

# Automation of 5G network slicing security using intent-based networking

Md. Zahirul Islam<sup>1</sup>, Syed Md. Galib<sup>1</sup>, Md. Humaun Kabir<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh

<sup>2</sup>Department of Physics, Jashore University of Science and Technology, Jashore, Bangladesh

## Article Info

### Article history:

Received Apr 4, 2024

Revised Aug 7, 2024

Accepted Sep 3, 2024

### Keywords:

5G network

Address resolution protocol spoofing

Distributed denial of service attack

Intent-based networking

Network slicing

## ABSTRACT

Network slicing is a fundamental technological advancement that facilitates the provision of novel services and solutions within the realm of 5G and the forthcoming 6G communications. Numerous challenges emerge when implementing network slicing on a large-scale commercial level since it necessitates comprehensive control and automation of the entire network. Cyberattacks, such as distributed denial of service (DDoS) and address resolution protocol (ARP) spoofing, can significantly disrupt the performance and accessibility of slices inside a multi-tenant virtualized networking infrastructure due to the shared utilization of physical resources. This article employs intent-based networking (IBN) to identify and address diverse threats through automated methods. A conceptual framework is presented in which the IBN manager is integrated into the network-slicing architecture to facilitate the implementation of automated security controls. The proposed work is assessed using an experimental test bed. The study's findings indicate that the network slice's performance exhibits improvement when successful detection and mitigation measures are implemented. This improvement is observed in various metrics: availability, packet loss, response time, central processing unit (CPU) and memory utilization.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Syed Md. Galib

Department of Computer Science and Engineering, Jashore University of Science and Technology

Jashore 7408, Bangladesh

Email: galib.cse@just.edu.bd

## 1. INTRODUCTION

Network slicing (NS) [1] is a groundbreaking concept that allows for the creation of mobile networks as needed. One of the fundamental concepts of 5G network slicing is the cost-effective operation of multiple virtual logical networks [2] on a shared physical infrastructure. The ability to allocate resources as needed enables 5G network slicing to be flexible and adaptable to various social situations with challenging environmental conditions. Network slicing, enabled by the combination of network function virtualization (NFV) [3] and software-defined networking (SDN) [4], represents a highly advantageous approach for telecommunications operators. It allows them to create and manage customized networks that efficiently cater to the changing requirements of different vertical industrial applications. Network slicing enables vertical industries to leverage virtualized infrastructure assets to effectively deploy their application platforms with customized resource capacity and network functions. Nevertheless, the process of network slicing entails the creation of numerous virtual networks on the 5G physical infrastructure and the utilization of shared network resources. This approach has the potential to introduce new vulnerabilities and elevate the risk of attacks. As a result, the emergence of security threats in 5G networks will require innovative security solutions that go beyond conventional approaches. Chen *et al.* [5] highlight the potential security risks

associated with the use of shared network resources. These risks include cross-slice attacks and resource hijacking. These studies indicate that attackers can take advantage of incorrect configurations or vulnerabilities in shared resources to launch cross-boundary attacks, which can have a significant impact on multiple users and services. Therefore, it is crucial to develop a thorough security framework that covers potential risks, necessary requirements, and helpful suggestions to ensure the secure implementation and operation of 5G network slicing.

Foukas *et al.* [6] explored the network slice design's various layers and their challenges. The authors discussed network slice design but not layer security. Side-channel attacks and inter- and intra-slice risks were not addressed in the middle layer of the design. This absence allows for 5G network slice security research. Afolabi *et al.* [7] explored 5G network slicing, including software to construct and manage slices and related ideas. These security risks must be examined to understand their complexities. Zhang [8] detailed 5G network slicing fundamentals. Network function virtualization, software-defined networking, slice management, and radio access networks (RAN) slicing were covered by the author. The summary of network slicing security issues ignored 5G network slices' vulnerabilities, threats, and attacks. Mathew [9] discusses NS security problems in another article. NS has two main issues: security and RAN implementation. Experts suggest that by combining the isolation and versatility of slice allocation with encryption, authentication, and manual slice allocation, certain security issues can be effectively addressed. One negative of isolation is that it only reduces a few risks. Isolation alone cannot stop the widespread attacks and hazards. When implementing the slice, these difficulties must be carefully considered. Chandini *et al.* [10] examined network slice security throughout their study. The research landscape also emphasizes inter and intra-slice communication mechanisms inside network slices. However, NS attacks were not addressed, and effective solutions and mitigation techniques were not discussed. Barakabitze *et al.* [11] discuss issues with SDN and NFV, the technologies that enable network slices. They explored 5G network slicing with SDN and NFV and also provided other technological viewpoints on slicing and addressed field SDN and NFV adoption problems. Network slicing requires many challenges and risks to be resolved. Olimid and Nencioni [12] studied network slicing principles and security trends. Slice lifespan and communication security threats were also prioritized in the investigation. To address these issues, it suggested specific methods. Cao *et al.* [13] evaluated network slicing security. They focus on 3GPP 5G network security and network slice security as a wider 5G application. While certain network slice security issues are fixed, the slice solo still has many weak points that need to be explored. The endeavor is further hampered by the lack of adequate security mitigation measures. Wang and Liu [14] examined network slice duration and management system security problems. However, they focus on vehicular networks and the risks of vehicle-specific slices. They do not specify security risk solutions. Reinforcement learning-based attack recovery systems that could work in real life were also studied.

Vidhani and Vidhate [15] examined 5G security issues. They discussed 5G and NS problems. However, many problem-related issues and risks are ignored. In addition, they offered NS security solution concepts and stressed physical host mutual authentication. A side channel thread exposes cryptographic data on the shared hardware device, compromising security. Dangi *et al.* [16] researched network slice architecture and machine learning (ML) in network slicing. They explored privacy, identifying the risks of machine learning-based network analysis. User privacy violations have inspired research into ML model-based data privacy protection methods. AI/ML was discussed to improve service delivery in some segments. Since AI/ML slices are self-learning, security features are easier to integrate. Network slicing attacks were studied by Salahdine *et al.* [17]. They attacked vulnerable areas with inter/intra-slice and lifecycle attacks. They also suggested security methods to reduce risks and prevent specific attacks. A vulnerable region needs considerable research on attacks, including technological and managerial attacks. Abood and Abdul-Majeed [18] explored the factors that enable slicing technologies and their hazards. Many technologies enable slicing, including NFV, virtual machines, containers, and others. This is only a minor fraction of network slicing's security issues, underscoring the need for a more thorough analysis. Abir *et al.* [19] examined network-slicing deployment issues in healthcare. They found fresh cybersecurity vulnerabilities that could compromise patient data and weaken medical device apps. Cyber threats in one domain raise security problems in other domains due to similar weaknesses throughout implementation. Sing *et al.* [20] have examined network slice threats and attacks and fixed security issues. Slicing security was discussed. Network slicing threats and attack avenues were also described. However, the work only covers a few attacks and threats, and more situations and mitigation methods are needed. Sukumar *et al.* [21] stressed the necessity of privacy and security in 5G network slicing. Their priority was segment resource management and synchronization. The researchers suggested homomorphic encryption for network slice security [22]. This encryption method allows computations and communications on encrypted data without decryption. They also explored secure multi-party computation (SMPC), which allows multiple entities to communicate without releasing raw data. This strategy ensures participant anonymity. There are still certain problems with

the security of 5G network slicing that need to be addressed. These concerns require enhancements in the security policies indicated in Table 1 and the study mentioned earlier.

Table 1. Summary table of literature on 5G network slicing security

Author	Year	Contribution to Security Factors	Remarks
Foukas <i>et al.</i> [6]	2017	The author discussed the structure of network slice architecture and its various layers.	Threats and attacks are excluded from coverage.
Afolabi <i>et al.</i> [7]	2018	The authors presented an initial summary of the inter-slice risks and difficulties that affect the federated architecture of slicing.	There is still a significant need for extensive investigation on security concerns related to slicing.
Zang [8]	2019	The author discussed the various aspects and ideas pertaining to network slicing.	Threats and attacks are excluded from coverage.
Mathew [9]	2020	The significance of RAN in network slicing was discussed, along with the associated security concerns.	Their focus was on utilizing isolation as a mitigation approach for various attacks; however, isolation can effectively address other attacks.
Chandini <i>et al.</i> [10]	2020	The researchers analyzed the many stages of a slice's existence and the security risks that can occur both across different slices and within a single slice.	Incidents and potential risks in all susceptible regions of slicing are not included.
Barakabitze <i>et al.</i> [11]	2020	The authors discussed the difficulties arising from implementing slicing-enabling technologies such as software-defined networking (SDN) and network function virtualization (NFV).	Attacks and threats related to network slicing are not addressed.
Olimid and Nencioni [12]	2020	The authors discussed the security trends related to the communication type and lifecycle of slices.	The discussion should include examining attacks and threats targeting more sensitive parts of slices and the strategies and methods for mitigating them.
Cao <i>et al.</i> [13]	2020	Security trends in 3GPP networks, including requirements for network slices, were discussed by the authors.	The authors examined the issue of security within network slices within the larger framework of a 5G network.
Wang and Liu [14]	2022	The authors specifically focused on addressing security challenges in vehicular slicing.	A concrete answer needs to be found to the problem that was raised, and problems with other types of slices also need to be fixed.
Vidhani and Vidhate [15]	2022	The authors investigated the security difficulties associated with 5G.	The topic of Network Slices vulnerabilities was not addressed.
Dangi <i>et al.</i> [16]	2022	The authors presented a framework for network slicing using machine learning, which encompasses potential risks and security breaches throughout the lifecycle of a network slice.	In addition to a slice's lifecycle, exploration of many vulnerable points of interest is necessary.
Salahdine <i>et al.</i> [17]	2022	The author discussed the topics of inter-slice and intra-slice security, as well as lifecycle security.	It is imperative to address attacks and dangers that are associated with other vulnerable areas.
Abood and Abdul-Majeed [18]	2023	The authors specifically focused on addressing only the threats associated with network slice enablers.	Threats and attacks about additional vulnerable areas of slices were not addressed.
Abir <i>et al.</i> [19]	2023	The authors explored the practical application of the 5G network in the healthcare sector.	The topic of attacks and threats was not addressed.
Sing <i>et al.</i> [20]	2023	The authors examined threat vectors and attack vectors within the realm of technical security.	No countermeasures were proposed to address the discussed attacks.
Sukumar <i>et al.</i> [21]	2024	The authors discuss the necessity of enhancing privacy and security in network slices.	The issue of attacks and threats on network slices is not adequately addressed while emphasizing the need for security in network slices.
Wala <i>et al.</i> [23]	2024	The authors thoroughly examine the potential security risks and vulnerabilities that may arise from the security architecture in 5G. They offer guidance on the optimal strategies for 5G network administrators to ensure the security of their networks.	Threats and attacks about additional vulnerable areas of slices were not addressed.

A viable strategy to deal with these difficulties is to utilize intent-based networking (IBN), an ongoing initiative introduced in the internet engineering task force (IETF) internet draft [24]. IBN is a novel networking approach that involves capturing decisions known as intents, translating them into policies, and configuring the physical/virtual network infrastructure based on those policies. This research presents an IBN-based network-slicing framework that offers an autonomous approach to managing cybersecurity. The system enables the creation, adaptation, and enforcement of cybersecurity policies dynamically, thereby mitigating the detrimental effects of cyber-attacks. The research work presented here has several notable contributions:

- Develop a conceptual framework with the IBN manager integrated into the network-slicing architecture to facilitate the implementation of automated security controls.
- Address the issue of distributed denial of service (DDoS) attacks, specifically focusing on TCP flooding and address resolution protocol (ARP) spoofing through the implementation of an experimental test bed.
- Compare the proposed model's performance with that of the static network slicing architecture using the parameters of availability, packet loss, response time, CPU, disk, and memory utilization.

The following sections of this work are organized in the following way. Section 2 provided a detailed and sequential account of the experimental approach, focusing on the methods. Section 3 provides a detailed account of the experimental procedure and the outcomes obtained from the experiment. The findings of the results are further elaborated upon in this part as well. Section 4 presents the final findings and conclusions of this study endeavor.

## 2. METHOD

The main objective of this research is to develop, implement, assess, and validate innovative architectural solutions, methods for specifying and enforcing policies, and security mechanisms. These will enable the network component to organize and configure itself to effectively counteract cybersecurity attacks autonomously. To do this, the SDN architecture will be expanded by incorporating IBN, enabling the creation, modification, and enforcement of cybersecurity policies dynamically illustrated in Figure 1. The methodology consists of the following steps:

- Initially, a Mininet emulator is established within a virtual environment to identify and mitigate DDoS attacks. The proposed method utilizes entropy-based techniques and is implemented as a Python script in SDN environments that is integrated into an SDN controller.
- Another method is created in a similar Mininet context by comparing the IP header with the Ethernet header to detect ARP spoofing. The implementation of both the detection and mitigation methods is carried out by a Python script within the context of SDN settings, which is seamlessly integrated into an SDN controller.
- A framework is proposed to integrate the IBN manager with the SDN controller in the network slicing architecture. This integration aims to automate the process of attack detection and mitigation.
- An experimental test environment has been set up to assess the performance of a network slicing framework in comparison to a static framework. Various parameters are being considered in this evaluation.

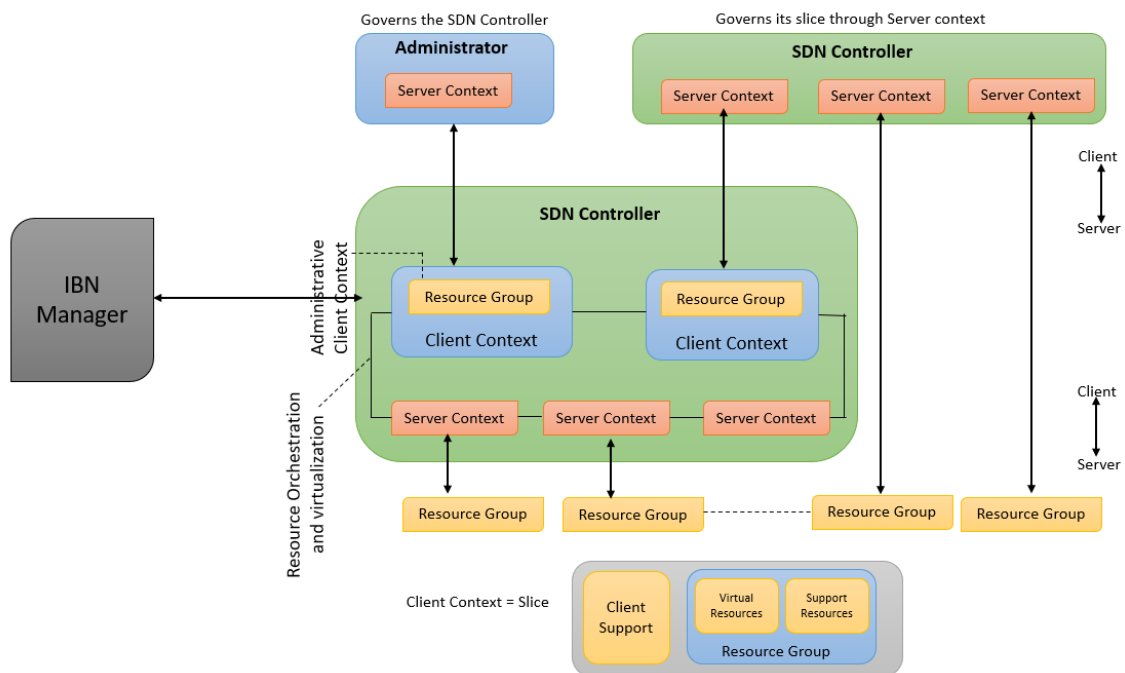


Figure 1. Modified architecture of SDN with IBN

### 2.1. DDoS attack detection and mitigation

DDoS attack, the victim is subjected to a barrage of incoming traffic that originates from numerous diverse sources. This phenomenon renders the prevention of the attack through the blocking of a singular source unfeasible. Sample Entropy is a technique used to detect DDoS attacks in SDN environments. DDoS detection involves two key components: window size and a threshold. The size of the window can be determined either by a specific time interval or by the number of packets. The calculation of entropy is performed within this specific context to quantify the level of uncertainty associated with the upcoming packets.

### 2.2. Measuring the randomness

The primary rationale for selecting entropy is its capacity to quantify the level of randomness inside a network. There is a direct relationship between the level of randomness and the level of entropy. As randomness increases, entropy also increases, and vice versa. Consider a set of data, denoted as  $W$ , which contains  $n$  elements. Let  $X$  represent an event that occurs within this set. Next, the occurrence of event  $X$  in situation  $W$  is demonstrated (2). To get the entropy, denoted as  $H$ , we compute the probability of each element in the set and then add them together, as seen in (3).

$$W = \{X_1, X_2, X_3, \dots, X_n\} \quad (1)$$

$$P_i = \frac{x_i}{n} \quad (2)$$

$$H = \sum_{i=1}^n P_i \log P_i \quad (3)$$

When all elements have equal probabilities, the entropy reaches its maximum. When one element is more prevalent than the others, the entropy decreases. The window size refers to the size of  $W$ . When dealing with a continuous stream of incoming data, such as packet headers, it is necessary to divide it into equal sets known as windows. Every element in the window is tallied along with its frequency. As an example, if the window contains 64 elements and each element appears only once, the resulting entropy value will be 1.80. When a single element occurs 10 times, the resulting entropy value is 1.64. This characteristic of entropy will be utilized to compute the level of unpredictability in the SDN controller.

#### 2.1.2. Entropy for DDoS detection

This research utilizes entropy as a method for detecting DDoS attacks in SDN. Understanding DDoS detection using entropy requires considering two crucial factors: window size and threshold. The window size can be determined by either a specific time period or the number of packets. Entropy is calculated in this window to gauge the level of uncertainty in the upcoming packets. In order to identify an attack, it is necessary to establish a threshold. When the calculated entropy exceeds or falls below a certain threshold, an attack is detected, depending on the scheme. In the research work of Mousavi and St-Hilaire [25], it was mentioned that the threshold entropy for DDoS detection is 1.3 for the window size of 50. If the entropy falls below a certain threshold and five consecutive windows exhibit lower entropy than the threshold, it indicates the occurrence of an attack. The detecting and mitigating code follows the sequence of stages outlined in Figure 2.

### 2.2. Detection and mitigation of ARP spoofing attack

The term "ARP" is an acronym for address resolution protocol, a protocol utilized to establish a correspondence between an internet protocol (IP) address and the physical address of a computer within a local network. The ARP spoofing attack is employed as a means of executing cache poisoning by surreptitiously introducing counterfeit <IP, MAC> mappings into the ARP cache of targeted victims. The attack can be classified into two distinct categories, namely request attacks and response/reply attacks. The detecting and mitigating code follows the sequence of stages outlined in Figure 3.

One measure to mitigate the occurrence of ARP cache spoofing or poisoning among hosts within the same SDN environment is to implement preventive measures. The POX controller assesses the legitimacy of ARP packets by categorizing them into request and reply types and subsequently verifying if they adhere to specific criteria that classify them as malicious.

- Detection of ARP request attacks.
- Detection of ARP reply attacks.
- Mitigation of ARP spoofing attacks.

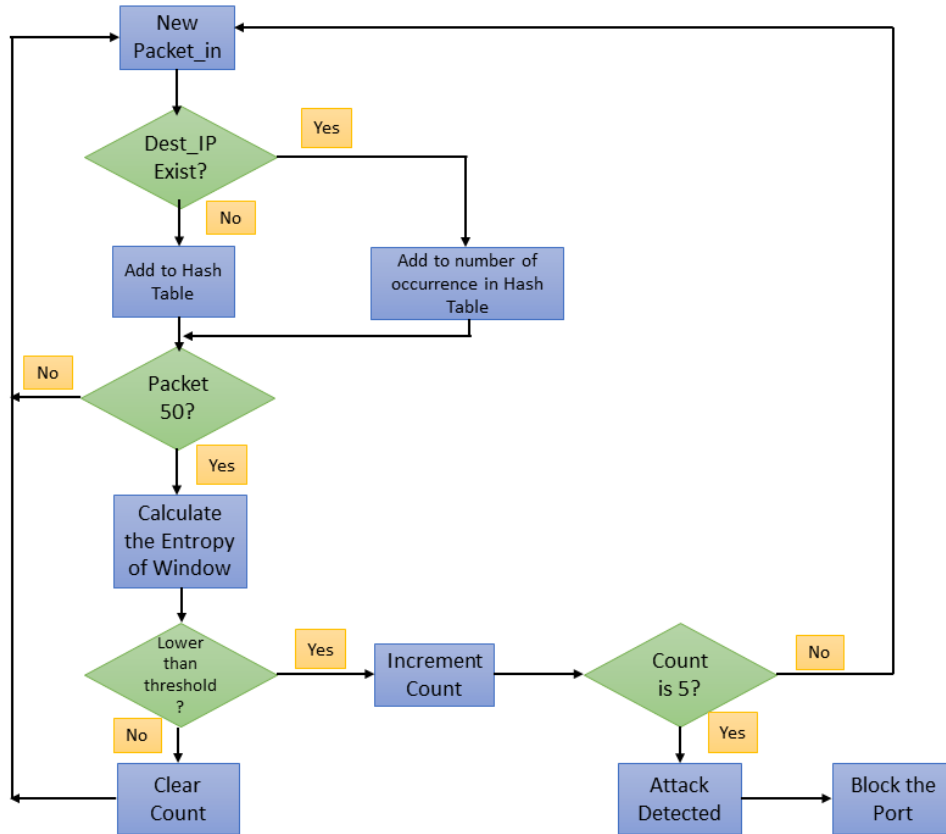


Figure 2. Flow chart of DDoS attack detection and mitigation

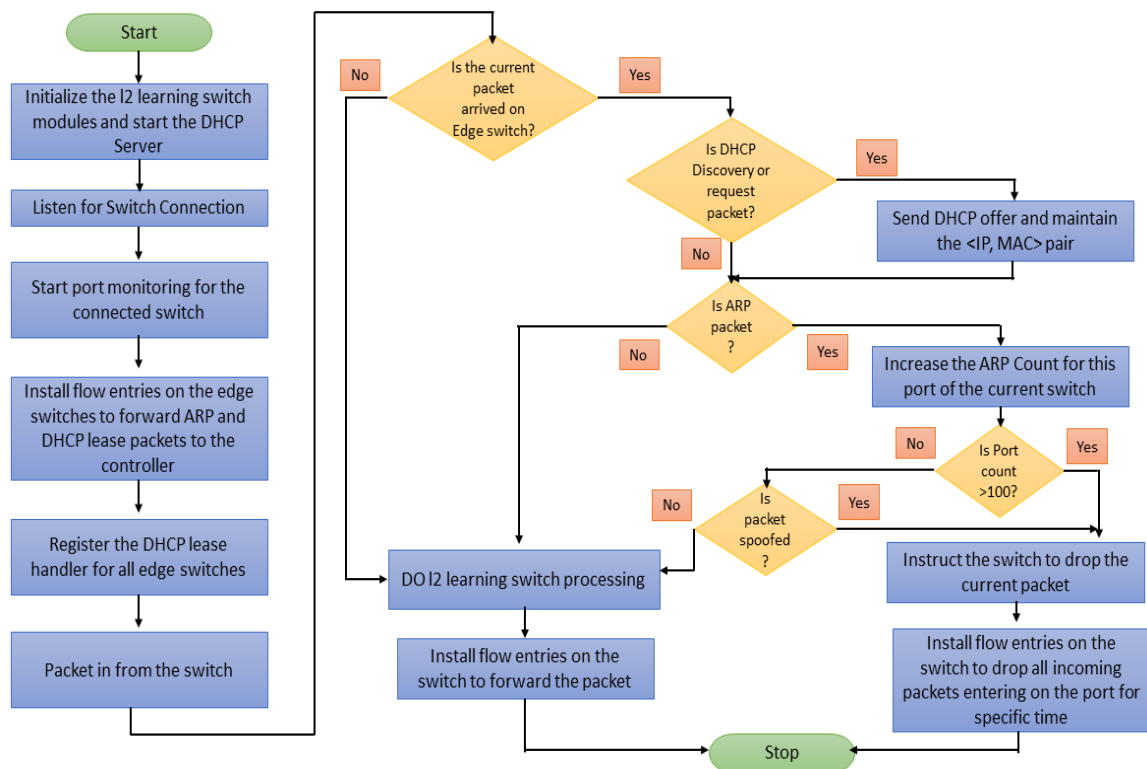


Figure 3. Flowchart of ARP spoofing detection

### 2.3. Proposed framework

Security issues are becoming more prominent as network-slicing technology develops further. There is a security policy that corresponds to the goals of each slice. Efficient management of security standards is crucial for each slice, as they may vary depending on the perspective of the network operator or the end user.

The security architecture of network slicing is depicted in Figure 4. Highlighting the crucial role of intent-based automation, secure platforms, and network analytics in ensuring the security of network slicing. Given the importance of network slicing in enabling network isolation, it becomes essential to prioritize the protection of each individual slice. Utilizing intent-based automation, with closed-loop control mechanisms to analyze intricate attack patterns, proves to be a highly effective approach in handling various complex attack scenarios. Ensuring the security of network slices is a critical concern throughout their entire life cycle, as they may provide more security compared to other types of public network connectivity. Understanding the significance of micro-segmentation is crucial for maintaining secure slice isolation in a multi-cloud system. The importance of machine learning in maintaining network slicing security has grown due to the rising complexity and sophistication of security attacks. This has made traditional algorithms insufficient for detecting these attacks, as noted by Dangi *et al.* [16].

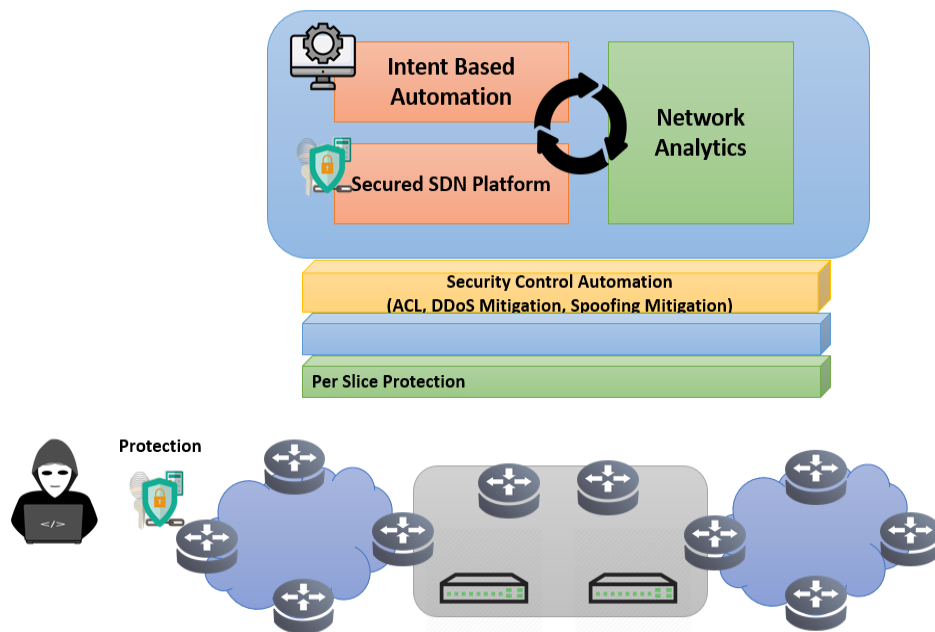


Figure 4. Proposed network slicing security architecture

### 2.4. Implementation and comparison

The conceptual framework with the IBN manager integrated into the network-slicing architecture to facilitate the implementation of automated security controls is developed in a simulation environment which is illustrated in the following section. Then compare the proposed model's performance with that of the static network slicing architecture using the parameters of availability, packet loss, response time, CPU, disk, and memory utilization.

## 3. RESULTS AND DISCUSSION

The experiment involves the deployment of a cutting-edge test bed for secure slice orchestration and management. This test bed consists of multiple components: the IBN platform, the open-source mobile network orchestrator (MANO), the open network operating system (ONOS) SDN slice controller, the monitoring system, and the Mininet host. These components work together to create a network slice that enables efficient data communication. The performance evaluation aims to analyze the effectiveness of our approach and assess the overall functionality of the network slice, rather than solely focusing on the performance of individual virtual functions. This study will consider the availability, packet loss, response time, disk usage, CPU consumption, and memory utilization as comparison metrics when comparing dynamic versus static architecture. Our goal is to confirm that the suggested architecture yields superior

results concerning the parameters specified before. To achieve this purpose, we employ open-source tools that can install network slices. The open-source MANO (OSM) platform functions as an orchestrator and manager of network services. It enables the efficient allocation of needed resources by establishing communication with the ONOS across both physical and virtual infrastructure. In addition, ONOS possesses virtualization capabilities that aid in the deployment of virtual network functions (VNFs) for both core and RAN networks. Table 2 presents a concise overview of the characteristics of the test-bed components.

Table 2. Experimental setup specifications and configurations

Components	System Specification
ONOS SDN controller	OS: Ubuntu 20.2 LTS RAM: 16 GB CPU: Core i5 (3 GHz) SSD: 500 GB
Open-source MANO	OS: Ubuntu 18.04 RAM: 16 GB CPU: Core i7 (3.6 GHz) HDD: 1 TB OSM Version: 7
IBN Tool/GUI	OS: Windows 10 RAM: 16 GB CPU: Core i5 (3 GHz) HDD: 1 TB Programming Language: Python Database: MySQL
Host (NS) 1-8	Mininet Virtual Box OS: Ubuntu 18 LTS RAM: 4 GB

The web-based graphical user interface (GUI) portal of the IBN platform is seen in Figure 5. This portal allows users to specify their desired service requirements by defining intents. Afterwards, the policy configurators transform these intentions into slice templates for the underlying orchestrators. Just like a data scientist, the slice template is sent to the OSM and ONOS SDN-RAN controller to distribute the slice resources across the core and RAN domains. Policy configurators in the IBN communicate with the OSM and RAN controller through the use of the representational state transfer (REST) application programming interface (API). Figure 5 shows the current deployment status of VNFs that have been set up through the IBN portal, using the OSM and ONOS frameworks.

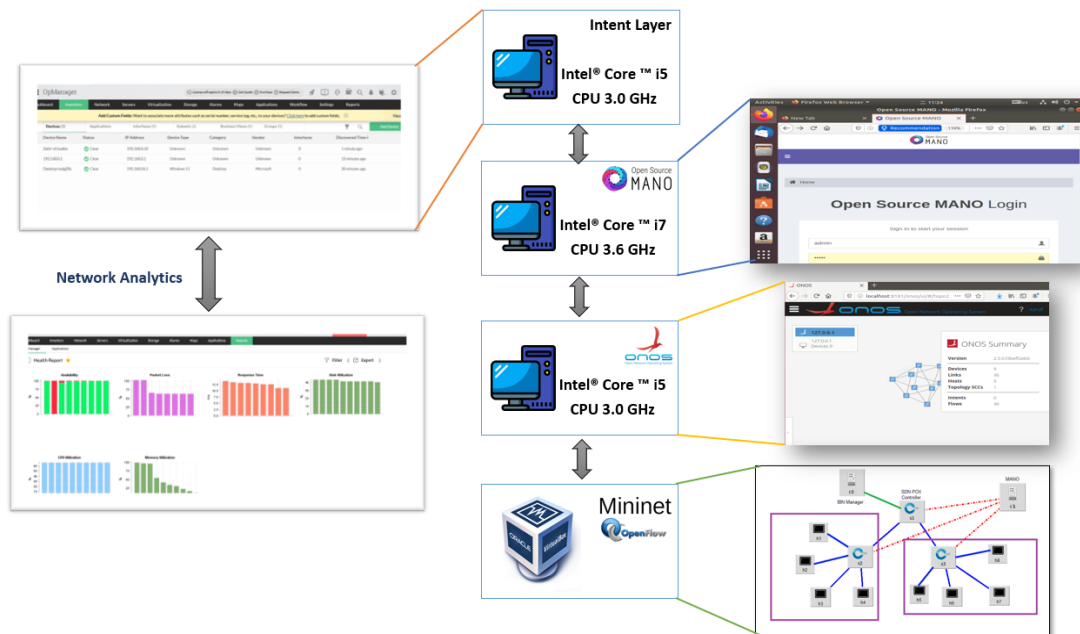


Figure 5. Experimental set-up of IBN-based slicing system



The ONOS framework is linked to 8 Mininet hosts that serve as representations of 8 network slices. These slices are specifically built for data exchange in mobile networks, particularly the internet. FlexRAN is a RAN controller that establishes a bridge connection between NSs and the RAN through the eNodeB. During the simulation, the traffic load for both NSs and RAN is spread randomly. A Python script, executed from a selected host in slice 1, runs a code that simulates launch traffic. This code produces a random source IP and delivers packets to randomly picked destinations among the hosts. Next, the SDN controller calculates the entropy, which exceeds the specified threshold. The threshold value for entropy and other parameters used in the IBN policy to detect the DDoS attack reported by Mousavi and St-Hilaire [25]. Subsequently, a separate python script, which includes the code to initiate an attack, is executed from certain hosts assigned to slice 7 and 8, targeting specific entities from slice 1 to 6. Once the attack is initiated, the entropy value decreases. The controller detects this decline and, using the intent layer policy, blocks the specific port in the switch if the entropy value drops below a given threshold. Subsequently, the port is deactivated. An analogous situation is also created with ARP spoofing. The research effort is strengthened by the use of an intent layer policy, which enables dynamic and rapid action to be done.

### 3.1. Impact of availability

The impact of network slice availability in two scenarios is depicted in Figure 6. The graph's horizontal axis depicts the quantity of network slices, while the vertical axis reflects the availability proportion. There are two distinct categories of data: the first is represented by the diamond grid, which signifies the availability of data in the absence of the implementation of the IBN policy, while the second category, represented by the diagonal stripe pertains to the availability data with the IBN security policy being implemented. The availability percentage of slice 1 through 6 is approximately zero, indicating that it is not accessible. The cause of this occurrence can be attributed to the DDoS attack initiated by the specific hosts from slice 7 and 8. The absence of a security policy results in the unavailability of the slice for the tenant due to this attack. In the second scenario, implementing the IBN security policy enables the detection and mitigation of potential attacks. In this scenario, the network slices remain accessible to the tenant. In addition to detecting and mitigating DDoS attacks, additional security risks such as ARP Spoofing are also identified and addressed in other network slices. As a result, implementing the IBN policy leads to a comparatively greater availability percentage.

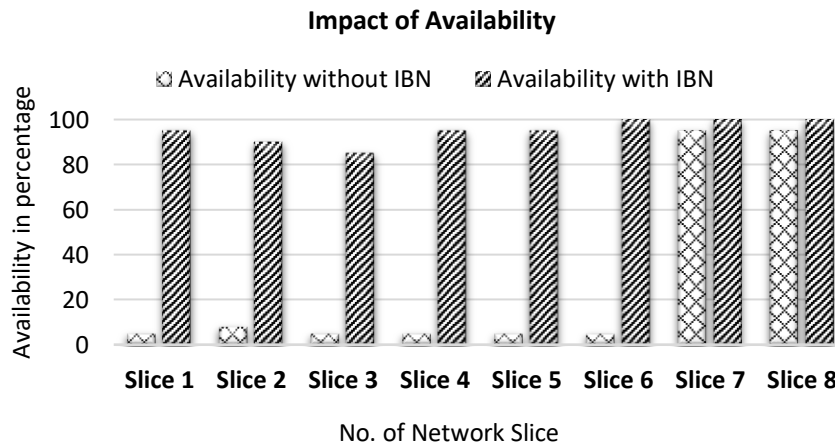


Figure 6. Impact of NS availability comparison

### 3.2. Impact of packet loss

The depiction of the impact of network slice packet loss in two circumstances can be observed in Figure 7. The graph's horizontal axis represents the number of network slices, while the vertical axis represents the packet loss percentage. There exist two distinct classifications of data: the initial classification is denoted by the diamond grid, which signifies the packet loss data without implementing the IBN policy. Conversely, the subsequent classification, represented by the diagonal stripes, pertains to the packet loss data when the IBN security policy is implemented. The observed packet loss percentages for slice 1 and 2 are significantly high, approaching 100%, which can be attributed to a combination of security attacks DDoS and firewall policy issues. It is worth noting that these two slices are located outside the local area network (LAN) confines. The network topology consists of a LAN where slices 3 to 8 are interconnected. The measured packet loss is

relatively minimal, which can be attributed to the occurrence of ARP spoofing. Based on the depicted figure, it is evident that the IBN security policy exhibits effective detection and mitigation of security attacks, resulting in a comparatively lower packet loss compared to the absence of the IBN security policy.

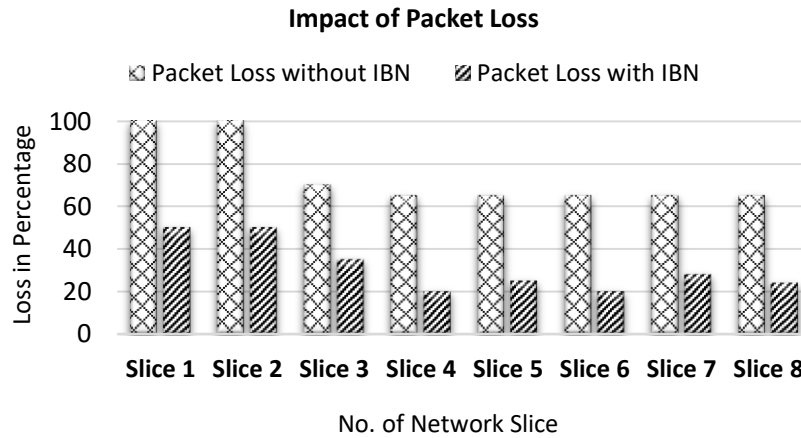


Figure 7. Impact of NS packet loss comparison

**3.3. Impact of slice response time**

The illustration of the influence of network slice reaction time in two scenarios can be viewed in Figure 8. The x-axis of the graph depicts the quantity of network slices, and the y-axis indicates the response time measured in milliseconds (ms). The graph demonstrates that network slices without implementing the IBN security policy exhibit a noticeably higher response time, specifically 12 ms. The achieved reaction time of 1 ms satisfies the specified criterion of the 5G network technology standard when the IBN security policy is used.

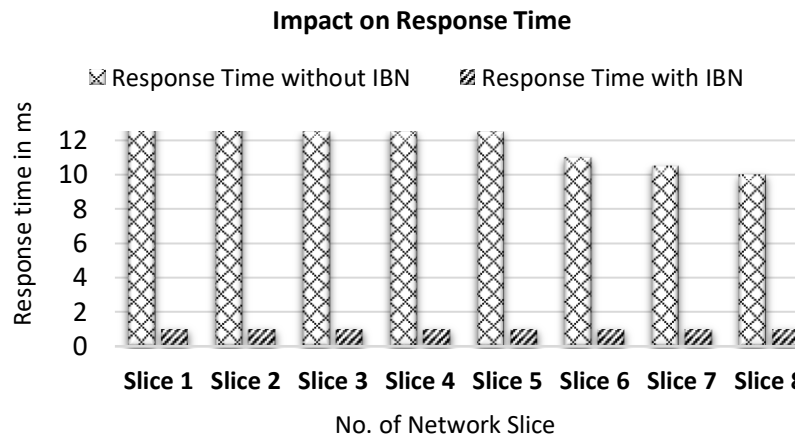


Figure 8. Impact of NS response time comparison

**3.4. Impact of disk utilization**

Figure 9 illustrates the influence of network slice disk utilization in two different circumstances. The graph's horizontal axis represents the number of network slices, while the vertical axis represents the percentage of disk utilization. The graph provides unambiguous evidence that network slices lacking the application of the IBN security policy exhibit a significantly higher level of disk utilization, especially ranging from 38% to 45% of the entire disc capacity. The utilization of disc space ranges from 20% to 35% of the overall capacity when employing the IBN security strategy, providing evidence of effective identification and resolution of security breaches.

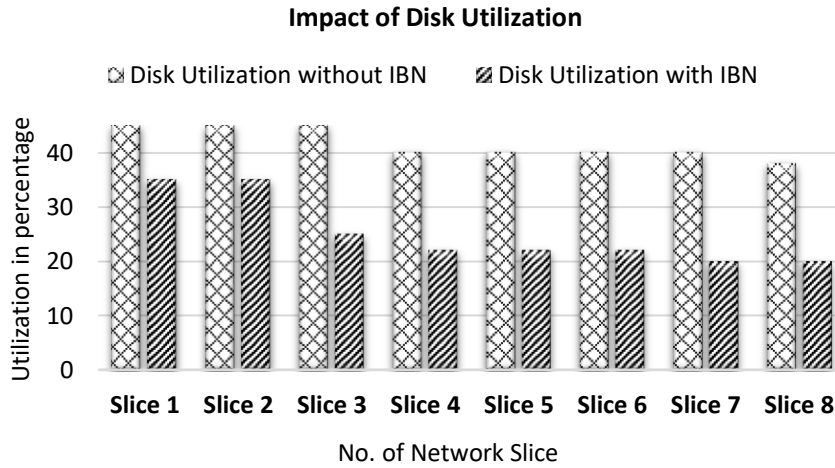


Figure 9. Impact of NS disk utilization comparison

**3.5. Impact of CPU utilization**

Figure 10 illustrates the network slice average CPU utilization for RAN controller representation in two scenarios. The x-axis of the graph shows the number of network slices, while the y-axis reflects the proportion of CPU utilization. The graph presents clear evidence indicating that network slices without implementing the IBN security policy demonstrate a notably elevated level of CPU utilization, particularly at 70%. The CPU utilization exhibits a range of 50% to 60% when using the IBN security strategy, indicating successful detection and remediation of security breaches. Regarding data connectivity, particularly concerning devices linked to the RAN through eNodeB, internet access, video calling, and other applications are utilized. The CPU use remains high even after reducing the number of attacks and before the attack generated i.e., 45% to 58%.

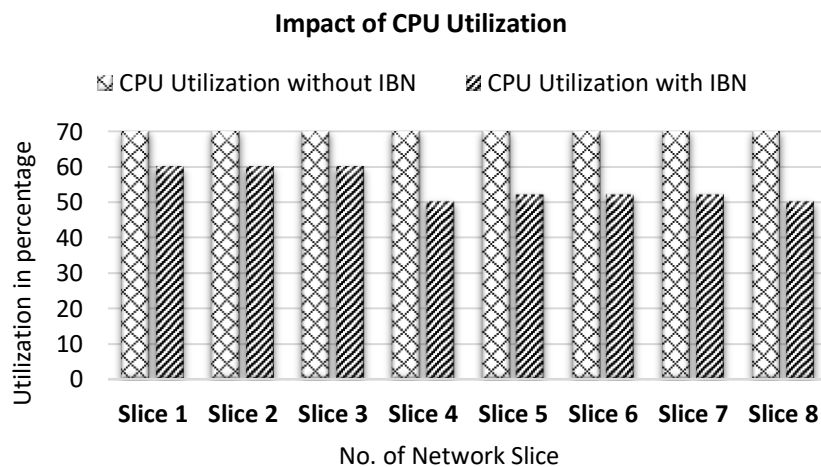


Figure 10. Impact of NS average CPU utilization comparison

**3.6. Impact of memory utilization**

The illustration of the influence of network slice memory utilization in two scenarios is depicted in Figure 11. The x-axis of the graph shows the number of network slices, whereas the y-axis reflects the proportion of memory utilization. The graph proves that network slices without implementing the IBN security policy have a much greater degree of memory utilization, mainly ranging from 35% to 90% of the total memory capacity. The IBN security policy demonstrates successful discovery and resolution of security breaches, as evidenced by using memory space ranging from 30% to 55% of the overall capacity.

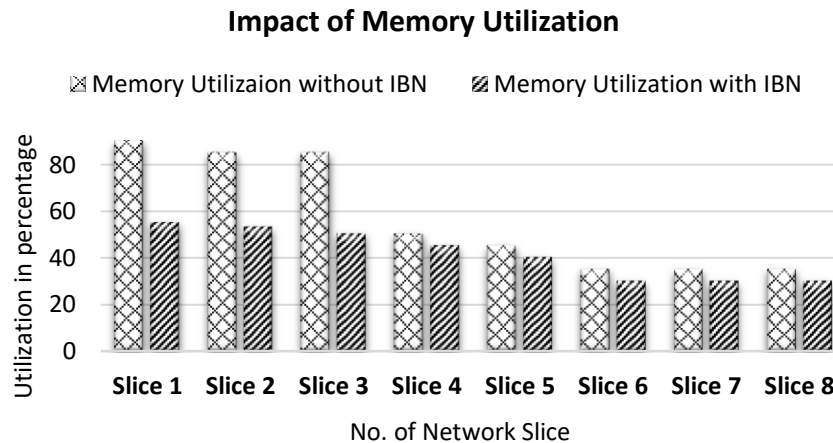


Figure 11. Impact of NS memory utilization

#### 4. CONCLUSION

Effective network slicing management is detailed in this article, along with the design and implementation of the system that uses intent-based technology. This framework's main goal is to automate the process of finding and preventing security breaches. The IBN system's policy configuration can be used to design a slice template's security. To speed up the deployment process, these configurations are then sent to the network orchestrator and SDN controller. Concerning its main characteristics, the framework has been empirically validated. Test results for availability, packet loss, response time, CPU, memory, and disk utilization demonstrate the installed system's remarkable effectiveness and capacity to manage growing demands. Extensive 5G testing is now quite difficult. The results obtained from our little testbed have great significance in this new area of research because they are based on actual experiments.

#### ACKNOWLEDGEMENT

The authors are grateful for a Doctor of Philosophy (Ph.D.) Research Fellowship from the ICT Division of the Ministry of Posts, Telecommunications, and Information Technology of the Government of the People's Republic of Bangladesh. The authors also acknowledge the partial funding from Jashore University of Science and Technology, Bangladesh for this research.




#### REFERENCES

- [1] P. Subedi *et al.*, "Network slicing: a next generation 5G perspective," *Eurasip Journal on Wireless Communications and Networking*, no. 1, Apr. 2021, doi: 10.1186/s13638-021-01983-7.
- [2] S. Wong, B. Han, and H. D. Schotten, "5G network slice isolation," *Network*, vol. 2, no. 1, pp. 153–167, Mar. 2022, doi: 10.3390/network2010011.
- [3] A. Cardenas and D. Fernandez, "Network slice lifecycle management model for NFV-based 5G virtual mobile network operators," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2020 - Proceedings*, Nov. 2020, pp. 120–125, doi: 10.1109/NFV-SDN50289.2020.9289883.
- [4] Y. Li and M. Chen, "Software-defined network function virtualization: a survey," *IEEE Access*, vol. 3, pp. 2542–2553, 2015, doi: 10.1109/ACCESS.2015.2499271.
- [5] Y.-Z. Chen, T. Y.-H. Chen, P.-J. Su, and C.-T. Liu, "A brief survey of open radio access network (O-RAN) security," *arXiv:2311.02311*, Nov. 2023.
- [6] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, May 2017, doi: 10.1109/MCOM.2017.1600951.
- [7] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: a survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018, doi: 10.1109/COMST.2018.2815638.
- [8] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, Jun. 2019, doi: 10.1109/MWC.2019.1800234.
- [9] A. Mathew, "Network slicing in 5G and the security concerns," in *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*, Mar. 2020, pp. 75–78, doi: 10.1109/ICCMC48092.2020.ICCMC-00014.
- [10] Chandini, S. Verma, Kavita, N. Z. Jhanjhi, M. N. Talib, and G. Kaur, "A canvass of 5G network slicing: architecture and security concern," *IOP Conference Series: Materials Science and Engineering*, vol. 993, no. 1, Dec. 2020, doi: 10.1088/1757-899X/993/1/012060.
- [11] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, Feb. 2020, doi: 10.1016/j.comnet.2019.106984.




- [12] R. F. Olimid and G. Nencioni, "5G network slicing: a security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020, doi: 10.1109/ACCESS.2020.2997702.
- [13] J. Cao *et al.*, "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 170–195, 2020, doi: 10.1109/COMST.2019.2951818.
- [14] J. Wang and J. Liu, "Secure and reliable slicing in 5G and beyond vehicular networks," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 126–133, Feb. 2022, doi: 10.1109/MWC.001.2100282.
- [15] S. M. Vidhani and A. V. Vidhate, "Security challenges in 5G network: a technical features survey and analysis," in *5th IEEE International Conference on Advances in Science and Technology, ICASST 2022*, Dec. 2022, pp. 592–597, doi: 10.1109/ICASST55766.2022.10039654.
- [16] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, "ML-based 5G network slicing security: a comprehensive survey," *Future Internet*, vol. 14, no. 4, Apr. 2022, doi: 10.3390/fi14040116.
- [17] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 23–38, 2022, doi: 10.1109/OJCS.2022.3161933.
- [18] M. J. K. Abood and G. H. Abdul-Majeed, "Classification of network slicing threats based on slicing enablers: a survey," *International Journal of Intelligent Networks*, vol. 4, pp. 103–112, 2023, doi: 10.1016/j.ijin.2023.04.002.
- [19] S. M. Abu Adnan Abir, M. Abuibaid, J. S. Huang, and Y. Hong, "Harnessing 5G networks for health care: challenges and potential applications," in *2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023*, Jul. 2023, vol. 21, pp. 1–6, doi: 10.1109/SmartNets58706.2023.10215757.
- [20] P. K. Singh, M. Brahma, P. Nath, and U. Ghosh, "A study on secure network slicing in 5G," in *Proceedings - 23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW 2023*, May 2023, vol. 2, pp. 52–61, doi: 10.1109/CCGridW59191.2023.00023.
- [21] A. Sukumar, A. Singh, A. Gupta, and M. Singh, "Enhancing security and privacy implications in 5G network slicing," in *2024 4th International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2024*, Jan. 2024, pp. 1–8, doi: 10.1109/ICAECT60202.2024.10469006.
- [22] E. Kline, S. Ravi, D. Cousins, and S. Rv, "Securing 5G slices using homomorphic encryption," in *IEEE Wireless Communications and Networking Conference, WCNC*, Apr. 2022, vol. 2022-April, pp. 43–48, doi: 10.1109/WCNC51071.2022.9771895.
- [23] F. B. Wala and M. Kiran, "5G network security practices: an overview and survey," *arXiv preprint arXiv:2401.14350*, Jan. 2024.
- [24] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, *Intent-based networking - concepts and definitions*, RFC 9315, Internet Research Task Force (IRTF), 2022.
- [25] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 International Conference on Computing, Networking and Communications, ICNC 2015*, Feb. 2015, pp. 77–81, doi: 10.1109/ICNC.2015.7069319.

## BIOGRAPHIES OF AUTHORS






**Md. Zahirul Islam**    obtained a B.Sc. (Hons) in electronics and telecommunication engineering (ETE) from Daffodil International University and an M.Sc. in information and communication technology (ICT) from IICT, Bangladesh University of Engineering and Technology (BUET). He is currently pursuing a Ph.D. in computer science and engineering at Jashore University of Science and Technology in Bangladesh. His research interests include cybersecurity, computer networking, and wireless communication. He is currently employed as an assistant professor at Daffodil International University. He can be reached via email at zahirete@student.just.edu.bd.



**Syed Md. Galib**    is a professor in the Department of Computer Science and Engineering (CSE) at Jashore University of Science and Technology (JUST), Bangladesh. He earned a bachelor of science in computer science and engineering from Khulna University in Bangladesh. He earned a master of science in computer engineering with a specialization in artificial intelligence from Dalarna University in Sweden. Swinburne University of Technology, Australia, conferred upon him a Ph.D. degree. His primary area of research is the application of artificial intelligence and image processing to the field of social development. He can be reached via email at galib.cse@just.edu.bd.



**Md. Humaun Kabir**    obtained a B.Sc. (Hons) and an MS in physics from the University of Dhaka, Bangladesh. He received a Ph.D. degree in information and communication engineering from Inha University in South Korea, and subsequently was awarded a post-doctoral fellowship at the same institution. In addition, he also served as a postdoctoral fellow at Hanyang University in the same country. His research interests encompass interference mitigation, molecular communication, nanonetworks, wireless body area networks, and nanochannel modeling. He can be reached at email: mhkabar@just.edu.bd.