.

[61] University of Dhaka. Faculty of Engineering and Technology, & Institute of Electrical and Electronics Engineers. (n.d.). ICIET 2019 : 2nd International Conference on Innovation in Engineering and Technology (ICIET) : 23-24 December, 2019, University of Dhaka, Dhaka, Bangladesh.

[62] Bull, P., Austin, R., Popov, E., Sharma, M., & Watson, R. (2016, August). Flow based security for IoT devices using an SDN gateway. In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) (pp. 157-163). IEEE.