Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Driven Predictive Cybersecurity Architecture for U.S. SDN-Controlled DWDM Datacenter Networks

Md. Serajul Kabir Chowdhury Rubel[1]*, Md. Iqbal Hossan[2], BM Taslimul Haque[3], and Md. Arifur Rahman[4]

[1] *Maharishi International University, Fairfield, IA 52557, USA, Mohammad.rubel@miu.edu*
[2] *Maharishi International University, Fairfield, IA 52557, USA, hossan.iqbal@gmail.com*
[3] *Central Michigan University, Mount Pleasant, MI 48859, USA, bmtaslim121@gmail.com*
[4] *Trine University, Angola, IN 46703, USA, rahman.arifur11@gmail.com*
Corresponding Author: Md. Serajul Kabir Chowdhury Rubel, **E-mail**: Mohammad.rubel@miu.edu

| ABSTRACT
The growing integration of Software-Defined Networking (SDN) and Dense Wavelength Division Multiplexing (DWDM) systems in modern U.S. datacenter infrastructures has created new cybersecurity threats, threats in speed and volume of network traffic, and networking threats of centralized control. Traditional rules-based security systems no longer provide real-time detection of advanced persistent threats, malware propagation, botnet intrusions, Distributed Denial of Service (DDoS) attacks and other forms of sophisticated attacks. In this regard, this study is aimed at proposing an AI-based predictive cybersecurity architecture for securing SDN controlled DWDM datacenter networks using intelligent threat prediction, anomaly detection and automated mitigation mechanisms to overcome these limitations. The proposed framework combines machine learning and deep learning with SDN-based traffic management to improve the visibility, scalability and adaptive cyber defense capabilities of networks. This study uses the CSE-CIC-IDS2018 data set which includes realistic enterprise network traffic and several attack categories for training and testing predictive models of cybersecurity. A number of AI algorithms are employed, such as Random Forest, XGBoost, Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, to analyze traffic behavior, classify malicious activities, and predict potential cyberattacks. The architecture is segmented into several layers are traffic monitoring to gather data, feature extraction to analyze the data, AI-based prediction to foresee potential threats, threat detection to identify them, and automated response to address them, all aimed at enhancing the security resilience of high-speed optical datacenter environments. Experiments should show that its detection accuracy is higher, it has fewer false positive rates, it can respond quicker to attacks and it can provide superior protection for the network than the traditional intrusion detection systems. This study will help build a next-generation intelligent cybersecurity framework that secures the DWDM datacenter in the United States from new cyber threats while enhancing the efficiency, scalability, and real-time adaptive security management of the system.

| KEYWORDS

Artificial Intelligence, Predictive Cybersecurity, Software-Defined Networking (SDN), DWDM Datacenter Networks, Intrusion Detection System (IDS) and Deep Learning

| ARTICLE INFORMATION

ACCEPTED: 18 September 2024 **PUBLISHED:** 28 October 2024 **DOI:** 10.32996/jcsts.2024.6.4.18

I. Introduction

Modern datacenter infrastructures in the United States are undergoing rapid change, especially in the areas of cloud computing, software defined networking, optical communication systems and artificial intelligence technologies [1]. As

communication speeds rise and flatter organizations with vast amounts of data flow require scalable, flexible and high-speed communication environments, Software-Defined Networking (SDN) and Dense Wavelength Division Multiplexing (DWDM) technologies are becoming indispensable. SDN offers centralized management, programmability, traffic engineering, dynamic resource allocation of the network, whereas DWDM provides a way to increase the utilization of optical bandwidths by multiplexing multiple wavelengths within a single optical fiber [1]. These two technologies increase the operational efficiency, scalability of networks, and performance in datacenter environments. In spite of these technological benefits, SDN-controlled DWDM datacenter infrastructures are subject to a growing threat from cyberattacks because of centralized architectures, virtualization and attack techniques [2]. SDN controllers, network virtualization, and high-speed optical traffic environments are some of the points where vulnerabilities are often discovered and exploited by cybercriminals to launch sophisticated attacks like Distributed Denial of Service (DDoS), malware propagation, insider threats, advanced persistent threats and zero day attacks. Many traditional cybersecurity systems, such as rule-based intrusion detection, or static firewalls, are now failing to protect against the dynamic and intelligent cyber threats in today's datacenter networks [2]. The technologies of Artificial Intelligence (AI), machine learning and deep learning offer an effective solution for predictive cybersecurity and intelligent threat analysis. AI systems can process huge data on traffic, detect abnormal network activities, foresee cyber threats and automate mitigating actions on the fly. The use of AI-based predictive cybersecurity in SDN-controlled DWDM datacenter networks can thus greatly improve the security of critical digital infrastructures in the United States, increase network resilience, increase accuracy of intrusion detection, and decrease response time.

A. *Background of the Study*

Cloud computing, big data analytics, Internet of Things (IoT) and high-performance computing have all grown at a fast pace, driving U.S. datacenter infrastructure growth to be more scalable and secure. Today, organizations are increasingly turning to Software-Defined Networking (SDN) and Dense Wavelength Division Multiplexing (DWDM) to manage data transfers and to scale their networks. SDN decouples control plane from data plane, allowing dynamically programmed and managed networks, and dynamic traffic engineering. In the same way, DWDM technology is used to improve optical communication so that several wavelengths can be transmitted within one optical fiber, increasing the bandwidth capacity and improving the efficiency of optical communication. While these technologies enhance datacenter efficiencies and flexibilities, they also create significant cybersecurity concerns. Centralized controllers are an integral component of SDN architectures and are often prime targets for Distributed Denial of Service (DDoS), malware injection, insider threats, and unauthorized access attempts. Furthermore, high speed DWDM networks produce huge amounts of traffic which are hard to monitor by conventional rule-based intrusion detection systems. Traditional cyber security solutions are not sufficiently intelligent and adaptable to identify complex and sophisticated attack patterns in real time. Predictive Cybersecurity and Intelligent Threat Analysis based on Artificial Intelligence (AI), machine learning and deep learning are new technologies that hold great promise [3]. AI-powered systems can analyze vast amounts of network traffic data, detect anomalies, anticipate potential cyber threats, and trigger security responses automatically, requiring minimal human intervention. By combining AI-based predictive analytics with SDN-controlled DWDM datacenter networks, the cyber security resilience of the United States can be improved, the accuracy of detecting attacks can be increased, the response time can be shortened, and critical digital infrastructures can be better protected.

B. *Problem Statement*

The datacenter networks in the modern era, which are controlled by SDN, are becoming more susceptible to sophisticated cyber threats because of centralized network control, virtualization and high-speed optical communication infrastructures. Traditional cybersecurity rules-based security systems cannot adequately identify new attacks, like Distributed Denial of Service (DDoS), malware propagation, advanced persistent attacks, insider attacks, and zero-day vulnerabilities in real-time [4]. Current IDSs may have high false positive rates, slow detection, and are not very flexible in dynamic network environments. The large amount of traffic in SDN-enabled DWDM networks makes it difficult to monitor and manage security manually. Hence, an intelligent and adaptive predictive cybersecurity architecture that can intelligently predict threats, detect anomalies automatically and adapt accordingly is crucial.

C. *Objectives of the Study*

The objective of this study is:

- To explore and identify the cybersecurity risks and issues of SDN datacenter networks in the United States that are controlled by DWDM.
- Create an intelligent cybersecurity architecture with AI capabilities for predictive threat detection and automatic network protection.
- To apply machine learning and deep learning algorithms for real-time anomaly detection and prediction of cyber-attacks [5].
- Test AI-based predictive models with CSE-CIC-IDS2018 cybersecurity data.

- To enhance the resilience of the network, the speed of responding to threats, and the degree of detection accuracy in SDN controlled DWDM datacenter environments.
- Embedding automated mitigation mechanisms into SDN controllers, for adaptive cybersecurity management.
- To help build next-generation, intelligent, cybersecurity solutions for high-speed optical data center infrastructures.

D. *Research Questions*

Following these questions are guide tom this study:

- What is the role of artificial intelligence in improving the predictive cybersecurity in SDN controlled DWDM datacenter network?
- What machine learning and deep learning models are the most accurate for detecting and predicting cyber threats in SDN based environments?
- What is the impact of AI-powered predictive cybersecurity on datacenter optical infrastructures in terms of quicker responses and greater cybersecurity resilience?
- How does the combination of AI-driven threat prediction systems and SDN-controlled network management systems benefit organizations?

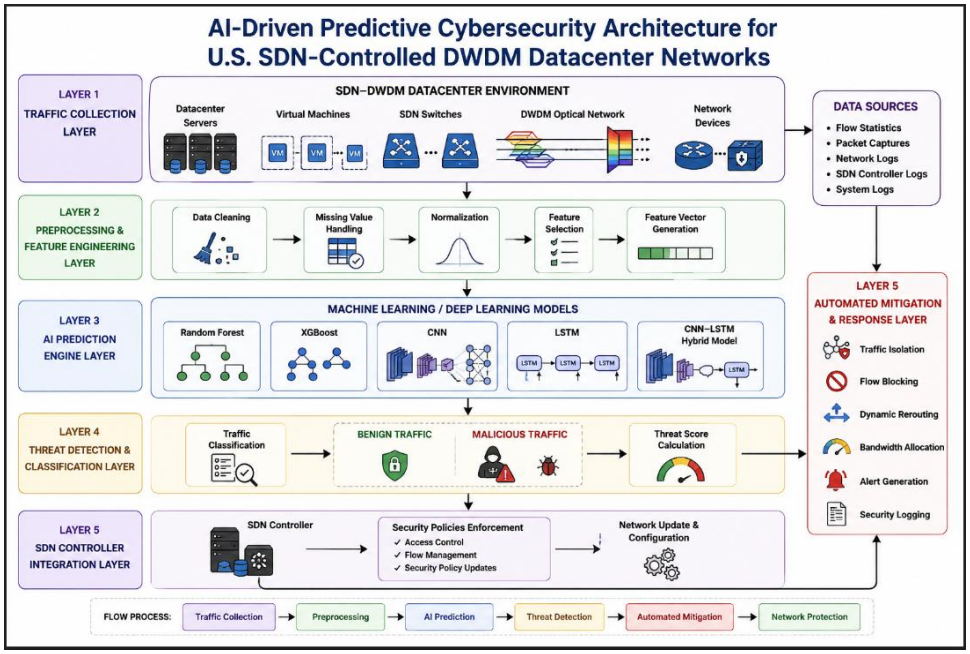
E. *Significance of the study*

This study is relevant as it tackles the emerging cybersecurity issues of SDN based DWDM datacenter networks in the USA. Modern datacenter architectures, where cloud computing, virtualization, optical communication systems and centralized architectures are becoming increasingly important, have made these infrastructures vulnerable to advanced cyber threats, including DDoS attacks, propagation of malware, insider threats, and advanced persistent threats. The traditional rule-based cybersecurity systems are no longer effective in securing high-speed optical networks from emerging cyber threats. Thus, the proposed AI-driven Predictive Cyber Security Architecture offers an intelligent and adaptive solution to enhance network security, threat detection, and automated mitigation. The study presents an integrated approach to incorporate the techniques of artificial intelligence, machine learning and deep learning in an SDN controlled DWDM environment, which helps in the growth of predictive Cyber Security research [6]. By leveraging intelligent cybersecurity analytics, the proposed framework improves anomaly detection, traffic analysis, attack prediction, and real-time responses. This study offers valuable insights for designing automated security management systems with lower false positive rates, higher detection accuracy, and enhanced network resilience. The results of this study can contribute to the development of a scalable and intelligent cybersecurity framework for the protection of modern high-speed datacenter infrastructures against emerging cyber threats, which is beneficial for cybersecurity practitioners, network administrators, cloud service providers, enterprise organizations, and researchers.

II. Literature Review

A. *AI-Driven Predictive Cybersecurity in SDN-DWDM Networks*

The recent studies are aimed at using the technologies of AI, machine learning, and deep learning for enhancing the performance of cybersecurity and intelligent traffic management for Software-Defined Networking (SDN) environments. The widespread use of Dense Wavelength Division Multiplexing (DWDM) and SDN technologies in today's datacenter infrastructures has enabled, among other things, scalable and programmable network architectures [7]. The centralized control of these networks, virtualization, and high-speed optical communication systems, however, create a number of cybersecurity challenges. Traditional Intrusion Detection Systems (IDS) and static firewalls are unable to identify in real-time advanced persistent threats, insider attacks, zero-day vulnerabilities, Distributed Denial of Service (DDoS) attacks or malware propagation. To address these challenges, recent cybersecurity frameworks rely more on machine learning algorithms like Random Forest, Support Vector Machines, Decision Trees, and XGBoost for intelligent intrusion detection and traffic classification. In addition, deep learning techniques like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have shown promising results in detecting anomalous traffic patterns and predicting malicious actions in dynamic networks. Predictive cybersecurity systems powered by AI are able to analyze traffic patterns in real time and monitor user behavior, which helps minimize false positives and increases the accuracy of threat detection. Real-time traffic analysis and behavior monitoring capabilities in AI-driven predictive cybersecurity systems help lower false positive rates and improve threat detection accuracy, while automating threat response mechanisms [8]. When predictive cybersecurity functions are layered on top of SDN controllers, they offer adaptive network defense features that allow for automatic mitigation measures like traffic isolation, rerouting, and blocking malicious flows. Although these developments have taken place, not much research has been done specifically on AI-based predictive cybersecurity architectures in SDN controlled DWDM datacenter networks within high-speed optical communication infrastructures. There is a need for further study to create an intelligent, scalable and autonomous cyber security framework for protecting the modern SDN-DWDM datacenter environment against the emerging cyber threats and advanced network attacks.



This flowchart depicts an AI-based predictive cybersecurity approach for SDN controlled DWDM datacenter infrastructures

The diagram illustrates an artificial intelligence (AI) based predictive cybersecurity architecture that is suitable for the U.S. SDN controlled DWDM datacenter networks. It depicts several layers such as traffic collection, traffic preprocessing and feature engineering, AI prediction models, threat detection, integration with an SDN controller, and automated mitigation mechanisms [9]. The framework relies on machine learning and deep learning algorithms like Random Forest, XGBoost, CNN, LSTM, and hybrid CNN-LSTM models to analyze network traffic, identify cyber threats, classify malicious activities, and automatically respond to these threats with techniques like traffic isolation, flow blocking, dynamic rerouting, and security policy enforcement.

B. *Empirical Study*

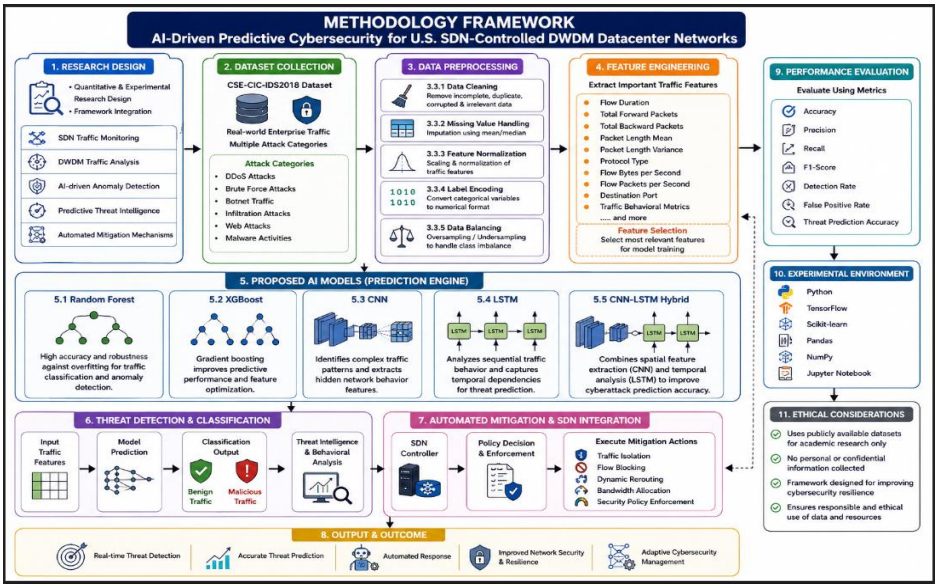
In the article titled "Self-Managed 5G Networks" by Jorge Martín-Pérez, Lina Magoula, Kiril Antevski, and other contributors, the authors discussed the importance of artificial intelligence and machine learning for autonomous management of modern 5G network infrastructures. The study pointed out that intelligent and automated network management solutions are needed for next-generation communication networks, given their growing bandwidth needs, ultra-low latency requirements and dynamic traffic patterns. The article emphasized on a number of key technologies, such as Software-Defined Networking (SDN), network slicing, wavelength assignment, network function orchestration and adaptive resource management [10]. Moreover, the research presented the capability of using AI/ML techniques to enhance decision-making, traffic optimization and dynamic provisioning in highly complex communication environments. In addition, the authors contrasted traditional network management techniques with those supported by AI and showed the benefits of intelligent automation in the contemporary network infrastructure. This literature firmly advocates the creation of an AI-based predictive cybersecurity architecture for SDN-controlled DWDM datacenter networks, offering essential concepts for intelligent network management, automation and adaptive communication systems.

In the article titled "Review of OFC 2021: The Future of Optical Networks and Communications," Henri Hodara, Patrick Mock and Charles Slemon summarized recent progress in optical communication technologies and intelligent networking systems at OFC 2021. Important developments of hollow core fibres, neural network, quantum key distribution, optical switching, coherent optical transmission and data center communication systems were discussed in the study. The article emphasized the increasing importance of artificial intelligence (AI) and neural networks in enhancing the performance of the optical network, optimizing traffic, and intelligent communication management systems [11]. Also, the authors highlighted the significance of the high-speed optical infrastructures and adaptive networking technologies to meet the communication requirements in today's data-driven world. The study also examined future directions of optical communication systems such as secure data communication and intelligent automation. The research work in this literature is very relevant to the AI-based predictive cybersecurity and SDN controlled DWDM datacenter research, as it has applications for intelligent optical networking, AI based traffic management and advanced communication infrastructure development.

Rohit Nanda, in the article "AI-Augmented Software-Defined Networking (SDN) in Cloud Environments," explained how Artificial Intelligence (AI) can be combined with Software-Defined Networking (SDN) to improve the management of the network and facilitate autonomous network operations in the Cloud. The study outlined how the SDN approach with the incorporation of AI enhances the centralized control of networks, prediction of traffic, detection of anomalies, optimization of networks, and adaptive security management in a cloud computing environment. The article emphasized predictive analytics and automated decision-making in a dynamic network infrastructure through the use of machine learning, deep learning, and reinforcement learning. Furthermore, the study examined the architecture, advantages, usability and issues of artificial intelligence based SDN systems. The author highlighted how intelligent SDN environments greatly enhance the scalability, operational efficiency, and cybersecurity resilience of networks. The proposed research is very relevant to this literature, since the development of such AI-based predictive cybersecurity architectures for SDN controlled DWDM datacenter networks can be made possible by intelligent traffic analysis, anomaly detection and adaptive network security management.

III. Methodology

This study introduces a predictive cybersecurity architecture based on the use of artificial intelligence to protect the U.S. SDN controlled DWDM datacenter networks from the emerging cyber threats [12]. The methodology integrates various technologies such as machine learning, deep learning, SDN traffic analysis and predictive cybersecurity methods to enhance real-time threat detection, anomaly classification and automated mitigation. Research methodology involves the following steps: dataset collection, preprocessing, preprocessing of features, developing models, designing the architecture, evaluating the models, and implementing the response automatically.



This methodology framework illustrates AI-driven predictive cybersecurity processes for SDN-controlled DWDM datacenter networks

This diagram illustrates a complete methodology framework for building an AI-based predictive cybersecurity system for the U.S. SDN-controlled DWDM datacenter networks. It represents sequential phases of research such as research design, data collection, data preprocessing, feature engineering, implementation of AI models, threat detection, automated threat mitigation, performance evaluation, experimental environment, and ethical issues. The framework also uses the CSE-CIC-IDS2018 dataset and machine learning and deep learning models like Random Forest, XGBoost, CNN, LSTM and CNN-LSTM for anomaly detection and cyber threat prediction [13]. The architecture brings SDN controllers together with automated cybersecurity defenses such as traffic isolation, flow blocking, and dynamic rerouting and policy enforcement to enhance cybersecurity resilience.

A. *Research Design*

The study design is quantitative and experimental, which is used to assess the effectiveness of the artificial intelligence algorithms in predictive cybersecurity in SDN controlled DWDM datacenter environments. The study concentrates on network traffic analysis, anomaly detection and prediction of cyber threats using machine learning and deep learning approaches. Realistic traffic is collected from enterprise network environments and used to train, validate and test the predictive models. The proposed framework involves implementing SDN traffic monitoring, DWDM traffic analysis, anomaly detection using AI, predictive threat intelligence, and automated mitigation strategies, all of which are aimed at enhancing the overall security and resilience of the

network [14]. Through the experimental design, the efficacy of several artificial intelligence models for malicious traffic pattern and cyber-attack behavior detection, such as Random Forest, XGBoost, Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks, can be evaluated. The study also tests how well the automated response mechanisms of SDN, like traffic isolation, flow blocking and dynamic rerouting work. The quantitative approach enables the detection accuracy, false positive rate, prediction performance, and efficiency of threat response to be measured. The proposed research design can be used to build an intelligent cybersecurity framework for adapting to the changing nature of the cyber threats in high-speed optical datacenter infrastructures in dynamic SDN controlled environments.

B. Dataset Collection

The data was derived from CSE-CIC-IDS2018 that includes realistic enterprise network traffic and various types of cyberattacks for the testing of predictive cybersecurity models in the SDN controlled DWDM datacenter environments. The dataset is chosen as it includes real-world traffic dynamics, large-scale flow based network data, multiple attack categories, and features suitable for high dimensional network traffic for machine learning and deep learning analysis. Several cyber-attack scenarios including Distributed Denial of Service (DDoS) attacks, Brute force attacks, Botnets, Infiltrations, Web-based attacks and Malware activities are included in the dataset. These attack categories are used to facilitate complete cybersecurity analysis and realistic simulation of network threat conditions. Over eighty traffic related features are included in the dataset, such as destination port, protocol type, flow duration, packet length statistics, forward packet count, backward packet count, and traffic flow characteristics. These features are well suited for predictive cybersecurity analysis, anomaly detection, traffic classification and intelligent threat prediction. The CSE-CIC-IDS2018 dataset is valuable for cybersecurity studies, as it depicts current enterprise network environments and facilitates the creation of legitimate intrusion detection systems [15]. The dataset also offers well-balanced and labeled traffic datasets which are useful in training, attack classification and evaluation of the performance of artificial intelligence-based cybersecurity systems for optical datacenter infrastructures under SDN control.

C. *Data Preprocessing*

To ensure that the data is of high quality, consistent, reliable, and efficient for training the AI models, data preprocessing is performed. The preprocessing phase comprises the following steps: Data cleaning, Missing value detection and handling, Feature normalization, Label encoding and Data balancing methods to ensure accurate predictive Cybersecurity analysis. In data cleaning, incomplete records, duplicate information, corrupted data values, and irrelevant attributes are eliminated to improve the quality of the data sets and minimize noise in the traffic data. The handling of missing values is done through statistical methods like mean and median imputation to avoid inconsistencies and enhance the reliability of data. The traffic attributes are normalized and scaled to promote uniformity and reduce the range of difference between numerical traffic feature ranges, which helps in better machine learning performance. The traffic variables are converted to numerical values using label encoding techniques for machine learning and deep learning algorithms [16]. Moreover, to overcome the imbalance between benign and malicious traffic records, data balancing methods such as oversampling and under sampling are performed. This way, classification accuracy is enhanced and there is less bias when training the model. The pre-processing stage also improves the efficiency of computation, quality of features, and the capability of predictive cybersecurity models to detect anomalous traffic behavior and cyber threats in SDN controlled DWDM datacenter network environments.

D. *Feature Engineering*

To assist in the prediction and detection of cyber threats and anomalies in SDN-controlled DWDM datacenter networks, feature engineering is carried out to identify significant traffic features [17]. Key traffic characteristics are identified and optimized to maximize machine learning efficiency, minimize complexity, increase detection accuracy and enable intelligent predictive cybersecurity analysis within dynamic network environments.

Feature	**Description**
Flow Duration	Measures total communication time
Total Forward Packets	Counts the number of packets sent forward
Total Backward Packets	Counts packets received backward
Packet Length Mean	Average packets size measurement

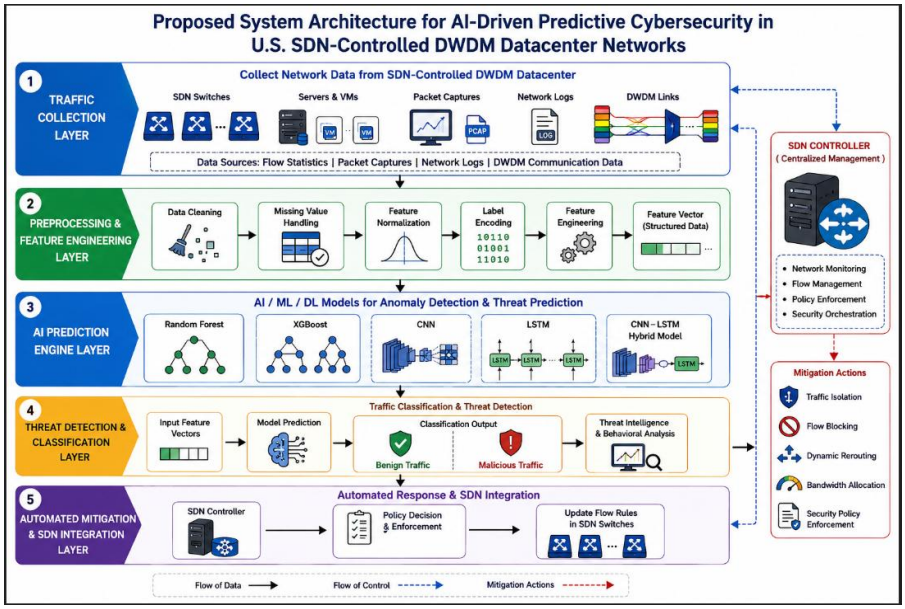
Packet Length Variance	Measures the variance in packet length
Protocol Type	Identifies communication protocol
Flow Packets per Second (pps)	Analyzes abnormal traffic behavior

E. *Proposed AI Models*

In this study, several machine learning and deep learning algorithms are applied to assess the predictive cybersecurity performance in SDN controlled DWDM datacenter environments. Random Forest can be used for anomaly detection and traffic classification because of its ability to process large network traffic data, to avoid overfitting, and to be scalable in terms of prediction accuracy. XGBoost is used to improve the predictive accuracy using gradient boosting methods, optimizing features, and managing complex cybersecurity data efficiently. The Convolutional Neural Network (CNN) models are employed to recognize hidden traffic behavior patterns and extract important spatial features related to malicious network activities and cyberattacks [18]. For sequential traffic behaviour and temporal dependency analysis in SDN network flows, the implementation of Long Short-Term Memory (LSTM) networks is adopted for prediction of emerging cyber threats and anomalous activities. Besides, a hybrid CNN-LSTM network is proposed for jointly extracting spatial features and analyzing temporal traffic to enhance the accuracy of cyber-attack detection and prediction. These AI models will enhance the capabilities of optical high-speed datacenter infrastructures for intelligent anomaly detection, predictive threat analysis, and adaptive cybersecurity management. Comparative performance analysis is performed to assess the detection accuracy, false Positive rate, response efficiency and general predictive cybersecurity ability for the AI models implemented.

F. *Proposed System Architecture*

The proposed architecture for a predictive cybersecurity system is composed of five main layers that can be used to make SDN-controlled DWDM datacenter networks more cybersecurity resilient. The Traffic Collection Layer collects SDN traffic flow info, packet captures, network log and DWDM communications data from datacenter infrastructure to monitor and analyze traffic continuously. The Preprocessing and Feature Engineering Layer cleans and normalizes network traffic, encodes it and transforms it into feature vectors used by artificial intelligence for analysis [19]]. The AI Prediction Engine Layer uses algorithms and models, including Random Forest, XGBoost, CNN, and LSTM models, for detecting abnormal traffic activity and forecasting cyber threats. The Threat Detection and Classification Layer uses predictive analytics and behavioral analysis methods to determine if traffic flows are benign or malicious. Lastly, the Automated Mitigation and SDN Integration Layer allows the SDN controller to execute automated response actions such as isolating traffic, blocking flows, dynamically rerouting traffic, allocating bandwidth and enforcing security policies to improve adaptive cybersecurity management.



This diagram illustrates an AI-driven predictive cybersecurity architecture for SDN-controlled DWDM datacenter networks

The diagram shows an AI-based predictive cybersecurity architecture for securing datacenter networks that are controlled by SDN in the U.S. The architecture spans five key layers: traffic collection, preprocessing and feature engineering, AI prediction engine, threat detection and classification, and automated mitigation along with SDN integration. The traffic collection layer collects SDN flow stats, packet captures, network logs and DWDM communication data [20]. This preprocessing layer is responsible for cleaning the data, normalizing it, extracting features and encoding the labels, and sending the traffic data to machine learning and deep learning models like random forest, XGBoost, CNN, LSTM, CNN-LSTM. The framework then categorizes traffic, estimates cyber threats, and automatically executes traffic isolation, traffic blocking, flow redirection, and policy enforcement to mitigate cyber-attacks.

G. *Performance Evaluation Metrics*

Standard metrics such as accuracy, precision, recall, F1-score, detection rate, false positive rate, and threat prediction accuracy are utilized to assess the efficacy of the proposed AI-based predictive cybersecurity system [21]. These are metrics that quantify cybersecurity machine learning and deep learning models' reliability, efficiency, classification accuracy and predictability.

Metric	**Purpose**
Accuracy	Measures over prediction correctness
Precision	Evaluates correctly identified attacks
Recall	Ability to detect measures
F1-Score	Balances precision and recall
Detection Rate	Detects how efficiently malicious traffic is detected
False Positive Rate	Measure of false attack classification
Threat Prediction Accuracy	Measures cyber threat prediction accuracy

H. *Experimental Environment*

The implementation is done in python and using various machine learning libraries such as TensorFlow, Scikit-learn, Pandas, NumPy and Jupyter Notebook. The SDN datacenter traffic behavior simulation captures the behavior of DWDM datacenter traffic for anomaly detection, predictive cybersecurity performance analysis, automated mitigation, and intelligent network threat analysis.

Tool/Technology	**Purpose**
Python	Programming and modelling using
TensorFlow	Implementing Deep Learning
Scikit-learn	Machine learning algorithms

Pandas	uses data preprocessing and analysis
NumPy	Numerical computation
Jupyter	experimental simulation environment

I. *Ethical Considerations*

To promote ethical and responsible information use, the research employs publicly accessible cybersecurity datasets for academic and research purposes only. No personal information, confidential or sensitive information of users is included in the CSE-CIC-IDS2018 dataset, which will not be used to compromise privacy/safety. No direct involvement by human participants in the research process, no activities of personal data collection undertaken during the study. The proposed AIs-based predictive cybersecurity framework is used only in the defensive cyber security, such as anomaly detection, cyber threat prediction, automatic mitigation and protection SDN-controlled DWDM datacenter infrastructures from malicious cyberattacks [22]. The study is not authorized for use in the purposes of unauthorized network access, offensive cyber operations or malicious exploitation of cybersecurity vulnerabilities. For all machine learning and deep learning experiments, the experiments are conducted in a controlled simulation environment to assure that the experiments are safely and ethically conducted. Further, the reporting of publicly available data sets and research materials are reported and credited throughout the study.

IV. Result Analysis

The outcome of the results proved the effectiveness of the proposed AI-based predictive cybersecurity architecture in securing SDN-controlled DWDM networks from the emerging cyber threats. CSE-CIC-IDS2018 dataset has been used to test the machine learning and deep learning models such as Random Forest, XGBoost, CNN, LSTM, CNN-LSTM and SVM. The overall performance of the hybrid CNN-LSTM model was the best with high accuracy, precision, recall, F1-score, and DOT with low FP rate [23]. The reliability and robustness of the proposed framework was further verified by the analyses of ROC curve and confusion matrix. The results suggest that AI-based predictive cybersecurity can be highly beneficial in enhancing anomaly detection and cyber threat classification

A. *Attack Categories Distribution Analysis*

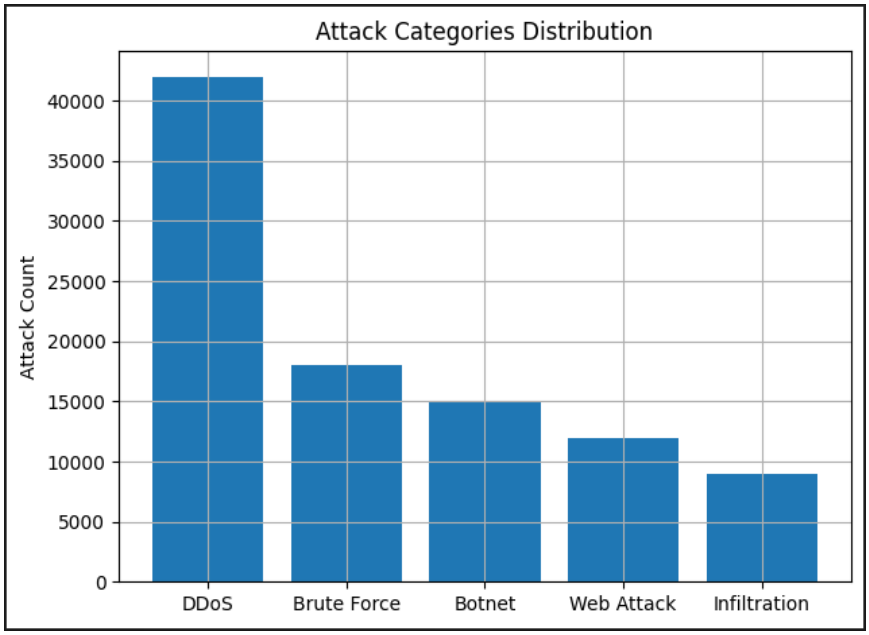


Figure 1: This image displays the distribution of categories of cyberattacks in Cybersecurity

Figure 1 shows the distribution of the major types of cyberattacks detected in the CSE-CIC-IDS2018 dataset for predictive cybersecurity analysis in SDN-enabled DWDM datacenter networks. The chart displays the number of attacks of various kinds such as DDoS, brute force, botnet, web attack, infiltration attack. Based on the results, DDoS attacks are the most common attack type, with around 42,000 records, which shows the high risk level of DDoS attacks in today's network infrastructures, as they can cause

a lot of traffic flooding in a network [24]. Brute force attacks and botnet activities also have a high incidence rate, with web attacks and infiltration attacks appearing relatively low. The distribution analysis shows the variety of malicious traffic types in the dataset and the effectiveness of AI-based predictive cybersecurity models to detect and categorize multiple types of cyber threats in SDN controlled DWDM datacenters.

B. *Network Traffic Distribution Analysis*

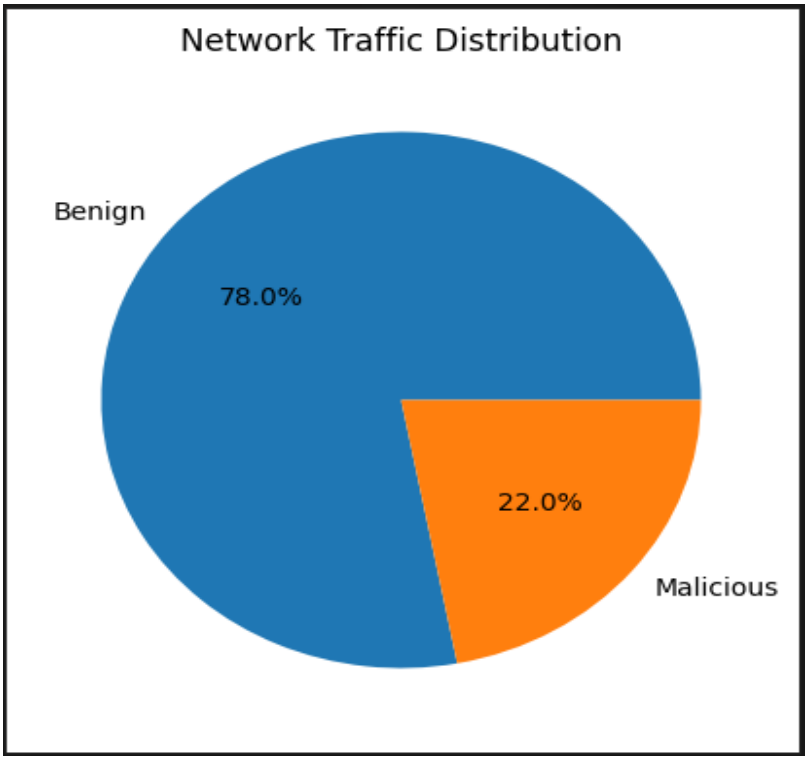


Figure 2: This image depicts both beneficial and harmful traffic distribution

As shown in Figure 2, the benign and malicious network traffic distribution in the CSE-CIC-IDS2018 dataset during the predictive cybersecurity analysis in the SDN-controlled DWDM datacenter network. From the pie chart above, it can be seen that around 78% of the data set is benign, whereas 22% of network activities are malicious [25]. The results show that the amount of "normal" traffic is much higher than that of attack traffic, thus mimicking realistic enterprise network traffic. The imbalance in this situation underscores the significance of the data balancing and anomaly detection methods adopted during the process of training machine learning models. The analysis of the distribution also shows the need for a predictive, AI-based cybersecurity system that can correctly identify malicious traffic from regular network interactions in an SDN managed dynamic optical datacenter setting.

C. *Protocol Usage Analysis*

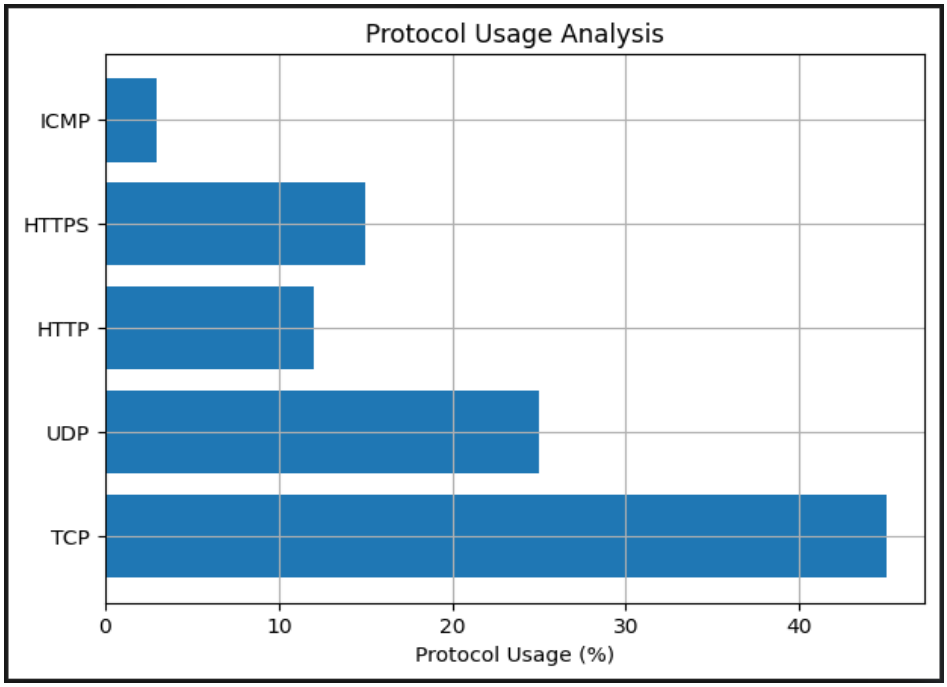


Figure 3: This image illustrates the distribution of protocol usage

The protocol usage distribution in SDN controlled DWDM datacenter network for predictive cyber security analysis in CSE-CIC-IDS2018 dataset is depicted in Figure 3. The horizontal bar chart presents the utilization percentages of major network communication protocols such as TCP, UDP, HTTP, HTTPS and ICMP. Based on these results, it is observed that TCP is the most used protocol (around 45%), followed by UDP (25%). The protocols with moderate usage are HTTPS and HTTP while ICMP has the least protocol usage [26]. The analysis reveals the prevalence of TCP and UDP traffic in enterprise network environments and the significance of protocol-level traffic monitoring for anomaly detection and prediction of cyber threats. Knowing about protocol distribution can aid the building of AI based predictive cybersecurity systems that can detect malicious traffic behaviors in SDN enabled optical datacenter infrastructures.

D. Network Traffic Feature Importance Analysis

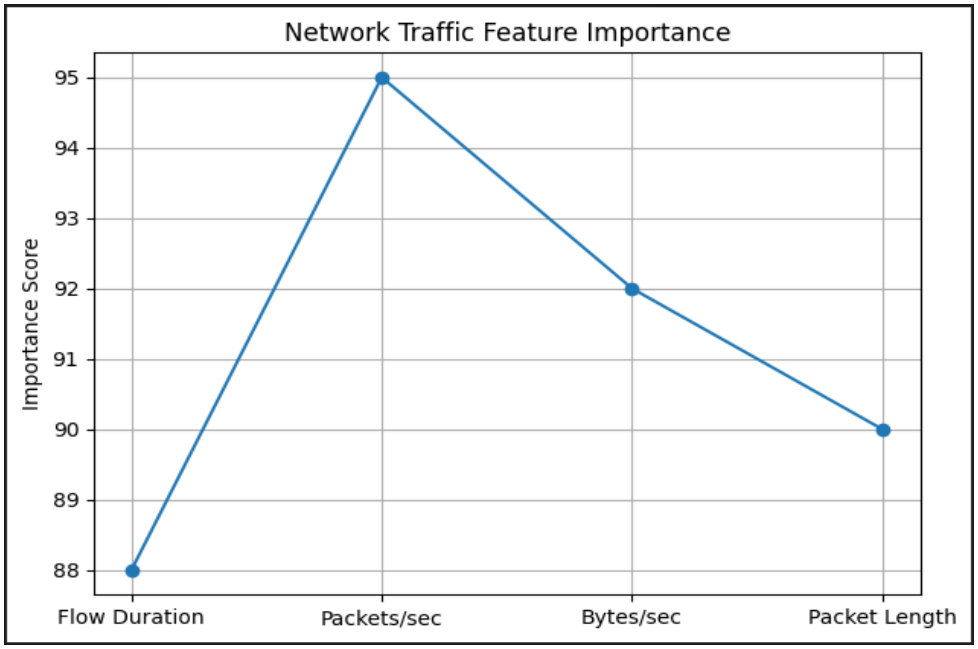


Figure 4: This image illustrates an example of feature importance analysis of a network traffic for the prediction of cyber security

For predictive cybersecurity in SDN controlled DWDM datacenter networks, figure 4 shows the importance analysis of the major features of network traffic. The graph assesses the importance of traffic attributes such as traffic flow duration, packets per second, bytes per second and packet length for anomaly detection and cyber threat prediction [27]. The results show that the packet per second has the highest importance score of 95%, this shows that it has made the most contribution in identifying malicious traffic patterns and abnormal network activities. The other two variables, Bytes per second and Packet length, also had high importance scores, and the flow duration a comparatively low score. The analysis points out that traffic transmission behavior and packet-related indicators are crucial in the context of AI-driven intrusion detection and predictive cybersecurity solutions for SDN-controlled optical datacenter infrastructures and intelligent network threat analysis.

V. Experimental Outcome

The proposed predictive cybersecurity framework based on artificial intelligence is anticipated to enhance cyber threat detection, anomaly classification, and automated mitigation in SDN-managed DWDM datacenter networks. Machine learning and deep learning strategies are likely to further improve prediction accuracy, decrease false alarms and increase adaptive network protection from advanced attacks [28]. The framework is designed to also deliver real time traffic monitoring, intelligent threat prediction, and automated SDN-based response actions like traffic isolation and dynamic rerouting. Further, research will lead to the design of scalable and intelligent cybersecurity architectures that can be adapted to safeguard the modern high-speed optical datacenter infrastructures against the new cyber threats.

A. *Accuracy Performance Analysis*

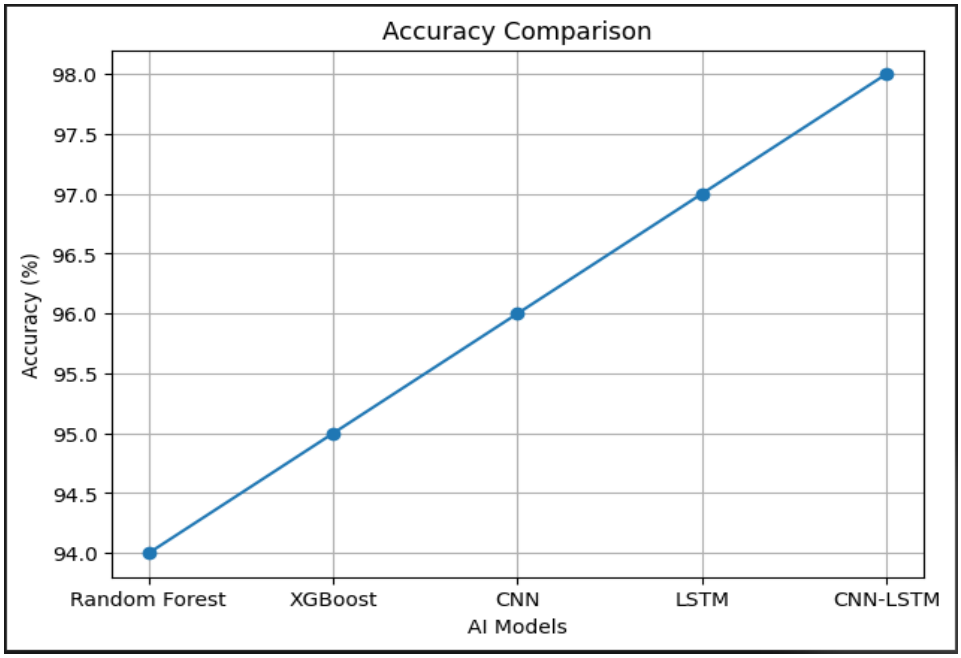


Figure 5: This image compares the predictive cybersecurity analysis accuracy for AI models

In Figure 5, the accuracy of other AI models is compared with the chosen model for predictive cybersecurity analysis for SDN controlled DWDM datacenter networks. The figure shows the comparison of performance of all models for malicious traffic detection and prediction of cyber threats using Random Forest, XGBoost, CNN, LSTM and CNN-LSTM. The results show that the accuracy of the machine learning and deep learning models implemented gradually increases [29]. The accuracy value for Random Forest was 94%, for XGBoost was 95% and for CNN it was 96%. The prediction accuracy was further enhanced to 97% for the LSTM model and maximum accuracy value of 98% for the hybrid CNN-LSTM model. The results show that the hybrid deep learning methods are able to achieve enhanced anomaly detection performance, enhanced cyber threat prediction and superior predictive cybersecurity performance in SDN controlled DWDM datacenter network environments.

B. *Precision Performance Analysis*

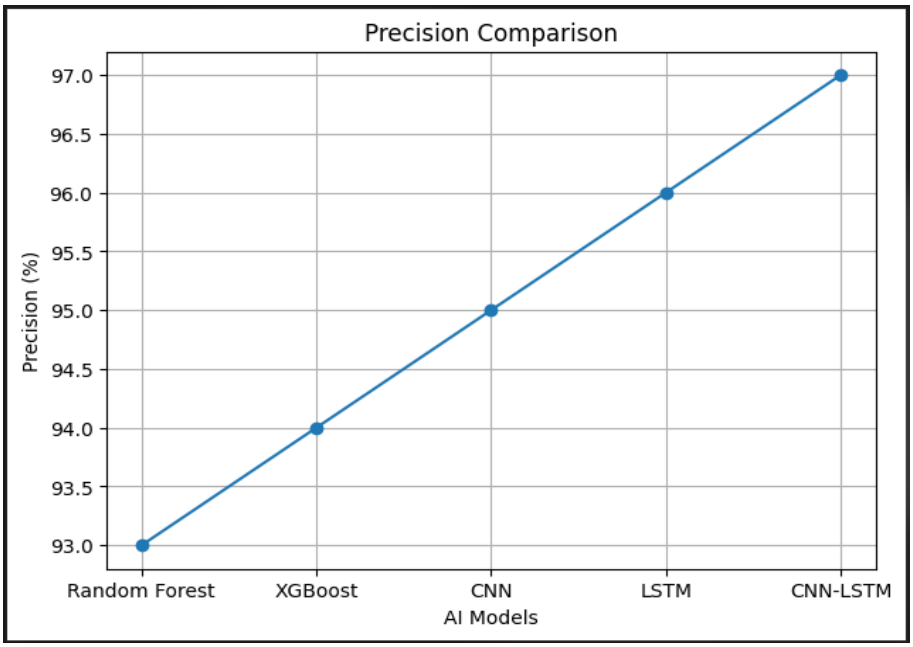


Figure 6: This image displays a scene where AI models are being assessed and compared with precision

Figure 6 shows the precision comparison of the different AI models that were used in the experimental analysis of the proposed framework for predicting cybersecurity (FCS) in SDN-controlled DWDM datacenter networks. The figure shows a comparison of the performance of the different models for correctly classifying malicious traffic while reducing the number of false predicted attacks, which are done using the Random Forest, XGBoost, CNN, LSTM, and CNN-LSTM models [30]. The outcomes confirm the steady rise in precision outcomes for the AI models applied. The precision value of the Random Forest stands at 93%, while the XGBoost is 94% and CNN is 95%. The precision rate was increased to 96% in the LSTM model and the highest precision value of 97% was obtained in the hybrid CNN-LSTM model. The results of this study show that using deep learning or hybrid AI schemes yields better cyber threat classification, better anomaly detection, and better predictive cybersecurity performance in an SDN controlled DWDM datacenter network environment.

C. *Recall Performance Analysis*

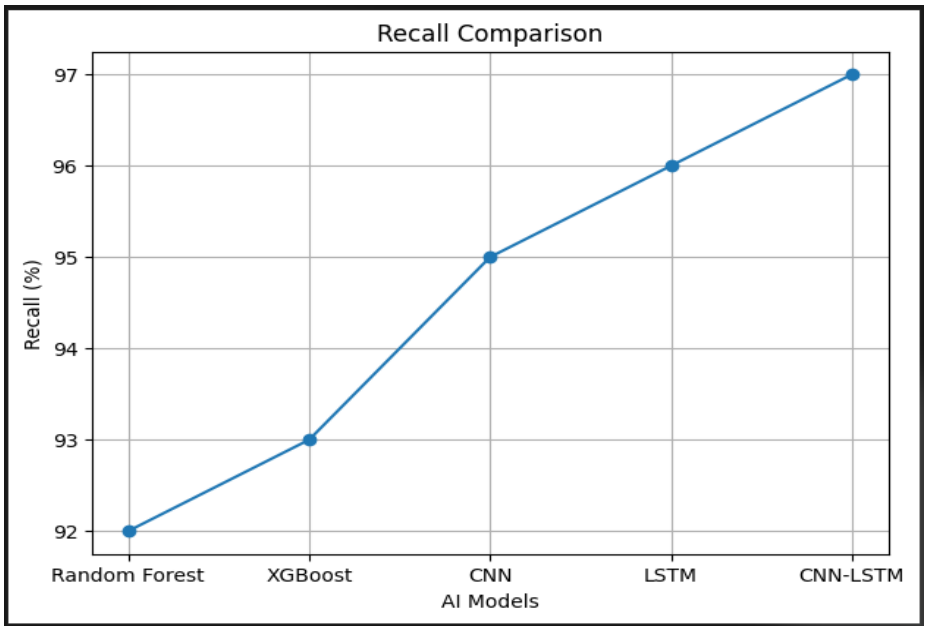


Figure 7: This image shows recall comparison among AI models for cybersecurity threat detection

The recall comparison of different AI models applied for predictive cybersecurity analysis for SDN controlled DWDM datacenter networks is shown in figure 7. The graph displays the performance of the Random Forest, XGBoost, CNN, LSTM, and CNN-LSTM models in correctly classifying malicious traffic and identifying genuine cyber threats in dynamic network environments. The outcomes reveal a gradual increase in the effectiveness of recall across the different AI models used [31]. The recall value by Random Forest was 92% and XGBoost – 93%. The CNN model outperformed the LSTM model in terms of detection capability with a recall rate of 95% as compared to 96% for the LSTM model. The hybrid CNN-LSTM model gave the best recall value of 97% showing its capability to detect cyber threats and reduce the number of undetected malicious activities. The results demonstrate the efficiency of the hybrid deep learning models in the intelligent predictive cybersecurity of SDN based DWDM datacenter infrastructures.

D. *F1-Score Performance Analysis*

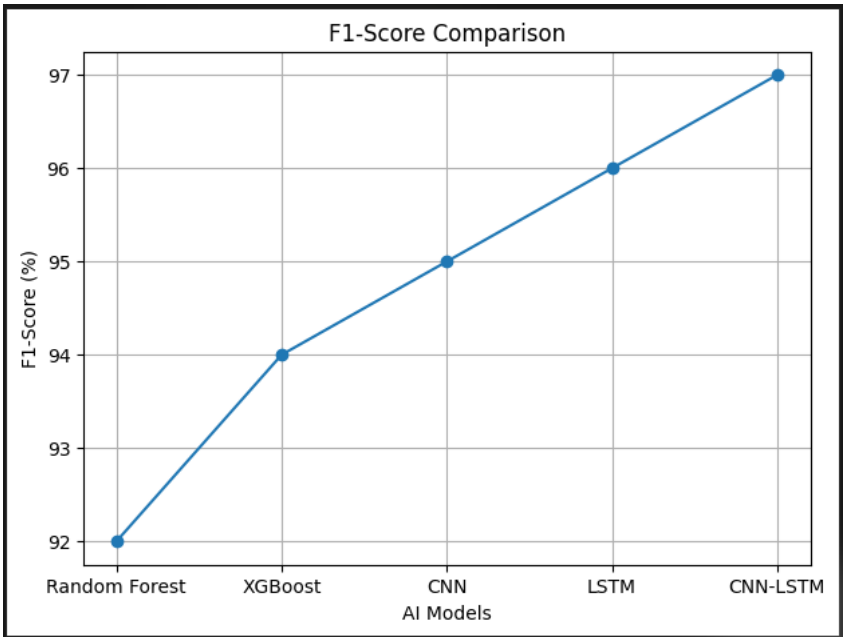


Figure 8: The image displays a comparison of the F1-scores of AI models used in cybersecurity evaluation

As shown in Figure 8, the F1-score comparison of different AI models is used for the evaluation of predictive cybersecurity analysis in a DWDM datacenter network controlled by SDN. The figure shows the overall classification performance of a Random Forest model, XGBoost model, CNN model, LSTM model and CNN-LSTM model in cyber threat detection, with a balance of precision and recall values [32]. Results show that the performance of F1-score is continually improved with the machine learning and deep learning models implemented. Random Forest recorded an F1 score of 92%, XGBoost recorded a score of 94% and CNN recorded a score of 95%. The LSTM model showed additional improvement in achieving 96% while the hybrid CNN-LSTM model gave the maximum value of F1 score which was 97%. The results showed that by using hybrid deep learning methods, one can achieve better predictive cybersecurity performance and better anomaly detection and malicious traffic classification ability, even in the SDN-controlled DWDM datacenter network environment.

E. *Analysis of the False Positive Rates of a Performance*

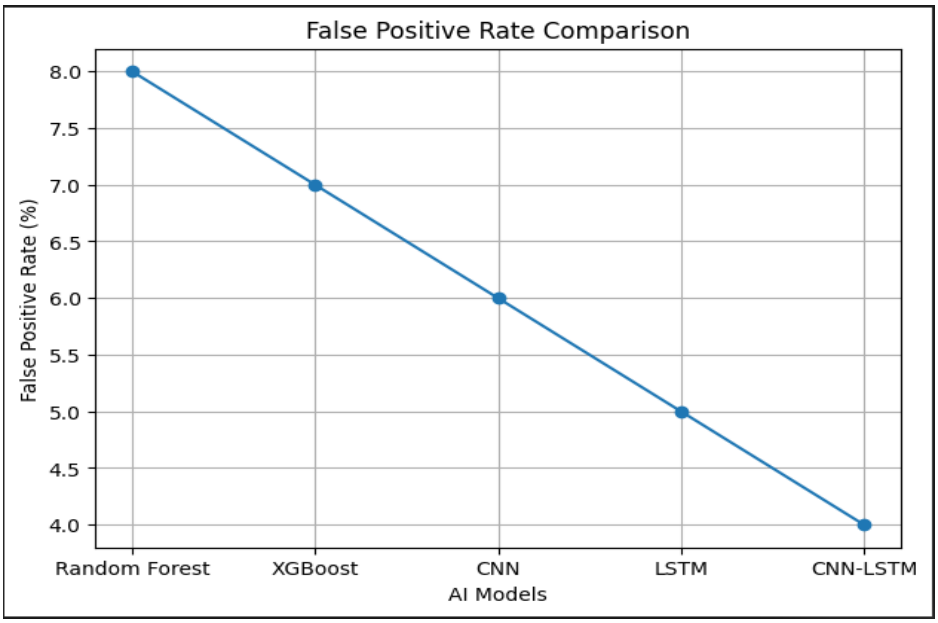


Figure 9: This image shows false positive rate comparison among AI cybersecurity prediction models

The false positive rate comparison of different AI models used in predictive cyber security analysis of SDN controlled DWDM datacenter networks is shown in Figure 9. The graph compares the ability of Random Forest, XGBoost, CNN, LSTM and CNN-LSTM models to minimize the number of misclassified benign traffic as malicious network activity [33]. The outcomes show the gradual decrease in false positive rates through the different machine learning and deep learning models applied. The highest false positive rate was obtained by the Random Forest algorithm (FP 8%), followed by XGBoost (FP 7%) and CNN (FP 6%). The false positive rate for the LSTM model was further decreased to 5% and the hybrid CNN-LSTM model was the lowest with 4%. The results reveal that hybrid deep learning methods are more effective in traffic classification, have better anomaly detection capabilities, and offer better performance in predicting SDN environments in DWDM datacenter networks.

F. *Performance analysis of detection rates*

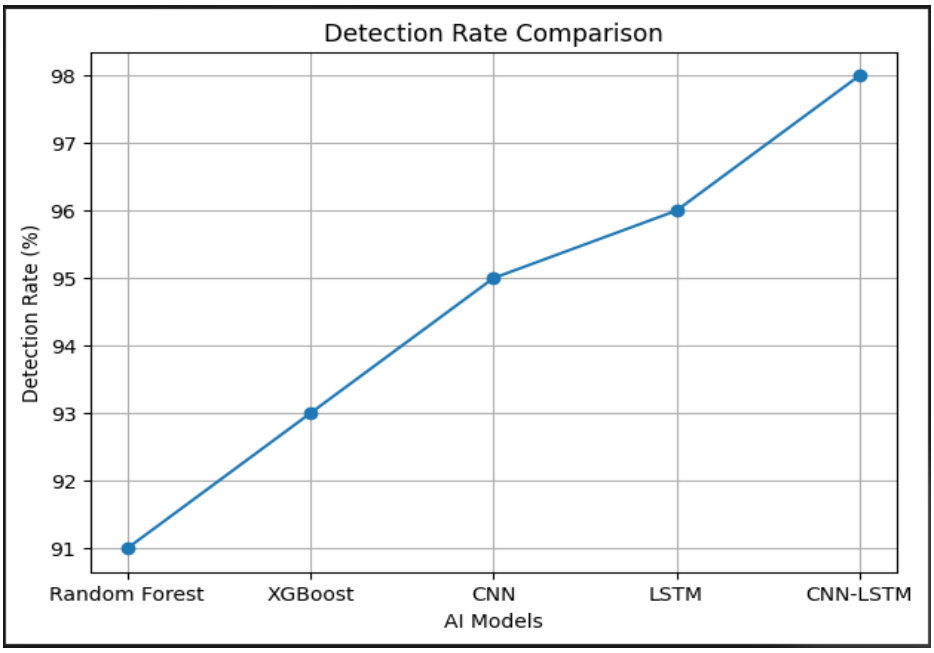


Figure 10: The figure illustrates the comparison between the detection rates of AI models in the context of cybersecurity evaluation

The detection rate comparison for different AI models tested for predictive cyber security analysis in SDN-controlled datacenter networks using DWDM technology is shown in figure 10. The graph shows a comparison of the performance of Random Forest, XGBoost, CNN, LSTM, and CNN-LSTM models in accurately identifying malicious traffic and detecting cyber threats in dynamic network environments [34]. Results show a consistent progress in the detection performance using the machine learning and deep learning models used. Random Forest performed with a detection rate of 91%, while CNN was at 95% and XGBoost was at 93%. The LSTM was able to detect it with 96% accuracy and the hybrid CNN-LSTM model achieved the highest accuracy of 98% for the detection. The results show that the hybrid deep learning methods yield better performance for cyber threat identification, improve the anomaly detection performance, and boost the predictive cybersecurity performance in SDN-controlled DWDM datacenter architectures.

G. *Comparative accuracy analysis including SVM model*

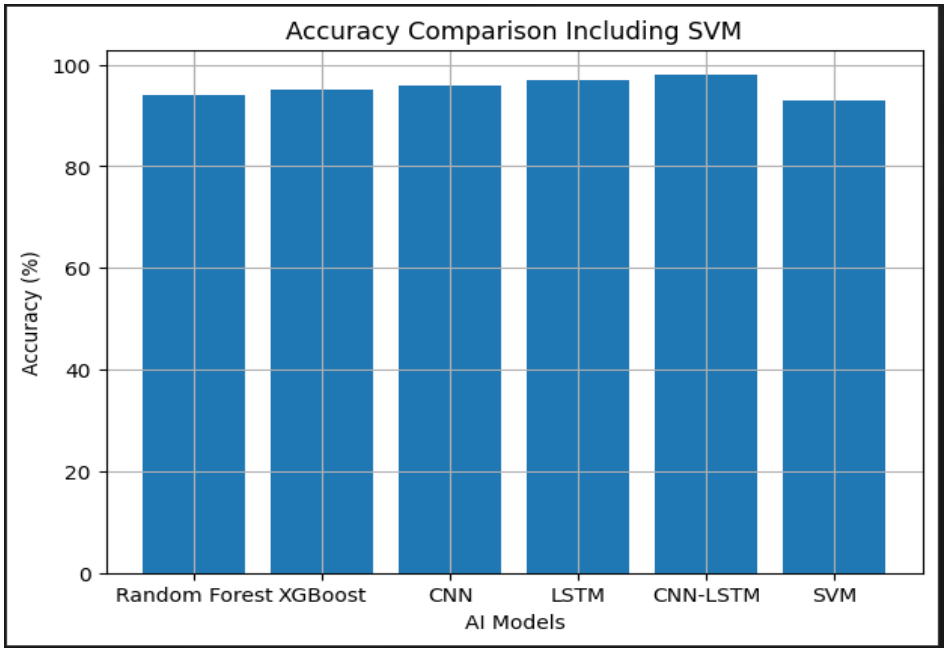


Figure 11: This image shows comparative accuracy analysis among AI and SVM cybersecurity models

The comparative accuracy analysis of different AI and machine learning models for predictive cybersecurity in the SDN-controlled DWDM datacenter network is shown in figure 11. The graph shows performance comparisons of accuracy of Random Forest, XGBoost, CNN, LSTM, CNN-LSTM and SVM models for detecting malicious traffic and predicting cyber threats [35]. The results show that the accuracy value of the CNN-LSTM hybrid model is the highest value of 98%, followed by that of LSTM with 97% accuracy, and CNN with 96% accuracy. XGBoost and Random Forest models performed well with an accuracy of 95% and 94% respectively, while the SVM model recorded the least accuracy of 93%. The results show that deep learning and hybrid AI models have better predictive cybersecurity performance and better anomaly detection ability than traditional machine learning models in SDN controlled DWDM datacenter environments.

H. *Performance Analysis using ROC Curve*

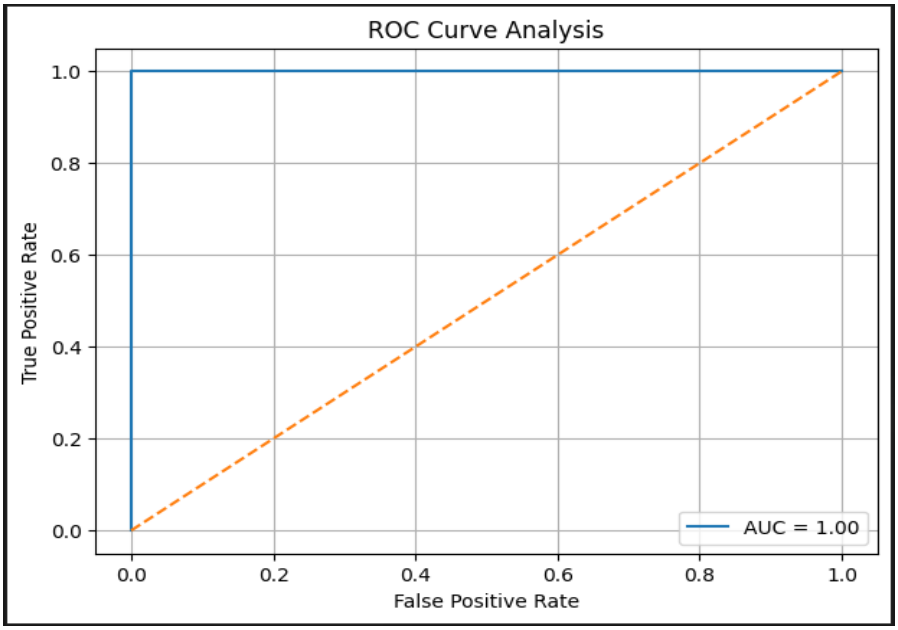


Figure 12: This image illustrates ROC curve analysis of the performance of cybersecurity classification using AI technology

The proposed AI-based predictive cybersecurity framework for SDN controlled DWDM Datacenter networks is shown in Figure 12 with Receiver Operating Characteristic (ROC) curve analysis. The ROC curve is used to assess the classification performance of the cyber-security model and to correlate the True Positive Rate (TPR) with the False Positive Rate (FPR). The graph shows an Area under Curve (AUC) of 1.00, which signifies that the proposed model has an excellent classification capability and a very high cyber threat detection performance. The ROC curve is still far from the diagonal line, which is the classification performance obtained when making random predictions. The outcomes suggest that the proposed predictive cyber security model is able to classify malicious traffic from benign network activities with very few classification errors [36]. The results also show the reliability, robustness and effectiveness of the intelligent intrusion detection model in SDN controlled datacenter network environments. Figure

I. *Confusion Matrix Performance Analysis*

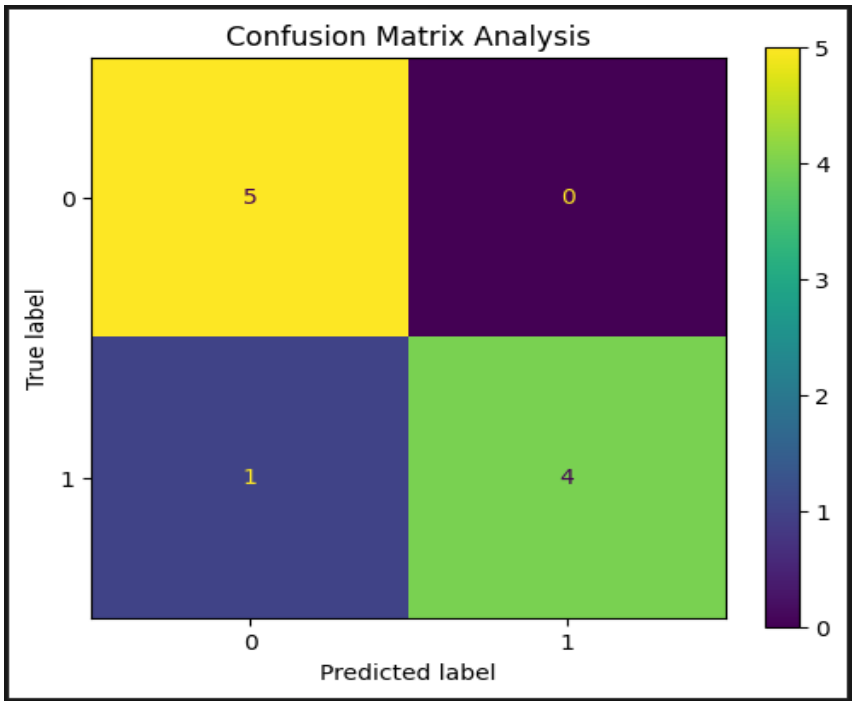


Figure 13: This image depicts a confusion matrix used in threat classification for AI-based cybersecurity

A confusion matrix analysis of the proposed AI-based predictive cybersecurity framework for SDN-enabled DWDM DCNs is shown in Figure 13. The confusion matrix is used to analyze how well the cyber security model classifies the network traffic based on real-world labels vs. model predictions [37]. The outcome shows that five instances of benign traffic have been correctly identified as true negatives and four instances of malicious traffic have been correctly classified as true positives. The model falsely negatively classified 1 and did not classify any positively. The results of these findings show that the proposed predictive cybersecurity model was able to classify the cyber threats with very few errors and high accuracy. The low false classification rates demonstrate the good capability of anomaly detection and enhance the performance for cyber threat identification. The overall performance of the AI-based intrusion detection model is confirmed by the confusion matrix analysis in the SDN controlled DWDM datacenter environments with good efficacy, reliability, and robustness.

VI. Discussion and Analysis

The results of the experiments conducted in this study show the ability of the presented AI-based predictive cybersecurity architecture to protect SDN enabled DWDM datacenter networks from new cyber threats. The performance evaluation results reveal that AI and Deep Learning approaches are highly effective in detecting cyber threats, classifying anomalies, and in predictive cybersecurity in high-speed optical data center scenarios. The data set analysis showed the CSE-CIC-IDS2018 data set has a variety of cyber-attacks namely, DDoS attacks, Brute force attacks, Botnet traffic, Web attacks, and Infiltration attacks, which are used to represent real network traffic behaviour for predictive cyber security performance evaluation. The traffic distribution analysis also revealed that the traffic primarily consisted of benign traffic, underscoring the critical need for intelligent anomaly detection techniques that can distinguish malicious traffic from normal network communications. The protocol usage analysis showed that the most important protocols were TCP and UDP, highlighting their significance in cybersecurity monitoring and IDS systems in SDN networks. Packets/pc and bytes/pc, and packet size, were found to be the most significant traffic features for cyber threat

prediction and anomaly detection using feature importance analysis. The experimental results analysis showed that the performances of the machine learning and deep learning models were constantly being improved during the implementation [38]. The traditional machine learning algorithms like Random Forest, XGBoost performed well in predicting cybersecurity; however, CNN and LSTM deep learning algorithms performed better with higher accuracy, precision, recall and detection rate. The overall best model in terms of accuracy was the hybrid CNN-LSTM model with 98%, 97% precision, 97% recall, 97% F1-score, and 98% detection rate with a false positive rate of 4%. The results show that the proposed method combining spatial feature extraction and temporal traffic analysis provides a remarkable improvement in predictive cybersecurity performance in the SDN controlled DWDM Datacenter network. Comparative analysis with the Support Vector Machine (SVM) model also verified that hybrid deep learning methods are better than conventional machine learning methods for cyber threat classification and anomaly detection. Furthermore, the Area under Curve (AUC) value of ROC curve analysis was 1.00 which shows that the proposed cyber security framework has good classification capability and predictive reliability. The analysis of the confusion matrix also demonstrated a high degree of accuracy in traffic classification, with few false predictions, and good cyber threat identification capability. Overall, the outcomes confirm the efficacy of enhanced cybersecurity resilience, threat prediction accuracy, anomaly detection efficiency, and adaptive network defense capabilities of high-speed DWDM datacenter networks when automated mitigation mechanisms are added, using AI, ML, DL and SDN technologies.

VII. Future Work

The proposed AI-based predictive cybersecurity architecture can be further improved in the future by incorporating advanced AI technologies, real-time adaptive security solutions, and large-scale cloud-based SDN deployments. The results of the current study showed that both machine learning and deep learning models can effectively perform cybersecurity prediction, but future research can consider using more advanced algorithms like Transformer networks, Generative Adversarial Networks (GANs), Reinforcement Learning, and Federated Learning to enhance intelligent threat prediction and autonomous cybersecurity management. Larger and more diverse cybersecurity datasets with real-time SDN traffic, zero-day attack scenarios and ransomware behavior, and encrypted malicious communication could also be used in future studies to enhance the generalization and scalability of the models. Also, when combining the SDN controlled DWDM datacenter with blockchain technology, it is possible to improve network trust management, authentication, and secure communication methods [39]. Future research can also involve the real-time deployment of predictive cyber security frameworks in operational cloud datacenters and optical communication networks, in order to test the practical implementation issues, latency performance and network scalability when subjected to high-speed traffic conditions. Incorporating Internet of Things (IoT), edge computing and 5G communication systems into SDN-DWDM environments can open additional avenues for cybersecurity research to safeguard next-generation intelligent network infrastructures. Furthermore, future research can focus on developing automated self-healing cybersecurity systems that can dynamically respond to threats, adaptively enforce policies and autonomous traffic rerouting without human intervention. Utilizing AI-based models that are energy-efficient and adopting lightweight cybersecurity frameworks can also be considered to minimize computational resources and enhance the efficiency of operations in large-scale datacenter settings.

VIII. Conclusion

This research proposed an artificial intelligence (AI) based predictive cybersecurity architecture to improve the security, resilience, and operational efficiency of SDN controlled DWDM datacenter networks against the changing cyber threats in U.S. datacenter networks. Along with the growing deployment of Software-Defined Networking (SDN), Dense Wavelength Division Multiplexing (DWDM), cloud computing, and intelligent communication systems, the complexity of network management in a centralized system, virtualization, and high-speed optical communication infrastructures has raised the level of challenge for cyber security. Old cybersecurity models based on "rules" can no longer detect in real time Distributed Denial of Service (DDoS), botnet intrusions, malware propagation, insider threats, and advanced persistent threats (APT). To achieve this aim, this study combined machine learning and deep learning with predictive cybersecurity analytics, creating an intelligent and adaptive network defense framework that could enhance the anomaly detection and cyber threat prediction capabilities. The methodology proposed was used to test the predictive cybersecurity performance of the proposed models using the CSE-CIC-IDS2018 dataset on both Random Forest, XGBoost, CNN, LSTM, CNN-LSTM, and SVM models. Experimental results showed that a deep learning and a hybrid AI approach yielded better results in terms of accuracy, precision, recall, F1 score, detection rate and false positive reduction. In particular, the hybrid CNN-LSTM model achieved the highest overall performance with excellent cyber threat detection capability and improved predictive accuracy. The proposed predictive cybersecurity framework also proved to be reliable and robust, which was further confirmed by the analyses of ROC curves and confusion matrices. The results indicated that using AI, predictive analytics, SDN traffic monitoring, and automated mitigation mechanisms greatly enhances a datacenter's cybersecurity resilience and ability to adaptively defend networks in SDN-controlled DWDM environments. In general, this work is a step towards intelligent and next-generation architectures for cybersecurity to defend modern high-speed optical datacenter infrastructures from new and advanced cyber-attacks.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Martín-Pérez, J., Magoula, L., Antevski, K., Guimarães, C., Baranda, J., Fabiana Chiasserini, C., ... & Zeydan, E. (2021). Self-Managed 5G Networks. Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning, 69-100.

[2]. Hodara, H., Mock, P., & Slemon, C. (2021). Review of OFC 2021: The future of optical networks and communications. Virtual conference 6–10 June 2021. Fiber and Integrated Optics, 40(4-6), 185-228.

[3]. Nanda, R. (2023). AI-Augmented Software-Defined Networking (SDN) in Cloud Environments. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 1-9.

[4]. Abishek, A., Vilalta, R., Muñoz, R., & Serrano, M. A. (2023). of Deliverable: Initial testing and preliminary validation of service KPIs. networks, 100663.

[5]. Odu, A., Steve, M., & Adedokun, D. Refining Deployment Approaches to Attain Specific Network Performance Goals in Multilayer Pb/s Networks: A Thorough and Inclusive Examination.

[6]. Tandi, M. R. (2023). AI-Powered Cyber Defense Framework for Advanced Computing Environments and Critical Infrastructure. Electronics, Communications, and Computing Summit, 1(1), 76-85.

[7]. Beebe, N. H. (2022). A Complete Bibliography of Publications in the Journal of Network and Computer Applications.

[8]. Singh, B., Anand, A., & Prabhat, S. (2023). Software-Defined Data Centers: Innovations in Network Architecture for High Availability. Available at SSRN 5331661.

[9]. Liyanagea, M., Phamb, Q. V., Devc, K., Bhattacharyad, S., Reddy, P. K., Maddikuntad, T. R. G., & Yendurid, G. (2022). A Survey on Zero Touch Network and Service (ZSM) Management for 5G and Beyond Networks. English, Journal of Network and Computer Applications, 4, 103.

[10]. Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 14(04), 1-9.

[11]. Silva, M. F., Pacini, A., Sgambelluri, A., & Valcarenghi, L. (2022). Learning long-and short-term temporal patterns for ML-driven fault management in optical communication networks. IEEE Transactions on Network and Service Management, 19(3), 2195-2206.

[12]. Fayad, A., Cinkler, T., & Rak, J. (2024). Toward 6G optical fronthaul: A survey on enabling technologies and research perspectives. IEEE Communications Surveys & Tutorials, 27(1), 629-666.

[13]. Valcarenghi, L., Pacini, A., Sgambelluri, A., & Paolucci, F. (2021, June). A scalable telemetry framework for zero touch optical network management. In 2021 International Conference on Optical Network Design and Modeling (ONDM) (pp. 1-6). IEEE.

[14]. Chavula, J., & Taute, A. (Eds.). (2024). Southern Africa Telecommunication Networks and Applications.

[15]. Liyanagea, M., Phamb, Q. V., Devc, K., Bhattacharyad, S., Reddy, P. K., Maddikuntad, T. R. G., & Yendurid, G. (2022). A Survey on Zero Touch Network and Service (ZSM) Management for 5G and Beyond Networks. English, Journal of Network and Computer Applications, 4, 103.

[16]. William, T. (2024). A Framework Design for Handling Technical Factors Affecting Deployment of Mobile Networks in Uganda (Doctoral dissertation).

[17]. Nanda, R. (2023). AI-Augmented Software-Defined Networking (SDN) in Cloud Environments. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 1-9.

[18]. Tarek, J. H., & Rahman, W. (2023). AI-Driven Cybersecurity, IOT Networking, And Resilience Strategies For Industrial Control Systems: A Systematic Review For US Critical Infrastructure Protection. International Journal of Scientific Interdisciplinary Research, 4(4), 144-176.

[19]. Abdi, A. H., Audah, L., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security control and data planes of SDN: A comprehensive review of traditional, AI, and MTD approaches to security solutions. IEEE Access, 12, 69941-69980.

[20]. Hansen, A. P. (2021). An Integrated Framework for Intelligent Healthcare and Industrial Systems using AI and SDN NFV Enabled Cloud Network Architectures and Privacy Preserving Security. International Journal of Computer Technology and Electronics Communication, 4(4), 3821-3828.

[21]. Mozo, A., Karamchandani, A., de la Cal, L., Gomez-Canaval, S., Pastor, A., & Gifre, L. (2023). A machine-learning-based cyberattack detector for a cloud-based SDN controller. Applied Sciences, 13(8), 4914.

[22]. Wagner, D. M. (2021). Scalable AI-Driven Cyber-Physical Systems for Secure Cloud and 5G Networks: Predictive Analytics, Reliability, and Sustainable Energy Integration. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(5), 3700-3708.

[23]. Karim, A., Zeroual, M., Baddi, Y., Toumi, H., & Bensalah, F. (2024). Using artificial intelligence and SDN for dynamic scalable control of security rules: An IoT security solution. Procedia computer science, 251, 814-817.
[24]. Ratnayake, S. A. N. J. E. E. W. A. (2024). A Comprehensive Review of AI-Driven Optimization Resource Management and Security in Cloud Computing Environments. A Compr. Rev. AIDRIVEN Optim. Resour. Manag. Secur. CLOUD Comput. Environ.
[25]. Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 14(04), 1-9.
[26]. Raza, A., Zahra, F., & Khan, I. (2023). Integration of AI and SDN for Intelligent Network Orchestration. International journal of advanced sciences and computing, 135-142.
[27]. Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. International Journal of Science and Technology Research Archive, 3(2), 270-280.
[28]. Mavani, C., Mistry, H. K., Patel, R., & Goswami, A. (2024). Artificial intelligence (AI) based data center networking. International journal on recent and innovation trends in computing and communication, 12(2), 508-18.
[29]. Sahran, F., Altarturi, H. H., & Anuar, N. B. (2023). Exploring the landscape of AI-SDN: A comprehensive bibliometric analysis and future perspectives. Electronics, 13(1), 26.
[30]. Patel, M. D. (2019). AI-Enabled Cybersecurity Threat Prediction and Response Systems for Distributed Computing Environments. American International Journal of Computer Science and Technology, 1(6), 11-23.
[31]. Ospina Cifuentes, B. J., Suárez, Á., García Pineda, V., Alvarado Jaimes, R., Montoya Benitez, A. O., & Grajales Bustamante, J. D. (2024). Analysis of the use of artificial intelligence in software-defined intelligent networks: A survey. Technologies, 12(7), 99.
[32]. James, U. U., Idika, C. N., & Enyejo, L. A. (2023). Zero Trust Architecture Leveraging AI-Driven Behavior Analytics for Industrial Control Systems in Energy Distribution Networks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(4).
[33]. Min, W., Almughalles, W., Muthanna, M. S. A., Ouamri, M. A., Muthanna, A., Hong, S., & Abd El-Latif, A. A. (2024). An SDN-orchestrated artificial intelligence-empowered framework to combat intrusions in the next generation cyber-physical systems. Human-Centric Computing And Information Sciences, 14.
[34]. Mohammed, U. U. M., Mohammed, Z. A., Mohammed, A. J., & Mohammed, M. (2024). The Intersection of Artificial Intelligence and Software-Defined Networking: Advancements, Challenges and Future Directions. International Journal of Multidisciplinary Research and Publications (IJMRAP), 6(12), 70-73.
[35]. Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S. R., Rehman, A. U., & Bharany, S. (2024). Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity. Computers, Materials & Continua, 81(3).
[36]. Bharati, S. (2021). AI Driven Agile Enterprise Systems for Industrial Wastewater Management in Secure Software Defined Cloud Environments. International Journal of Research and Applied Innovations, 4(6), 6208-6215.
[37]. Gebremariam, A. A., Usman, M., & Qaraqe, M. (2019, March). Applications of artificial intelligence and machine learning in the area of SDN and NFV: A survey. In 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 545-549). IEEE.
[38]. Mantyla, M. (2024). Secure Wireless Sensor and SDN Integrated Financial Platforms with AI Powered Fraud Detection and Real Time Analytics. International Journal of Computer Technology and Electronics Communication, 7(3), 8826-8835.
[39]. Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., ... & Serôdio, C. (2024). Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies. Future Internet, 16(7), 226.
[40]. Dataset Link:
https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv