

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/376953392>


Optimizing Network Security and Performance Through the Integration of Hybrid GAN-RNN Models in SDN-based Access Control and Traffic Engineering

Article in International Journal of Advanced Computer Science and Applications · December 2023
DOI: 10.14569/IJACSA.2023.0141262

CITATIONS
8

READS
132


7 authors, including:



Ganesh Khekare
Vellore Institute of Technology

48 PUBLICATIONS 393 CITATIONS


SEE PROFILE



Naga Prasanthi
Lakireddy Bali Reddy College of Engineering

17 PUBLICATIONS 35 CITATIONS


SEE PROFILE



Dr. Mohammed Saleh Al Ansari
University of Bahrain

126 PUBLICATIONS 604 CITATIONS

SEE PROFILE



Yousef Abubaker Mohamed Ahmed El-Ebiary
Universiti Sultan Zainal Abidin | UniSZA

148 PUBLICATIONS 1,431 CITATIONS

SEE PROFILE

Optimizing Network Security and Performance Through the Integration of Hybrid GAN-RNN Models in SDN-based Access Control and Traffic Engineering

Ganesh Khakare¹, Dr.K.Pavan Kumar², Kundeti Naga Prasanthi³, Dr. Sanjiv Rao Godla⁴,
Venubabu Rachapudi⁵, Dr. Mohammed Saleh Al Ansari⁶, Prof. Ts. Dr. Yousef A.Baker El-Ebiary⁷

Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India¹

Sr Asst.Prof, Dept.of IT, Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada -07²

Dept.of CSE, Lakireddy Balireddy College of Engineering, Mylavaram³

Professor, Department of CSE (Artificial Intelligence & Machine Learning), Aditya College of Engineering & Technology, Surampalem, Andhra Pradesh, India⁴

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522302⁵

Associate Professor, College of Engineering-Department of Chemical Engineering, University of Bahrain, Bahrain⁶
Faculty of Informatics and Computing, UniSZA University, Malaysia⁷

Abstract—By offering flexible and adaptable infrastructures Software-Defined Networking (SDN) has emerged as a disruptive technology that has completely changed network provisioning and administration. By seamlessly integrating Hybrid Generative Adversarial Network-Recurrent Neural Network (GAN-RNN) modeling into the foundation of SDN-based traffic engineering and accessibility control methods, this work presents a novel and comprehensive method to improve network efficiency and security. The proposed Hybrid GAN-RNN models address two important aspects of network management: traffic optimization and access control. They combine the benefits of Generative Adversarial Networks (GANs) and Recurrent Neural Networks (RNNs). Traditional traffic engineering techniques frequently find it difficult to quickly adjust to situations that are changing quickly within today's dynamic networking environments. The models' capacity to generate synthetic traffic patterns that nearly perfectly replicate the complexity of real network traffic demonstrates the power of GANs. Network administrators can now allocate resources and routing methods more dynamically, as well as in responding to real-time network inconsistencies, due to this state-of-the-art technology. The technique known as Hybrid GAN-RNN addresses the enduring problem of network security. With their reputation for continuous learning and by utilizing Python software, recurrent neural networks (RNNs) are at the forefront of developing flexible management of access rules. With an incredible 99.4% accuracy rate, the "Proposed GAN-RNN" approach outperforms the other approaches. A comprehensive evaluation of network traffic and new safety risks allow for the immediate modification of these policies. This work is interesting because it combines hybrid GAN-RNN algorithms to strengthen security protocols with adaptive access control while also optimizing network efficiency through realistic traffic modeling.

Keywords—Software-defined networking; generative adversarial networks; recurrent neural networks; traffic engineering

I. INTRODUCTION

Network performance directly impacts the efficiency of operations within an organization. Faster data transfer and lower latency lead to increased productivity, reduced downtime, and better user experiences, all of which are critical in today's fast-paced digital world [1]. Slow or unreliable networks result in poor user experiences. This can frustrate customers, employees, and partners, leading to dissatisfaction and potentially driving them away. Ensuring a high-performing network enhances user satisfaction and loyalty. In an era where data is a valuable asset, efficient network performance is crucial for transferring large volumes of data quickly and securely [2]. This is especially important for industries like healthcare, finance, and media, where sensitive information needs to be transmitted reliably. Cyber security threats are on the rise, and networks are prime targets for attacks. A secure network helps protect sensitive data, prevents unauthorized access, and mitigates risks associated with data breaches, which can have severe legal, financial, and reputational consequences. Many industries and organizations must adhere to strict regulatory compliance standards regarding data security and privacy. Maintaining a secure network is essential to meeting these requirements and avoiding legal penalties. A well-optimized network ensures that network resources, such as bandwidth and hardware, are used efficiently. This reduces costs associated with network maintenance and upgrades while maximizing resource availability [3]. Network failures or security breaches can disrupt business operations, leading to downtime and financial losses. Ensuring network resilience and security is crucial for business continuity and disaster recovery planning. As businesses grow, their network needs often grow too. A well-optimized network can scale to accommodate increased traffic, new devices, and expanding operations without

sacrificing performance or security. Organizations with high-performing, secure networks can gain a competitive advantage [4]. They can offer faster services, better customer experiences, and innovative solutions that competitors with subpar networks may struggle to match. Improved network performance and security enable the adoption of advanced technologies like IoT (Internet of Things), cloud computing, and AI, which can drive innovation and digital transformation within an organization. Innovative solutions are required due to the constantly changing network infrastructure landscape in order to improve security and performance. SDN, or software-defined networking, has become a game-changing network management technology that gives network administrators the freedom to customize access control and traffic engineering [5]. In order to enhance network performance and security in SDN settings, this study investigates a unique method that combines hybrid generative adversarial networks (GANs) with recurrent neural networks (RNNs). The project intends to address important issues in traffic engineering and access control by smoothly integrating these cutting-edge machine learning approaches, leading to ultimately more effective and secure network operations [6]. The article digs into the principles of Software-Defined Networking (SDN) and discusses how it applies to contemporary network architecture. It gives an overview of how SDN can provide centralized network administration and dynamic traffic engineering by separating the control and data planes. As a prelude to the suggested remedy, the section also illustrates the difficulties in optimizing traffic flows in SDN settings [7].

The use of techniques based on machine learning has a lot of potential to enhance network performance in several ways. ML algorithms have the capacity to analyse network data, adjust to changing circumstances, and make choices in real time, which can improve network operations' efficiency, dependability, and security. ML models can spot unusual network activity that may indicate security risks or performance problems. Network assaults may be swiftly detected and responded to by intrusion detection systems (IDS) and intrusion prevention systems (IPS) driven by ML, improving security while minimizing service interruption [8]. Applications will perform better and use resources more effectively as a result of getting the resources they require when they need them. To maintain equitable server utilization, ML models may track server load and distribute requests that arrive around servers. Based on past data and user behavior, ML may help forecast future network requirements [9]. This can assist network administrators in making plans for infrastructure or capacity modifications so that the network is ready to meet growing demand. For instance, during periods of high demand, they might give priority to particular sorts of traffic. GANs use a loss function that guides the training process. The generator's loss depends on how well the discriminator is fooled, while the discriminator's loss is based on its ability to distinguish real from fake data. The training aim to find a balance where the generator generates highly convincing data and the discriminator becomes uncertain about its classifications. Access control in the context of SDN is covered in the second part. It explains the idea of dynamic access control lists and discusses the significance of access control for network security [10]. It examines the difficulties

with access control in SDN, highlighting the requirement for more sophisticated and flexible security mechanisms.

The merging of Hybrid GANs and RNNs, the research's main novelty, is presented in the publication. It describes how RNNs may examine this data to find patterns and abnormalities using synthetic network traffic data produced by GANs. This hybrid strategy tries to simultaneously improve network security and performance. The practical use of the hybrid GAN-RNN models for traffic engineering is covered in this section. It offers information on how dynamic network traffic flow optimization may be accomplished using synthetic traffic data produced by GANs. The advantages of this strategy are explored in terms of decreased congestion, enhanced Quality of Service (QoS), and effective resource utilization. The research examines the use of hybrid GAN-RNN models in SDN access control. It explains how RNNs may inspect network traffic data for irregularities and security risks. The flexibility of this strategy to changing security threats is discussed, as is how it enhances access control by dynamically updating access lists in response to threat detection in real time. The article covers the overall effects of incorporating Hybrid GAN-RNN models into SDN settings, highlighting the enhancements to network security and performance. It also describes possible future avenues for study and application in the area of SDN-based traffic engineering and access management. The current limitation of these investigations is the lack of focus on scalability and real-world implementation, which makes it difficult to actually apply suggested security solutions in intricate network systems. Furthermore, there isn't much talk about possible interoperability issues, resource limitations, and how well these solutions may change to meet new threats in the cyberspace. A more thorough examination of these factors might improve the research findings' relevance and efficacy in real-world contexts.

Key contributions of the research include:

- Using traffic trends produced by GANs, SDN controllers can optimize the allocation of network resources, reducing latency and enhancing QoS. RNN-based authorization rules continuously identify trends in network activity, minimising potential vulnerabilities and adapting to new threats.
- By automating both access control and traffic design, the method lessens the operational load on the network's management and promotes more effective resource utilization.
- Assessing the efficacy of the hybrid GAN-RNN models in SDN scenarios through multiple simulations and real-world experiments. The results show notable gains in network security and effectiveness, highlighting the approach's potential for contemporary network management.
- This study offers a ground-breaking framework for utilizing the powers of hybrid GAN-RNN models to optimize software-defined networking. The next phase of network administration is anticipated with the

integration of flexible access controls and realistic traffic generation.

The Section I provides an overview of the paper. The Section II reviews existing literature and emphasizes the gap in addressing techniques for network security enhancement. Section III defines the central research problem concerning driver drowsiness detection complexities. Section IV outlines data collection, preprocessing, feature extraction, and the integration of Hybrid GAN-RNN. Section V presents empirical findings, compares classifier performance, and explores implications and future research directions in Section VI, which is solidifying the research's significance in Network security.

II. RELATED WORKS

Ramprasath and Seethalakshmi [11] examines a crucial element of SDN, focusing on the requirement for improved security controls in SDN systems. By separating the information plane from the control plane, SDN enables on-demand services and the ability to configure networks dynamically. The study correctly highlights the fact that, despite the fact that SDN controls traffic flows and flow labels based on Open Flow virtual switches successfully, it lacks built-in security safeguards to combat malicious traffic, such as Denial-of-Service (DoS) assaults, which can significantly lower service availability. It is laudable that the paper's main emphasis is on identifying and reducing DoS threats by dynamically setting firewalls within SDN setups. The study makes an effort to close this security gap by using dynamic access control lists. This study's noteworthy feature is the use of Mininet to simulate SDN with dynamic access control list attributes. This enables real-world testing and experimentation. The practical relevance of the findings is given more weight by this empirical confirmation. The work would benefit from a more thorough examination of the exact methods and tools employed for DoS attack detection and mitigation inside the SDN environment to further strengthen its contribution. Readers would have a better grasp of the suggested strategy if more information was provided about the dynamic access control list implementation and the standards for differentiating malicious from normal traffic. In order to reduce DoS attacks, the article tackles a critical security issue in SDN systems and offers a potential solution using dynamic access control lists. The research offers important insights towards strengthening the security of SDN systems by fusing theoretical understanding with real-world testing. The study would be even more helpful and effective if it elaborated on the technical specifics of the suggested strategy.

Vimal et al. [12] provides a fascinating and current investigation into how integrating Internet of Things (IoT) devices might improve the security of Software-Defined Networks (SDN), with an emphasis on boosting information access control using encryption. The research's emphasis on creating a strong infrastructure for IoT devices is well-placed given the quick spread of IoT devices. The notion of a stability routing protocol, which evaluates the reliability of devices and packet flows, is introduced in this work. To create dependable SDN routes, this method makes use of the mutual trust between network components, Quality of Service (QoS), and

energy circumstances. An important advancement is the incorporation of SDN architecture into the Cognitive Protocol Network (CPN) technology platform to improve energy efficiency. A novel strategy for tackling security issues is the use of stochastic neural networks (SNNs) for decentralized decision-making based on data gleaned from perceptual packets. It is a praiseworthy effort to include these components into SerIoT approaches to provide IoT encryption for information access control. The implementation of various techniques and technologies, particularly the precise approaches utilized for IoT encryption and access control, might need more explicit explanations in the study. The complexity of the study would also be increased by providing more detail on how the suggested network infrastructure solves issues like erratic connectivity, constrained cryptographic capacity, and energy restrictions. The study emphasizes the significance of tackling cluster instability for platform efficiency as well as the necessity of collaboration. A deeper grasp of the research's practical relevance might be provided by providing additional information on the difficulties and potential solutions linked to these issues.

Shin et al. [13] addresses the potential of Software-Defined Networking to improve network security as it goes into a crucial and modern junction of technology. Because it can separate control logic from conventional network hardware, SDN has attracted a lot of interest as a transformational technology that can improve network administration and innovation. The authors note that despite its capabilities, SDN is still largely disregarded by the security community, highlighting the underutilized potential of SDN in the area of network security. The article presents a thorough overview of the prospects offered by this technology by meticulously evaluating how the distinctive features and capabilities of SDN may strengthen network security and the larger information security process. This in-depth analysis of SDN's potential to advance network security research creates fresh directions for future study in this crucial area. The article does a good job of outlining the main ideas and goals, but it might make a bigger impact if it went into more detail with examples or case studies of how SDN has been used to successfully handle security issues. Giving readers specific examples of how SDN is used to enhance network security can help readers understand the real-world applications of the technology and may encourage more research projects. The report effectively discusses the important role that SDN may play in strengthening network security and sheds light on an exciting yet underappreciated field of study. It is a useful tool for academics and professionals who want to strengthen network security in the context of a changing technological environment by utilizing SDN's capabilities. Extending on actual use cases and useful implementations might increase the paper's impact and usefulness.

Ahmad et al. [14] focuses on the use of machine learning (ML) approaches to thwart Denial of Service (DoS) and Distributed DoS (DDoS) attacks inside the SDN framework. It provides a timely analysis of the essential confluence between Software Defined Networking (SDN) and security. With its logically centralized control plane, SDN offers enhanced network administration as a viable response to a number of

issues in conventional networks. But because of the security flaws introduced by this centralization, SDN control systems are becoming tempting targets for malicious attacks. Given ML's shown efficacy in finding security vulnerabilities, the paper made a sound decision to use ML approaches for recognizing and mitigating DoS and DDoS attacks. It is a useful addition to test these ML approaches in practice in an SDN system, especially by subjecting the SDN controller to DDoS attacks. It offers useful perceptions on the applicability and constraints of ML-based security methods for upcoming communication networks. The work may benefit from a more in-depth examination of the various ML approaches used and the standards for judging their efficacy. Readers would comprehend the use of ML models or algorithms to SDN security more clearly if examples or case studies of these applications were given. This article discusses security flaws resulting from centralized control, a serious issue in the SDN space. The work offers a significant addition to the area by outlining and assessing ML strategies to defend against DoS and DDoS assaults within SDN. It highlights the value of ML-based solutions in securing upcoming communication networks and provides a viable path for boosting network security. The paper's usefulness and effect would be increased with additional clarification of the ML approaches employed.

Pérez-Díaz et al. [15] provides a significant and pertinent addition to the continuing problem of LR-DDoS attack mitigation in the context of Software-Defined Networks (SDN). Due to the notoriously difficult-to-detect nature of LR-DDoS assaults and the potential harm they pose in SDN environments, a flexible modular architecture for their detection and mitigation has been developed. The study utilizes Machine Learning models such as J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron and Support Vector Machines to train an Intrusion Detection System (IDS). Despite the inherent difficulties presented by LR-DDoS assaults, the assessment of these ML models using the Canadian Institute of Cyber security (CIC) DoS dataset showed a remarkable detection rate of 95%. One of the key advantages of this study is the practical implementation of the open network operating system (ONOS) controller within a Mini-net virtual machine, which tries to faithfully imitate real production network circumstances. This strategy strengthens the paper's credibility and explains how it may be used in real-world network security settings. The article also emphasizes that the intrusion prevention detection system successfully mitigates all assaults identified by the IDS, highlighting the usefulness of the suggested architecture in LR-DDoS attack detection and mitigation. This study presents a novel approach that combines ML approaches with a flexible modular architecture to solve the ongoing problem of LR-DDoS assaults in SDN systems. Its potential as a formidable tool for network security is highlighted by its easy deployment and remarkable detection results. The impact of the work would be increased and new insights would be provided for security practitioners and academics with a more thorough investigation of the difficulties and model choices.

Latif et al. [16] discusses security, a key concern in the context of the Industrial Internet of Things environment. Smart cities, agriculture, and healthcare are just a few areas

where IIoT is crucial due to its integration of sensors, devices, and databases. This study acknowledges the distinct security risks that the IIoT presents as a result of its integration into more complex operational systems. In this research, a unique method for anticipating and detecting several cybersecurity attacks—including denial of service, malicious operation, malicious control, data type probing, espionage, scan, and incorrect setup—that are frequently seen in IIoT contexts is presented. It undertakes a comparison analysis with conventional machine learning methods including artificial neural networks, support vector machines, and decision trees, and proposes a lightweight random neural network (RaNN) as the foundation for its prediction model. The study's main conclusions show that the suggested RaNN-based model performs admirably, with accuracy rates of 99.20%, precision, recall, and the F1 score all above 99%. The model also has short prediction duration of 34.51 milliseconds. These findings show how well the RaNN model predicts and recognises IIoT cybersecurity threats. The work makes an important addition to the area since it tackles the urgent demand for reliable security solutions in IIoT. It is an intriguing option for boosting IIoT security since it uses a lightweight RaNN model and performs better than conventional approaches.

The claimed accuracy gains of 5.65% for IoT security over cutting-edge machine learning algorithms is notable and demonstrates the practical applicability of this study. Nevertheless, when using this approach in complex IIoT contexts, it's critical to take into account potential limits, such as the range and variety of attack scenarios, and scalability, including real-world deployment issues. Despite this, the article offers a useful framework for more study and advancement in the field of IIoT security, including the potential for real-world use in securing vital industrial systems. While the previously discussed works provide important insights into various aspects of protecting SDN and addressing cybersecurity concerns within the IIoT framework, a common shortcoming of these studies is the lack of comprehensive real-world implementation and evaluation. Although some studies employ simulation techniques, little is known regarding whether the proposed solutions can be scaled and applied in complex, real-world large-scale network environments. A more thorough analysis of the potential challenges and setbacks that came across throughout the development of their safety processes, such as issues with interoperability, resource constraints, and adaptability to evolving attack strategies, would also greatly increase the study's practical significance and utility.

III. PROBLEM STATEMENT

Although SDN presents the possibility of dynamic and adaptable network management, efficiency optimization and security remain major obstacles. Lack of integrated security measures to thwart malicious traffic, particularly Denial-of-Service (DoS) attacks, is one of the major problems that can seriously impair service availability. Many times, existing SDN solutions are unable to adequately handle these security issues. As such, the development of a comprehensive strategy that enhances security protocols while simultaneously optimizing network performance is imperative. The purpose of

this research is to determine how well a hybrid GAN-RNN approach, which sets firewalls dynamically using dynamic access control lists, can handle this dual challenge. Furthermore, it aims to provide a new solution that improves network safety and efficiency in SDN environments.

The ability of the proposed Hybrid GAN-RNN method to focus on both security concerns and network efficiency optimizing in SDN systems is what makes it effective. By using Generative Adversarial Networks (GANs) to simulate feasible traffic patterns and Recurrent Neural Networks (RNNs) for adaptable controls on access, this method offers a multidimensional solution. GANs can be used to model various traffic scenarios, and RNNs can be used to flexibly set access control rules based on real-time threat detection to achieve optimal network designs. This hybrid paradigm effectively adapts to changing network conditions and security threats, significantly enhancing the overall resilience of SDN systems. Moreover, employing the Mini net for real-world assessment boosts the practical value of the results and increases the possibility of their successful implementation in operational networks. More information about the specific methods and tools employed for DoS attack detection and avoidance in an SDN environment is required in order to improve the strategy's effectiveness.

IV. PROPOSED HYBRID GAN-RNN FOR NETWORK SECURITY

The proposed methodology represented in Fig. 1 starts with the collection of network traffic data, which is then meticulously pre-processed to cleanse, format, and extract relevant features. A tailored Generative Adversarial Network (GAN) architecture is crafted to generate synthetic traffic patterns that closely resemble real network data. These synthetic patterns are crucial for enhancing security analysis. Simultaneously, a Recurrent Neural Network (RNN) is employed to predict network attacks based on the generated traffic patterns. The RNN learns to recognize temporal patterns and anomalies in the data, aiding in the proactive identification of potential security threats. Following the hybrid GAN-RNN approach, the system's performance is thoroughly analyzed, assessing its ability to generate realistic traffic and predict attacks accurately. Additionally, a

comparative evaluation is conducted to benchmark the proposed methodology against existing approaches, providing insights into its effectiveness in bolstering network security.

A. Data Collection

The CICIDS2017 dataset provides a valuable resource for improving network performance and security through the utilization of Hybrid GAN-RNN models within Software-Defined Networking (SDN) environments. This dataset incorporates both benign network traffic and a wide range of common attacks, making it a suitable foundation for our research and development in the field of networks security and optimization. The CICIDS2017 dataset offers a comprehensive view of network traffic, encompassing benign background traffic and real-world attack scenarios. The dataset is constructed with meticulous attention to realism, featuring the following key components: Generated using the B-Profile system, the dataset simulates the naturalistic behaviors of 25 users engaging in various protocols such as email, HTTP, FTP, HTTPS, and SSH. This component mimics real-world user interactions, contributing to the authenticity of the dataset. The dataset represents a complete network infrastructure, including components like Modem, Firewall, Switches, Routers, and a diverse array of operating systems (e.g., Ubuntu, Windows, and Mac OS X). This realistic topology ensures that the dataset mirrors complex network environments. The CICIDS2017 dataset incorporates real attacks from the Attack-Network, enabling researchers to analyze and develop security measures against a wide range of threats. This includes the most up-to-date common attacks, adding relevance to the research context [17].

B. Data Pre-processing using Handling Missing Values

The time series dataset representing network-wide traffic states, which is denoted as X . This dataset encompasses observations collected over time, each of which corresponds to a specific time step. The dimensionality of the dataset is determined by the amount of sensor stations in the network, denoted as D . Mathematical representation of this time series dataset X as follows in Eq. (1):

$$X = \{x_1, x_2, \dots, x^T\}^T \in \mathbb{R}^{T \times D} \quad (1)$$

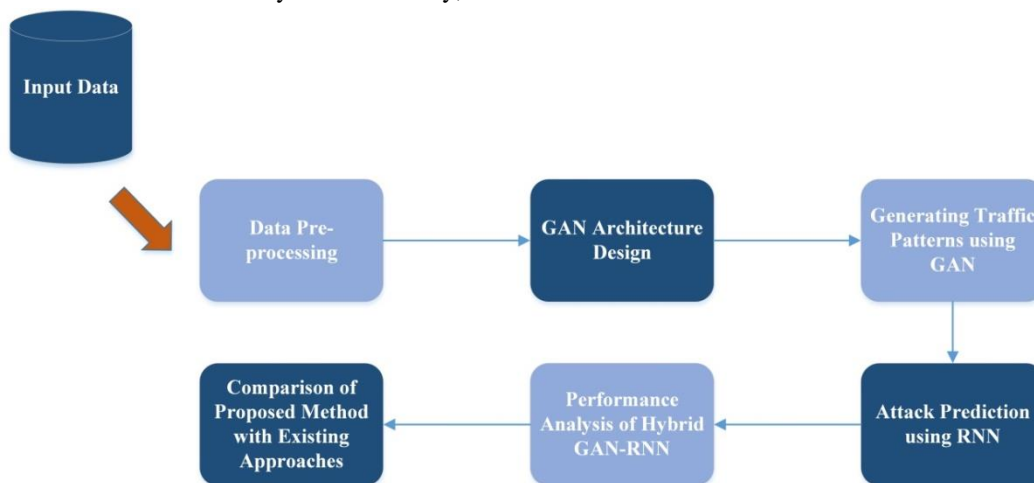


Fig. 1. Proposed workflow.

T Signifies the total number of time steps in our dataset. D signifies the number of sensor stations distributed across the network. Each vector x_t^d , associated with time step t , belongs to the real numbers \mathbb{R}^D . This vector encapsulates the traffic state information of the D sensor stations at that specific time [18].

Within this vector, each element x_t^d corresponds to the traffic speed observed at the d -th sensor station. This research discusses "traffic state," It specifically focuses on traffic speed. This definition aligns with the characteristics of the datasets we employ, particularly those used in our experimental section. Traffic sensors, such as inductive looping detector, may encounter failures due to various reasons, including wire insulations breakdown, damage from building activities, or electronic unit failures. These sensors failures result in missing values within our collected data. To address the issue of missing values, Research employs a masking vector m_t , which is binary and takes values from the set $\{0, 1\}$, to indicate whether traffic states are missing at a specific time step t . The masking vectors for x_t is defined as follows in Eq. (2):

$$m_t^d = \begin{cases} 1, & \text{if } x_t^d \text{ is observed} \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

Consequently, for a given traffic state data sample X in $\mathbb{R}^{T \times D}$, derivation of a corresponding masking data sample M , is represented in Eq. (3):

$$M = \{m_1, m_2, \dots, m_T\} \in \mathbb{R}^T \times D \quad (3)$$

The traffic state prediction problem revolves around the objective of learning a function $F(\cdot)$. This function is designed to map T historical traffic state data observations to the subsequent traffic state data at the next time step. This problem can be formally described as in Eq. (4):

$$F([x_1, x_2, \dots, x^T]; [m_1, m_2, \dots, m^T]) = [x_{T+1}] \quad (4)$$

where, F aims to predict the traffic state at time step $T + 1$ depend on the historical traffic state data up to time step T ,

taking into account the masking information to handle missing values.

C. Hybrid GAN-RNN Architecture for Generating Traffic Patterns and Access Control

The Hybrid GAN-RNN architecture is designed to enhance network security by generating realistic network traffic patterns and making access control decisions based on those patterns. This architecture comprises two main components: a Generative Adversarial Network (GAN) for traffic pattern generation and a Recurrent Neural Network (RNN) for access control. The hybrid GAN-RNN architecture is shown in Fig. 2. In the GAN component, the generator (G) takes random noise (z) as input and generates synthetic traffic patterns ($X_{\text{synthetic}}$). The discriminator (D) then evaluates these synthetic patterns and real traffic patterns (X_{real}), aiming to distinguish between them. The objective is to train the generator to produce traffic patterns that are indistinguishable from real ones, while the discriminator becomes more adept at differentiating real from synthetic patterns. This adversarial training process is guided by a GAN loss function that encourages the generator to improve its pattern generation capabilities. The discriminator's formal objective is to acquire characteristics θ_d that maximize the likelihood of properly categorizing both training and produced data; the generator's objective is to discover settings θ_g that minimize $\log 1 - D(G(z))$. the following two-player minimax game with value functions $V(G, D)$ is therefore played by the two neural networks.

$$V(G, D) = \max_D \min_G \{E_x [\log D(x)] + E_z [\log(1 - D(G(z)))]\} \quad (5)$$

where, $G(z)$ is the created false data provided by the noise vector z , $D(G(z))$ is the estimated chance of a fake instance being honest, and $D(x)$ is the estimated likelihood of an actual model being real generated by the discriminating neural networks. The generator theoretically learns to produce genuine samples when it reaches equilibrium.

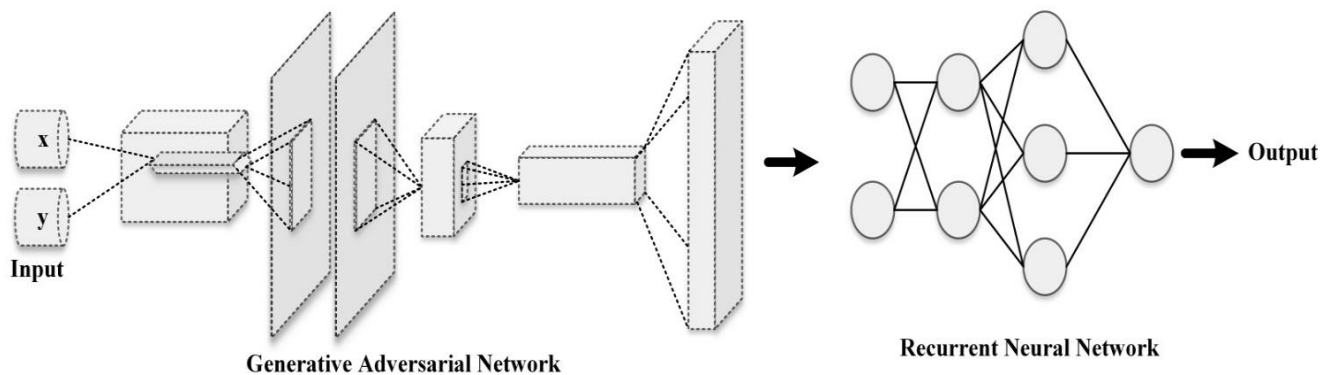


Fig. 2. Hybrid GAN-RNN architecture.

Algorithm 1: Hybrid GAN-RNN Algorithm for Network Security Enhancement

Input: Network Traffic data

Output: Predicting the attack in Network traffic data

Load input data

$$X = \{x_1, x_2, \dots, x_T\}^T \in \mathbb{R}^{T \times D}$$

// data acquisition

Preprocess network traffic data

Cleanse and Handling missing traffic data's, and normalize.

//handling missing values

Split the data into training and testing sets.

Generation of Traffic Patterns

// GAN Training

Initialize the GAN model with a generator (G) and discriminator (D).

Train the GAN by iteratively optimizing G and D

Generate synthetic traffic patterns using G

Calculate the GAN loss based on D's ability to distinguish real from synthetic patterns.

Back propagate the loss and update the G and D weights.

Repeat until convergence or a predefined number of epochs

Attack Prediction

//RNN Training

Initialize the RNN model for attack prediction.

Define the RNN architecture, loss function, and optimizer.

Train the RNN using the generated synthetic traffic patterns

Input the synthetic traffic data sequence to the RNN

Calculate the loss based on the predicted attacks and actual labels (ground truth).

Back propagate the loss and update the RNN weights

Repeat until convergence or a predefined number of epochs

Prediction of Attack in Network

//RNN

Evaluate the hybrid GAN-RNN system's performance using testing data

//Performance Evaluation

Measure the accuracy of attack predictions

Calculate other relevant metrics such as precision, recall, and F1-score

Assess the quality of generated traffic patterns

The RNN component processes the generated traffic patterns ($X_{\text{synthetic}}$) and performs access control. For this purpose, the RNN can employ a LSTM architecture, which allows it to consider temporal dependencies in the traffic data. The RNN's internal state (ht) evolves as it processes the traffic patterns, and at each time step, it produces access control decisions (yt) through a Softmax layer. These decisions can take various forms, such as binary access control (allows or deny) or multiclass access policies based on the traffic content and context.

The key innovation of this architecture lies in its combination of GAN and RNN components. The GAN generates synthetic traffic patterns that are realistic and diverse, reflecting various network activities. The RNN, in turn, leverages these patterns to make access control decisions in real-time. This approach enables a more dynamic and adaptable access control system that can respond effectively to evolving network conditions and potential security threats. During training, the entire hybrid architecture is optimized through a joint loss function that balances the GAN loss and the access control loss. This ensures that the generated traffic patterns are not only realistic but also suitable for access control decision making. The RNN's parameters are fine-tuned to make accurate access control decisions based on the generated patterns, thereby enhancing network security.

V. RESULTS AND DISCUSSION

The result section provides a comprehensive evaluation of the proposed network security enhancement method, employing various evaluation metrics such as accuracy, precision, recall, and F1-score. The analysis begins with a comparison of the method's accuracy on different datasets, highlighting the notably high accuracy of the "Proposed GAN-RNN" approach on the CICIDS2017 dataset. A comparative assessment with existing methods further underscores the method's superiority, showcasing exceptional precision, recall, and F1-score. Graphs depict the performance trends,

demonstrating the model's convergence and its ability to generalize to unseen information. The training and testing graphs illustrate the model's progression, while the loss graph reveals its capacity to avoid overfitting. The results validate the effectiveness of the proposed methods in network intrusion detection, emphasizing its potential to enhance network security with impressive accuracy and robustness. The practical usefulness of the Hybrid GAN-RNN technique extends to dynamic business networks, allowing for adaptive routing and resource allocation. Its 99.4% accuracy in cybersecurity guarantees quick access policy changes, which are essential for sectors like banking and healthcare and improve overall network security and efficiency.

A. Evaluation Metrics

Four assessment measures were used in the study to evaluate the designs: F1-score, accuracy, precision, and recall. Such specific variables are described as in Eq. (6), (7), (8) and (9):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

$$F1score = \frac{2*Recall*Precision}{Recall+precision} \quad (9)$$

TP is the number of information that, irrespective of every one of the types of information which was genuinely positive, was precisely identified as positive. TN is the number of information that, irrespective of all the results which was truly negative, were properly identified as negatives. The number of variables that the equation incorrectly categorized as negative despite the fact they had been positive in the input data is represented by the letter FN. The number of values that the algorithm incorrectly categorized as positive when they had been negative in the source data is known as false positives, or

FP. The percentage of the number of information that the algorithm identified as being positive to the number of positive results that were really present in the collection of data is known as recall. Precision can be defined as the proportion of the entire amount of information that the model properly identified as positive to the number of data which the algorithm categorized as positive. Lastly, as mentioned in, the F1-score represents the harmonious average of recall and precision Top of Form [19].

This Table I present the performance results of different intrusion detection methods on these datasets, with the "Proposed GAN-RNN" method achieving notably high accuracy on the CICIDS2017 dataset at 99.4%. It's important to note that the choice of dataset and the specific evaluation metrics used can significantly impact the reported accuracy, and the effectiveness of a method may vary depending on the dataset's characteristics and the complexity of the network security task.

The graph in Fig. 3 depicts, the methods consistently outperform others across multiple datasets and which ones may excel in specific contexts. This comparison aids in the selection of the most robust intrusion detection method for diverse network security environments, contributing to informed decision-making in network security strategy.

Table II presents a comparative overview of different methods applied to network intrusion detection, showcasing their performance across multiple evaluation metrics. It includes the methods GRU, CNN, B-GRU, and the "Proposed GAN-RNN." the "Proposed GAN-RNN" method exhibits exceptional accuracy, achieving an impressive 99.4%, surpassing the other methods in the accuracy metric.

Furthermore, it excels in precision with a score of 99.25%, ensuring a high proportion of correctly classified positive predictions. It demonstrates remarkable recall at 99.6%, effectively capturing a significant portion of actual positive instances. The F1-score, a balanced measure of precision and recall, remains strong at 99.4%, further affirming the method's robustness in network intrusion detection, making it a highly promising approach for bolstering network security.

The Graph represents in Fig. 4 shows the performance comparison of different intrusion detection methods on various metrics, including accuracy, precision, recall, and F1-score.

Fig. 5 represents the training and testing graph for the proposed network security enhancement method illustrates the model's performance throughout the training process. During the training phase, the metrics are plotted as they evolve with each epoch, showing how the model learns and improves its performance over time. The testing phase is also depicted on the same graph, showcasing how the model generalizes to unseen data. This graph provides a clear visualization of the model's convergence and its ability to avoid overfitting or underfitting, thus assisting in the evaluation and refinement of our network security enhancement approach. The testing accuracy attained is 99.4%.

Fig. 6 represents the training and testing loss graph is a graphical representation that illustrates the changes in the loss function values of a machine learning or deep learning model during both the training and testing phases. The testing loss curve reveals the model generalizes to unseen data, and ideally, it should exhibit a similar decreasing trend, indicating that the model is not overfitting.

TABLE I. ACCURACY COMPARISON OF DATASET

Dataset	Methods	Accuracy
KDD99 [20]	DT	92.3
UNSW-NB15 [20]	LR	85.56
CICIDS2017	Proposed GAN-RNN	99.4

TABLE II. PERFORMANCE COMPARISON WITH EXISTING METHODS

Methods	Accuracy	Precision	Recall	F1-score
GRU [21]	99	99	99	99
CNN [21]	97.7	97.4	98.2	99
B-GRU [21]	98.74	98.9	99	99
Proposed GAN-RNN	99.4	99.25	99.6	99.4

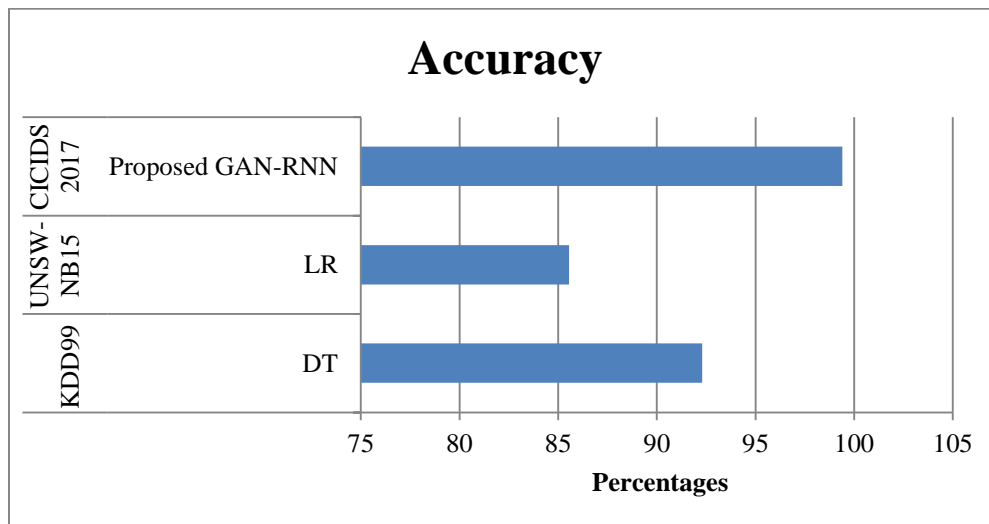


Fig. 3. Dataset comparison.

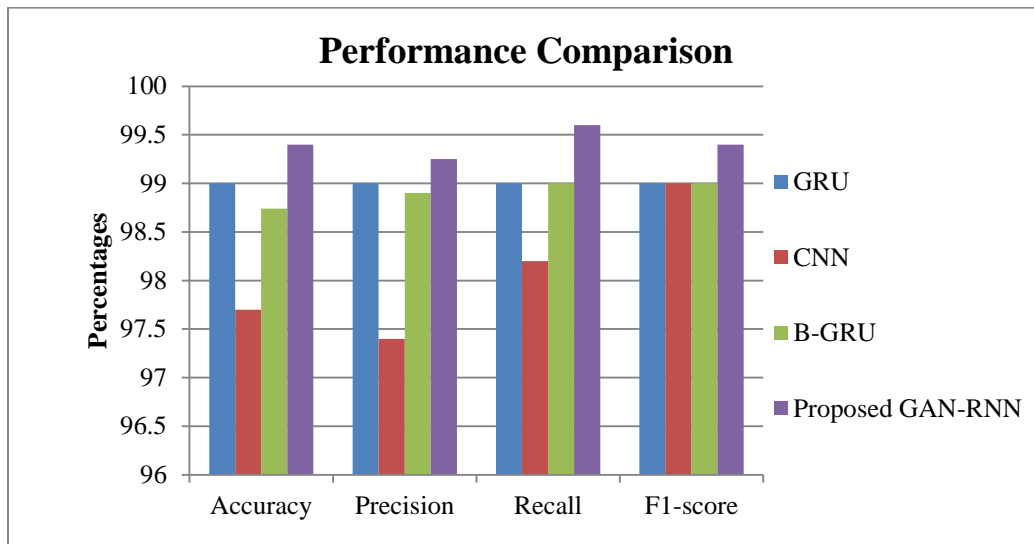


Fig. 4. Evaluation of performance with existing approaches.

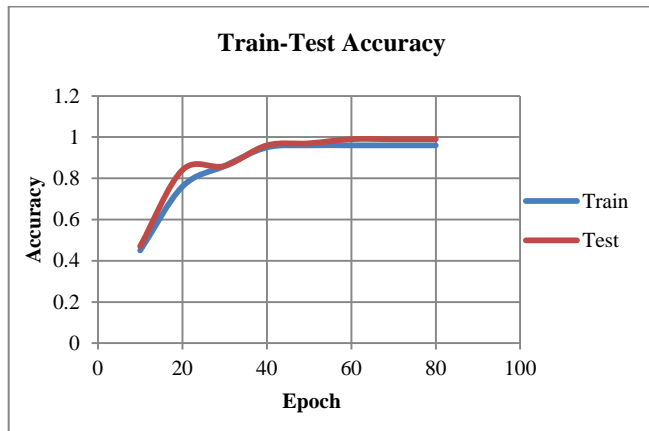


Fig. 5. Training and testing accuracy.

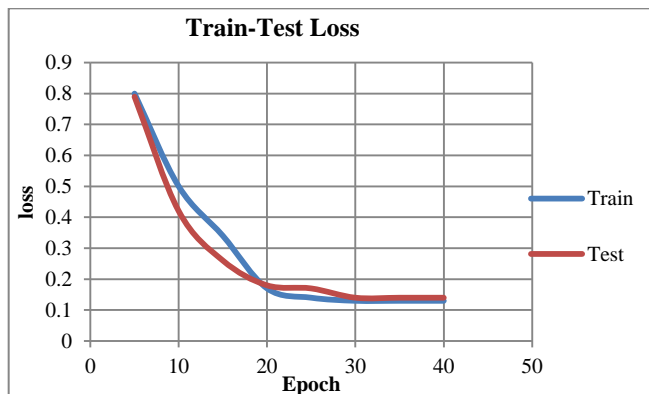


Fig. 6. Training and testing loss.

The Fig. 7 displays a Generative Adversarial Network with Recurrent Neural Network (GAN-RNN) model's Receiver Operating Characteristic (ROC) curve. The model's ability to distinguish between classes, especially in issues with binary classification, is represented graphically by the ROC curve. The true positive rate (sensitivity) during each threshold, which ranges from 0 to 0.7, is paired with a corresponding

threshold value in the table. The true positive rate tends to rise in tandem with the threshold, suggesting that the model is becoming more accurate at identifying positive instances. The true positive rate increases gradually from 0.07 to 0.994 as the threshold increases, indicating that the GAN-RNN model has high discriminatory power. This indicates that the model performs well in classifying positive instances, demonstrating its efficacy in achieving high sensitivity across a range of threshold values.

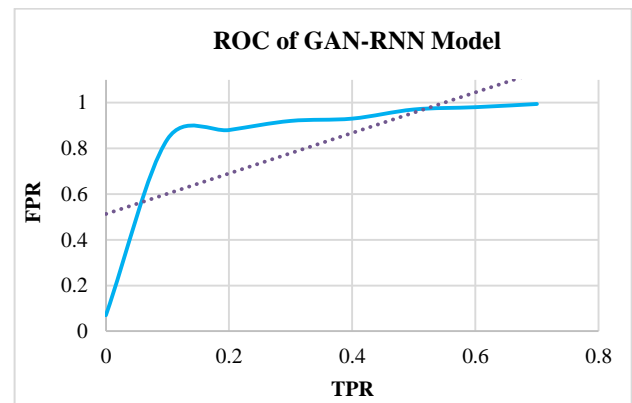


Fig. 7. ROC of GAN-RNN model.

B. Discussion

The accuracy of several methods for identifying intrusions on a range of datasets is assessed at the outset of the findings section. The efficiency results for the three different datasets—KDD99, UNSW-NB15, and CICIDS2017—are shown in Table I. On the CICIDS2017 dataset, the "Proposed GAN-RNN" approach notably obtains a very high accuracy value of 99.4%. This extraordinary accuracy demonstrates how well the approach works in a specific dataset to recognize network security problems. However, given that network data can differ greatly in complexity and feature sets, it is imperative to recognize that the selection of dataset is a critical factor in deciding accuracy. As a tool for comparing datasets, the chart in Fig. 3 shows how the techniques

continually perform better than others on a variety of datasets. It makes it possible to pinpoint the approaches that work best in certain situations. The comparison is essential because it helps choose the most reliable intrusion detection technique for various network security scenarios. The graph presents the overall efficacy of the "Proposed GAN-RNN" approach, indicating a potential option for improving network security on a variety of datasets.

Table II provides an extensive comparative analysis of various intrusion detection techniques, such as GRU, CNN, B-GRU, and the "Proposed GAN-RNN." The "Proposed GAN-RNN" approach performs exceptionally well according to a number of evaluation parameters. It is noteworthy for achieving a 99.4% accuracy rate, which is higher than the other approaches. The technique also performs exceptionally well in terms of precision (99.25%), guaranteeing a large percentage of accurately identified positive predictions. Furthermore, it exhibits exceptional memory (99.6%), successfully catching a substantial proportion of true positive cases. At 99.4%, the F1-score—a measure that strikes a compromise between recall and precision—remains robust. All of these findings support the "Proposed GAN-RNN" approach's robustness and dependability in detecting network intrusions. Because of its exceptional performance, the approach offers both accuracy and precision in spotting security issues, making it a very viable alternative to strengthen network security. The suggested network security enhancement approach is thoroughly evaluated in the results section, which highlights its remarkable accuracy, precision, recall, and F1-score. It demonstrates how the approach can continuously beat other approaches on various datasets, which makes it a strong option for secure network application. These results provide insightful information that may be used to make well-informed decisions about network security planning and technological implementation. The access control as well as traffic engineering systems that are now dependent on network security may not be scalable, may have trouble adapting to changing threats in real-time, and may find it difficult to properly handle growing cyber threats [8].

VI. CONCLUSION AND FUTURE WORK

In the framework of SDN-based traffic management and access control, hybrid GAN-RNN models were proposed and their efficacy was shown in the present investigation. The results obtained suggest that this novel technique holds significant potential for improving software-defined network security and performance. The Hybrid GAN-RNN design has demonstrated notable gains in network effectiveness and threat reduction through the creation of realistic patterns of traffic and accurate access control choices. In today's intricate and constantly evolving network systems, the capacity to detect abnormalities, adjust to changing conditions, and optimize traffic flows is an essential skill. The suggested technique's high recall, accuracy, and precision highlight its potential as a vital resource for network managers and security experts. This strategy has the ability to enable enterprises to strengthen their safety posture, maximize resource efficiency, and handle their networks more effectively as the network environment changes. Through the integration of Hybrid GAN-RNN models within SDN, this study considerably

improves knowledge while improving the efficiency and security of networks. Results validate hypotheses and lay the groundwork for more investigation into adaptive access management and optimizing traffic in dynamic contexts in the future.

Provide means by which access control policies can be automatically modified in response to threat assessments and network conditions in real time, enabling more flexible and responsive security. Instead of depending only on historical data, investigate real-time analysis abilities that allow the system to identify and address security threats and operational issues as they arise. To convert created traffic trends into useful network configurations and rules, tighten the connection with SDN controllers. In multi-domain or mixed-cloud situations, when network intricacy and safety issues are heightened, expand the Hybrid GAN-RNN technique to optimize network security and performance. To ensure resilience in the midst of sophisticated dangers, assess the proposed method's resistance against adversarial assaults that attempt to interfere with traffic patterns or evade control of access. To handle increasing threats, future research might focus on improving the hybrid GAN-RNN method's scalability and flexibility. A more thorough and forward-thinking approach would involve looking into effective ways of managing larger networks and new security challenges.

REFERENCES

- [1] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.
- [2] V. Kapoor and R. Yadav, "A Hybrid Cryptography Technique for Improving Network Security," *IJCA*, vol. 141, no. 11, pp. 25–30, May 2016, doi: 10.5120/ijca2016909863.
- [3] C. Yu, J. Lan, Z. Guo, and Y. Hu, "DROM: Optimizing the Routing in Software-Defined Networks With Deep Reinforcement Learning," *IEEE Access*, vol. 6, pp. 64533–64539, 2018, doi: 10.1109/ACCESS.2018.2877686.
- [4] N. Awadallah Awad, "Enhancing Network Intrusion Detection Model Using Machine Learning Algorithms," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 979–990, 2021, doi: 10.32604/cmc.2021.014307.
- [5] Muthukumar V., V. V. Kumar, R. B. Joseph, M. Munirathanam, and B. Jeyakumar, "Improving Network Security Based on Trust-Aware Routing Protocols Using Long Short-Term Memory-Queueing Segment-Routing Algorithms," *International Journal of Information Technology Project Management*, vol. 12, no. 4, pp. 47–60, Oct. 2021, doi: 10.4018/IJITPM.2021100105.
- [6] S. Akbar, J. A. Chandulal, K. N. Rao, and G. S. Kumar, "Improving network security using machine learning techniques," in *2012 IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, India: IEEE, Dec. 2012, pp. 1–5. doi: 10.1109/ICCIC.2012.6510197.
- [7] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," *Sensors*, vol. 22, no. 13, p. 4730, Jun. 2022, doi: 10.3390/s22134730.
- [8] S. Anbalagan et al., "Machine-Learning-Based Efficient and Secure RSU Placement Mechanism for Software-Defined-IOV," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13950–13957, Sep. 2021, doi: 10.1109/JIOT.2021.3069642.
- [9] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in SDN using machine learning approach," in *2016 IEEE Conference on Network Function Virtualization and*

- Software Defined Networks (NFV-SDN), Palo Alto, CA: IEEE, Nov. 2016, pp. 167–172. doi: 10.1109/NFV-SDN.2016.7919493.
- [10] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, “Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014, doi: 10.1109/COMST.2014.2320099.
- [11] J. Ramprasath and V. Seethalakshmi, “Secure access of resources in software-defined networks using dynamic access control list,” *Int J Communication*, vol. 34, no. 1, p. e4607, Jan. 2021, doi: 10.1002/dac.4607.
- [12] V. Vimal et al., “Enhance Software-Defined Network Security with IoT for Strengthen the Encryption of Information Access Control,” *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–10, Oct. 2022, doi: 10.1155/2022/4437507.
- [13] S. Shin, L. Xu, S. Hong, and G. Gu, “Enhancing Network Security through Software Defined Networking (SDN)”.
- [14] A. Ahmad, E. Harjula, M. Ylianttila, and I. Ahmad, “Evaluation of Machine Learning Techniques for Security in SDN,” in *2020 IEEE Globecom Workshops (GC Wkshps, Taipei, Taiwan: IEEE*, 2020, pp. 1–6. doi: 10.1109/GCWkshps50303.2020.9367477.
- [15] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, “A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning,” *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
- [16] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, “A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network,” *IEEE Access*, vol. 8, pp. 89337–89350, 2020, doi: 10.1109/ACCESS.2020.2994079.
- [17] “CICIDS2017.” <https://www.kaggle.com/datasets/cicdataset/cicids2017> (accessed Sep. 18, 2023).
- [18] Z. Cui, R. Ke, Z. Pu, and Y. Wang, “Stacked Bidirectional and Unidirectional LSTM Recurrent Neural Network for Forecasting Network-wide Traffic State with Missing Values,” *arXiv*, May 23, 2020. Accessed: Sep. 19, 2023. [Online]. Available: <http://arxiv.org/abs/2005.11627>.
- [19] B. Jang, M. Kim, G. Harerimana, S. Kang, and J. W. Kim, “Bi-LSTM Model to Increase Accuracy in Text Classification: Combining Word2vec CNN and Attention Mechanism,” *Applied Sciences*, vol. 10, no. 17, p. 5841, Aug. 2020, doi: 10.3390/app10175841.
- [20] N. Moustafa and J. Slay, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Information Security Journal: A Global Perspective*, vol. 25, no. 1–3, pp. 18–31, Apr. 2016, doi: 10.1080/19393555.2015.1125974.
- [21] H. Wang and W. Li, “DDoSTC: A Transformer-Based Network Attack Detection Hybrid Mechanism in SDN,” *Sensors*, vol. 21, no. 15, p. 5047, Jul. 2021, doi: 10.3390/s21155047.