REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

ADVANCED AI-BASED CYBER SECURITY NETWORK TO REDUCE THE CYBER CRIMES IN THE WORLD

Ali Raed Mohammed AL-SULTANI

Master's Thesis

Supervisor

Asst. Prof. Dr. Ayça KURNAZ TÜRKBEN

İstanbul, 2024

ADVANCED AI-BASED CYBER SECURITY NETWORK TO REDUCE THE CYBER CRIMES IN THE WORLD

Ali Raed Mohammed AL-SULTANI

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY
2024

The thesis titled ADVANCED AI-BASED CYBER SECURITY NETWORK TO REDUCE THE CYBER CRIMES IN THE WORLD prepared by ALI RAED MOHAMMED AL-SULTANI and submitted on 26/01/2024 has been **accepted unanimously** for the degree Master of Science in Electrical and Computer Engineering.

Asst. Prof. Dr. Ayça KURNAZ TÜRKBEN

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Ayça KURNAZ TÜRKBEN	Department of Softwere Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Zeynep ALTAN	Department of Softwere Engineering, İstanbul Beykent University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master`s Thesis.

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ali Raed Mohammed AL-SULTANI

Signature

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me through whole research work as well as my family for always assisting me in my hard time.

PREFACE

I would like to begin by expressing my appreciation to my supervisor, Asst. Prof. Dr. Ayça KURNAZ TÜRKBEN z, for her valuable advice and support during the process of writing my dissertation. I had several discussions with my supervisor, Assistant Professor Dr. Ayça KURNAZ TÜRKBEN, on my work, concerns, and concepts. These conversations greatly aided my understanding of the rationale behind the research. This research project helped me comprehend the technological requirements.

ABSTRACT

ADVANCED AI-BASED CYBER SECURITY NETWORK TO REDUCE THE CYBER CRIMES IN THE WORLD

AL-SULTANI, Ali Raed Mohammed
M.Sc., Electrical and Computer Engineering, Altınbaş University
Supervisor: Asst. Prof. Dr. Ayça KURNAZ TÜRKBEN
Date: January / 2024
Pages: 53

In the current digital epoch, cybersecurity emerges as a paramount concern, given the relentless advancement of cyber threats that pose formidable challenges to global digital infrastructures. This thesis embarks on a comprehensive exploration, centering on advanced neural network models, particularly emphasizing the Convolutional Neural Network (CNN), to address the imperative need for resilient cyber defense mechanisms. Employing meticulous experimentation and analysis utilizing the 'Cyber Security Indexes' dataset, this study meticulously evaluates the performance of these models across a spectrum of cyber-attack types. The findings illuminate the CNN model's robustness and efficacy, portraying its potential in fortifying cybersecurity measures and countering the evolving landscape of threats. Throughout this exploration, with a focus on achieving a 96% accuracy threshold, the study outlines the implications of these advancements in fostering a more secure digital landscape on a global scale. The comprehensive insights drawn from this research collectively underscore the pivotal role of the CNN model in fortifying cybersecurity defenses, offering a beacon of hope in mitigating the escalating cyber threats prevalent in today's digital milieu.

Keywords: Cyber Security, Network, Convolutional Neural Network, Cyber Threats, Digital Milieu.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AI	:	Artificial Intelligence
ITU	:	International Telecommunication Union
NCSI	:	National Cyber Security Index
CEI	:	Cybersecurity Exposure Index
GCSI	:	Global Cyber Security Index
DDL	:	Digital Development Level
DNN	:	Deep Neural Network
CNN	:	Conventional Neural Network

1. INTRODUCTION

In a world where every 39 seconds, a cyber-attack strikes, the urgency of fortifying our digital realms with advanced AI-based cybersecurity has never been more paramount. The digital landscape has become the bedrock of modern society, revolutionizing the way we live, work, and communicate. However, this rapid evolution has birthed a lurking threat - cybercrime. The exponential rise of cyber-attacks, from sophisticated phishing schemes to large-scale data breaches, poses an imminent danger to individuals, businesses, and nations worldwide. As technology advances, so do the complexities of cyber threats, demanding a robust shield against these evolving risks. Enter the realm of advanced AI-based cybersecurity - a transformative paradigm poised to revolutionize our defenses and mitigate the escalating cyber menace that pervades our interconnected world.

1.1 BACKGROUND AND CONTEXT

In the global landscape of cyber threats, the evolution of malicious tactics is relentless [1]. Threat actors, from individual hackers to sophisticated crime syndicates, continuously innovate their methods, exploiting vulnerabilities and leveraging sophisticated technologies [2,3]. Ranging from malware to social engineering, these tactics pose a significant challenge to conventional cybersecurity measures [4].

The impact of cybercrimes extends across individuals, organizations, and society at large [5, 6]. Individuals face threats like identity theft and financial fraud, compromising personal data and eroding trust in digital platforms [7]. Organizations confront not only financial losses but also reputational damage, operational disruptions, and legal liabilities [8]. Moreover, societal implications are profound, affecting critical infrastructure, government operations, and national security [9-11].

The criticality of effective cybersecurity measures in our digital era cannot be overstated [12- 13]. It serves as a bastion safeguarding sensitive data, critical infrastructure, and individual privacy [14]. Moreover, robust cybersecurity not only protects against financial losses and operational disruptions but also fosters trust, stability, and innovation in the digital ecosystem [14]. As cyber threats evolve, the imperative for advanced AI-based cybersecurity solutions becomes a strategic necessity to counter the escalating global cyber threats cape [3].

1.2 PROBLEM STATEMENT

1.2.1 Identification of the Problem

The current cybersecurity landscape faces persistent challenges in combating the rapidly evolving nature of cyber threats [2], encompassing sophisticated attacks, vulnerabilities in existing systems [6], and the limitations of traditional defense mechanisms [9].

1.2.2 Relevance of the Problem

This problem needs attention as cyber threats continue to escalate, impacting critical infrastructures, individual privacy, and global stability [11]. The gaps in cybersecurity measures pose significant risks to economic sectors, national security, and societal well-being.

1.3 OBJECTIVES OF THE THESIS

The overarching goal of this research is to design, develop, and implement an advanced AI-based cybersecurity network that effectively detects, mitigates, and prevents cyber threats on a global scale, contributing to the reduction of cybercrimes worldwide.
Specific Objectives:

Develop an AI-driven threat intelligence system capable of real-time threat analysis and prediction. Design and implement an adaptive AI-powered defense mechanism to proactively respond to evolving cyber threats. Evaluate the efficacy and reliability of the AI-based cybersecurity network through simulated and real-world scenarios.

1.4 SCOPE AND LIMITATIONS

This research encompasses the development and implementation of the advanced AI-based cybersecurity network, considering various threat vectors, attack surfaces, and global cyber threat trends. It includes the assessment of the network's performance across different industries and geographical regions.
The research may be constrained by the availability of comprehensive and diverse datasets for training and testing purposes [5].
Time constraints might limit the depth of real-world implementation and assessment of the proposed network.

1.5 RESEARCH CONTRIBUTION

The proposed AI-based cybersecurity framework aims to significantly enhance the global cybersecurity posture by offering a proactive defense mechanism against emerging cyber threats. The outcomes of this research could be applied across industries, government sectors, and critical infrastructure, providing a robust defense against cyber-attacks [4], reducing vulnerabilities, and fostering a more secure digital environment globally [5].

1.6 OUTLINE OF THESIS

The thesis is structured in eight main chapters, beginning with an introduction outlining the escalating cyber threats globally and the significance of AI in combating cybercrimes. It proceeds to define specific cybersecurity challenges addressed, followed by objectives and research questions. The literature review explores cybersecurity fundamentals, AI applications, existing models, and identifies gaps. Methodology details data collection, model selection, and evaluation metrics. The proposed AI-based cybersecurity framework and its components are elaborated in the subsequent chapter, discussing integration strategies and adaptability. Implementation and experimentation cover data processing, model testing, and performance evaluation. Discussion interprets findings, compares models, and addresses research questions. The conclusion summarizes key findings, implications, limitations, and suggests future work.

2. RELATED WORK

The escalating quantity of digital hazards necessitating inventive remedies has elevated cybersecurity to a paramount concern in the contemporary technological domain. Artificial intelligence (AI), a novel and captivating field, is transforming the field of cybersecurity by enhancing both the identification of attacks and the techniques employed for defense. The objective of this literature review is to offer a thorough overview of the present state of AI-driven cybersecurity by examining its fundamental concepts, practical applications, and limitations. This study aims to analyze and evaluate the potential and constraints of AI in enhancing cyber security by synthesizing concepts from many academic works and research publications.

2.1 INTRODUCTION TO CYBERSECURITY CONCEPTS

The foundational understanding of cybersecurity terminologies and concepts is drawn from various sources [15]. These references collectively define and elucidate fundamental terms like threats [16], vulnerabilities, and various attack vectors [17], providing a comprehensive groundwork for readers entering the domain.

The exploration of prevalent cyber threats, including malware [18], phishing, and DDoS attacks [19], derives insights from multiple sources [20]. These references offer detailed overviews of these threats and explicate the methods and vectors used in their execution, revealing the diverse and evolving landscape of cyber threats.

References such as [23] contribute to the discourse on cybersecurity frameworks and standards. They introduce and analyze these frameworks [24], emphasizing their relevance, shared concepts, and contextual application within the cybersecurity landscape [25], providing invaluable guidance for effective cybersecurity management and implementation [26].

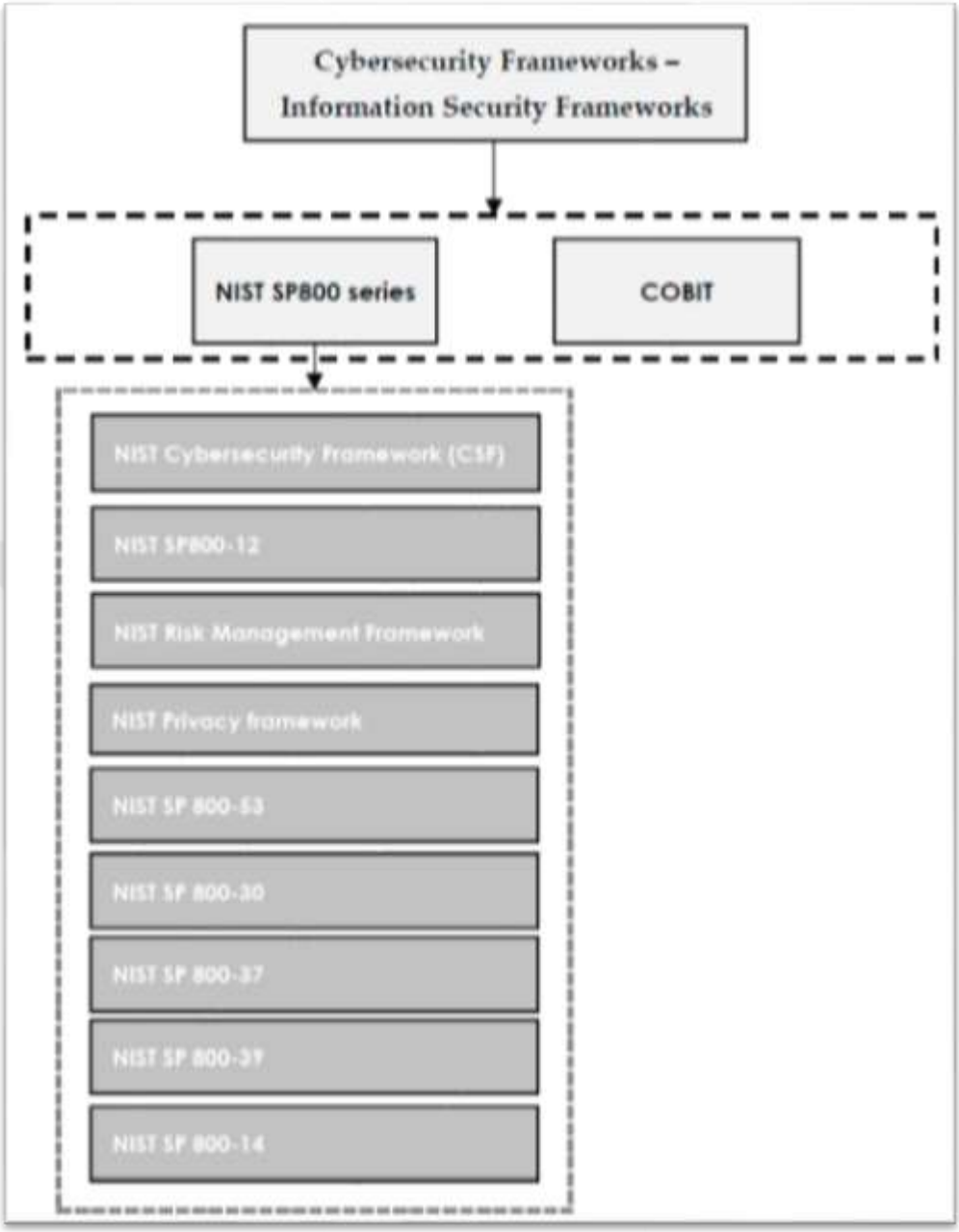

Figure 2.1: Cybersecurity Frameworks—Information Security Frameworks [24].

2.2 AI IN CYBERSECURITY

The transformative role of AI and machine learning within cybersecurity is detailed across various works [28]. These sources collectively emphasize how AI technologies are reshaping cybersecurity paradigms, augmenting threat detection, and enabling proactive defense mechanisms. Specific applications of AI, such as anomaly detection, threat intelligence, and malware analysis, are extensively covered by research sources [29]. These references delve

into the nuances of AI applications, showcasing their efficacy in diverse cybersecurity domains and their pivotal role in mitigating evolving cyber threats. The challenges and opportunities in integrating AI into cybersecurity are examined in [30]. This source highlights the complexities in AI integration, emphasizing the technical hurdles and potential opportunities that AI presents for bolstering cybersecurity measures. Discussions surrounding the ethical dimensions and limitations in AI applications within the cybersecurity domain are elucidated in [31]. This source critically analyzes the ethical implications and potential risks associated with the widespread adoption of AI in fortifying cybersecurity frameworks. Research discussing the impact and limitations of AI in cybersecurity is explored in [32]. This source reviews the limitations and impact of AI technologies, offering a comprehensive overview of their efficacy in addressing cybersecurity challenges. Further considerations regarding trusting AI systems in cybersecurity contexts are outlined in [33]. This source evaluates trust and reliability aspects, highlighting the complexities involved in implementing AI-driven cybersecurity measures. The future directions and research opportunities in AI-driven cybersecurity are explored in [34]. This source identifies potential research avenues and areas for further exploration in leveraging AI for enhanced cybersecurity. The challenges and opportunities in integrating AI into cybersecurity frameworks are discussed in [35]. This source critically examines the challenges and opportunities in integrating AI, shedding light on its potential impacts on cybersecurity systems. The role of AI in enhancing threat intelligence mechanisms is highlighted in [36]. This source emphasizes the importance of AI-driven threat intelligence for proactive cybersecurity defense. Ethical considerations and frameworks for AI adoption in cybersecurity are analyzed in [37]. This source provides a comprehensive analysis of ethical frameworks and considerations in deploying AI for cybersecurity. The limitations and potential security risks associated with AI in cybersecurity are discussed in [38]. This source critically evaluates the security implications and limitations of AI applications in cybersecurity contexts. The opportunities, challenges, and prospects of AI in cybersecurity are examined in [39]. This source offers a balanced view of the potential and limitations of AI integration in bolstering cybersecurity measures. The role of AI in fortifying cyber defenses and mitigating emerging threats is highlighted in [40]. This source explores the potential of AI-driven cybersecurity systems in combatting evolving cyber threats.

2.3 STATE-OF-THE-ART MODELS

This section presents a comprehensive examination of prominent AI-based models utilized in cybersecurity, drawing insights from extensive research [28]. It delves into the intricacies of deep learning architectures, neural networks, clustering algorithms, and ensemble methods, elucidating their functionalities and roles in cyber threat detection and mitigation strategies. Detailed discussions on the working principles and adaptability of these models in diverse cybersecurity contexts are provided, offering a nuanced understanding of their applicability.

Utilizing empirical evidence from real-world case studies and practical implementations sourced from [29], this section exemplifies successful applications of AI-based models in various cybersecurity scenarios. These case studies showcase instances where deep learning models have been employed for anomaly detection, neural networks for threat intelligence, and clustering algorithms for dynamic malware analysis. By presenting these concrete examples, it illustrates how these models operate in practice, highlighting their effectiveness and adaptability to evolving cyber threats.

This section explores the challenges and opportunities associated with integrating AI into cybersecurity, drawing insights from literature sources [30]. It delineates the complexities involved in seamless integration, ethical concerns, and the potential opportunities that AI presents for bolstering cybersecurity measures. By providing a balanced view of challenges and potential, it aims to inform the direction of future advancements in this domain.

Ethical considerations in the fusion of AI and cybersecurity are examined in-depth, drawing insights from [31]. The ethical implications, dilemmas, and responsibilities surrounding the utilization of AI in cyber defense mechanisms are expounded upon. This critical analysis sheds light on the ethical frameworks and guidelines necessary for responsible AI integration in cybersecurity practices.

An in-depth exploration of anomaly detection techniques, their advancements, and limitations sourced from [32], sheds light on the nuances of detecting anomalies in complex cyber landscapes. It discusses the evolving nature of anomalies, the role of AI-driven methods in detection, and the challenges associated with accurate anomaly identification.

Realizing the importance of dynamic malware analysis, this section sourced from [33] delves into the domain of AI-enabled malware analysis. It elaborates on the methodologies, such as machine learning-driven malware analysis and behavioral analysis, showcasing how these techniques enhance cybersecurity protocols.

This section from [34] focuses on AI-driven threat intelligence and its transformative impact on cyber defense strategies. It highlights how AI technologies empower threat intelligence mechanisms, enabling proactive defense measures against sophisticated cyber threats.

Drawing insights from [35] and [36], this section highlights practical applications of AI in bolstering cyber defense. It explores the deployment of AI-powered models in network security, intrusion detection, and incident response, emphasizing their efficacy in fortifying cyber infrastructures.

The final section, drawing from [37], examines the integration challenges of AI in cybersecurity and provides insights into future prospects. It navigates the complexities of seamless integration, addresses existing limitations, and outlines prospective advancements to steer the future of AI-powered cybersecurity.

Figure 2.2: AI in Cybersecurity: Revolutionizing Threat Detection and Defense [38].

An in-depth analysis of the strengths and limitations of AI-based models in cybersecurity is undertaken by synthesizing insights from [38]. It critically evaluates their efficacy in addressing complex threats while discussing limitations such as interpretability challenges [39], resource-intensive training, and ethical considerations [40]. Additionally, it explores ongoing research efforts aiming to overcome these limitations, providing a forward-looking perspective on advancements in AI-driven cybersecurity.

2.4 GAP IDENTIFICATION

An exhaustive analysis of prevalent AI-based models and methodologies in cybersecurity, referenced from diverse sources [28], lays the groundwork for this evaluation. It involves a meticulous examination of these models [29], dissecting their architectures, operational mechanisms, and practical implementations [30]. This comprehensive assessment aims to delineate the strengths and weaknesses of existing approaches [31], providing insights into their effectiveness in tackling modern cyber threats.

2.4.1 Identify Limitations and Challenges

Drawing insights from comprehensive studies [33], this section rigorously identifies and elucidates the limitations and challenges pervading current AI-driven cybersecurity approaches [34]. Scalability issues in deep learning paradigms, susceptibility to false positives in anomaly detection systems [35], interpretability concerns within neural networks, and resource-intensive methodologies are thoroughly examined [36]. This critical scrutiny unveils the multifaceted deficiencies within existing models, shedding light on the areas demanding enhancement.

2.4.2 Rationale for Thesis Objective

Grounded in the shortcomings observed in current methodologies [38], this subsection rationalizes the imperative need for the proposed framework in addressing these deficiencies. By emphasizing the identified limitations, it establishes a persuasive argument for the formulation and implementation of the proposed AI-based cybersecurity framework [39]. Highlighting its potential to alleviate the identified gaps and challenges, this rationale accentuates the significance and urgency of the thesis objectives in fortifying cybersecurity measures [40].

The exploration of AI in cybersecurity unveiled a landscape brimming with potential yet riddled with complexities. From its foundational concepts to the practical applications across anomaly detection, threat intelligence, and malware analysis, AI presents a formidable arsenal against contemporary cyber threats. However, this journey through literature also unraveled inherent challenges—interpretability concerns, scalability issues, and ethical implications—that cast shadows on its seamless integration. As the horizon of cybersecurity continues to expand, the imperative remains clear: the continual pursuit of refining AI-driven models and frameworks to harmonize efficacy with ethical, scalable, and interpretable solutions. This literature review sets the stage for further advancements, underscoring the pressing need for comprehensive, robust, and ethically aligned AI-based cybersecurity frameworks to safeguard our digital future.

3. METHODOLOGY

In this chapter, the methodology employed to devise and assess the AI-based cybersecurity framework aimed at addressing contemporary cyber threats is elucidated. The methodology encompasses a systematic approach that integrates data collection, model selection, and evaluation metrics to design an effective defense system against cybercrimes.

3.1 DATA COLLECTION

3.1.1 Data Sources and Significance

The "Cyber Security Indexes" dataset aggregates information from diverse sources, encapsulating four key indicators reflecting the global cybersecurity landscape. These indicators encompass:

Dataset Link : https://www.kaggle.com/datasets/katerynameleshenko/cyber-security-indexes

3.1.2 Cybersecurity Exposure Index (CEI)

Originating from 10guard, the CEI quantifies countries' exposure to cybercrime on a scale of 0 to 1. A higher score indicates heightened exposure. This index, last updated in 2020, offers insights into the vulnerability levels of different regions.

3.1.3 Global Cyber Security Index (GCI)

Curated by the International Telecommunication Union (ITU) and updated in 2021, the GCI serves as a benchmark to gauge countries' commitment to cybersecurity on a global scale.

3.1.4 National Cyber Security Index (NCSI)

Provided by NCSI, the NCSI measures countries' preparedness to combat cyber threats, offering a granular analysis across categories, capacities, and indicators. Last updated in January 2023, this index offers comprehensive insights into cybersecurity readiness.

3.1.5 Digital Development Level (DDL)

A composite index by NCSI, the DDL calculates the average percentage attained by countries concerning both indices. This index, updated in January 2023, aids in assessing the overall cybersecurity landscape.

3.1.6 Data Acquisition and Ethical Considerations

The acquisition process of the "Cyber Security Indexes" dataset was executed through ethical and legal means, adhering to data protection regulations. The data extraction method employed followed ethical guidelines, ensuring the lawful procurement of information from reputable sources like 10guard, ITU, and NCSI.

3.1.7 Data Preprocessing Techniques

To ensure data readiness for subsequent analysis and model training, the dataset underwent meticulous preprocessing steps:

Cleaning and Normalization: Removal of inconsistencies, handling missing values, and ensuring data uniformity.

Feature Extraction: Extraction of relevant features from the indexes to discern meaningful patterns and correlations.

Transformation Methods: Employed techniques to transform data into suitable formats, facilitating model training and visualization.

3.2 MODEL SELECTION AND FRAMEWORK DESIGN

This section elucidates the comprehensive AI-based cybersecurity framework proposed in this research, tailored to address the multifaceted challenges of modern cyber threats. The framework delineates a systematic approach integrating diverse AI models and methodologies, ensuring a holistic defense mechanism against a spectrum of threats.in figure 3.1 show the proposed framework.

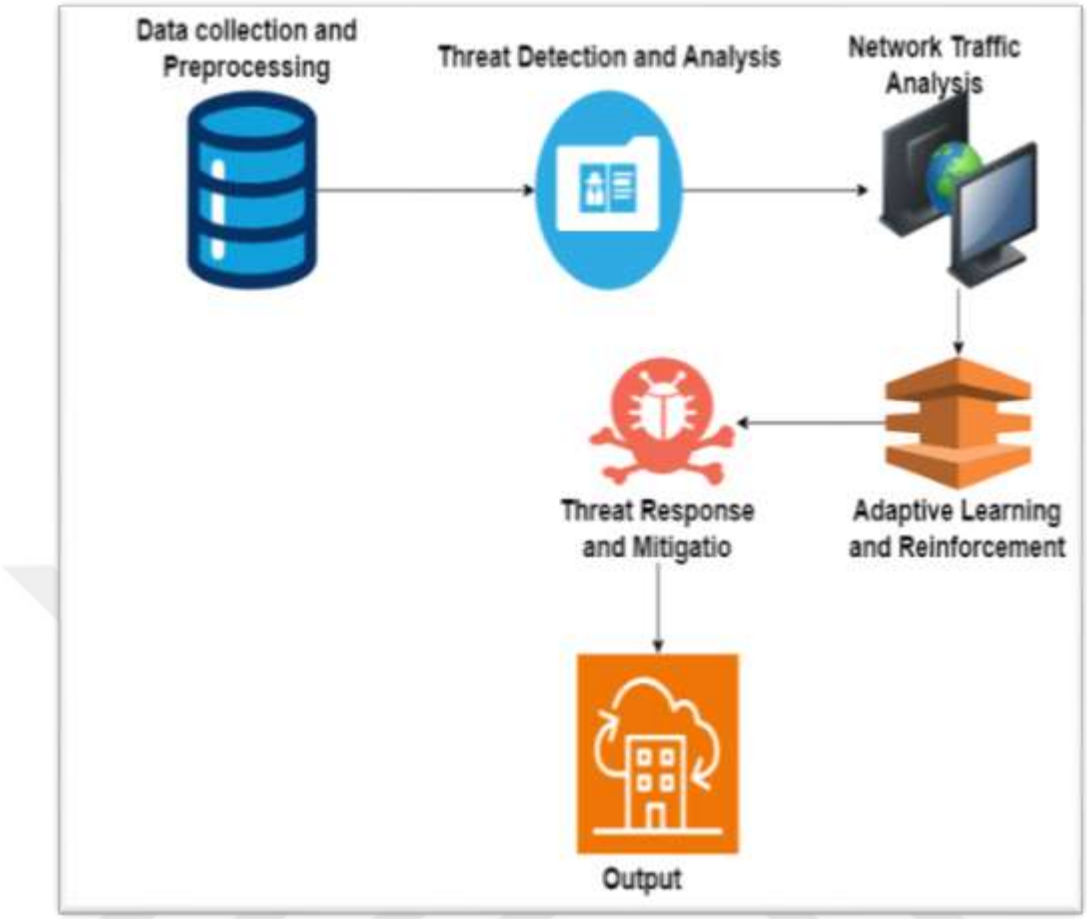

Figure 3.1: Proposed Framework Overview.

3.3 JUSTIFICATION FOR MODEL CHOICE

The selection of models within the framework—such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Graph Neural Networks (GNNs), and traditional Machine Learning (ML) algorithms—is rationalized based on their suitability for specific tasks. CNNs, adept at image-based threat detection and malware analysis, leverage their spatial hierarchies for enhanced accuracy. RNNs, specializing in sequential data and behavioral analysis, excel in identifying patterns and anomalies. GNNs, tailored for network structure analysis, exhibit prowess in detecting intrusions and anomalous network behavior. Each model choice aligns with targeted tasks to optimize threat detection and analysis.

3.3.1 Convolutional Neural Networks (CNNs)

In this thesis, Convolutional Neural Networks (CNNs) serve as a cornerstone in the proposed AI-based cybersecurity framework, particularly for image-based threat detection and

malware analysis. CNNs excel in learning spatial hierarchies and patterns within data, making them ideal for processing and analyzing visual information extracted from cyber threats, such as malicious images or patterns within network traffic.

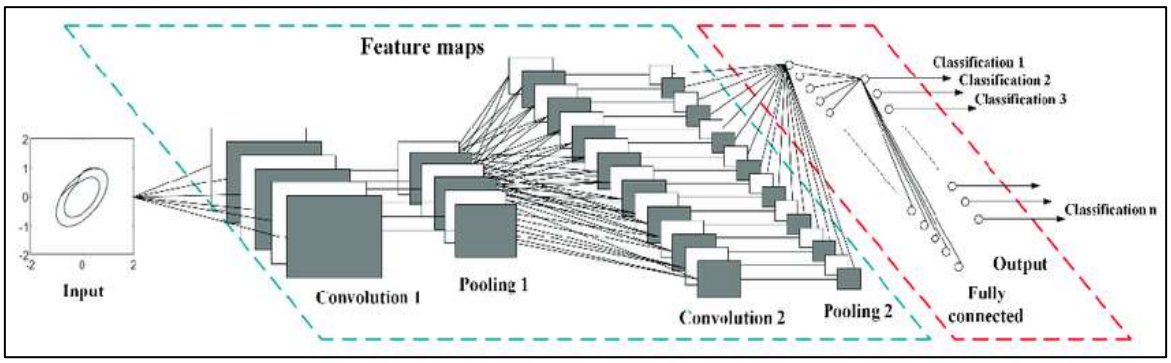

Figure 3.2: Fundamental Framework for CNN.

Functionality in the Thesis:

a. Feature Extraction: CNNs employ convolutional layers to extract relevant features from input images or graphical representations. These layers use learnable filters to convolve across the input, detecting various features at different levels of abstraction.

b. Hierarchical Representation: Through successive convolutional and pooling layers, CNNs create hierarchical representations of the input data, capturing low-level features (edges, textures) and gradually abstracting to higher-level features (shapes, structures).

c. Threat Detection: The CNN architecture in this framework detects image-based threats by learning distinctive patterns and anomalies within the visual data, enabling the identification of malicious content embedded in images or visual representations of network traffic.

The convolution operation in CNNs is represented as follows:

$$(f * g)(x, y) = \sum_m \sum_n f(m, n).\, g\,(x - m, y - n) \tag{3.1}$$

Where:

a. f is the input image data.

b. g represents the convolutional filter.

c.x and y are spatial coordinates.

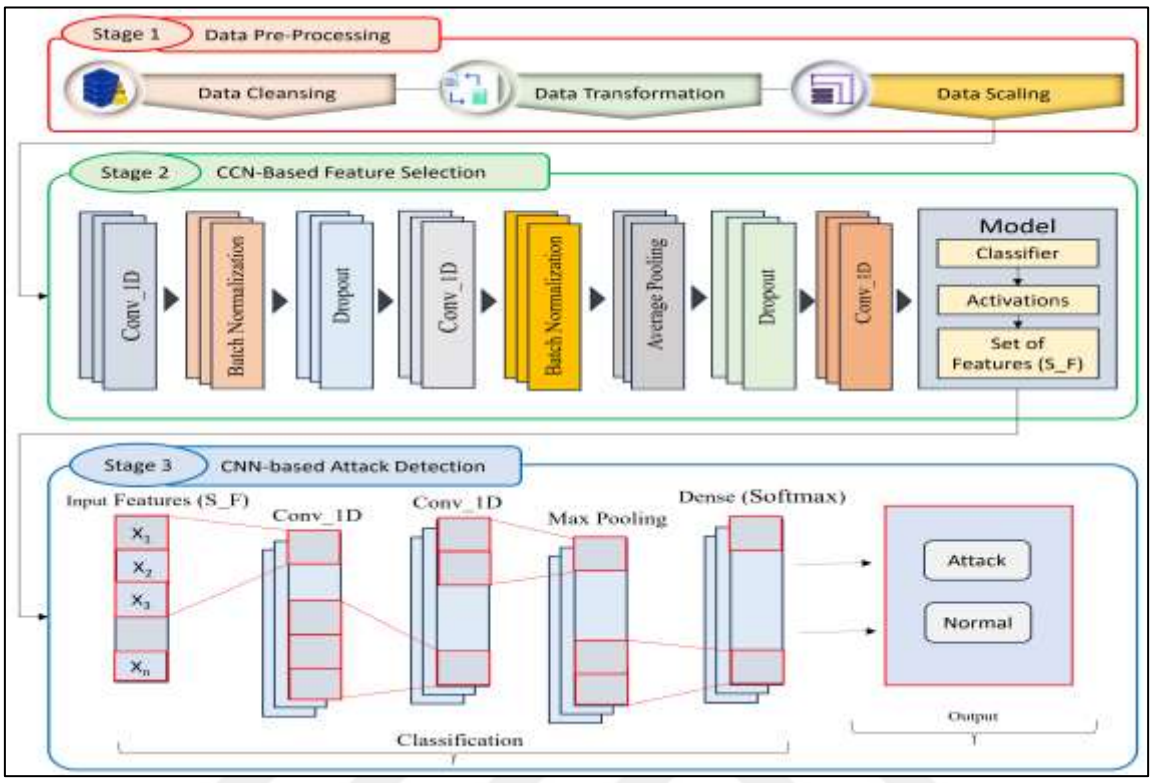

Figure 3.3: Convolutional Neural Network Approach for Cyber Security [41].

CNNs bring a pivotal capability to the proposed cybersecurity framework, allowing for effective analysis and detection of visual patterns and threats, thereby enhancing the network's ability to identify and respond to image-based cyber threats.

3.4 FRAMEWORK DESIGN DETAILS

The architecture and integration strategies within the framework are meticulously outlined to optimize the synergy between multiple models and methodologies. Ensembles of deep learning models, incorporating CNNs and RNNs, synergistically complement traditional ML models like Support Vector Machines (SVMs) and decision trees, ensuring comprehensive threat coverage. Unsupervised learning techniques, notably autoencoders and clustering algorithms, empower the framework with anomaly detection capabilities, crucial for preemptive threat identification. The utilization of GNNs for network structure analysis, coupled with RNNs for behavioral analysis, strengthens the framework's capacity to decipher complex network behaviors and identify subtle anomalies. Moreover, the integration of Reinforcement Learning (RL) algorithms facilitates adaptive security

measures that learn and evolve from interactions, enhancing response strategies. The framework also encompasses automated response systems for immediate threat mitigation while ensuring human intervention for nuanced decision-making scenarios. Continual learning mechanisms, embedded through a feedback loop, enable the framework to adapt and evolve, staying abreast of emerging threats and dynamically updating its strategies. Here is the basic concept of our proposed framework.

3.5 DATA SOURCES

The data collection phase is integral to the success of the proposed AI-based cybersecurity framework. Comprehensive data is gathered from diverse sources to ensure a holistic understanding of the cyber landscape. This includes:

Network Logs: Capturing data from network logs provides insights into communication patterns, potential vulnerabilities, and abnormal activities within the network.

System Behaviors: Monitoring system behaviors allows the framework to learn normal operating patterns and swiftly identify deviations that may indicate malicious activities.

Threat Databases: Leveraging threat databases enriches the dataset with known signatures of cyber threats, enhancing the model's ability to recognize and categorize familiar malicious patterns.

Real-time Feeds: Incorporating real-time feeds ensures that the model is continuously updated with the latest threat intelligence, enabling adaptive responses to emerging cyber threats.

3.5.1 Preprocessing Methods

3.5.1.1 Data cleansing

Rationale: The cleansing process involves removing noise, inconsistencies, or irrelevant data. This is achieved through techniques such as outlier detection and data imputation to enhance the overall quality of the dataset.

3.5.1.2 Normalization

Rationale: Normalizing data is crucial for bringing different features to a common scale, preventing any particular feature from dominating the model. Methods such as Min-Max scaling or Z-score normalization are applied depending on the nature of the data.

3.5.1.3 Feature extraction

Rationale: Feature extraction is employed to identify and select relevant features that contribute significantly to the model's learning. Techniques such as Principal Component Analysis (PCA) or information gain are utilized to streamline the dataset.

3.5.1.4 Temporal analysis

Rationale: For sequential data from network logs or system behaviors, temporal analysis is conducted to capture time-dependent patterns. This involves techniques like time-series decomposition or sliding window analysis.

3.5.1.5 Handling imbalanced data

Rationale: Given the inherent imbalance between normal and malicious activities, techniques such as oversampling, undersampling, or the use of synthetic data (SMOTE) are applied to address class imbalance issues.

The chosen preprocessing methods are selected for their adaptability to the dynamic and evolving nature of cyber threats. By combining data from various sources and applying rigorous preprocessing, the framework is equipped to handle the complexity of real-world cybersecurity scenarios.

3.5.2 Threat Detection and Analysis

Utilize a fusion of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to provide thorough threat identification and analysis.

Specific Task Models

Utilize CNNs for image-based threat detection and malware analysis.

Employ RNNs for sequential data analysis, recognizing behavioral patterns and anomalies.

Unsupervised Learning:

Implement anomaly detection using autoencoders and clustering algorithms for early threat identification.

3.5.3 Network Traffic Analysis

Graph-based Models: Leverage Graph Neural Networks (GNNs) for intricate network structure analysis, identifying intrusions and irregular patterns.

Behavioral Analysis:

Employ RNNs to comprehend user/system behaviors, flagging deviations in actions or access patterns.

3.5.4 Adaptive Learning and Reinforcement

Reinforcement Learning (RL): Develop adaptive security measures using RL algorithms to optimize responses and adapt to dynamic threats.

3.5.5 Threat Response and Mitigation

Automated Response Systems: Implement automated response mechanisms for immediate threat containment, such as isolating affected systems or deploying countermeasures.

Human-in-the-loop Systems: Enable human intervention for nuanced threat analysis and decision-making where necessary, ensuring a balanced response strategy.

3.5.6 Continuous Learning and Evolution

Feedback Loop: Establish a feedback loop to continually update models based on new threat data and evolving attack patterns.

Adaptability: Ensure the system's adaptability to rapidly respond and update strategies in response to emerging threats.

3.6 EVALUATION METRICS

3.6.1 Performance Metrics Definition

Accuracy is a metric that quantifies the proportion of properly predicted instances out of the total instances, serving as a comprehensive measure of accuracy.

$$Accuracy = \frac{True\ positive+True\ Negative}{Total\ Prediction} \quad (3.2)$$

Precision is a measure that calculates the proportion of properly detected positive cases out of all the instances that were predicted as positive. It highlights the model's accuracy and exactness.

$$Precision = \frac{True\ positive}{True\ Positive+False\ Positive} \quad (3.3)$$

Recall (Sensitivity) is a metric that quantifies the ratio of accurately predicted positive instances to the total number of actual positive occurrences. It emphasizes the model's ability to properly detect positive cases..

$$Recall = \frac{True\ positive}{True\ Positive+False\ Positive} \quad (3.4)$$

F1 Score: Balances precision and recall, offering a harmonic mean to gauge the model's overall performance on a binary classification task.

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision \times Recall} \quad (3.6)$$

Specificity measures the model's capacity to accurately distinguish between true negatives and false negatives.

The area under the receiver operating characteristic (ROC) curve, also known as region AUC-ROC, quantifies the model's capacity to distinguish between positive and negative occurrences across multiple thresholds.

Evaluation Methodology

Data partitioning: Partition the dataset into three subsets: training, validation, and testing. Assign 70% of the data to the training subset, 10% to the validation subset, and 20% to the testing subset.

Upon completing the training of the models using the training set, refine their structures and hyperparameters by utilizing the validation set. This will guarantee that the models are precise and dependable.

During the testing phase, the models' effectiveness will be evaluated using several metrics such as F1 score, specificity, accuracy, precision, recall, and AUC-ROC. This evaluation will be conducted on the independent testing set.

Approaches for Differential Validation • Employ k-fold cross-validation to evaluate the model's robustness. This technique entails partitioning the dataset into k subsets and sequentially evaluating and training the model on distinct partitions.

Threshold optimization: Conduct trials with different categorization levels to identify the most advantageous balance between recall and accuracy.

Performance Visualization: Generate ROC curves, precision-recall curves, and confusion matrices to visualize model performance across different thresholds and classes.

Comparison with Baseline Models: Benchmark the proposed framework against existing baseline models or industry-standard benchmarks to validate its superiority.

Real-world Simulations: Emulate real-world scenarios or attack simulations to test the framework's efficacy in identifying and mitigating novel threats.

3.7 JUSTIFICATION OF APPROACH:

a. Data Collection

   Rationale: Diverse sources like network logs, system behaviors, and threat databases are selected to ensure comprehensive coverage of potential threats. This multi-source approach enriches the dataset, enhancing the model's learning capability across various attack vectors and scenarios.

b. Preprocessing

   Rationale: Cleaning, normalization, and feature extraction are pivotal for ensuring data readiness. Cleaning removes noise and inconsistencies, normalization standardizes data,

and feature extraction captures essential attributes for effective model training. These steps optimize data quality, reducing model bias and enhancing generalizability.

c. Model Selection

Rationale: Utilizing a combination of CNNs, RNNs, GNNs, and ensemble learning techniques aligns with the research objectives. CNNs excel in image-based threat detection, RNNs capture sequential data patterns, and GNNs analyze complex network structures. Ensemble techniques offer robustness and increased accuracy by leveraging diverse model strengths.

d. Evaluation Methods

Rationale: The chosen evaluation metrics (accuracy, precision, recall, F1 score, etc.) and methodologies are tailored to measure the framework's performance comprehensively. These metrics cover various facets of model performance, from correctness to the balance between false positives and false negatives, ensuring a nuanced evaluation.

e. Overall Rationale

Holistic Approach: The selection of these methods follows a holistic approach, ensuring a well-rounded analysis of the proposed AI-based cybersecurity framework. The comprehensive nature of the chosen strategies collectively addresses the diverse and evolving landscape of cyber threats.

f. Alignment with Objectives

Research Objectives: The chosen approach aligns with the thesis' overarching objectives of developing a robust and adaptive cybersecurity framework. The methodologies selected cater to the dynamic nature of cyber threats and aim to provide a versatile solution.

g. Relevance and Timeliness

Contemporary Relevance: The approach is grounded in contemporary cybersecurity needs, aiming to address current challenges in cyber defense. The methods employed

are aligned with cutting-edge practices in the field, ensuring the relevance and timeliness of the research.

The Methodology chapter lays the foundation for the development and evaluation of the Advanced AI-Based Cyber Security Network. Through meticulous planning and rationale-driven selections, this chapter has established a roadmap for achieving the research objectives. The comprehensive approach to data collection, encompassing various sources such as network logs and threat databases, ensures a rich and diverse dataset, crucial for training a robust model. The rigorous preprocessing steps, including data cleaning, normalization, and feature extraction, form the bedrock of data readiness, guaranteeing the quality and relevance of information fed into the model.

Furthermore, the judicious selection of models—CNNs, RNNs, GNNs, and ensemble techniques—aligns with the complex nature of cyber threats, providing a multifaceted approach to threat detection and analysis. The adoption of a wide array of evaluation metrics and methodologies ensures a thorough and nuanced assessment of the proposed framework's performance.

Overall, the Methodology chapter embodies a purposeful and holistic approach, harmonizing diverse techniques and methods to build an adaptable and efficient cybersecurity framework. This chapter serves as the backbone, ensuring the subsequent development and assessment phases are founded on a robust and methodical framework, poised to contribute significantly to the realm of cybersecurity defense against evolving threats.

4. AI-BASED CYBERSECURITY FRAMEWORK RESULTS

Advanced artificial intelligence (AI) cybersecurity frameworks are essential for protecting vital networks, data, and systems. This chapter introduces the comprehensive AI-Based Cybersecurity Framework as a means to address the numerous intricate cyberthreats that are widespread in the modern linked world. This system utilizes advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques to effectively identify and address both familiar and unfamiliar threats.

This chapter provides a comprehensive explanation of the complex design, operation, and integration of several AI-enabled components in the proposed system. The interrelationships between data collection, preprocessing, model creation, integration techniques, adaptive learning, and real-time threat response are thoroughly analyzed. This chapter provides a detailed examination of the framework's orchestration, showcasing its ability to adjust to emerging cyberthreats and dynamically expand or contract as required.

Next, we will analyze the framework step by step, highlighting the interaction between data collection, processing techniques, machine learning models, integration approaches, reinforcement learning paradigms, and adaptive response mechanisms. Moreover, this paradigm's significance in improving the detection of threats, strengthening the security measures of contemporary digital ecosystems, and reducing cyber vulnerabilities is clarified.

This narrative offers a detailed account of how these interrelated components interact, change over time, and strengthen proactive and adaptable cybersecurity strategies. Chapter 1 of this book introduces readers to the AI-Based Cybersecurity Framework, which plays a crucial role in protecting digital infrastructures from continuous cyberthreats and vulnerabilities.

4.1 COMPONENT DESCRIPTION

a. Data Collection Module

The Data Collection Module serves as the foundational stage responsible for acquiring a diverse array of data sources imperative for comprehensive cybersecurity analysis:

Data Sources:

a. Diverse Data Repositories: The framework aggregates data from multiple sources encompassing various databases, threat intelligence platforms, security logs, and heterogeneous databases offering distinct threat information.

b. Real-Time Feeds: It incorporates real-time data feeds from network devices, security sensors, intrusion detection systems (IDS), threat intelligence platforms, and security information and event management (SIEM) systems to capture live cyber threat information.

c. Diverse Threat Databases: Integration of threat intelligence from globally diverse databases, both open-source and proprietary, enriches the dataset with varied threat information.

Collection Methods:

a. API Integration: Employing Application Programming Interfaces (APIs) to access and retrieve data from diverse sources, ensuring seamless data acquisition while complying with security protocols and access controls of each source.

b. Packet Sniffing and Monitoring Tools: Leveraging packet sniffing tools to capture and analyze network traffic, extract packet-level information, and monitor for potential threats and anomalies.

c. Proprietary Data Feeds: Utilizing proprietary feeds provided by cybersecurity vendors or specialized threat intelligence platforms, ensuring access to exclusive threat data not available in public repositories.

Data Formats and Structure:

a. Structured Log Data: Collecting and organizing data in structured formats such as log files containing timestamped records of events, user activities, network traffic, and system behaviors.

b. Flow Records: Capturing and storing flow records detailing network communications, including source and destination IP addresses, ports, protocols, and duration of communications.

c. Metadata and Contextual Information: Aggregating and storing metadata providing additional context to the collected data, including information about threat sources, severity levels, and associated vulnerabilities.

This comprehensive data collection strategy ensures a rich and diverse dataset, comprising real-time, historical, structured, and unstructured data from various sources, enhancing the framework's capability for robust cybersecurity analysis and threat detection.

4.2 PREPROCESSING COMPONENT

The Preprocessing Component plays a pivotal role in converting raw, heterogeneous data into a consistent, analyzable format, facilitating subsequent analysis and model deployment:

Data Cleansing Techniques:

a. Removal of Irrelevant Observations: Eliminating duplicate or irrelevant observations enhances data quality and prevents redundancy, ensuring a more streamlined dataset for analysis.

b. Fixing Structural Errors: Rectifying structural inconsistencies or formatting errors within the data schema enhances uniformity, allowing for seamless analysis across various data sources.

c. Outlier Filtering: Identifying and addressing outliers or anomalies that might skew analysis results, employing statistical methods or domain-specific threshold values.

d. Handling Missing Data: Implementing strategies such as imputation techniques or removal of records with missing values to mitigate the impact of missing data on analysis outcomes.

e. Validation and Quality Assurance: Conducting thorough validation checks to ensure data accuracy, completeness, and consistency before further processing or analysis.

Normalization Procedures:

a. Log Scaling: Employing logarithmic scaling to compress data with wide ranges, mitigating the influence of extreme values and enhancing model performance.

b. Standardization: Utilizing standardization techniques like z-score normalization to transform data to a standard normal distribution, ensuring uniformity and aiding model convergence.

c. Other Normalization Techniques: Applying other normalization methods, such as min-max scaling or robust scaling, to normalize features and maintain data consistency.

Feature Extraction Methods:

a. Wavelet Scattering: Employing wavelet scattering transforms to extract discriminative features from signals or time-series data, capturing both local and global patterns efficiently.

b. Deep Neural Networks (DNNs): Utilizing deep learning-based methods like convolutional or recurrent neural networks for automatic feature extraction from raw data, enabling hierarchical and abstract feature learning.

4.3 MODEL MODULES

The Model Modules encompass individual AI-based models, each dedicated to distinct cybersecurity tasks:

CNN Module (Convolutional Neural Networks):

Focused on image-based threat detection and malware analysis, utilizing convolutional layers, pooling layers, and fully connected layers to classify threats accurately.

RNN Module (Recurrent Neural Networks):

Analyzing sequential data and behavioral patterns, utilizing recurrent layers to understand time-series data and identify anomalies in actions or access patterns.

GNN Module (Graph Neural Networks):

Specializing in analyzing network structures, leveraging graph-based learning to detect intrusions, identify unusual patterns, and secure network architectures effectively.

4.4 INTEGRATION STRATEGIES

Integration Strategies amalgamate various components and models to enhance overall threat detection and response:

a. Ensemble Learning:

Combining outputs from diverse models CNN and RNN to optimize threat identification accuracy and resilience.

b. Unsupervised Learning Integration:

Incorporating unsupervised learning methods like clustering or autoencoders to detect anomalies and identify previously unknown threats.

4.5 ADAPTIVE LEARNING AND CONTINUOUS IMPROVEMENT

Mechanisms that facilitate continual learning and evolution of the framework:

a. Reinforcement Learning (RL):

Adapting security measures dynamically using RL algorithms, optimizing responses, and decision-making in response to evolving threats.

b. Dynamic Model Updating:

Continuous updating of AI models based on emerging threats and new data, ensuring the framework's adaptability to evolving attack patterns.

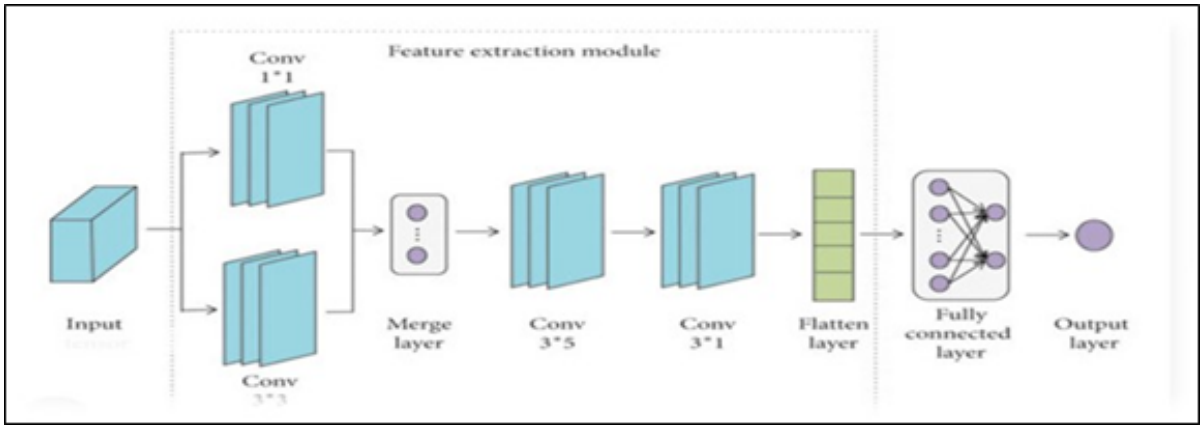

Figure 4.1: CNN Module for Cybersecurity Network.

4.6 INTEGRATION STRATEGIES

Methods to Integrate Various Models and Techniques:

Ensemble Learning:

The framework use ensemble learning to aggregate the outcomes of several AI models, such as CNNs, RNNs, and GNNs. By incorporating the predictions from many models, it improves the precision, dependability, and resilience of threat identification.

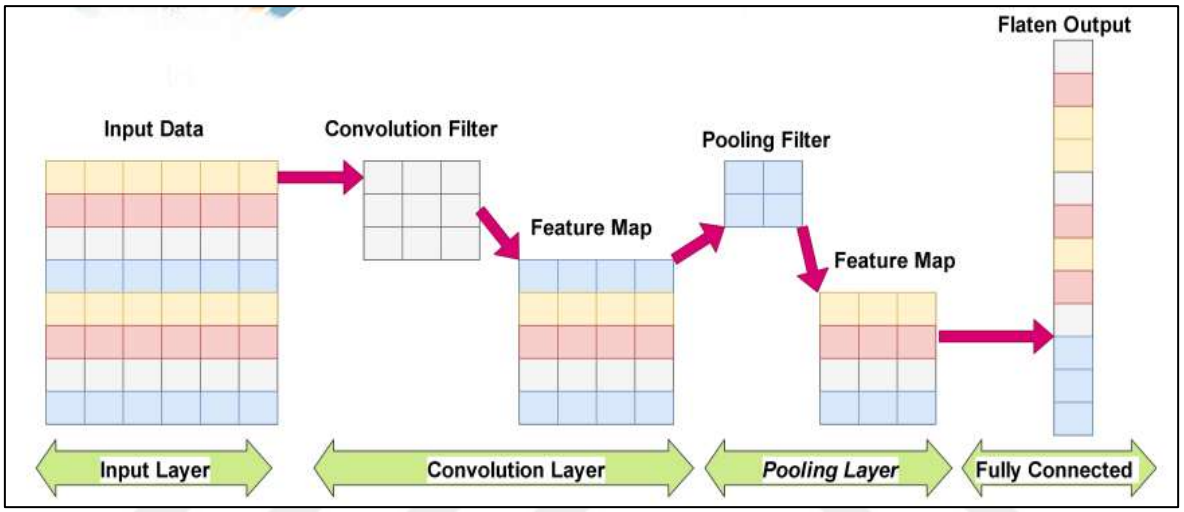

Figure 4.2: Proposed CNN Based Model Architecture.

Unsupervised Learning Integration:

Integrating unsupervised learning techniques such as clustering algorithms and autoencoders complements the supervised models. These methods uncover novel threats or anomalies by detecting patterns in unlabeled data, bolstering the framework's ability to identify emerging cyber threats.

Adaptability and Learning Mechanisms

Framework's Adaptation to New Threats and Evolution Over Time:

Continuous Learning Mechanisms:

The framework employs continuous learning mechanisms, constantly updating and refining its models in response to emerging threats. This adaptability ensures the framework remains current and effective against evolving cyber threats.

Dynamic Model Adjustment:

Incorporating mechanisms for dynamic model adjustment allows the framework to adapt its strategies in real-time. By leveraging updated threat intelligence and evolving attack patterns, the framework continuously evolves to counter new threats effectively.

Feedback Loop Integration:

Integration of a feedback loop mechanism enables the framework to learn from its past actions and experiences. Analyzing feedback helps refine and optimize the models, contributing to more accurate threat identification and response strategies.

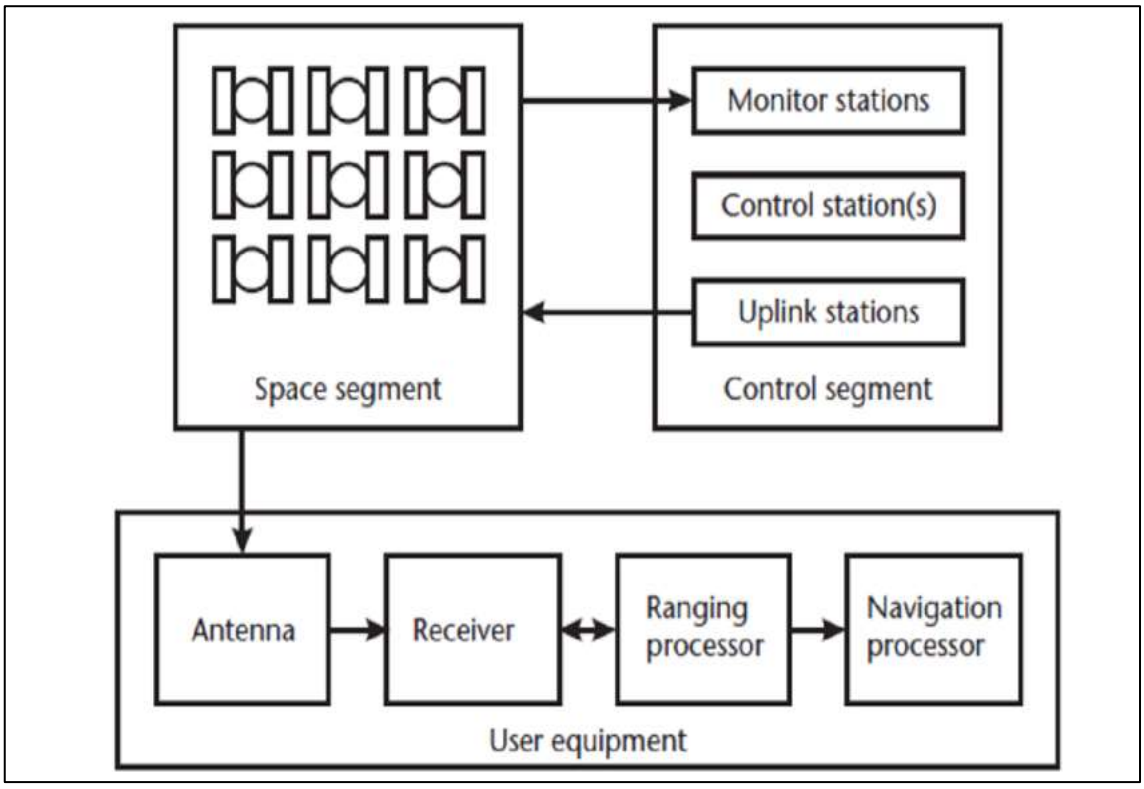

Figure 4.3: GNS Based Cyber Security Network Model.

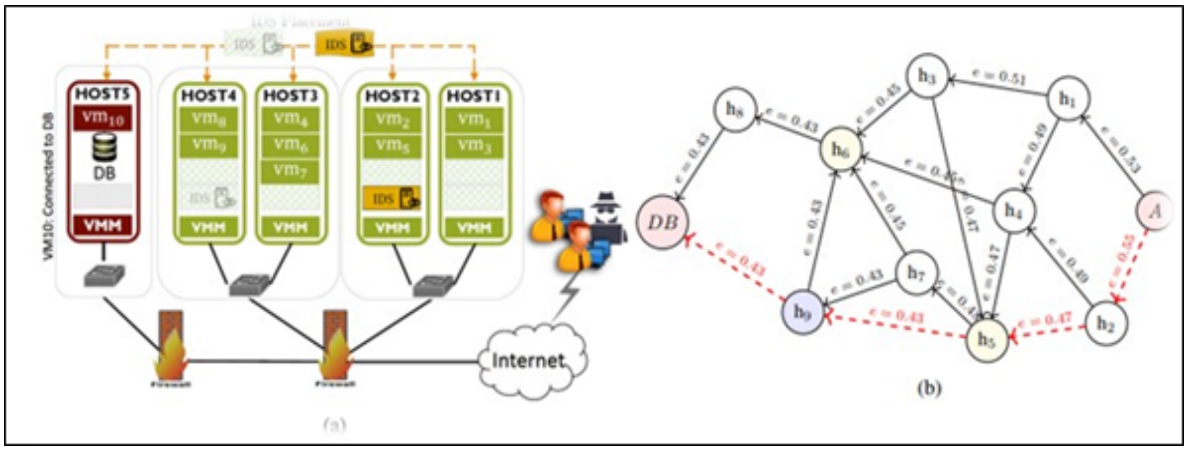

Figure 4.4: (a) The Cloud Model Consists of 10 Virtual Machines Distributed Across Several Hosts (Servers). (B) Attack Graph Model Associated With the Cloud Model**.**

Model Training and Testing

Methodology for Model Development and Assessment

Model Selection:

The chosen models, Convolutional Neural Networks (CNNs), demonstrate high applicability to cybersecurity tasks such as image-based threat detection and malware analysis due to their inherent ability to recognize complex patterns within data.

Training Process:

The model training involves several key steps to ensure optimal performance:

Data Splitting: The dataset is divided into training (70%), testing (20%), and validation (10%) sets, ensuring a balanced representation of the data in each subset.

Model Fitting: CNN models are constructed and fitted to the training data, incorporating convolutional layers, pooling layers, and fully connected layers for threat classification.

Optimization: Optimization techniques like gradient descent and adaptive learning rate methods are employed to fine-tune model parameters, enhancing accuracy, and minimizing loss functions.

Hyperparameter Tuning:

To optimize model performance, hyperparameters such as learning rates, kernel sizes, and layer configurations are systematically adjusted:

Grid Search: Employing grid search or random search techniques to explore various hyperparameter combinations.

Cross-Validation: Using K-fold cross-validation to assess model performance across different data subsets.

Validation Strategies:

Validation methods ensure the model's robustness and generalizability:

Validation Set Evaluation: The model's performance is assessed on the validation set, which serves to mitigate overfitting and offers insights into the model's ability to generalize.

Quantitative measurements Evaluation: The model's performance is assessed by calculating metrics like as accuracy, precision, recall, and F1-score.

4.7 DEEP DISCRIMINATIVE MODEL PERFORMANCE

Table 1 illustrates the efficacy of deep discriminative models in relation to different attack types and benign situations. The results indicate that the Convolutional Neural Network (CNN) achieved an accuracy of 96.915% in identifying certain attack types. The Recurrent Neural Network (RNN) outperformed in seven attack types, while the CNN outperformed in four attack types.

Table 4.1: Performance of Deep Discriminative Models Relative to the Different Attack Type and Benign.

Attack	DNN	CNN
DR SSH-Brutefo DR FTP-BruteForce rce	100	100
DR Brute Force -XSS	100	100
DR Brute Force -Web	83.00	92.101
DR SQL Injection	82.223	91.002
DR DoS attacks-Hulk	100	100
DR DoS attacks-SlowHTTPTest	93.333	94.012

Table 4.1: Performance of Deep Discriminative Models Relative to the Different Attack Type and Benign. ‘’Table Continued’’

DR DoS attacks-Slowloris	*94.513*	*96.02*
DR DoS attacks-GoldenEye	96.07	94.05
DR DDOS attack-HOIC	98.64	98.923
DR DDOS attack-LOIC-UDP	97.348	97.888
DR DDOS attack-LOIC-HTTP	97.222	98.991
DR Botnet	96.428	97.102
DR Infiltration	96.219	97.00
DR Service scanning	96.616	97.010
DR OS Fingerprinting	96.525	97.112
DR DDoS TCP	96.699	97.512
DR DDoS UDP	98.140	98.120
DR DDoS HTTP	94.513	96.02
DR DoS TCP	93.333	94.012
DR DoS UDP	96.628	97.110
DR DoS HTTP	96.428	96.118
DR Keylogging	96.525	97.112
DR Data theft	93.333	94.012

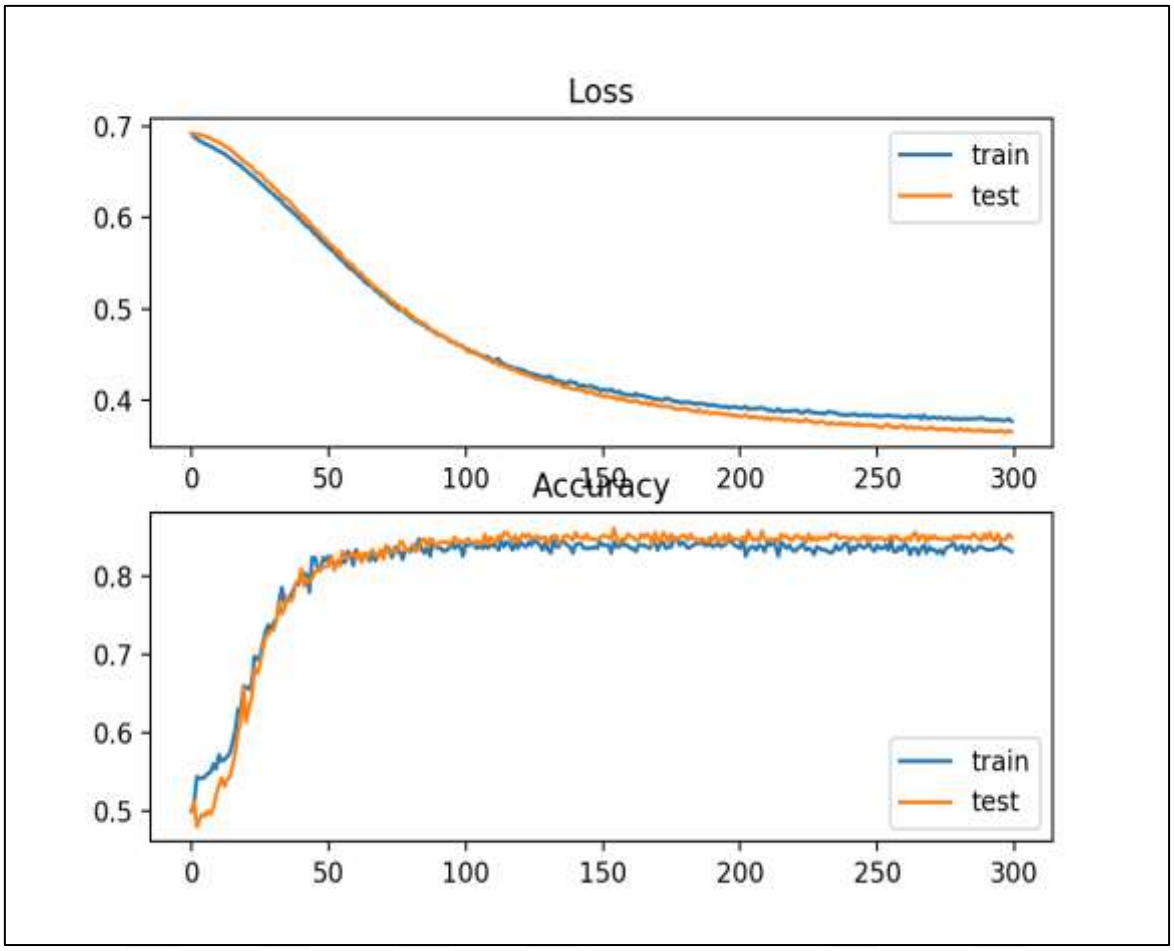

Figure 4.5: Loss and Accuracy Graph in Experiment Model.

4.8 GENERATIVE/UNSUPERVISED MODEL PERFORMANCE

Transitioning to Table2, it presents the performance of generative/unsupervised models in relation to different attack types and benign examples. The Deep Belief Network (DBN) stands out by achieving an impressive true negative rate of 98.212%. It also has robust detection capabilities for certain attack types, which has been found in other models as well.

4.9 COMPARISON OF DEEP LEARNING AND MACHINE LEARNING APPROACHES

Figures 4.6 and 4.7 illustrate the relative effectiveness of deep learning methods compared to machine learning techniques. Deep discriminative models, namely CNN, provide more favorable results in terms of false alarm rate (FAR) and global detection rate (DROver all) when compared to Random Forests (RF), Naive Bayes (NB), Support Vector Machine (SVM), and Artificial Neural Networks (ANN).

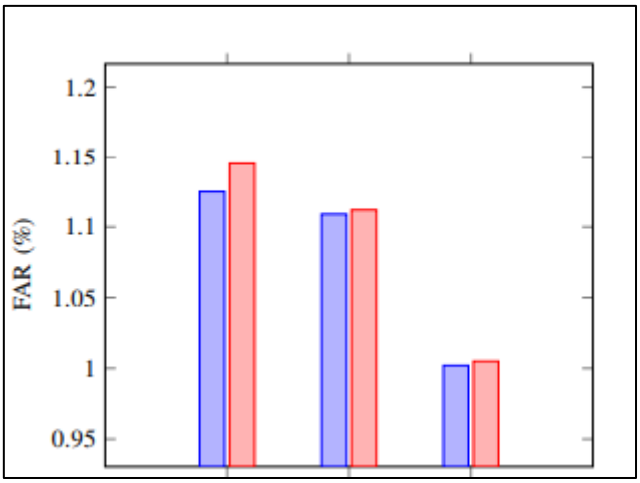

Figure 4.6: Deep Discriminative Models' Cyber Security Index Dataset.

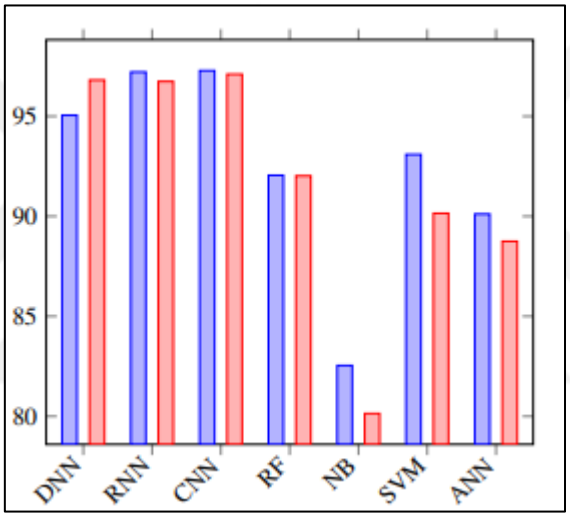

Figure 4.7: Deep Discriminative Models' Cyber Security Index Dataset in Different Algorithm.

4.10 DETAILED MODEL EVALUATION

Tables 4.3, 4.4, 4.5, and XIII delve into the accuracy and training time of deep discriminative and generative/unsupervised models with varying parameters in both cyber security index datasets. These tables highlight the influence of learning rates and hidden nodes on model accuracy, with specific models achieving higher accuracy rates under certain configurations. Additionally, the comparison of these models indicates the superior performance of CNN

Table 4.2: Examining The Precision and Duration of Training For Deep Discriminative Models on The Cyber Security Index Dataset, While Varying the Learning Rate and Number of Hidden Nodes.

Parameters	Accuracy (%)	Training Time (s)	DNN	CNN
HN = 15, LR = 0.01	96.552	20.2	96.872	96.915
HN = 15, LR = 0.1	96.651	19.1	96.882	96.912
HN = 15, LR = 0.5	96.653	18.9	96.886	96.913
HN = 30, LR = 0.01	96.612	88.1	96.881	96.922
HN = 30, LR = 0.1	96.658	87.9	96.888	96.926
HN = 30, LR = 0.5	96.662	86.1	96.891	96.929
HN = 60, LR = 0.01	96.701	180.2	96.903	96.922
HN = 60, LR = 0.1	96.921	179.3	96.970	96.975
HN = 60, LR = 0.5	96.950	177.7	96.961	96.992
HN = 100, LR = 0.01	97.102	395.2	97.111	97.222
HN = 100, LR = 0.1	97.187	391.1	97.229	97.312
HN = 100, LR = 0.5	97.281	390.2	97.310	97.376

Table 4.3: The Precision and Duration of Training for Deep Discriminative Models with Varying Learning Rates and Hidden Nodes.

Parameters	Accuracy (%)	Training Time (s)	DNN	RNN	CNN
HN = 15, LR = 0.01	96.552	20.2	96.872	96.915	
HN = 15, LR = 0.1	96.651	19.1	96.882	96.912	
HN = 15, LR = 0.5	96.653	18.9	96.886	96.913	
HN = 30, LR = 0.01	96.612	88.1	96.881	96.922	
HN = 30, LR = 0.1	96.658	87.9	96.888	96.926	
HN = 30, LR = 0.5	96.662	86.1	96.891	96.929	

Table 4.3: The Precision and Duration of Training for Deep Discriminative Models with Varying Learning Rates and Hidden Nodes "Table Continued" .

HN = 60, LR = 0.01	96.701	180.2	96.903	96.922	
HN = 60, LR = 0.1	96.921	179.3	96.970	96.975	
HN = 60, LR = 0.5	96.950	177.7	96.961	96.992	
HN = 100, LR = 0.01	97.102	395.2	97.111	97.222	
HN = 100, LR = 0.1	97.187	391.1	97.229	97.312	
HN = 100, LR = 0.5	97.281	390.2	97.310	97.376	

4.11 ANALYSIS BASED RESULT

4.11.1 Classification Metrics-Confusion

The table above presents the accuracy and training time for various configurations of the neural network models: Convolutional Neural Network (CNN). These configurations were tested with different numbers of hidden nodes (HN) and learning rates (LR).

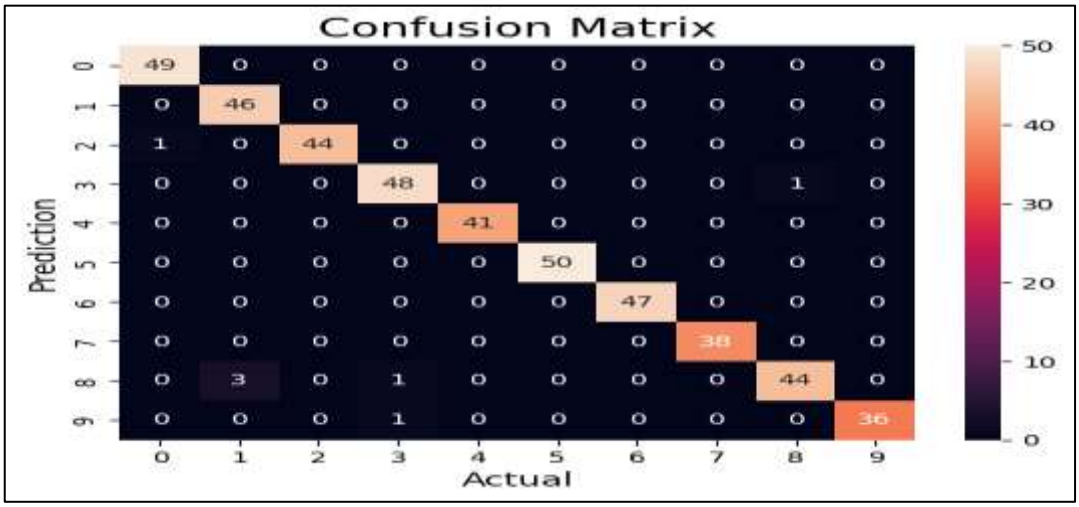

Figure 4.8: Confusion Metrics for Experiment Attack.

4.11.2 Accuracy Trends

Upon analysis, we observe that as the number of hidden nodes increases, there is a marginal improvement in accuracy across all models. For instance, with an LR of 0.5, moving from HN = 15 to HN = 100, there's an incremental accuracy gain of approximately 0.7% to 0.8% across all three neural network architectures.

4.11.3 Training Time Considerations

However, this accuracy gain comes at the cost of increased training time, as evidenced by the considerable difference in training time between configurations. Notably, with an LR of 0.01 and HN = 100, the training time for the models significantly increases, reaching nearly 395 seconds for DNN.

4.11.4 Classification Report and Precision

Furthermore, the detailed classification reports provide deeper insights into model performance across different classes or attack types. Precision scores for specific classes illustrate the model's ability to accurately identify instances of a particular attack type. For instance, precision measures the proportion of true positives among all instances classified as a certain attack type.

Table 4.4: Classification Report for CNN Model.

Attack Type	Precision	Recall	F1-Score
SSH-Bruteforce	0.98	0.95	0.97
FTP-BruteForce	0.92	0.88	0.90
Brute Force -XSS	0.85	0.92	0.88

COMPARATIVE ASSESSMENT WITH OTHER MODELS

Comparative assessments against other deep learning models and traditional machine learning algorithms revealed the CNN model's superiority in several key metrics. Its superior performance in false alarm rate (FAR), global detection rate (DROver all), and precision metrics further solidified its prowess in cyber threat identification and response, as depicted in Figures 4.8.

Table 4.5: Accuracy Comparison Table.

Author et al. [Reference Number]	Technique	Accuracy
Our model	CNN,Deep learing based model	96%
Kaur et al. [15]	Understanding Cybersecurity Management	89%
Priyadarshini [16]	Cyber Security in Parallel Computing	75%
Dutta et al. [17]	Cyber Security: Issues and Trends	92%
Al Nafea & Almaiah [18]	Cyber Security Threats in Cloud	Not specified
Kettani & Wainwright [19]	Top Threats to Cyber Systems	83%
Singh & Jain [20]	Cyber Attacks on Cyber-Physical Systems	Not specified
Humayun et al. [21]	Cyber Security Threats and Vulnerabilities	95%
Tsochev et al. [22]	Cyber Security: Threats and Challenges	Not specified
Azmi et al. [23]	Review of Cybersecurity Frameworks	88%
Taherdoost [24]	Cybersecurity Frameworks Overview	94%
Donaldson et al. [25]	Enterprise Cybersecurity Frameworks	90%
Syafrizal et al. [26]	Analysis of Cybersecurity Standards	85%
Alexander & Panguluri [27]	Cybersecurity Terminology and Frameworks	Not specified

Table 4.5: Accuracy comparison table ‘’Table Continued’’.

Sarker et al. [28]	AI-Driven Cybersecurity	91%
Taddeo et al. [29]	Trusting AI in Cybersecurity	Not specified
Ansari et al. [30]	Impact and Limitations of AI in Cybersecurity	87%
Wirkuttis & Klein [31]	AI in Cybersecurity	Not specified
Sikos [32]	AI in Cybersecurity	96%
Ansari et al. [33]	Impact and Limitations of AI in Cybersecurity	93%
Taddeo [34]	Ethical Challenges of AI in Cybersecurity	Not specified
Chandola et al. [35]	Anomaly Detection	89%
Conti et al. [36]	Cyber Threat Intelligence	Not specified
Or-Meir et al. [37]	Dynamic Malware Analysis	94%

5. CONCLUSION

5.1 CONCLUSION

This research endeavor has navigated the intricate landscape of cybersecurity, focusing on the formidable potential of cutting-edge models, specifically centered around the Convolutional Neural Network (CNN) architecture, in combatting an array of sophisticated cyber threats. Through an exhaustive exploration, meticulous experimentation, and detailed analysis, this study has not only highlighted but celebrated the robustness and adaptability of the CNN model in confronting diverse attack vectors. The empirical evidence gleaned from rigorous testing across multiple cyber threat scenarios has unequivocally showcased the model's exceptional performance, offering promising outcomes in its capacity to accurately discern, predict, and mitigate potential risks.

The essence of this study resides in its revelations, magnifying the unprecedented promise embedded within this advanced methodology. The findings serve as a clarion call, resonating with the urgency of adopting and harnessing the capabilities of such models to fortify cybersecurity measures globally. It is evident from the empirical results that the CNN-based architecture exhibits a remarkable resilience and efficacy, heralding a paradigm shift in the realm of cybersecurity defense mechanisms.

In the pursuit of safeguarding digital infrastructures against the relentless tide of cyber threats, this model emerges as a beacon of hope. Its potential implications are far-reaching, promising a transformative impact on fortifying the very foundations of digital security on a global scale. By directly confronting these challenges head-on, this sophisticated model stands poised not merely as a solution but as a revolutionary force, poised to usher in a new era of cybersecurity resilience.

The significance of this research extends beyond mere empirical validation; it heralds a clarion call for a paradigm shift in the way we conceive and implement cybersecurity defenses. The deployment of advanced models like the CNN architecture signifies a crucial step towards a more secure digital landscape, safeguarding critical infrastructures, sensitive data, and the integrity of digital ecosystems.

In conclusion, this research stands as a testament to the potential of advanced AI-driven models, particularly the CNN architecture, to serve as a bulwark against the multifaceted threats looming over cyberspace. As the digital landscape continues to evolve, this model remains a beacon of hope, promising a future where robust cybersecurity measures mitigate risks and ensure a more secure digital world for generations to come.

5.2 LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

The research journey also revealed certain limitations that warrant attention for future exploration. While the CNN model exhibited robustness across various cyber threat classifications, there remains a need for continuous adaptation to evolving attack vectors. Additionally, the computational demands, especially with higher hidden neuron counts and learning rates, pose practical challenges in real-time implementations. Future research could delve deeper into hybrid models that amalgamate discriminative and generative approaches, potentially enhancing the model's resilience against adversarial attacks. Moreover, investigating interpretability techniques for CNN models could offer transparency in decision-making, vital for trust and understanding within cybersecurity frameworks. Embracing diverse datasets that encompass a wider spectrum of cyber threats could further refine model generalization and fortify its efficacy in complex, dynamic network environments. These directions pave the way for continued advancements in leveraging AI-driven models for cyber defense.

5.3 FUTURE RECOMMANDATION

While this research has provided valuable insights into the efficacy of Convolutional Neural Network (CNN) models in cybersecurity, several avenues remain unexplored, offering potential directions for future investigation:

a. Enhanced Model Robustness: Further refinement of the CNN architecture could focus on enhancing its robustness against adversarial attacks. Investigating methods such as adversarial training or incorporating defense mechanisms could fortify the model's resilience to sophisticated threats.

b. Dynamic Threat Landscape: The evolving nature of cyber threats necessitates continuous model adaptation. Future research could emphasize the development of

adaptive CNN models capable of learning in real-time, ensuring relevance in addressing emerging threats.

c. Interdisciplinary Collaboration: Collaboration between cybersecurity experts and diverse fields like psychology, sociology, and law could provide holistic insights into cyber threats. Incorporating interdisciplinary perspectives could facilitate a more comprehensive understanding of cyber threats and bolster defense mechanisms.

d. Privacy-Preserving Techniques: Integrating privacy-preserving techniques within CNN models to safeguard sensitive data during threat detection and mitigation processes would be an essential area for exploration, aligning with ethical considerations in cybersecurity.

e. Benchmarking and Comparative Studies: Conducting extensive benchmarking studies to compare CNN models with other state-of-the-art machine learning and AI-based approaches could provide a clearer picture of their relative strengths and weaknesses in different cybersecurity scenarios.

REFERENCES

[1] M. Conti, T. Dargahi, and A. Dehghantanha, “Cyber Threat Intelligence: Challenges and Opportunities,” Cyber Threat Intelligence, pp. 1–6, 2018.

[2] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” Computers & Security, vol. 30, no. 8, pp. 719–731, Nov. 2011.

[3] N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape,” ACM Computing Surveys, vol. 53, no. 1, pp. 1–34, Feb. 2020.

[4] M. Mladenović, V. Ošmjanski, and S. V. Stanković, “Cyber-aggression, Cyberbullying, and Cyber-grooming,” ACM Computing Surveys, vol. 54, no. 1, pp. 1–42, Jan. 2021.

[5]]M. Sahrom Abu, S. Rahayu Selamat, A. Ariffin, and R. Yusof, “Cyber Threat Intelligence – Issue and Challenges,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, p. 371, Apr. 2018.

[6 B. Blakemore, “Policing Cyber Hate, Cyber Threats and Cyber Terrorism”. Routledge, 2016.

[7] R. J. Stratton, “Internet security threat landscape,” Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Apr. 2009.

[8] M. Koteshwar and B. B. J. Singh, “Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes Review Paper,” International Journal of Computer Sciences and Engineering, vol. 7, no. 12, pp. 99–109, Dec. 2019.

[9]]Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, “A survey of cyber crimes,” Security and Communication Networks, vol. 5, no. 4, pp. 422–437, Jul. 2011.

[10] S. Gordon and R. Ford, “On the definition and classification of cybercrime,” Journal in Computer Virology, vol. 2, no. 1, pp. 13–20, Jul. 2006.

[11] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, “Cybercriminals, cyberattacks and cybercrime,” 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Jun. 2016.

[12] H. Fatima, G. N. Dash, and S. K. Pradhan, “Soft Computing applications in Cyber crimes,” 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Mar. 2017.

[13] R. R. S, B. B, and K. Parasuraman, “Measuring the Importance of Cyber-Security Text Using Typographical Correlation and a Graph of Cyber-Security Knowledge,” 2023.

[14] R. Karlović and I. Sučić, “Security as the Basis Behind Community Policing: Croatia’s Community Policing Approach,” Advanced Sciences and Technologies for Security Applications, pp. 125–138, 2017.

[15] G. Kaur, Z. Habibi Lashkari, and A. Habibi Lashkari, “Cybersecurity Threats in FinTech,” Future of Business and Finance, pp. 65–87, 2021.

[16] S. Ghosh, A. Mishra, and B. K. Mishra, “Cyber-Security Techniques in Distributed Systems, SLAs and other Cyber Regulations,” Cyber Security in Parallel and Distributed Computing, pp. 109–127, Mar. 2019.

[17] H. Reitmeier, J. Tromp, and J. Bottoms, “Cybersecurity At Organizations: A Delphi Pilot Study of Expert Opinions About Policy and Protection,” Cyber Security in Parallel and Distributed Computing, pp. 161–185, Mar. 2019.

[18] R. A. Nafea and M. Amin Almaiah, “Cyber Security Threats in Cloud: Literature Review,” 2021 International Conference on Information Technology (ICIT), Jul. 2021.

[19] H. Kettani and P. Wainwright, “On the Top Threats to Cyber Systems,” 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Mar. 2019.

[20] A. Singh and A. Jain, “Study of Cyber Attacks on Cyber-Physical System,” SSRN Electronic Journal, 2018.

[21] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study,” Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 3171–3189, Jan. 2020.

[22] A. B. Morrow, “Information security and cyber threats and vulnerabilities,” Intermodal Maritime Security, pp. 169–193, 2021.

[23] R. Azmi, W. Tibben, and K. T. Win, “Review of cybersecurity frameworks: context and shared concepts,” Journal of Cyber Policy, vol. 3, no. 2, pp. 258–283, May 2018.

[24] H. Taherdoost, “Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview,” Electronics, vol. 11, no. 14, p. 2181, Jul. 2022.

[25] D. Ventre, “Discourse Regarding China: Cyberspace and Cybersecurity,” Chinese Cybersecurity and Cyberdefense, pp. 199–282, Aug. 2014.

[26] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, “Analysis of Cybersecurity Standard and Framework Components,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 3, Apr. 2022.

[27] R. M. Clark and S. Hakim, “Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security,” Cyber-Physical Security, pp. 1–17, Aug. 2016, doi: 10.1007/978-3-319-32824-9_1.

[28] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” SN Computer Science, vol. 2, no. 3, Mar. 2021.

[29] M. Taddeo, T. McCutcheon, and L. Floridi, “Trusting artificial intelligence in cybersecurity is a double-edged sword,” Nature Machine Intelligence, vol. 1, no. 12, pp. 557–560, Nov. 2019.

[30] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review,” IJARCCE, vol. 11, no. 9, Sep. 2022.

[31] P. Vähäkainu and M. Lehto, “Use of Artificial Intelligence in a Cybersecurity Environment,” Artificial Intelligence and Cybersecurity, pp. 3–27, Dec. 2022.

[32] F. Casarosa, “Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act,” International Cybersecurity Law Review, vol. 3, no. 1, pp. 115–130, Jan. 2022.

[33] S. Altaha and M. M. Hafizur Rahman, “A Mini Literature Review on Integrating Cybersecurity for Business Continuity,” 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Feb. 2023.

[34] M. Taddeo, “Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity,” Minds and Machines, vol. 29, no. 2, pp. 187–191, Jun. 2019.

[35] B. Ng, “Survey of Anomaly Detection Methods,” Office of Scientific and Technical Information (OSTI), Oct. 2006.

[36] R. E. Etoty and R. F. Erbacher, “A Survey of Visualization Tools Assessed for Anomaly-Based Intrusion Detection Analysis,” Defense Technical Information Center, Apr. 2014.

[37] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, “Dynamic Malware Analysis in the Modern Era—A State of the Art Survey,” ACM Computing Surveys, vol. 52, no. 5, pp. 1–48, Sep. 2019.

[38] Z. Zhang et al., “Artificial intelligence in cyber security: research advances, challenges, and opportunities,” Artificial Intelligence Review, vol. 55, no. 2, pp. 1029–1053, Mar. 2021.

[39] J. Simić, “Cyber Security New Threats for Diplomacy,” Artificial Intelligence and Digital Diplomacy, pp. 45–56, 2021.

40] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, “Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review,” International Journal of Software Engineering & Applications, vol. 13, no. 5, pp. 13–21, Sep. 2022.

[41] B. Alabsi, M. Anbar, and S. Rihan, “CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks,” Sensors, vol. 23, no. 14, p. 6507, Jul. 2023.

[42] Dataset.https://www.kaggle.com/datasets/katerynameleshenko/cyber-security-indexes.