

Comparative Study of Data Transfer in SDN Network Architecture in IoT

Zahra Askarinejadamiri^{a*}, Negar Nourani^b, Nastaran Zanjani^c

^a Department of Computer Engineering, Refah University College, Tehran, Iran; Askarinejad@refah.ac.ir^a, nouraninegar99@yahoo.com^b, Zanjani@refah.ac.ir^c

ABSTRACT

The Internet of Things (IoT) has gained significant attention in recent years, with the proliferation of connected devices and the need for efficient data transfer in IoT networks. Software-Defined Networking (SDN) has emerged as a promising solution to address the challenges of network management and optimization in IoT environments. This paper presents a comparative study of data transfer in SDN network architecture in IoT, focusing on the benefits, challenges, and future perspectives of integrating SDN and IoT. Given the crucial role of security in IoT, this paper seeks to access a secure architecture for computer networks to provide a solution for security challenges. To achieve this, a comparative analysis of two SDN architectures is conducted in this research. We have utilized the Mininet software, which serves as a laboratory for software-defined networks, to implement and simulate these SDN architectures. The results of this study are based on a comparison of the two secure architectures using DITG tables. This comparative study offers valuable insights into the integration of SDN in IoT network architecture and its influence on data transfer.


Keywords—Internet of Things, Software-Defined Networks (SDN), network security, Mininet software

1. Introduction

The Internet of Things embodies a connected set of anyone, anything, anytime, anywhere, any service, and any network. Today's technological world faces a rapidly growing phenomenon—the Internet of Things—where all human life devices are connected to each other. The aim of the Internet of Things is to provide an infrastructure for simplifying secure and reliable exchanges between objects [1]. The Internet of Things is a major trend in next-generation technologies, impacting a wide range of businesses and envisioning it as smart object communication and identifiable device infrastructure with extensive benefits. The current internet connects everyone, but with the Internet of Things, everything connects to each other. IoT generally refers to a wide range of objects and items in our environment, from washing machines and refrigerators to lighting and HVAC systems, connected to the internet and controllable through smartphone apps and tablets. Today, the internet has transformed into a digital community, where nearly everything is interconnected and accessible from anywhere. Managing network equipment in such a space holds significant importance. Traditional networks have numerous vulnerabilities in this regard and will not be efficient for the current environment. Security in data transfer is crucial in the Internet of Things. For instance, in the medical field, while IoT has brought a significant transformation, the high sensitivity of the domain presents challenges. For example, dissemination of incorrect medical information could lead to loss of life, followed by tarnished medical institution credibility, or constant patient monitoring requires powerful data centers and suitable infrastructure.

The term security in IoT encompasses a wide range of concepts and security requirements such as privacy, authentication, integrity, authorization, and access control, which are provided through various security mechanisms. The security situation in IoT is complex and sensitive. With the expansion of IoT in contemporary societies, security threats are advancing, and smart devices are continuously attacked [2]. An attacker could manipulate physical equipment, such as medical devices, alter encryption code, or destroy devices. Given this extensive network of connected devices and the exchange of information between them, security concerns and individuals' inability to control privacy become evident. Alongside the widespread use of IoT in various centers to mitigate security challenges and privacy concerns, the intrusion of hackers into computer networks and artificial intelligence requires the efforts and actions of legislators, policymakers, and system designers to identify solutions and countermeasures against threats and attacks. Therefore, this study seeks a secure architecture for existing computer networks in the IoT field.

However, the diverse and dynamic requirements of these IoT systems present significant challenges in ensuring the received quality of data. One approach that holds promise for addressing these challenges is Software-Defined Networking (SDN). SDN allows for dynamic control and management of network resources, enabling differentiated quality levels for different IoT tasks in heterogeneous wireless networking scenarios. However, the open interfaces in SDN also introduce new security risks, which can potentially disrupt the functioning of SDN-based IoT systems. In this article, we will explore the concept of SDN-based IoT security and in this regard, Software-Defined Networking (SDN) architectures, a

 <http://dx.doi.org/10.22133/ijwr.2024.421267.1186>

Citation Z. Askarinejadamiri, N. Nourani, N. Zanjani, "Comparative Study of Data Transfer in SDN Network Architecture in IoT," *International Journal of Web Research*, vol.6, no.1, pp.95- 104, 2023, doi: <http://dx.doi.org/10.22133/ijwr.2024.421267.1186>.

*Corresponding Author

Article History: Received: 18 May 2023; Revised: 8 June 2023; Accepted: 13 July 2023.

Copyright © 2022 University of Science and Culture. Published by University of Science and Culture. This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International license (<https://creativecommons.org/licenses/by-nc/4.0/>). Noncommercial uses of the work are permitted, provided the original work is properly cited.

part of secure network architectures, are examined in this research.

SDN is a new generation of networking that has simplified network management operations significantly by introducing a series of changes to network architecture. In an SDN network, a network administrator can manage the network through software-based coding. In a software-defined network, adding, removing, or changing network functionality and behavior won't require hardware modifications. Instead, the network administrator can achieve this through brief adjustments in software or source code [3]. Traditional IP networks (legacy networks) had extensive applications, but their weaknesses lay in high complexity and management difficulties. Managing IP networks is challenging from two perspectives: one is network configuration according to predefined policies, and the other is reconfiguration in response to failures, traffic loads, and changes. Additionally, traditional networks possess vertical integration, meaning that data and control levels are integrated and not separated.

SDN, or Software-Defined Networking, represents a new pattern or architecture that reduces network management complexity and centralizes network control by breaking this vertical integration and physically separating network control from router and switch levels. This way, the control of multiple network devices is achieved through software in a centralized point. In fact, SDN, with its introduced changes to network architecture, has provided intelligent control in software-defined networks in a holistic manner [4]. Network administrators can, within a short time, manage, secure, and optimize their organization's network resources through SDN applications. The most crucial feature of SDN, distinguishing it from legacy networks, is its flexibility, evident in SDN networks. The key to this success lies in separation.

In the modern world of information technology, the concept of the Internet of Things holds great significance and characteristics. This technology has numerous advantages, such as cost reduction, time savings, and object intelligence. It is also applicable in various fields, such as medicine and agriculture. However, its challenges cannot be overlooked. Among the foremost challenges of this technology are security and the issue of data privacy. In the Internet of Things, every connected device can potentially serve as a gateway to the IoT infrastructure or personal data. Therefore, before designing security architecture in IoT, a framework must be provided to identify all angles and factors related to its security. Hence, the identification of all security-related factors in IoT can prevent threats and attacks, ensuring security in data encryption on devices and network transmission routes, data collected by sensors, data stored in databases, and service provision security.

The rapid growth of Internet of Things (IoT) devices has led to an increasing demand for efficient data transfer in Software-Defined Networking (SDN) architectures. This study aims to compare and analyze different data transfer methods within SDN network architecture in the context of IoT applications. By examining the security aspects of various data transfer approaches, this research seeks to identify the most suitable method for handling IoT data in SDN environments. The findings of this comparative study will contribute to the optimization of data transfer mechanisms in

SDN-based IoT networks, leading to improved network efficiency and reliability.

This focused introduction sets the stage for the comparative study and highlights its significance in addressing the challenges of data transfer in SDN network architecture within the context of IoT. The objective of this comparative study is to delve deeper into the realm of securing data transfer within SDN network architecture for IoT applications. By analyzing different security mechanisms and protocols available, we aim to provide insights into the strengths and weaknesses of various approaches [5]. Throughout this study, we will explore the fundamental concepts of SDN network architecture and its integration with IoT. We will highlight the unique security challenges that arise in this context and discuss how different security mechanisms can be employed to mitigate risks. In essence, this research seeks to answer the question of how the SDN network architecture can be utilized in IoT for its security enhancement.

Overall, this comparative study aims to contribute to the existing body of knowledge in the field of network security by shedding light on the various approaches to securing data transfer in SDN network architecture for IoT. By understanding the strengths and weaknesses of different security mechanisms, organizations can make informed decisions to protect their IoT deployments and ensure the privacy and integrity of their data.

2. Background

The Internet of Things is a new paradigm known as the "Internet of the Future," and its main idea is to connect all objects in the world to the Internet. IoT integrates various sensors, objects, and smart nodes that can communicate with each other without human intervention. Currently, it has wide-ranging applications in smart networks, healthcare, and transportation. IoT aims to create extensive applications for improving human life and the global economy. As a result, significant business opportunities will emerge in the field of IoT.

According to the Global Competitiveness Index (GCI), several countries, including Iran, are transitioning from factor-based economies to efficiency-driven economies and are striving to improve their competitive positions [6]. One of the foundations of competitiveness is readiness to embrace new technologies. Therefore, to enhance global competitiveness, necessary readiness must be acquired to face emerging technologies that are expected to have a considerable impact on future competition. According to a Gartner report in 2015, the Internet of Things is one of the areas that will receive significant attention in the future. In many countries, the Internet of Things is considered a leading technology and has received investment. Alongside IoT development, security issues such as data privacy, access control, secure communication, and data storage security have emerged [7, 8]. The rapid growth of IoT tools and services has led to the development of numerous vulnerable and insecure nodes. One of the central challenges in IoT implementation is security. This challenge encompasses concepts such as authentication, access control, privacy, secure architecture, and structure. Due to the extensive scale of the IoT infrastructure, security and privacy challenges are more significant compared to other IoT challenges. To successfully establish the IoT infrastructure, security and privacy must be given serious attention. When

billions of things are interconnected, precise security mechanisms are needed to protect information, data sharing over the IoT transmission medium, and individual privacy.

In the rapidly evolving landscape of the Internet of Things (IoT), where billions of devices are interconnected, securing data transfer has emerged as a critical concern. With the advent of Software-Defined Networking (SDN) network architecture, managing and securing the massive influx of data has become even more complex. IoT devices, ranging from sensors and actuators to wearable devices and smart appliances, generate an enormous amount of data that needs to be transferred securely across networks. This data often includes sensitive information such as personal and financial data, as well as critical operational data for industries like healthcare and manufacturing. Ensuring the confidentiality, integrity, and availability of this data has become paramount.

SDN network architecture provides a centralized approach to network management, allowing for dynamic and flexible network configurations. However, this shift towards centralization also introduces new security challenges. Traditional network security measures are often insufficient to protect against sophisticated attacks that target the SDN controller or the communication channels between the controller and the network devices.

Table (1) provides a summary of some of the research carried out in the field of IoT security:

Table 1. Research paper on IOT Security

<i>Description</i>
A review of applications, technology, and challenges in IoT research, focusing on security challenges related to data confidentiality, privacy, and trust [8].
Examines IoT applications in smart health, smart buildings, smart energy management, and smart cities. Addresses challenges such as secure communication, data exchange, and energy optimization [9].
Presents a roadmap for studying challenges such as privacy, trust, object identification, and access control. Analyzes the impact and role of each security component in the overall system [10].
Discusses the rapid growth of IoT and its applications, as well as potential security and forensic challenges [11].
Proposes three executable security schemes for IoT based on a layered structure for IoT architecture [12].
Explores the application of IoT in agriculture for quality production and addresses challenges including software, organizational, communication network, and security challenges [13].
Examines the application, and challenges of specific IoT use cases. Addresses unique object identification, standardization, privacy, physical object preservation, information confidentiality, and network security [14].
Assault vectors as recorded by Open Web Application Security Extend (OWASP) concern the three layers of an IoT framework, which are equipment, communication interface and interfaces/services. Subsequently, the execution of IoT security relief ought to include the security engineering at all IoT layers. [15]
The expanding number and portability make them more appealing to assailants. In this manner, numerous methods have been coordinates to secure IoT, such as confirmation, accessibility, encryption, and information judgment. Interruption discovery frameworks (IDSs) are an viable security device that can be improved utilizing machine learning (ML) and profound learning (DP) calculations. [16]
This paper portrays a novel arrange interruption location show based on machine learning procedures pointing to make strides discovery rate within the Web of Things environment. [17]

The Internet of Things technology has always been a topic of discussion in the IT field, and to leverage its benefits, we need to address its challenges. Addressing these challenges is essential because the technology is expanding and being used more widely. Security is one of the most significant issues raised in the context of the Internet of Things. In IoT, every connected device can potentially serve as a gateway to the IoT infrastructure or personal data. Security and privacy concerns are vital, but with the introduction of complexity, security vulnerabilities and potential weaknesses in areas such as collaboration capabilities, compositions, and self-decisions, new risks related to IoT have emerged. Given that complexity leads to new vulnerabilities in services, the risk of privacy breaches in IoT increases. The implementation of the Internet of Things must be approved by law, ethics, society, and policy, considering legal challenges, systemic approaches, technical challenges, and business challenges.

Therefore, in this section, we delve into exploring solutions to enhance the security of the Internet of Things (IoT). Given the security challenges mentioned in the previous section, having a robust and secure architecture for IoT networks can be among the most important solutions to address IoT security challenges. One of the latest architectures discussed in the network domain is Software-Defined Networking (SDN), which has different structures and conditions from a security perspective.

Software-Defined Networking (SDN) is an approach in computer networks that empowers network administrators to manage network services through a higher-level abstraction. This is achieved by separating the decision-making system regarding traffic routing (control plane) from the underlying system responsible for directing packets to the chosen destination (data plane) [18]. The inception of SDN dates back to shortly after the release of Java by Sun Microsystems in 1995. SDN is a dynamic, manageable, cost-effective, and adaptable architecture that aims to be suitable for bandwidth-intensive applications of today. The OpenFlow protocol is a fundamental element of the SDN architecture [19]. The architecture of such a network is as follows: 1) Programmable directly, 2) Agile, 3) Centrally managed, 4) Programmatically configured, 5) Based on open and vendor-agnostic standards, and is independent of traditional network system producers. Custom-configured devices create a susceptible error-prone environment.

Furthermore, they cannot fully utilize the capabilities of the physical network infrastructure. This has led to a paradigm shift in the network industry and is known as Software-Defined Networking. Benefits such as programmability, task virtualization, and easy network management can be provided using the SDN platform. On the other hand, POX is defined as an open-source SDN controller resource based on Python, primarily used for rapid development and initial prototyping of new network applications. In a paper by Dr. Norman and Dr. Mahdi, performance metrics such as service latency, bandwidth used, received packets, and bytes were measured and recorded using network monitoring tools like iperf and ITG-D to evaluate the performance of the POX controller and operational performance. The results of this research suggest using the POX controller for rapid development and prototyping of network control systems and also a framework for interacting with openflow switches [20].

2.1. Literature review:

This section presents a review of previous research and literature focusing on Software-Defined Networking (SDN) networks in the context of Internet of Things (IoT) applications. The review encompasses studies that have explored the integration of SDN and IoT, with a specific emphasis on data transfer mechanisms, network architecture, and security preservation. By examining the findings and methodologies of these previous studies, this section aims to establish a comprehensive understanding of the existing body of knowledge in the field of SDN networks for IoT. The insights gathered from this review will inform the comparative analysis presented in this paper, shedding light on the evolution and current state of research in this domain.

Securing data transfer in SDN networks for IoT involves implementing robust encryption protocols, authentication mechanisms, and access control policies [21]. Encryption ensures that the data remains confidential even if intercepted, while authentication verifies the identities of devices and users accessing the network. Access control policies enable the enforcement of fine-grained permissions and restrictions, preventing unauthorized access to sensitive data.

Furthermore, the comparative study of different security approaches in SDN networks for IoT is crucial. It helps identify the strengths and weaknesses of various security mechanisms, enabling organizations to make informed decisions about implementing the most effective solutions for their specific requirements. By prioritizing the security of data transfer in SDN network architecture for IoT, organizations can mitigate the risks associated with unauthorized access, data breaches, and potential disruptions to critical operations [22]. Implementing robust security measures not only safeguards sensitive information but also fosters trust among stakeholders and ensures the long-term success and sustainability of IoT deployments.

The integration of Software-Defined Networking (SDN) and Internet of Things (IoT) has paved the way for a more interconnected and intelligent world. However, as with any technological advancement, there are inherent security challenges that need to be addressed to ensure secure data transfer within the SDN network architecture for IoT. One of the primary challenges is the vulnerability of IoT devices themselves [23]. Many IoT devices are resource-constrained and lack robust security mechanisms, making them easy targets for attackers. These devices often have limited processing power and memory, making it difficult to implement complex security protocols. Another challenge lies in the centralized control plane of SDN networks. While the centralized control provides flexibility and agility, it also becomes a single point of failure and a potential target for attacks [20]. A compromise in the control plane can have severe consequences, as it can lead to unauthorized access, data manipulation, and disruption of services.

Furthermore, the dynamic nature of SDN networks introduces new security concerns. The ability to dynamically allocate resources and reroute traffic opens up potential vulnerabilities that can be exploited by attackers [24]. This includes the risk of unauthorized access to network elements, unauthorized modifications to network policies, and the potential for man-in-the-middle attacks.

Additionally, the sheer volume of data generated by IoT devices poses a significant challenge for security. The massive influx of data from sensors, devices, and applications requires robust encryption and authentication mechanisms to protect the confidentiality and integrity of the data [25, 26]. Without proper security measures in place, sensitive information can be intercepted, tampered with, or stolen, compromising the privacy of individuals and organizations. Addressing these security challenges requires a comprehensive approach that encompasses both hardware and software solutions. It involves implementing secure communication protocols, access control mechanisms, intrusion detection systems, and encryption algorithms specifically designed for resource-constrained IoT devices. Furthermore, continuous monitoring and auditing of the network infrastructure are necessary to identify and mitigate potential security breaches. Securing data transfer in SDN network architecture for IoT is a complex task that requires careful consideration of the unique security challenges posed by IoT devices and the dynamic nature of SDN networks. By understanding these challenges and implementing appropriate security measures, organizations can ensure the confidentiality, integrity, and availability of their data, fostering trust in the interconnected world of IoT.

There are many studies which are focus on securing transferring data. In order to address the security challenges of SDN-based IoT systems, the study propose a novel security model called Middlebox-Guard (M-G). M-G is designed to reduce network latency, manage dataflow, and ensure the safe operation of SDN-based IoT networks. The model consists of several key components and mechanisms that work together to enhance security performance and manage dataflow effectively [26]. In other Study compares four SDN networks. Performance of networks with different numbers of controllers (1, 2, 3, 4) was evaluated. Concludes that network performance increases with the number of controllers. Used DITG tables for architecture comparison [27] One of the key aspects of the M-G model is the placement of middleboxes at the most appropriate locations within the network. These middleboxes are responsible for enforcing security policies and ensuring that data is transferred securely. To determine the optimal placement of middleboxes, M-G utilizes dataflow abstraction and a heuristic algorithm that takes into account different security policies. By placing the middleboxes strategically, M-G aims to minimize network latency and improve the overall security of the IoT system [28].

Load balancing is another crucial aspect of managing dataflow in SDN-based IoT systems. M-G proposes an online Linear Program (LP) formulation to handle load balance effectively. This formulation takes into account the network traffic and allocates resources dynamically to ensure that the dataflow is distributed evenly across the network. By implementing load balancing mechanisms, M-G aims to prevent congestion and optimize the overall performance of the IoT system [21].

The integration of SDN in wireless networks and its enhancements to optical and wireless networks have been explored in the context of IoT. Researchers have analyzed the support for the OpenFlow protocol in existing wireless networks and discussed the benefits of using SDN in wireless networks [29]. SDN has also been proposed as a solution to address the challenges of network management and optimization in IoT environments, particularly in terms of

scalability and mobility [30]. Additionally, SDN has been integrated with optical and wireless networks to improve data protection during transmission and storage in IoT systems.

The integration of SDN and IoT presents numerous opportunities for future research and development. Knowledge-driven SDN has been identified as a potential approach to enhance IoT networks by leveraging IoT data and enabling intelligent decision-making (Li et al., 2020). Future research can focus on exploring the potential of knowledge-driven SDN for IoT and developing new architectures and frameworks that leverage the capabilities of SDN to address the evolving challenges in IoT environments. Additionally, research can be conducted to further optimize data transfer in IoT networks by leveraging edge computing, fog computing, and the efficient utilization of network resources [31].

The literature available on the topic of data transfer in SDN network architecture within the context of IoT encompasses several notable studies. "An Agile Privacy-Preservation Solution for IoT-based Smart City using Different Distributions" presents a comprehensive approach to privacy preservation in IoT-based smart cities, shedding light on the importance of secure data transfer and privacy protection in IoT networks. The study emphasizes the significance of efficient data transfer methods in ensuring privacy and security within IoT environments [32]. Similarly, "A Dynamic SDN-based Privacy-Preserving Approach for Smart City Using Trust Technique" introduces a dynamic privacy-preserving approach for smart cities, leveraging Software-Defined Networking (SDN) and trust techniques. This paper underscores the relevance of privacy preservation and secure data transfer in the context of smart cities, aligning with the objectives of our comparative study [33].

Furthermore, another study contributes valuable insights into forwarding and caching schemes in Information-Centric Software-Defined Networks. The paper explores innovative approaches to data transfer and caching, highlighting the importance of efficient data dissemination and retrieval in SDN environments [34]. The study introduces a method for privacy preservation in IoT-SDN integration environments, emphasizing the importance of secure data transfer and privacy protection in integrated IoT and SDN systems. The study addresses the critical aspects of privacy preservation and secure data transfer, aligning with the objectives of our comparative study [35, 36]. Similarly, "A Method for Privacy-Preserving in Smart City with Software Defined Networking" presents a method for privacy preservation in smart cities using Software-Defined Networking (SDN). This paper underscores the relevance of privacy preservation and secure data transfer in the context of smart cities, contributing to the understanding of privacy-preserving techniques within SDN environments.

These seminal works provide a strong foundation for understanding the challenges and opportunities related to data transfer in SDN network architecture within IoT applications. By building upon the findings and methodologies presented in these studies, our comparative analysis aims to contribute to the advancement of data transfer mechanisms in SDN-based IoT networks, ultimately enhancing network efficiency, scalability, and security. SDN architecture can provide several security benefits, such as centralized control and visibility, network segmentation, and policy-based management. By using SDN, security policies can be easily enforced throughout

the network, and traffic can be monitored and analyzed in real-time.

A comparative analysis between traditional IoT networks and SDN-based IoT networks has been conducted to evaluate the performance improvements achieved by SDN. The analysis focuses on metrics such as latency, jitter, and throughput. The results demonstrate that SDN-based IoT networks significantly improve network efficiency by reducing network overheads and enhancing communication between nodes and controllers [37]. The average latency and jitter percentile improvements achieved by SDN-based IoT networks are substantial, highlighting the benefits of SDN in optimizing data transfer in IoT environments and decrease complexity.

Traditional security mechanisms such as firewalling have been deployed at the edge of the Internet. These mechanisms are used to protect the network against external threats. However, these mechanisms are insufficient for securing the next-generation Internet. The edgeless architecture of the Internet of Things raises further concerns about network access control and software validation. In the context of IoT, there isn't a simple solution for managing interactions between each node [38]. For instance, if a thing becomes compromised by a virus, this issue could spread throughout the network without proper control.

One of the main advantages of SDN is network segmentation, which allows for the creation of virtual networks that are isolated from one another. This can help prevent lateral movement of threats within the network, as well as limit the scope of any potential breaches. Another benefit of SDN is the ability to apply policies based on specific criteria, such as user identity or application type [39]. This can help ensure that only authorized traffic is allowed on the network, and that any potential threats are blocked. Overall, SDN architecture can provide a more secure and flexible network infrastructure, allowing organizations to better protect their data and assets.

3. Research methodology

With the exponential growth of internet-connected devices, ensuring secure networks remains one of the toughest challenges for network administrators. Safeguarding such vast and heterogeneous networks is a daunting task. In this context, the emerging paradigm of Software-Defined Networking (SDN) introduces significant opportunities and potential to overcome these challenges more efficiently. In this section, we first introduce two SDN architectures and describe metrics of performance of data transferrin . Then we implement these two SDN architecture in the Mininet simulator. Then, we compare these architectures based on network security requirements to determine which architecture is better suited for a secure Internet of Things.

The SDN architectures were designed and implemented using the Mininet simulator. The Miniedit software, an option within Mininet, was utilized to create the network architectures, which include hosts, switches, controllers, and virtual links. The Mininet simulator supports both traditional routing and SDN using the OpenFlow protocol. This allowed for the creation and implementation of the SDN architectures in a controlled virtual environment for research and educational purposes. Software-Defined Networking (SDN) is a novel architecture in computer networks that enables

network management at a higher level. This is achieved by separating the decision-making layer about traffic routing (control plane) from the underlying layer responsible for packet forwarding to the selected destination (data plane). SDN decouples the network's control plane from its data plane. This is accomplished by switches using "rules" defined by a centralized component, the SDN controller, to guide traffic. The communication between SDN switches and the controller is implemented using protocols like the OpenFlow protocol.

The reason for choosing software-defined networks for IoT security lies in SDN's ability to offer ample opportunities for network protection in a more efficient and flexible manner. In the SDN architecture, network devices do not make transport decisions. Instead, network devices communicate with a dedicated node called the SDN controller to receive appropriate transport decisions. Various protocols can be used by network devices to communicate with the controller, with OpenFlow being the most common one. OpenFlow defines control messages that enable the SDN controller to securely connect with network devices, query their current state, and install forwarding instructions. Moreover, OpenFlow provides comprehensive and flexible traffic management through twelve fields in packet headers to match network traffic.

In this study in order to evaluate performance of data transfer can be measured using various metrics, including:

Total Time: This metric refers to the total duration taken for the complete data transfer process, from the initiation of the transfer to its completion. It provides a holistic view of the time required for the entire data transfer operation.

Average Bitrate: Average bitrate is the average rate at which bits are transmitted over a specific period of time. It measures the average data transfer speed and is often expressed in bits per second (bps) or a higher unit such as kilobits per second (Kbps) or megabits per second (Mbps). This metric offers insights into the average data transmission speed over the entire transfer process.

Average Packet Rate: The average packet rate measures the average number of packets transmitted per unit of time. It provides information about the frequency of packet transmission and is useful for assessing the efficiency of data transfer in terms of packet delivery rates.

In this study two architecture of SDN will be analyzed to present a guideline for using this secure network. These metrics, provide a comprehensive understanding of the efficiency of data transfer in SDN architectures.

4. Experimental Evaluation of SDN Architectures

As mentioned in the previous section, this research requires the Mininet simulator for SDN architecture implementation. Since Mininet is installed on Linux, we first install VMware software as a virtual machine on our device and then implement the Linux operating system on it. Mininet simulator encompasses different components, one of which is Miniedit, considered as a lab for Mininet. This lab includes sections for controllers, switches, and etc. Two architectures are considered in this study, with their implementation detailed in Figure1 and Figure 2.

Our architecture has an SDN network with Network Access Points (NAPs) at its edges. Each NAP is identified by

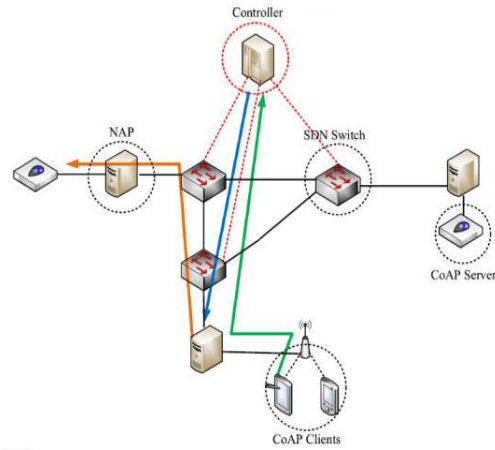


Figure. 1. The first Architecture of SDN

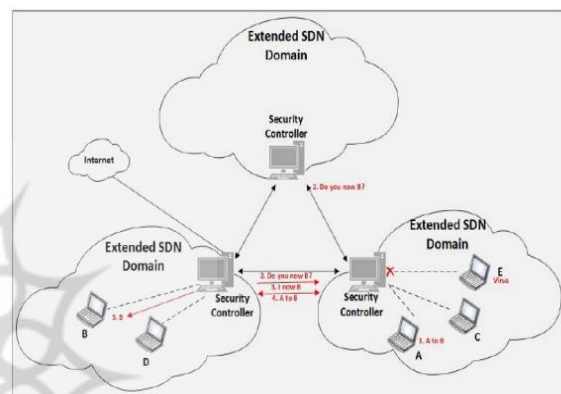


Figure. 2. The second Architecture

an NAP ID, and all NAPs recognize all ID NAPs. NAPs are connected to the SDN network using SDN switches. When we mention "an OpenFlow protocol exists in a NAP," it means that the NAP uses it to connect to the network.

Packet forwarding between NAPs is conducted using the Bloom filter method. In essence, each main network link is identified by a specific bit array, known as a link identifier. Path identifiers are stored in IPv6 address fields, making it straightforward to create appropriate flow rules for Bloom filter-based transport. Specifically, from a high-level perspective, each SDN switch is configured with an OpenFlow rule on every interface. This rule examines a subnet mask within the destination IPv6 address and, upon successful validation, forwards the packet from the respective interface. This validation occurs across all interfaces, allowing a packet to be sent through multiple interfaces. OpenFlow rules needed for implementing Bloom filter-based transport are installed once during network initialization. Path identifiers within our architecture are bidirectional, meaning a path identifier used to send a packet from A NAP to B NAP can also be utilized for sending packets from B to A. Another intriguing aspect of path identifiers is their potential for combining to create multi-cast trees. For instance, given the $B \rightarrow A$ Path identifier representing the path from A NAP to B NAP, and another path identifier $C \rightarrow A$ Path for the path from A NAP to C NAP, combining the $B \rightarrow A$ and $C \rightarrow A$ paths results in a new path identifier that can be used for multicasting packets from A

NAP to B and C NAPs. Ultimately, our system assumes that the SDN controller knows the network topology, all link identifiers, and URI CoAPs associated with each NAP, offering a "Northbound" API that enables resource owners to install, update, or remove them.

In the next proposed architecture (figure2) featuring multiple SDN domains, we assume that within each domain, there is one SDN controller or multiple SDN controllers. These controllers exclusively manage devices within their respective domains, with a domain representing an organizational network or a data center. A SDN-based architecture for the Internet of Things requires a scalable and extensive connection across numerous SDN domains. To achieve such broad-ranging communication, we introduce a new type of controller within each domain: the root controller, also referred to as the border controller. Some hierarchical architectures suggest distributing control functions for optimization and distribution in SDN. We suggest not distributing control functions across multiple controllers, but rather distributing routing and security rule functions to each border controller. Additionally, these controllers are responsible for establishing connections and exchanging information with other SDN border controllers. In this architecture, we have four hosts, where two are connected to one controller, and the other two are connected to another controller. Both controllers are then connected to a central controller. The overarching principle of network security is to expand SDN domains into multiple domains, with each controller in each domain exchanging its security rules. SDN controllers exist that act as security guardians at the periphery of the evolved SDN domain to ensure network safety. Secure connections can be established between domains by merely adding SDN controllers. Only recognized traffic can be accepted. While controllers know their own domain policies, they are unaware of policies in other domains. Consequently, when a node seeks to establish communication with another node from a different domain, the flow must be directed toward the Controller Security, also known as the Controller Border, which queries neighboring security controllers to ascertain knowledge of the intended destination.

5. Result and discussion

5.1. Comparative Analysis of the Performance of Two SDN Architectures

In Architecture Number One, all three hosts are connected to three switches, and each of these switches is connected to a single controller. However, in Architecture Number Two, we consider having one controller for each SDN domain. This feature in Architecture Number Two makes it a more secure option compared to Architecture Number One. Considering that other influential factors exist in computer networks, in this study, we compare the secure Architectures Number One and Number Two based on their other features to determine which architecture is more optimal for IoT in the medical field.

In the Mininet environment, there is a capability called DITG that evaluates network traffic and presents network details in the form of a table. We obtained the DITG table for both architectures (Figures 3 and 4).

Based on the DITG tables for both architectures, the differences between the two are as follows:

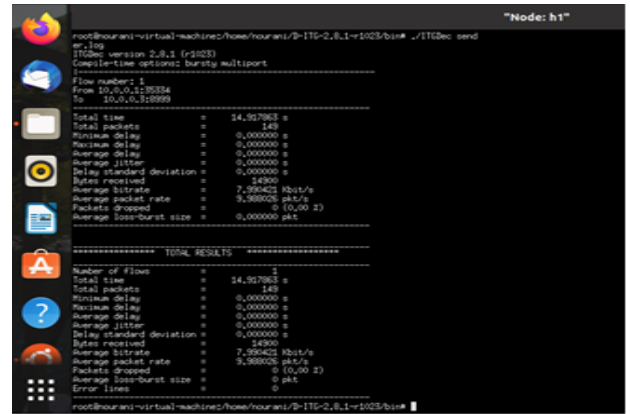


Figure 3. DITG table for Architecture Number One

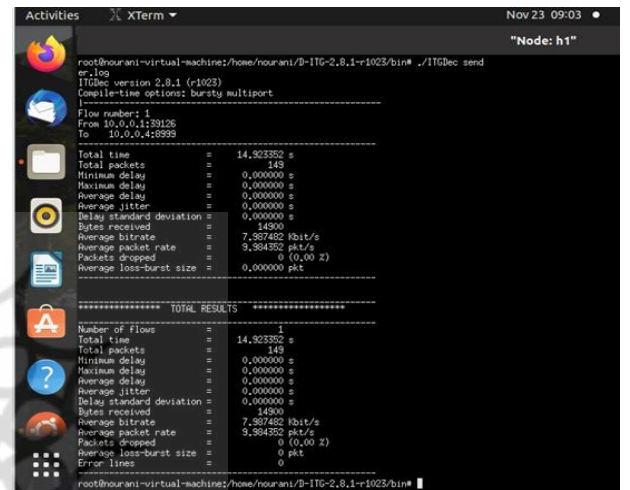


Figure 4. DITG table for Architecture Number Two

1. Total Time: In Architecture Number One, the total time is 14.917863, which is slightly lower than Architecture Number Two's total time of 14.923352. This indicates that packets will be sent faster in this architecture compared to the second architecture.
2. Average Bitrate: Average bitrate represents the rate of transferred bits from one location to another. In Architecture Number One, it's 7.990421, while in Architecture Number Two, it's 7.987482. This implies that more bits are transferred in less time in the first architecture.
3. Average Packet Rate: Similar to the previous cases, the average packet rate in Architecture Number One is 9.988026, while in Architecture Number Two, it's 9.984352. Architecture Number One has a slightly higher packet rate than Architecture Number Two. It's important to note that the number of sent packets is the same in both architectures.

Architecture Number Two offers higher security by assigning one controller per SDN domain. However, based on the DITG tables, Architecture Number One is faster. The choice of which architecture is better for our network depends on our priorities. Whether we prefer a faster network or a more secure one, considering that both architectures fall under the category of secure architectures. Comparing these two architectures through their simulations can lead to a better

decision on which SDN architecture to choose, depending on the specific conditions.

The wider context and limitations of the study are important aspects to consider. The findings of the study can be generalized to similar contexts and scenarios where software-defined networking (SDN) architectures are employed within Internet of Things (IoT) network environments. However, it is essential to acknowledge the specific scope and context of the study, as the findings may not be universally applicable to all IoT network architectures or SDN implementations. The assumptions made in the study include the assumption that the comparative analysis accurately reflects the performance characteristics of the two secure SDN network architectures under investigation. Additionally, it is important to recognize that the study's findings are based on a specific set of metrics and parameters related to data transfer performance, which may not encompass the full spectrum of factors influencing IoT network operations. Furthermore, the study's limitations include the potential for variations in network environments, hardware configurations, and operational conditions that may impact the generalizability of the findings. These considerations underscore the need for further research and validation in diverse IoT network settings to ascertain the broader applicability and robustness of the study's conclusions.

6. Conclusion

The potential benefits of the Internet of Things and its contribution to improving human life pave the way for the development of IoT. As challenges become gradually fewer, or they find suitable paths with minimal individual, societal, and environmental impacts. However, the Internet of Things requires further study to prevent vulnerabilities and misuse by intruders and malicious actors. Additionally, experts can enhance its security by implementing complex algorithms for exchanging information across different levels of the IoT.

In this study, we examined the Internet of Things, highlighted its pros and cons, and addressed security challenges. We explored the necessity of network architecture in solving security challenges and concluded that software-defined networking (SDN) architectures are among the secure network architecture options. Consequently, we compared two secure SDN network architectures. The comparison indicated that the first architecture exhibits higher transmission rates and faster speeds compared to the second architecture.

In conclusion, our in-depth exploration of the Internet of Things (IoT) and its integration with software-defined networking (SDN) has yielded valuable insights into the potential benefits and challenges associated with IoT network architecture. Through a comprehensive comparative analysis of secure SDN network architectures, we have uncovered significant findings that can guide decision-making for IoT experts and network architects. The superior transmission rates and faster speeds exhibited by the first architecture underscore its potential as a robust and efficient option for IoT network deployment, emphasizing the critical role of network architecture in optimizing data transfer performance.

Furthermore, the integration of SDN within IoT network architecture has been shown to offer a range of substantial benefits, including fault tolerance, energy management, scalability, load balancing, and security service provisioning. These advantages highlight the transformative impact of SDN

on IoT network management, paving the way for enhanced network efficiency and reliability. The observed improvements in total time, average bitrate, and average packet rate further underscore the tangible benefits of SDN-based IoT networks in optimizing data transfer performance.

As IoT continues to evolve and expand, the findings from this study provide actionable insights that can inform strategic decisions regarding the adoption of secure SDN network architectures within IoT environments. By leveraging these insights, IoT experts and network architects can make informed choices that align with the goals of enhanced performance, reliability, and security within IoT network infrastructure.

Understanding secure architecture in SDN data transfer offers a multitude of benefits, including enhanced network reliability, improved data integrity, and strengthened resilience against potential security threats. By comprehensively grasping the intricacies of secure architecture within SDN, network administrators and cybersecurity professionals can proactively implement robust security measures to safeguard data transfer processes. This understanding enables the identification and mitigation of vulnerabilities, thereby fortifying the network infrastructure and minimizing the risk of unauthorized access, data breaches, and malicious activities. Additionally, a deep understanding of secure architecture in SDN data transfer empowers organizations to uphold compliance with industry regulations and standards, fostering trust and confidence among stakeholders. Ultimately, this knowledge serves as a cornerstone for establishing a secure and resilient data transfer environment, underpinning the foundation for reliable and secure network operations within software-defined networking architectures.

Overall, this study contributes to the growing body of knowledge surrounding the integration of SDN in IoT network architecture, offering practical implications for the design, implementation, and management of efficient and secure IoT networks. The transformative potential of SDN in optimizing data transfer performance underscores its significance as a key enabler of enhanced IoT network efficiency and reliability.

Declarations

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

Authors' contributions

Zahra A: Conceived and design the study, Data collection, wrote and revised the manuscript;

Negar N: Data collection, Conduct simulation, Wrote manuscript.

N Zanjani: Assist data collection, revised manuscript.

Conflict of interest

The authors declare that no conflicts of interest exist.

Acknowledgements

If there is an acknowledgement, please include it. Regardless of how many acknowledgements you have, use the singular heading.

References

- [1] L. Hasanzadeh Garavand, M. Abdolhamid, and A. Zakery, "Presentation of IoT Policies Pattern in Iran through Applying of

- Thematic Analysis Method," *Modiriat-e-farda*, vol. 67, no. 67, p. 125-140, 2022. <https://doi.org/20.1001.1.22286047.1400.20.67.79>
- [2] M. Bayanati, "Security and privacy analysis based on Internet of Things in the fourth industrial generation (Industry 4.0)," *International Journal of Innovation in Management, Economics and Social Sciences*, vol. 3, no. 2, pp. 1-12, 2023. <https://doi.org/10.59615/ijimes.3.2.1>
 - [3] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274-283, 2022. <https://doi.org/10.1016/j.comcom.2021.09.029>
 - [4] N. Gupta, M. S. Maashi, S. Tanwar, S. Badotra, M. Aljebreen, and S. Bharany, "A comparative study of software defined networking controllers using mininet," *Electronics*, vol. 11, no. 17, p. 2715, 2022. <https://doi.org/10.3390/electronics11172715>
 - [5] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, "Towards Software-Defined Networking-based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects," *IEEE Access*, vol. 10, pp. 70850-70901, 2022. <https://doi.org/10.1109/ACCESS.2022.3188311>
 - [6] X. Sala-i-Martin *et al.*, "The global competitiveness index 2012–2013: Strengthening recovery by raising productivity," *The Global Competitiveness Report 2012–2013*, pp. 49-68, 2012. https://www3.weforum.org/docs/CSI/2012-13/GCR_Chapter1.1_2012-13.pdf
 - [7] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *arXiv preprint arXiv:1901.07309*, 2019. <https://doi.org/10.48550/arXiv.1901.07309>
 - [8] <https://doi.org/10.48550/arXiv.1901.07309>
 - [9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015. <https://doi.org/10.1016/j.comnet.2014.11.008>
 - [10] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, and P. Singh, "Secure and energy-efficient smart building architecture with emerging technology IoT," *Computer Communications*, vol. 176, pp. 207-217, 2021. <https://doi.org/10.1016/j.comcom.2021.06.003>
 - [11] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118-137, 2018. <https://doi.org/10.1016/j.dcan.2017.04.003>
 - [12] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544-546, 2018. <https://doi.org/10.1016/j.future.2017.07.060>
 - [13] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042-9053, 2019. <https://doi.org/10.1109/JIOT.2019.2926365>
 - [14] P. Nayak, K. Kavitha, and C. Mallikarjuna Rao, "IoT-enabled agricultural system applications, challenges and security issues," *IoT and analytics for agriculture*, pp. 139-163, 2020. https://doi.org/10.1007/978-981-13-9177-4_7
 - [15] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, 2021. <https://doi.org/10.1016/j.iot.2021.100420>
 - [16] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer networks*, vol. 148, pp. 283-294, 2019. <https://doi.org/10.1016/j.comnet.2018.11.025>
 - [17] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrou, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392-3411, 2023. <https://doi.org/10.1007/s11227-022-04783-y>
 - [18] A. Guezzaz, S. Benkirane, and M. Azrou, "A novel anomaly network intrusion detection system for internet of things security," in *IoT and smart devices for sustainable environment*: Springer, 2022, pp. 129-138. https://doi.org/10.1007/978-3-030-90083-0_10
 - [19] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317-2346, 2015. <https://doi.org/10.1109/COMST.2015.2474118>
 - [20] J. Tourrilhes, P. Sharma, S. Banerjee, and J. Pettit, "The evolution of SDN and OpenFlow: a standards perspective," *IEEE Computer Society*, vol. 47, no. 11, pp. 22-29, 2014. <https://www.hpl.hp.com/techreports/2014/HPL-2014-41.pdf>
 - [21] H. M. Noman and M. N. Jasim, "A proposed linear multi-controller architecture to improve the performance of software defined networks," in *Journal of Physics: Conference Series*, IOP Publishing, 2021, vol. 1773, no. p. 012008. <https://doi.org/10.1088/1742-6596/1773/1/012008>
 - [22] J. Li, J. Cai, F. Khan, A. U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu, "A secured framework for sdn-based edge computing in IOT-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479-135490, 2020. <https://doi.org/10.1109/ACCESS.2020.3011503>
 - [23] A. Sezgin and A. Boyacı, "A Survey of Privacy and Security Challenges in Industrial Settings," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, 2023, pp. 1-7. <https://doi.org/10.1109/ISDFS58141.2023.10131858>
 - [24] R. Roozbehi and M. Ghasemzade, "Use of Software Defined Networks to Enhance the Security of the Internet of Things," *Information Technology Innovations and applied communications*, no. 2, pp. 11-16, 2020.
 - [25] M. Priyadarsini and P. Bera, "Software defined networking architecture, traffic management, security, and placement: A survey," *Computer Networks*, vol. 192, p. 108047, 2021. <https://doi.org/10.1016/j.comnet.2021.108047>
 - [26] M. Babiker Mohamed, O. Matthew Alofe, M. Ajmal Azad, H. Singh Lallie, K. Fatema, and T. Sharif, "A comprehensive survey on secure software-defined network for the Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 1, p. e4391, 2022. <https://doi.org/10.1002/ett.4391>
 - [27] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250-10276, 2020. <https://doi.org/10.1109/JIOT.2020.2997651>
 - [28] S. Lee, J. Ali, and B.-h. Roh, "Performance comparison of software defined networking simulators for tactical network: Mininet vs. OPNET," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, 2019, pp. 197-202. <https://doi.org/10.1109/ICNC.2019.8685572>
 - [29] S. Lai, X. Yuan, S. F. Sun, J. K. Liu, R. Steinfeld, A. Sakzad, and D. Liu, "Practical encrypted network traffic pattern matching for secure middleboxes," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2609-2621, 2021. <https://doi.org/10.1109/TDSC.2021.3065652>
 - [30] H. Kar and G. Rather, "Multilayer software defined networking architecture for the internet of things," *International Journal of Computing and Digital Systems*, vol. 9, no. 4, pp. 735-745, 2020. <http://dx.doi.org/10.12785/ijcds/090420>
 - [31] D. Huynh-Van and Q. Le-Trung, "SD-IO-TR: an SDN-based Internet of Things reprogramming framework," *IET Networks*, vol. 9, no. 6, pp. 305-314, 2020. <https://doi.org/10.1049/iet-net.2019.0223>
 - [32] G. Sreekanth, S. A. N. Ahmed, M. Sarac, I. Strumberger, N. Bacanin, and M. Zivkovic, "Mobile Fog Computing by Using SDN/NFV on 5G Edge Nodes," *Comput. Syst. Sci. Eng.*, vol. 41, no. 2, pp. 751-765, 2022. <https://doi.org/10.32604/csse.2022.020534>
 - [33] M. Gheisari *et al.*, "An Agile Privacy-Preservation Solution for IoT-Based Smart City Using Different Distributions," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 356-362, 2023. <https://doi.org/10.1109/OJVT.2023.3243226>
 - [34] J. A. Alzubi *et al.*, "A dynamic SDN-based privacy-preserving approach for smart city using trust technique," in *2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, IEEE, 2022, pp. 1-5. <https://doi.org/10.1109/CFIS54774.2022.9756458>
 - [35] K. A. Raza, A. Asheralieva, M. M. Karim, K. Sharif, M. Gheisari, and S. Khan, "A novel forwarding and caching scheme for information-centric software-defined networks," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, 2021, pp. 1-8. <https://doi.org/10.1109/ISNCC52172.2021.9615667>
 - [36] S. Manimurgan, T. Anitha, G. Divya, G. C. P. Latha, and S. Mathupriya, "A survey on blockchain technology for network security applications," in *2022 2nd International Conference on Computing and Information Technology (ICCIIT)*, IEEE, 2022, pp. 440-445. <https://doi.org/10.1109/ICCIIT52419.2022.9711616>

- [37] M. Gheisari, G. Wang, S. Chen, and A. Seyfollahi, "A method for privacy-preserving in IoT-SDN integration environment," in *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, IEEE, 2018, pp. 895-902. <https://doi.org/10.1109/BDCloud.2018.00132>.
- [38] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-638, 2020. <https://doi.org/10.1109/TSC.2020.2966970>.
- [39] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, "Implementing a distributed firewall," in *Proceedings of the 7th ACM conference on Computer and communications security*, 2000, pp. 190-199.
- [40] N. S. Kalmykov and V. A. Dokuchaev, "Segment routing as a basis for software defined network," *T-Сomm-Телекоммуникации и Транспорт*, vol. 15, no. 7, pp. 50-54, 2021.



Zahra Askarinejad is a faculty member of the Computer Department at the Refah college university. She holds a Master's degree in software Engineering from APU University and a PhD in computer science in field of Software engineering from the University Putra Malaysia. Her areas of expertise include software engineering, IoT, requirement engineering, and HCI. Email: askarinejad@refah.ac.ir; ORCID: 0000-0002-7204-1384; Web of Science Researcher ID: JDM-5453-2023; Scopus Author ID: NA; Homepage: <https://refah.ac.ir/cv>



Negar Nourani received her B.S. degree in Software Engineering in 2020. Her research interests are Network, IoT and network design. Email: nouraninegar99@yahoo.com.



Nastaran Zanjani is a faculty member of the Computer Department at the Refah college university. She holds a Bachelor's degree in Electrical Engineering with a specialization in Electronics from the Shahid Beheshti University. She also has a Master's degree in Telecommunications Engineering from Khaje Nasir Toosi University and a PhD in Information Technology from the Queensland University of Technology in Australia. Her areas of expertise include information technology, and HCI. Email: m.soluki1999@gmail.com; ORCID: 0000-0002-5307-683X; Web of Science Researcher ID: NA; Scopus Author ID: NA ; Homepage: <https://refah.ac.ir/cv>.