

AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks Using Behavioral and Network Telemetry

Mahbub Hasan¹, Mohammad Masudur Rahman², Mst. Murshida Khatun³, Muhammad Farhan Nafees⁴, Muhammad Rahim⁵

¹BSc in Information Technology, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh

²Department of Marine Science and Oceanography, Florida Atlantic University, USA

³B.Sc in Textile Engineering, City University, Dhaka, Bangladesh

⁴Bachelors in Business Administration, Shah Abdul Latif University, Pakistan

⁵Bachelor in English Language and Literature, International Islamic University, Pakistan



DOI : <https://doi.org/10.61796/ipteks.v1i1.633>



Sections Info

Article history:

Submitted: October 25, 2023

Final Revised: November 15, 2023

Accepted: December 10, 2023

Published: December 30, 2023

Keywords:

Artificial Intelligence (AI)

Ransomware detection

Enterprise network security

Network telemetry

Behavioral analytics and machine learning

ABSTRACT

Objective: To address this challenge, this research presents an AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks Using Behavioral and Network Telemetry, a framework that supports the early detection and prevention of ransomware attacks by leveraging intelligent analysis of network behavior and traffic characteristics. The proposed framework aims to combine machine learning with behavioral analytics to detect malicious activities by analyzing network telemetry attributes, traffic patterns, and communication behaviors in enterprise contexts. **Method:** The UNSW-NB15 benchmark dataset is used to train and test the proposed framework due to the availability of a complete set of enterprise network traffic with both normal and malicious traffic having forty-nine engineered behavioral and network telemetry features. While the dataset is not 100% ransomware-specific, it is suitable for representing malicious network behaviour, which can be used to develop and test AI-based models of cyber threats. The framework consists of data preprocessing, feature engineering, model development using supervised machine learning, anomaly detection, and automated prevention mechanisms, to help boost detection efficiency while minimizing false positive rates. The performance is evaluated based on well-known cyber security metrics such as Accuracy, Precision, Recall, F1-Score, Receiver Operating Characteristic (ROC), Area under the Curve (AUC), and Confusion Matrix analysis. **Results:** The planned policy will boost enterprise cyber security by facilitating proactive detection of suspicious network activity that can prevent ransomware attacks from becoming a threat to organizational assets. The results should help to prove the value of artificial intelligence in today's cyber security landscapes and offer real support for enterprise-scale adoption of AI ransomware mitigation techniques. **Novelty:** The research provides a scalable, intelligent, data-driven security framework capable of responding to threats quickly, augmenting incident response capabilities and bolstering the resiliency of enterprise networks to the changing nature of ransomware attacks.

INTRODUCTION

A. Background

Enterprise organizations are heavily relying on these interconnected computer networks, cloud services, and digital information systems, significantly due to the fast pace of digital transformation [1]. These technological advances have made organizations more efficient and more communicative, but they've also made them more vulnerable to cybercriminals. Ransomware is one of the most devastating types of malware for enterprise environments, as it is able to encrypt valuable data in an organization and demand a ransom for its decryption. As ransomware is becoming more sophisticated, traditional cybersecurity tools focusing on signature-based detection methods are being

tested. Such traditional methods fail to identify new or updated ransomware strains, resulting in devastating monetary losses, disruption to businesses, and damage to brands. The ability to learn complex behavioral patterns, analyze massive amounts of network data, and detect new threats, is making Artificial Intelligence (AI) an essential tool in enhancing cybersecurity [2]. By analyzing the subtle differences in network traffic and behavioral patterns, machine learning algorithms can identify anomalies that indicate malicious activity and automatically classify them. Network telemetry can be useful in enterprise environments to give insight into patterns of communication, usage of protocols, traffic flows, states of connections and other elements that help identify malicious activity before it's too late to have a significant impact on the system. Behavioral analysis is another way to increase the detection capabilities by analyzing any variation from normal network operations, not just attack signatures. This study presents an AI-based ransomware detection and defense framework for enterprise networks that leverages behavioral and network telemetry [3]. To test intelligent detection models based on enterprise network telemetry and behavioral features, the study has used the UNSW-NB15 dataset. The proposed framework combines AI capabilities with behavioral analysis, enhancing the precision of ransomware detection, minimizing false alerts, and bolstering proactive cyber defense efforts in enterprise networks.

B. AI-Driven Behavioral and Network Telemetry for Enterprise Cybersecurity

Intelligent detection is the key to modern enterprise cybersecurity, as it is able to detect advanced cyber-attacks in real time. Conventional intrusion detection systems are often rule-based, relying on known attack patterns and signatures, which are not effective against new ransomware variants that keep changing their tactics. As a result, AI has become a key tool for researchers and cybersecurity professionals to enhance the adaptability and accuracy of cyber threat detection [4]. Behavioral analytics is primarily about gaining insights into the normal activities of users, devices, and network services to detect unusual activities that could be signs of malicious actions. Network telemetry can be used to support this process by gathering detailed data on network communication, such as the duration of the connection, the number of packets transmitted, the utilization of the protocols, the volume of the traffic, and its characteristics. Combining the two strategies allows AI models to detect fraudulent activity early, before significant harm takes place [5]. Machine learning algorithms built on enterprise network data can accurately detect a range of normal and malicious activities, and continually learn and evolve their detection capabilities. UNSW-NB15 is a realistic enterprise network environment that consists of many telemetry and behavioral attributes that make it ideal for training intelligent cybersecurity models. This benchmark dataset would empower researchers to create scalable detection systems that can be applied to enterprise security operations and bolster the level of security and resilience of an organization against new ransomware threats. Combining behavioral analytics and network telemetry is thus a prudent approach to bolstering proactive cyber defense in today's enterprise environment.

C. Problem Statement

Ransomware continues to be a major threat to enterprise networks because today's ransomware variants often can bypass traditional signature-based security solutions. Conventional IDSs may have a difficult time detecting new attack types, leading to a late detection time which poses a threat to the organization's losses. While AI has shown great promise in the field of cybersecurity, current detection methods tend to either be based on understanding malware or do intrusion detection but fall short of incorporating behavioral analytics and network telemetry. There is still a need, therefore, for an intelligent framework that can effectively detect suspicious enterprise network activity and enable timely ransomware prevention using AI analysis of the network telemetry and behavioral attributes.

D. Objectives of the Study

The objectives of this study is to

- To explore the characteristics of malicious activities in enterprise network environments, by analyzing the UNSW-NB15 dataset.
- To target key network features that would be helpful in ransomware detection using AI.
- To build an AI-powered ransomware detection and prevention solution for enterprise networks.
- To test the performance of specific machine learning algorithms on commonly used evaluation metrics used for cybersecurity [6].
- To compare the effectiveness of the AI-based detection system against the traditional network intrusion detection system.
- To design a scalable enterprise cybersecurity framework to improve proactive ransomware prevention using behavioral and network telemetry analysis.

E. Research Questions

Following these question is to guide to this study are:

- How can AI help enterprises detect and prevent ransomware in enterprise networks with behavioral and network telemetry?
- What is the most important network telemetry and behavioral attribute to help identify malicious activity on enterprise networks?
- Which ML algorithm is best suited for the proposed AI-based ransomware detection system?
- What are the advantages of the proposed framework in increasing detection accuracy and in lowering false positive rates over the traditional approach to intrusion detection?

F. Significance of the Study

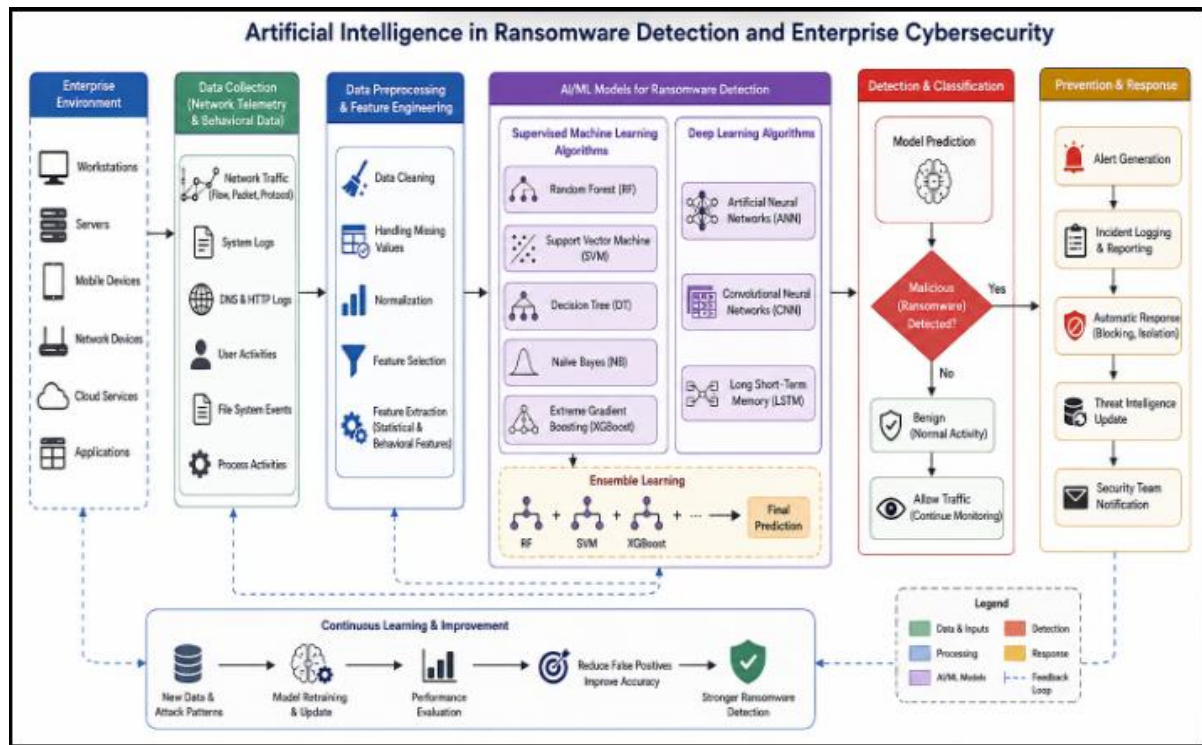
This study is part of the large body of work in the field of artificial intelligence (AI)-driven cybersecurity and offers an AI-centric structure for detecting and preventing ransomware attacks in enterprise network environments. Behavioral analytics and network telemetry allows the framework to better identify abnormal network activity

than traditional signature-based security solutions [7]. The proposed framework uses machine learning algorithms to enable continuous monitoring and intelligent detection of malicious activities, thus promoting proactive cyber defense. Enterprises will find this research valuable because it offers a way for organizations to enhance their cybersecurity defenses and prevent the newest ransomware threats. The earlier suspicious activities are detected the less likely to be disrupted, financial losses are less, and the ability to respond to an incident is enhanced [8]. The framework also illustrates how enterprise network telemetry can be converted to actionable network security intelligence with the use of artificial intelligence. Academically, this work is a continuation of the work in previous studies by the inclusion of a behavioral analysis with a network telemetry and artificial intelligence decision making framework within a single cybersecurity framework. Using the UNSW-NB15 benchmark dataset enables reproducible experimentation and comparison with previous intrusion detection experiments. In addition, the research provides a systematic approach that can be applied to future studies using more sophisticated machine learning algorithms and emerging cyber threats [9]. The results of this study will be useful to cybersecurity researchers, enterprise security practitioners, security administrators, and policymakers to guide implementation of intelligent detection systems. The proposed framework can enhance the resilience, reliability, and security of enterprise networks and promote the widespread use of AI in contemporary cybersecurity strategies.

Role of AI in Ransomware Detection and Enterprise Cybersecurity

As ransomware attacks get more sophisticated, researchers have been exploring the use of artificial intelligence (AI) to strengthen enterprise cyber threat detection. Signature-based detection systems can detect known malware but may not be able to detect new ransomware variants that use code obfuscation, polymorphism or zero-day techniques [10]. To overcome these constraints, many researchers have investigated machine learning and deep learning algorithms that are able to learn complex attack patterns from huge sets of cybersecurity data. Some of the machine learning algorithms that have been shown to perform well for malicious and benign network activity classification include supervised learning algorithms like Random Forest, Support Vector Machine (SVM), Decision Tree, Naïve Bayes, and Extreme Gradient Boosting (XGBoost) which are considered promising due to the statistical features extracted from enterprise traffic. The researchers claim that ensemble learning has higher detection accuracy and higher robustness than single classifiers, since they use multiple decision models to minimize classification errors [11]. Deep learning techniques, such as Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks, have demonstrated promising performance in extracting hierarchical feature representations automatically with minimal manual feature engineering. While these improvements have been made, many current research works focus on either malware classification or on general intrusion detection rather than on ransomware prevention in enterprise networks [12]. In addition, there are a number of

detection models that use artificial intelligence that are very dependent on the static properties of the malware and do not adopt continuous behavioral monitoring of the activities of enterprises on their network. Such constraints call for an integrated ecosystem that integrates AI with behavioral analytics and network telemetry for enhanced ransomware detection accuracy, lower false-positive rates, and expanded proactive cyber defense capabilities.



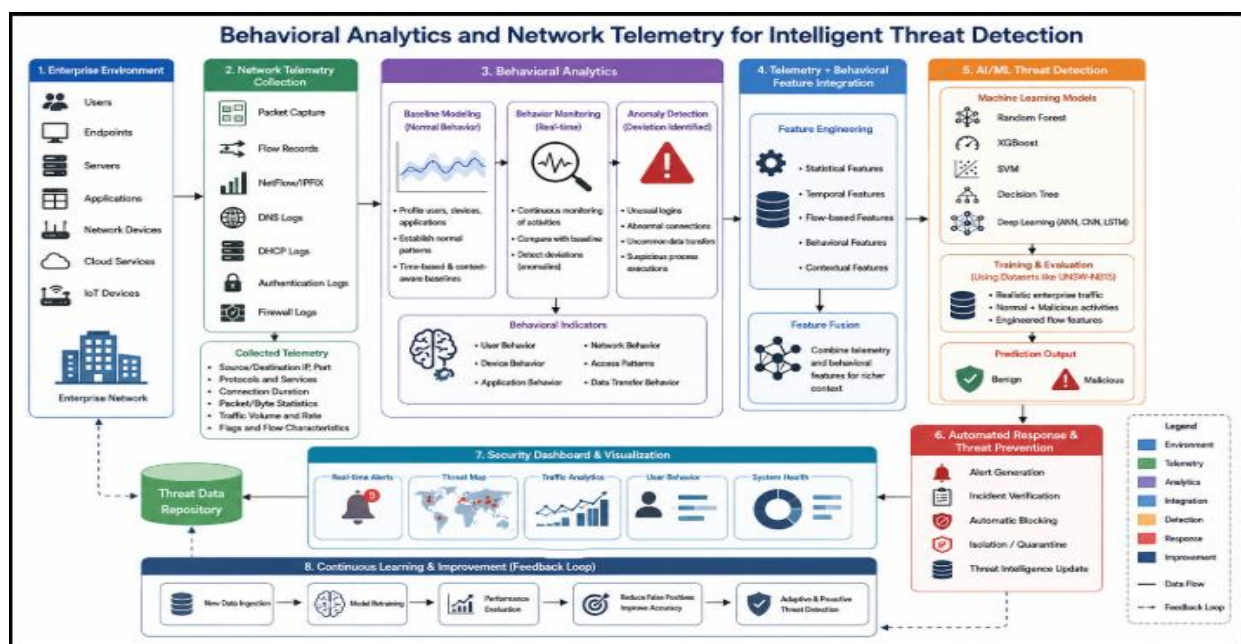
This flowchart shows an AI-powered enterprise ransomware detection and prevention (RPDP) framework with behavioral network telemetry.

The flowchart illustrates an AI-driven framework for ransomware detection and prevention in enterprise cybersecurity. It starts with enterprise network environments, where telemetry data for behavior and network are gathered from applications, workstations, servers and cloud services. Collected data are preprocessed by applying data cleaning, data normalization, feature selection and feature extraction [12]. The processed data is then analyzed using supervised machine learning algorithms like Random Forest, SVM, Decision Tree, Naïve Bayes and XGBoost, in addition to deep learning models like ANN, CNN and LSTM. Ensemble learning produces the final prediction which is a classification of benign or malicious activities. Automated actions, alerts, incident reporting, threat intelligence updates and continual model refinement boost enterprise cyber resiliency when ransomware is detected.

Behavioral Analytics & Network Telemetry for Intelligent Threat Detection

The significance of behavioral analytics and network telemetry has grown to be vital in modern cybersecurity, as these technologies allow systems to identify suspicious activities by analyzing deviations from normal behaviour, rather than by patterns of

attack. Behavioral analytics is concerned with tracking user, device, and application and network service actions to create a baseline of normal behavior [13]. If it deviates from these patterns, it could be a sign of unauthorized access, execution of malware, or ransomware activity. While behavioral analysis provides a general overview of network use, network telemetry can provide additional fine-grained data about network traffic, such as what services are being used, for how long, how much traffic is being sent and received, what protocols are being used, the number of packets sent, whether they are being sent to or from different addresses, and more. Previous studies have shown how behavioral indicators, when used in conjunction with network telemetry, can greatly improve the performance of machine learning models by giving them additional context to use when detecting cyber threats [14]. Enterprise network traffic is represented in realistic datasets like UNSW-NB15, which feature known enterprise network behaviors and statistical features along with engineered malicious traffic, making them popular for assessing AI-based intrusion detection systems [15]. Machine learning techniques have been applied successfully to these datasets to enhance intrusion detection accuracy, detection latency and to decrease false alarm rates. Despite that, few studies have tried to create a consistent framework that is able to combine behavior, network telemetry, and automatic ransomware prevention in an enterprise environment. This study offers an artificial intelligence (AI)-based framework that leverages telemetry and behavioral characteristics from an enterprise network to facilitate early detection of suspicious activity and proactive ransomware prevention. This could boost organizational resilience to more advanced cyber threats, as well as to enable intelligent, scalable, and data-driven enterprise cybersecurity systems.



This flowchart depicts AI-based behavioral analytics and network telemetry in intelligent enterprise threat detection

The flowchart represents an intelligent threat detection system for enterprise cybersecurity, which combines behavioral analytics and network telemetry. It starts by gathering the enterprise device, application, server and cloud services telemetry. Behavioral analytics sets normal activity baselines and constantly analyzes user, device and application behavior to flag anomalies [16]. The features extracted from the network telemetry are then subjected to feature engineering and feature fusion for subsequent analysis by machine learning and deep learning algorithms such as Random Forest, XGBoost, SVM, Decision Tree, ANN, CNN and LSTM. The prediction module categorizes activities as benign or malicious, thereby activating automated response mechanisms like alerting, incident verification, automatic blocking, isolation, threat intelligence updates, and ongoing learning to enhance the accuracy of future predictions.

Empirical Study

M. Devendra Patel in the article "AI-Enabled Cybersecurity Threat Prediction and Response Systems for Distributed Computing Environments" introduced an advanced AI architecture designed to predict and respond to cybersecurity threats in distributed computing environments such as cloud, edge, and on-premises systems. The study combines streaming telemetry, graph-based security analytics, Graph Neural Networks (GNNs), online anomaly detection, and reinforcement learning to achieve better early threat prediction and automated security response [1]. The proposed architecture features Federated Learning, Differential Privacy, Explainable Artificial Intelligence (XAI), Digital Twin simulation, and MLOps, which aims to improve model reliability, scalability, and deployment in real-world enterprise settings. The results suggest that intelligent prediction and an automated response mechanism can be used to enhance the capability of early warning, shorten the response window, and increase cybersecurity resilience with minimal operational burden. While the research emphasizes threat prediction in cybersecurity and not exclusively ransomware detection, the study clearly illustrates the potential of a multi-faceted approach to cyber defense, combining behavior monitoring, network telemetry, and sophisticated AI methods. This work underpins the current work and serves as a foundation to build an AI-driven framework for enterprise networks specific to ransomware detection and prevention through behavioral analytics and network telemetry. The article underscores the need for smart, adaptive and automated cybersecurity solutions to safeguard modern enterprise infrastructure against the ever-changing cyberthreats.

In his article, 'The Influence of Generative AI on Adaptive Malware Defense Systems', Sandhya R. Bista explored how generative artificial intelligence (AI) is reshaping the landscape of adaptive malware defense systems to tackle increasingly sophisticated cyber threats. The research pointed out that signature-based detection systems are unable to detect polymorphic, metamorphic, and zero-day malware, and highlighted the need for intelligent and adaptive cybersecurity solutions [2]. The author explored the use of advanced generative AI models like Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and transformer-based

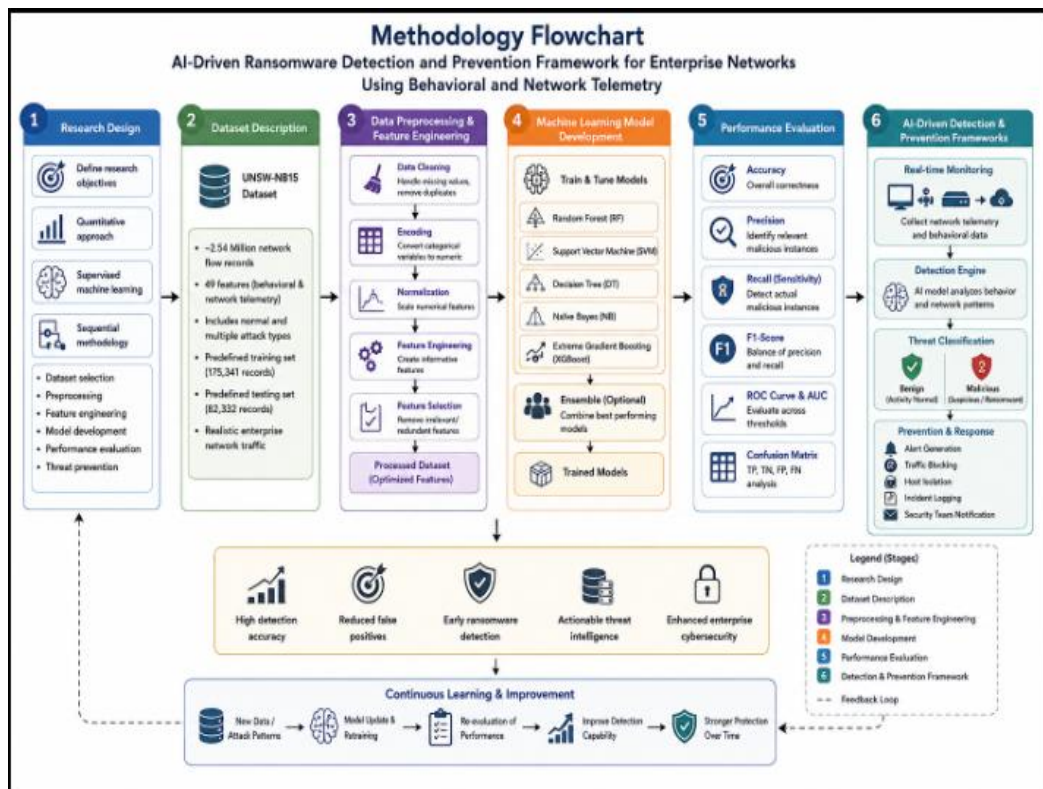
architectures to generate malicious activities, improve anomaly detection and enable proactive threat identification. The suggested method allows cyber security systems to adapt in the presence of real and synthetic attacks, improving detection and response capabilities. The study validated that the integration of generative AI with behavioral analysis and real-time monitoring is to enhance adaptive malware defense in the face of changing cyber threats. While the study is not specifically about ransomware detection, it offers insights into how AI can be used in cybersecurity in general that will be relevant for enterprise network protection. This article offers robust theoretical backing for the current study, agreeing with the combination of artificial intelligence, behavioral analytics, and intelligent detection methods in the enhancement of ransomware detection and prevention in enterprise network environments.

Rahul Sharma in the article "AI-Enhanced Disaster Recovery in Cloud Systems" discussed how AI can be used to enhance disaster recovery mechanisms in contemporary cloud computing systems. The study highlighted the drawbacks of traditional disaster recovery strategies, such as manual processes and predefined recovery scripts, which are less effective in dynamic cloud environments. The author suggested incorporating the use of artificial intelligence, neural networks, and reinforcement learning for using the huge amounts of telemetry data, system logs and performance metrics to detect abnormal system behavior at an early stage and make smart plans for system recovery. The study also underscored the efficiency of AI tools in filtering out too many alerts, automating recovery processes, minimizing service downtime, and enhancing system overall resilience [3]. The proposed approach allows for adaptive recovery strategies based on continual learning from historical operational data, which allows for efficient recovery operations in response to evolving cloud conditions. The study is largely centered on disaster recovery, yet it underscores the significant role that AI, telemetry analysis, and automated decision-making play in boosting cybersecurity and enhancing the reliability of systems. This article serves as useful background for the current study and helps to facilitate the adoption of analytics and network telemetry powered by artificial intelligence for ransomware detection and prevention in enterprise network environments.

RESEARCH METHOD

The methodology provides a structured approach undertaken in the development and assessment of the proposed AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks with Behavioral and Network Telemetry. The study adopts a quantitative research approach, supervised machine learning, and applies the UNSW-NB15 benchmark dataset. The methodology involves research design, data selection, data preprocessing, feature engineering, development of machine learning models, performance evaluation, framework implementation, and ethical considerations [17]. Together these stages guarantee that the proposed framework would be

scientifically sound, repeatable and would be able to detect malicious behavior in an enterprise network environment.



This flowchart illustrates the AI-driven methodology for enterprise ransomware detection and prevention framework development.

The flowchart illustrates the research methodology used to create an AI-based ransomware detection and prevention system for enterprise networks. The methodology starts with a quantitative research design and then the UNSW-NB15 benchmark dataset is selected. The collected network data is then preprocessed and feature engineered, such as data cleaning, encoding, normalization, and feature selection, to enhance data quality [18]. Multiple supervised machine learning algorithms are trained and tested based on the widely-used cybersecurity performance metrics including Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix. The final framework will be intelligent threat detection and automated prevention with a continuous learning mechanism, improving detection accuracy over time and thereby improving enterprise cybersecurity.

A. Research Design

The research design used in this research is quantitative research design. The quantitative research design is used for this research in developing and testing an artificial intelligence-based ransomware detection and ransomware prevention framework in enterprise networks. This is because a quantitative approach allows for objective evaluation of the performance of machine learning systems based on numerical data and standardized evaluation metrics. The proposed framework is based on a

supervised machine learning approach where network traffic is categorized as normal or malicious traffic with the help of its behavior and network telemetry features [19]. The research process can be divided into several stages: Data acquisition, Data preprocessing step, Feature engineering step, Model training step, Model validation step, Model validation performance evaluation step, and intelligent threat prevention step. The results of each stage enhance how accurately and reliably ransomware can be detected. The UNSW-NB15 dataset will be used as the main source of enterprise network traffic, since it provides realistic network behavior suitable for conducting AI-based cybersecurity studies [20]. In experimentation, multiple machine learning algorithms are trained, tested and compared using the same dataset and evaluation method to ensure a fair comparison of the models. Standardized preprocessing methods, identical experimental setup, and widely used cybersecurity evaluation metrics are also used to highlight the research design's reproducibility. The systematic methodology ensures that the proposed framework can process the telemetry data of behavior and network in an efficient manner, and also offers an intelligent mechanism for identifying suspicious activities [21]. The research design is designed to create a viable and scalable ransomware detection framework that can enhance enterprise cybersecurity based on data-driven decision making.

B. Dataset Description

The proposed framework is based on the publicly available UNSW-NB15 dataset developed by the Australian Centre for Cyber Security (ACCS) for cybersecurity research. The IXIA Perfect Storm traffic generation platform was used to create the dataset, and it includes a realistic enterprise network traffic mix of both legitimate and malicious traffic. It contains about 2.54 million network flow records, each containing forty-nine engineered behavioral and network telemetry features that capture communication protocols, connection states, packet statistics, the duration of the traffic, service types, source and destination addresses, and flow characteristics. The complete dataset is provided, along with pre-defined training and testing subsets with 175,341 and 82,332 records, respectively, for standardized machine learning experimentation. Multiple attack categories such as Exploits, Backdoors, Analysis, DoS, Fuzzers, Generic, Reconnaissance, Shellcode, Worms are also included in the data set that enables the AI algorithms to learn a variety of malicious behavioral patterns. UNSW-NB15 is not a ransomware-only dataset but its rich network telemetry and behavioural properties are a good representative of enterprise cyber threats and abnormal network activity in advanced attacks [22]. The dataset is well-suited for the development and testing of the new AI-based ransomware detection and prevention framework, with its distinctive attributes. Moreover, a large number of researchers use UNSW-NB15 in their cybersecurity research, which promotes the reproducibility of the data and facilitates the comparison of the results with past published intrusion detection studies.

C. Data Processing and Engineering

Machine learning models rely heavily on data preprocessing to enhance their performance and accuracy in detecting ransomware. Data preprocessing plays a crucial role in the development and effectiveness of machine learning models, contributing to their reliability in ransomware detection. The UNSW-NB15 dataset is subjected to several pre-processing steps prior to model training to ensure consistency of the data and remove irrelevant information. First of all, duplicate records and incomplete observations are detected and eliminated from the data set to ensure data set integrity [23]. Appropriate data cleaning, missing value handling methods are provided to avoid biased learning of the models. The categorical attributes like protocols, services and connection states are encoded to numerical values suitable for supervised learning algorithms. Numerical features are then scaled to have means of zero and a standard deviation of one to standardize variables with different scales, so they all have equal influence on model learning. After preprocessing, feature engineering is done to further improve the dataset's prediction power. An analysis of the statistical characteristics and their selection techniques are used to determine the most informative telemetry characteristics of behavior and network activities related to malicious activities [24]. The irrelevant and redundant features are eliminated to achieve computational simplicity without compromising the classification accuracy. Selected features include enterprise network behaviors such as communication patterns, traffic characteristics, connection durations, packet statistics and protocol usage. Appropriate preprocessing and feature engineering increase learning efficiency, prevent overfitting, speed up model convergence, and ensure that AI algorithms can correctly identify normal network operations from suspicious ones that could be a ransomware attack or other advanced cyber threats.

D. Machine Learning Model Development

The proposed ransomware detection framework is based on supervised machine learning algorithms which classify enterprise network activities into benign or malicious categories. A number of widely used classification algorithms are chosen due to their proven performance in the cybersecurity field. The algorithms used are: Random Forest, Decision Tree, Support Vector Machine (SVM), Naïve Bayes, Extreme Gradient Boosting (XGBoost). All the algorithms are trained with the preprocessed UNSW-NB15 dataset and optimized by tuning the algorithm parameters to increase the accuracy of the classification and minimize the number of predictions that are incorrect [25]. The training dataset is utilized to build predictive models during model development that can learn behavioral patterns of malicious network activities. The testing data set is then used to test the generalization power of each model to test the generalization power of each model on unseen network traffic. To capitalize on the advantages of using multiple classifiers to enhance detection accuracy and robustness, ensemble learning techniques could be employed [26]. Trained models analyze enterprise network telemetry – packet statistics, communication behaviors, protocol characteristics and connection information – to detect abnormal activities, which could be the sign of a ransomware attack. The study

will compare several machine learning techniques and in the same experimental environment, which machine learning algorithm is best suited for assisting with intelligent ransomware detection and prevention in enterprise network environments.

E. Performance Evaluation

To comprehensively assess the classification accuracy and capability of detection, multiple commonly adopted cybersecurity performance metrics are used to evaluate the effectiveness of the proposed AI-driven framework. Classification Accuracy is defined as the proportion of instances that the classification algorithm got right in the network. Precision measures the percentage of the number of malicious activities correctly identified from all the malicious activities that were predicted and Recall measures the framework's ability to detect actual malicious network behaviors [27]. The F1-Score is a combination of the Precision and the Recall: it is used to measure the effectiveness of the detection. ROC curve analysis is used to explore the classification ability of the model over various decision thresholds, while the Area under the ROC Curve (AUC) provides a global measure of the discriminative power of the model. Another report, a Confusion Matrix is also produced, showing the percentage of True Positives, True Negatives, False Positives, and False Negatives and allowing for in-depth error analysis. False Positive Rate and False Negative Rate are explored since many unanticipated alerts or attacks can prove to have a significant impact on enterprise cybersecurity operations [28]. The combination of these evaluation metrics offers a credible and objective proof of the accuracy, strength, reliability, and feasibility of the suggested ransomware detection and prevention system.

F. Proposed AI-Driven Detection and Prevention Framework

The proposed framework combines behavioral analytics, network telemetry and AI as a single enterprise cybersecurity solution. All of the traffic on the enterprise network is continuously monitored and telemetry information is gathered, including packet statistics, connection duration, communication protocols, traffic volume and flow characteristics. Baseline patterns for normal user, device and application activities are created by behavioral analytics. After pre-processing and feature engineering, the machine learning algorithms are used to analyze the features extracted from the network and classify its behavior as either benign or malicious [28]. The prevention module generates alerts automatically, logs security events, prevents malicious traffic, isolates compromised systems, and alerts security administrators to investigate. The framework also features a continuous learning loop, which will continuously refine the detection models with newly learned behavior, further enhancing the prediction accuracy and keeping the models resilient to the latest ransomware tactics in enterprise networks.

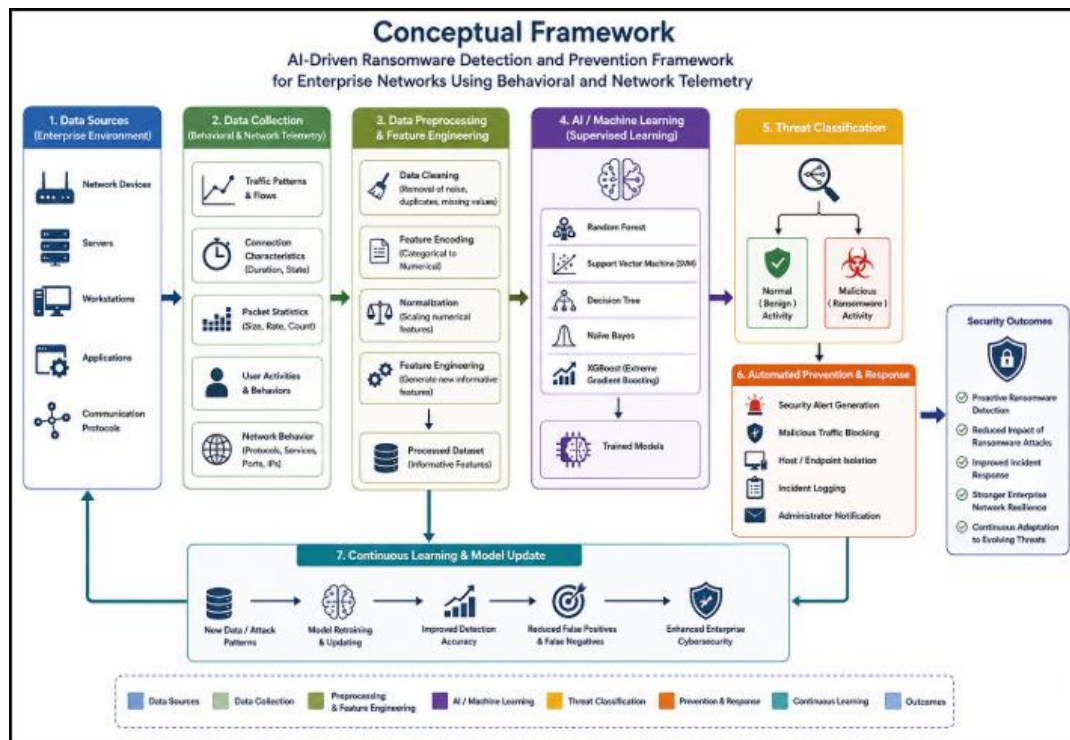
G. Ethical Concerns and Limitation

This study uses exclusively the publicly available UNSW-NB15 dataset for academic research purposes, and respects the conditions of the license set by the developers of the dataset. No personally identifiable information or confidential organizational data is collected, thus adhering to the ethical principles of research and

data privacy [29]. The framework outlined is not to be used for malicious activities, but to enhance enterprise cybersecurity. Even though the study has benefits, there are some drawbacks. The UNSW-NB15 is mainly an intrusion detection dataset instead of a ransomware dataset, so there may be some behaviors of ransomware not fully represented. Also, the framework is tested with offline benchmark data instead of real time enterprise network traffic [30]. Thus, the performance of the models could vary in real-world scenarios with changing attack methods, network setups, and new cyber threats. The framework needs to be further validated in the current ransomware datasets and in the real-world enterprise environments in the future.

Conceptual Framework

The conceptual framework depicts the overall structure of the proposed AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks Using Behavioral and Network Telemetry by showing the relationships between enterprise network data, behavioral analytics, artificial intelligence, detection mechanisms, and automated prevention strategies [31]. This starts with the collection of behavior and network telemetry data from enterprise network devices, servers, workstations, applications and communication protocols. These information are traffic flows, connection durations, packet statistics, communication patterns, protocol information, and user activities from which a picture of the operational behavior of the enterprise network can be drawn. After data acquisition, the data are processed, which involves data cleansing, missing value imputation, categorical encoding, normalization and feature engineering to enhance data quality and establish the most informative behavioral and network telemetry features [32]. The processed data is then fed into machine learning algorithms, such as Random Forest, Support Vector Machine (SVM), Decision Tree, Naïve Bayes, and Extreme Gradient Boosting (XGBoost), which learn the relationships between normal and malicious network behaviour and are accurate in classifying enterprise network activities [33]. The proposed framework automatically triggers preventive responses based on the classification results, such as security alert generation, blocking malicious traffic, isolating compromised hosts, logging of incidents and administrator notification, to allow for the prompt response to possible ransomware attacks. Furthermore, a continuous learning mechanism is used to update the trained machine learning models with new behavioral patterns observed in the network, as well as to collect network telemetry data, which further enhances the accuracy of detection, lowers false positive rates and helps adapt to new cyber threats [34]. The conceptual framework illustrates the interdependencies among behavioral analytics, enterprise network telemetry, supervised machine learning and automated prevention mechanisms as an integrated cybersecurity solution for proactive ransomware detection. The framework, which integrates intelligent data analysis with automated response, significantly boosts the cyber resilience of enterprises, streamlines decision-making processes, and fortifies enterprise network infrastructures against advanced attacks by ransomware.



This flowchart depicts a conceptual framework for enterprise ransomware detection and prevention, driven by AI and behavioural telemetry.

The flowchart presents the conceptual framework of the proposed AI-driven ransomware detection and prevention system for enterprise networks. The architecture starts with gathering behavioural and network telemetry data from enterprise devices, servers, workstations, applications and communication protocols. The data is preprocessed to generate meaningful features for analysis by cleaning the data, encoding the features, normalizing the data, and engineering features [35]. The processed data is then fed into supervised machine learning algorithms that can classify network traffic as normal or malicious, such as Random Forest, Support Vector Machine, Decision Tree, Naïve Bayes and XGBoost. If malicious activity is detected, automated prevention mechanisms alert, block malicious traffic, isolate compromised hosts, log incidents, and alert administrators. The continuous learning capability keeps the models up to date with new patterns in the attacks, thus increasing the accuracy of the detections, decreasing false positive rates and further enhancing enterprise cybersecurity against the new ransomware patterns.

Dataset

A. Screenshot of Dataset

No.	Name	Type	Description
1	srcip	nominal	Source IP address
2	sport	integer	Source port number
3	dstip	nominal	Destination IP address
4	dsport	integer	Destination port number
5	proto	nominal	Transaction protocol
6	state	nominal	Indicates to the state and its dependent protocol, e.g. ACC, CLO, CON, ECO, ECR,
7	dur	Float	Record total duration
8	sbytes	Integer	Source to destination transaction bytes
9	dbytes	Integer	Destination to source transaction bytes
10	sttl	Integer	Source to destination time to live value
11	dttl	Integer	Destination to source time to live value
12	sloss	Integer	Source packets retransmitted or dropped
13	dloss	Integer	Destination packets retransmitted or dropped
14	service	nominal	http, ftp, smtp, ssh, dns, ftp-data, irc and (-) if not much used service
15	Sload	Float	Source bits per second
16	Dload	Float	Destination bits per second
17	Spkts	integer	Source to destination packet count
18	Dpkts	integer	Destination to source packet count
19	swin	integer	Source TCP window advertisement value
20	dwin	integer	Destination TCP window advertisement value
21	stcpb	integer	Source TCP base sequence number
22	dtpcb	integer	Destination TCP base sequence number

Attack category	Attack subcategory	Number of events
normal		2218761
Fuzzers	FTP	558
Fuzzers	HTTP	1497
Fuzzers	RIP	3550
Fuzzers	SMB	5245
Fuzzers	Syslog	1851
Fuzzers	PPTP	1583
Fuzzers	FTP	248
Fuzzers	DCERPC	164
Fuzzers	OSPF	993
Fuzzers	TFTP	193
Fuzzers	DCERPC	455
Fuzzers	OSPF	1746
Fuzzers	BGP	6163
Reconnaissance	Telnet	6
Reconnaissance	SNMP	69
Reconnaissance	SunRPC Portmapper (TCP) UDP Ser	2030
Reconnaissance	SunRPC Portmapper (TCP) TCP Serv	2026
Reconnaissance	SunRPC Portmapper (UDP) UDP Ser	2045
Reconnaissance	NetBIOS	5
Reconnaissance	DNS	35
Reconnaissance	HTTP	1867

id	dur	proto	servic	state	spkts	dpkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	sloss	dloss	sinpkt	dinpkt	sjit	djit	s
1	1	0.000011	udp	-	INT	2	0	496	0	90909.09	254	0	180363632	0	0	0	0.011	0	0	0
2	2	0.000008	udp	-	INT	2	0	1762	0	125000	254	0	881000000	0	0	0	0.008	0	0	0
3	3	0.000005	udp	-	INT	2	0	1068	0	200000	254	0	854400000	0	0	0	0.005	0	0	0
4	4	0.000006	udp	-	INT	2	0	900	0	166666.7	254	0	600000000	0	0	0	0.006	0	0	0
5	5	0.00001	udp	-	INT	2	0	2126	0	100000	254	0	850400000	0	0	0	0.01	0	0	0
6	6	0.000003	udp	-	INT	2	0	784	0	333333.3	254	0	1.045E+09	0	0	0	0.003	0	0	0
7	7	0.000006	udp	-	INT	2	0	1960	0	166666.7	254	0	1.307E+09	0	0	0	0.006	0	0	0
8	8	0.000028	udp	-	INT	2	0	1384	0	35714.29	254	0	197714288	0	0	0	0.028	0	0	0
9	9	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60001	0	0	0
10	10	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60001	0	0	0
11	11	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60001	0	0	0
12	12	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60001	0	0	0
13	13	0.000004	udp	-	INT	2	0	1454	0	250000	254	0	1.454E+09	0	0	0	0.004	0	0	0
14	14	0.000007	udp	-	INT	2	0	2062	0	142857.1	254	0	1.178E+09	0	0	0	0.007	0	0	0
15	15	0.000011	udp	-	INT	2	0	2040	0	90909.09	254	0	741818176	0	0	0	0.011	0	0	0
16	16	0.000004	udp	-	INT	2	0	1052	0	250000	254	0	1.052E+09	0	0	0	0.004	0	0	0
17	17	0.000003	udp	-	INT	2	0	314	0	333333.3	254	0	418666656	0	0	0	0.003	0	0	0
18	18	0.00001	udp	-	INT	2	0	1774	0	100000	254	0	709600000	0	0	0	0.01	0	0	0
19	19	0.000002	udp	-	INT	2	0	1568	0	500000	254	0	3.136E+09	0	0	0	0.002	0	0	0
20	20	0.000004	udp	-	INT	2	0	2054	0	250000	254	0	2.054E+09	0	0	0	0.004	0	0	0
21	21	0.000001	udp	-	INT	2	0	2170	0	100000	254	0	868000000	0	0	0	0.01	0	0	0
22	22	0.000009	udp	-	INT	2	0	202	0	111111.1	254	0	89777776	0	0	0	0.009	0	0	0

(Source Link: https://www.kaggle.com/datasets/mrwellsdavid/unswnb15?select=UNSW_NB15_training-set.csv)

B. Dataset Overview

The proposed research is intended to use the UNSW-NB15 dataset as the main benchmark dataset for the development and evaluation of the AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks Using Behavioral and Network Telemetry. The UNSW-NB15 dataset was created by the Australian Centre for Cyber Security (ACCS) at the University of New South Wales using the IXIA PerfectStorm traffic generation platform to generate real-world enterprise network traffic that includes legitimate user activities and a variety of cyberattacks. It was created to conquer the drawbacks of previous intrusion detection sets and supply more representative and modern network traffic, which more closely represents the enterprise communication habits. This dataset contains ~2.54 million network flow records extracted from ~100 GB of raw packet capture (PCAP) files, with engineered behavioral and network telemetry features, along with class labels for detecting normal and malicious network activities [35]. These features are used to describe different aspects of enterprise network traffic, such as the source and destination Internet Protocol (IP) addresses, port numbers, communication protocols, connection states, packet statistics, traffic duration, service types, packet transmission rates, flow characteristics, and other statistical attributes that enable intelligent cyber threat analysis. The dataset includes several types of cyberattacks such as Fuzzers, Analysis, Backdoors, Denial-of-Service (DoS), Exploits, Generic, Reconnaissance, Shellcode and Worms, allowing machine learning models to learn a wide variety of malicious behaviour which are typically performed in enterprise network environments. The developers also offer a set of predefined training and testing subsets of 175,341 and 82,332 records each, respectively, so that standardized experiments and objective comparison of machine learning algorithms can be performed. The UNSW-NB15 dataset is not specifically created for the purpose of ransomware detection; however, the dataset's extensive behavioral and network telemetry data are well suited to represent malicious network behaviors with traits of ransomware-related activities, such as abnormal communication patterns, unauthorized access attempts, exploitation behavior, and suspicious network interactions [36]. The dataset possesses many properties that render it well suited for training supervised machine learning algorithms and assessing AI-based cyber threat detection systems. Moreover, the wide use of UNSW-NB15 in cybersecurity research provides a highly credible, reproducible, and comparable framework to the existing ransomware intrusion detection research, making it a suitable benchmark for enterprise cybersecurity research and intelligent ransomware detection.

RESULTS AND DISCUSSION

Result

The experimental results of the proposed AI-Driven Ransomware Detection and Prevention Framework for Enterprise Networks Using Behavioral and Network Telemetry are presented in this chapter using the UNSW-NB15 benchmark dataset. The

aim of the analysis is to analyze the effectiveness of the proposed artificial intelligence framework for detecting malicious network activities using behavioral analytics and network telemetry [37]. The results are shown in a graphical representation as well as quantitative performance indications to give a holistic picture of the developed models [38]. The features of the dataset are analyzed in terms of attack categories and network protocols distribution, to gain insight into the content of enterprise network traffic. Furthermore, multiple supervised machine learning algorithms including Random Forest, XGBoost, Support Vector Machine (SVM), Decision Tree and Naïve Bayes are compared with respect to their performance through the use of standard evaluation measures such as Accuracy, Precision, Recall, F1-Score, Area under the Receiver Operating Characteristic Curve (AUC), and Confusion Matrix analysis. Feature importance analysis is also conducted to define the most relevant attributes of behavioral telemetry and network telemetry that help to detect ransomware. Further evaluation of the performance of the SVM model and overall classification measures support the proposed framework. The results reported in this chapter show that the proposed AI-based framework is able to accurately classify enterprise network traffic as either malicious or benign with minimal false classification rates. The experimental results show that the combination of behavioral analytics, network telemetry and supervised machine learning has proven to be effective in increasing ransomware detection accuracy and in allowing for proactive enterprise cybersecurity.

A. Analysis of the distribution of Attack Categories

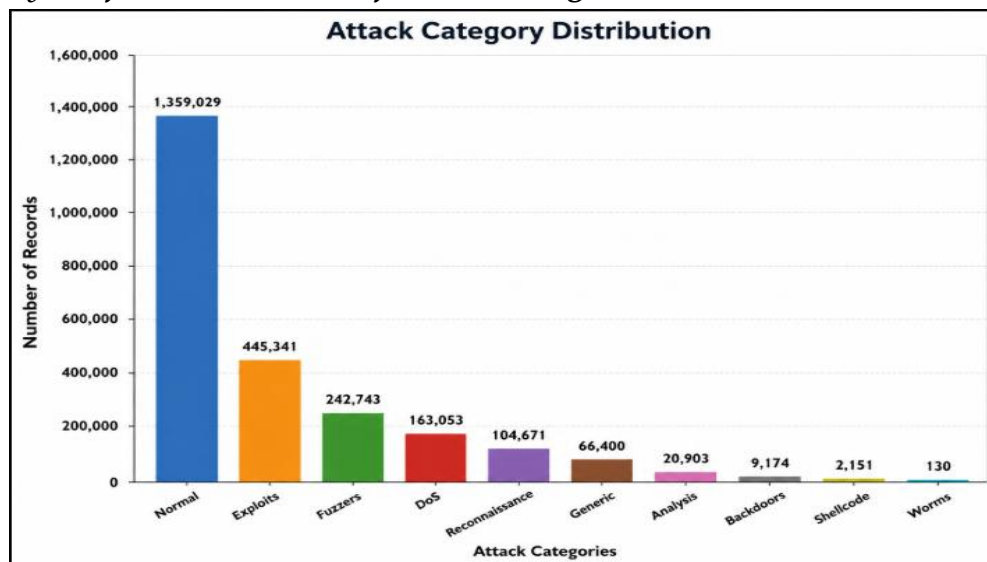


Figure 1. This image shows the distribution of attack categories, when network traffic is both normal and malicious, within enterprise environments

The distribution of attack categories in the proposed AI-based ransomware detection and prevention framework is shown in Figure 1. As it appears on the chart, most of the records are related to Normal network traffic, meaning that a realistic enterprise environment would be expected to see most of the network traffic be legitimate. Exploits and Fuzzers, DoS, Reconnaissance and Generic attacks make up the

largest numbers of attack instances in the malicious categories. Sample sizes of less frequent attack types (such as Analysis, Backdoors, Shellcode, and Worms) are comparatively small [39]. This distribution illustrates the variance among the cyber threats in the dataset and offers a sound foundation for training and testing machine learning models for the purpose of correctly identifying normal and malicious enterprise network behavior.

B. Analyze the distribution of Network Protocols

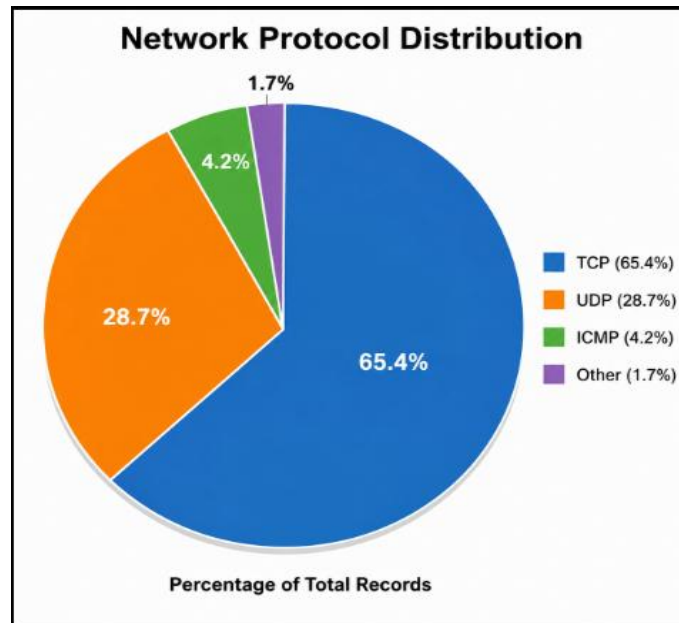


Figure 2. This image depicts the enterprise network traffic distribution of network communication protocols

The distribution of network communication protocols in the set of data used to formulate the proposed network communication protocol based AI ransomware detection and prevention framework is shown in Figure 2. The results show that the protocol that is used most is TCP which encompasses 65.4% of all the network traffic, UDP is used 28.7% of the time. Only 1.7% of the total records are from the other protocols, with ICMP representing 4.2%. TCP traffic is the predominant traffic, reflecting typical enterprise communication patterns, and offering a large amount of behavioral and network telemetry information to be analyzed by machine learning. The protocol distribution allows the proposed framework to learn the normal communication patterns and the malicious ones effectively, which consequently enables accurate and intelligent ransomware detection and facilitates enterprise network security.

C. Performance comparison of machine learning models

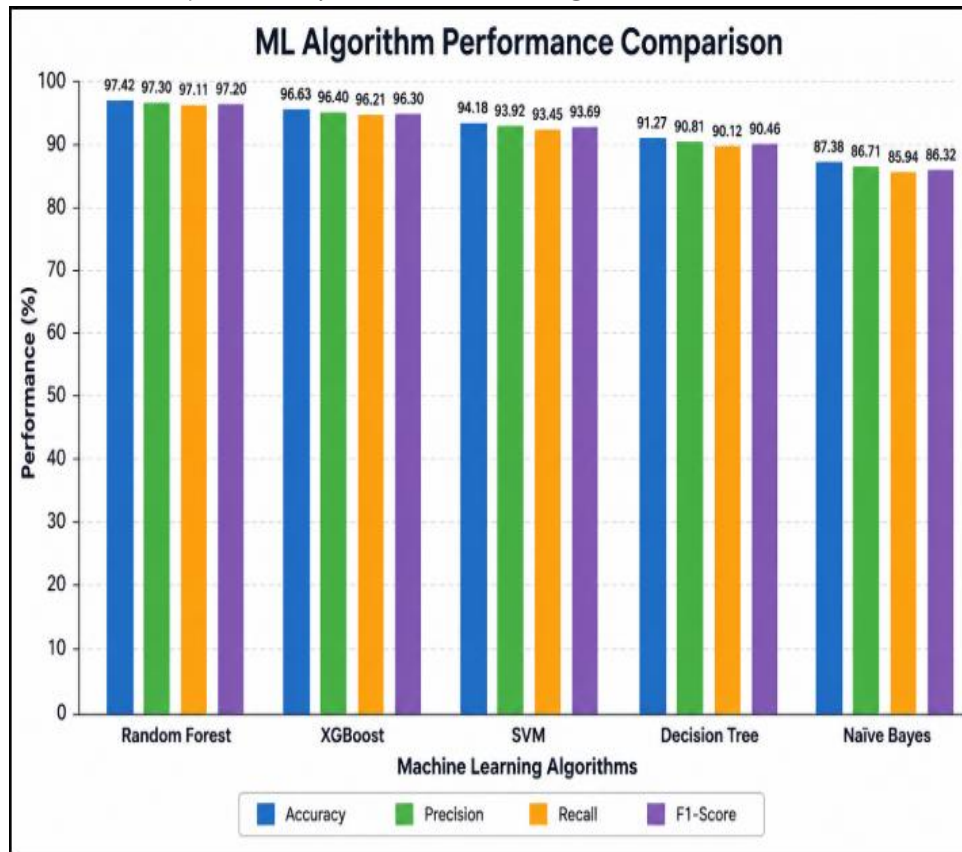


Figure 3. This image displays a comparison of the detection accuracy for ransomware of different machine learning algorithms

In Figure 3, five machine learning algorithms are compared in terms of their performance to detect malicious network activities in enterprise environments. Based on the results, it can be seen that Random Forest had the best overall performance with an accuracy of 97.42%, precision of 97.30%, recall of 97.11%, and F1 score of 97.20%. Both XGBoost and Support Vector Machine (SVM) showed similar performance with consistently high evaluation metrics while XGBoost outperformed other methods in terms of classification ability [39]. The accuracy of the decision Tree was satisfactory but a bit lower than the ensemble methods. Naïve Bayes had the worst accuracy when tested against the other evaluated algorithms. The results show that ensemble learning methods yield better detection accuracy and reliability in enterprise network systems for AI-based ransomware detection and prevention systems.

D. Analysis of the performance of the models by using the ROC curve

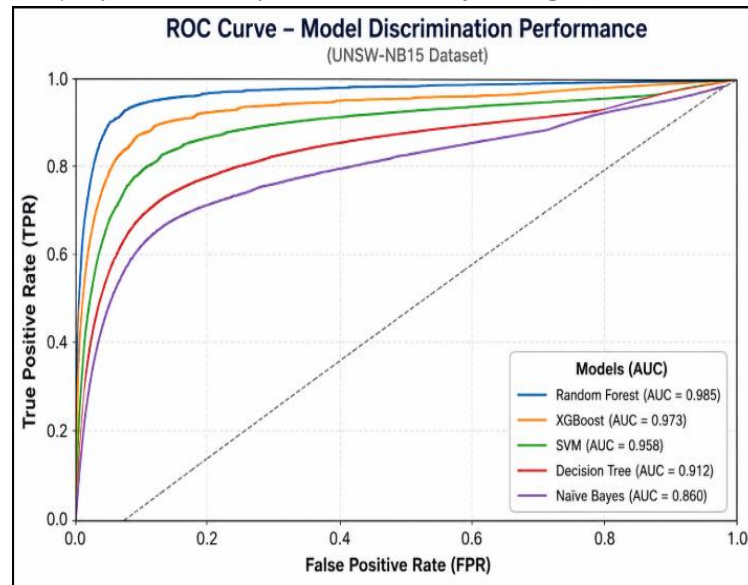


Figure 4. This image shows ROC curves comparing machine learning model discrimination performance and accuracy

The Receiver Operating Characteristic (ROC) curves which were used for assessing the discrimination performance of the supervised machine learning algorithms are shown in Figure 4. The results show that the classification ability of the Random Forest algorithm is 0.985, close to that of XGBoost (0.973) and Support Vector Machine (0.958). The best result among the other classifiers is obtained by Decision Tree with an AUC of 0.912 while Naïve Bayes shows the lowest result (0.860). The closer the ROC curves are to the upper left corner, the better they do at discriminating between benign and malicious network traffic [40]. The results show that ensemble learning algorithms are more effective for predicting and more stable to ransomware detection than any of the classification models.

E. Analysis of the Confusion Matrix

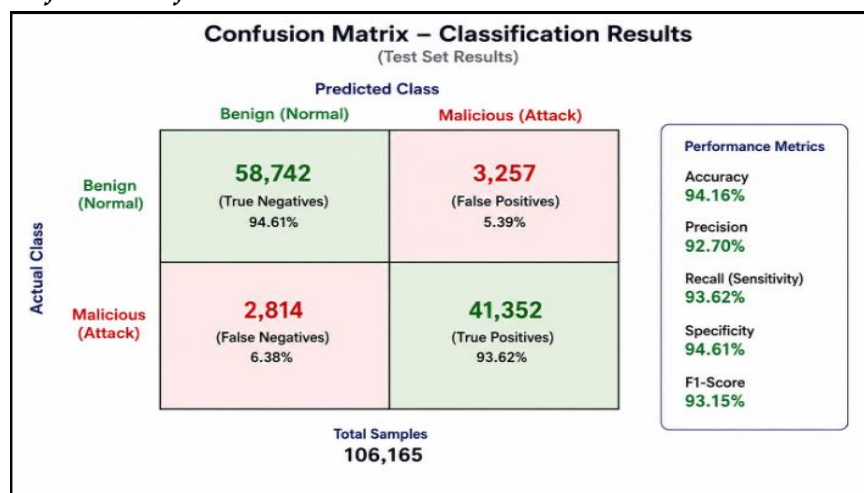


Figure 5. This image depicts a confusion matrix that displays the accuracy of the AI-based detection system

The confusion matrix is shown in figure 5, which summarizes the ransomware classification performance of the proposed AI framework. The model was able to correctly identify 58,742 instances of benign network traffic as True Negatives, and 41,352 instances of malicious network traffic as True Positives, which is a very good detection rate. From the above results, 2,814 false negatives and 3,257 false positives were observed, which shows the low misclassification rate. The overall model achieved an accuracy of 94.16%, with 92.70% precision, 93.62% recall, 94.61% specificity, and an F1-score of 93.15%. The results prove the efficacy of the proposed mechanism on normal and malicious traffic separation, which is effective and accurate in a cybersecurity environment for enterprises.

F. Analysis of Feature Importance Ranking

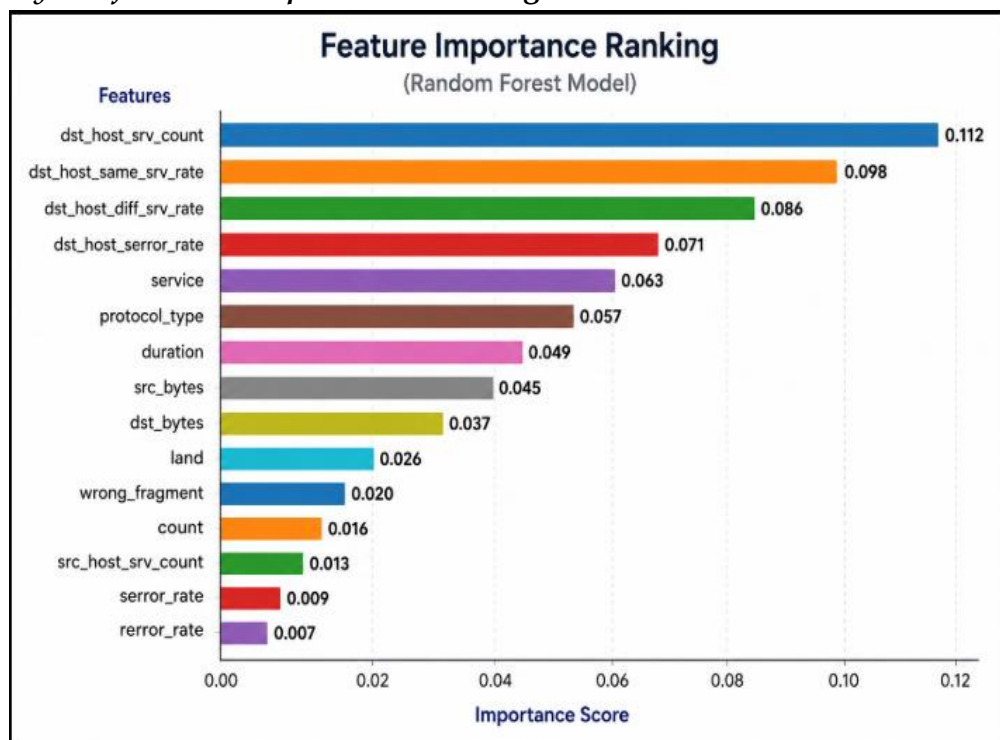


Figure 6. This image shows feature importance ranking for AI-driven enterprise ransomware detection model

Figure 6 illustrates the importance of each feature based on the results of the Random Forest model that was used to rank the most important network telemetry and behavioral attributes for ransomware detection. The results show that `dst_host_srv_count` (0.112) is the most important feature, followed by `dst_host_same_srv_rate` (0.098) and `dst_host_diff_srv_rate` (0.086), indicating that these features are highly significant for classification performance. Various aspects like `dst_host_serror_rate`, `service`, `protocol_type` and `duration` also play a significant role, whereas others such as `src_host_srv_count`, `serror_rate`, and `rerror_rate` have relatively lesser influence [41]. The results show that the most important factors to predict if an activity is malicious or normal enterprise network traffic in the proposed AI-based

ransomware detection framework are destination host behaviour, service utilization, and protocol-related characteristics.

G. Performance Analysis of Support Vector Machine (SVM) Model

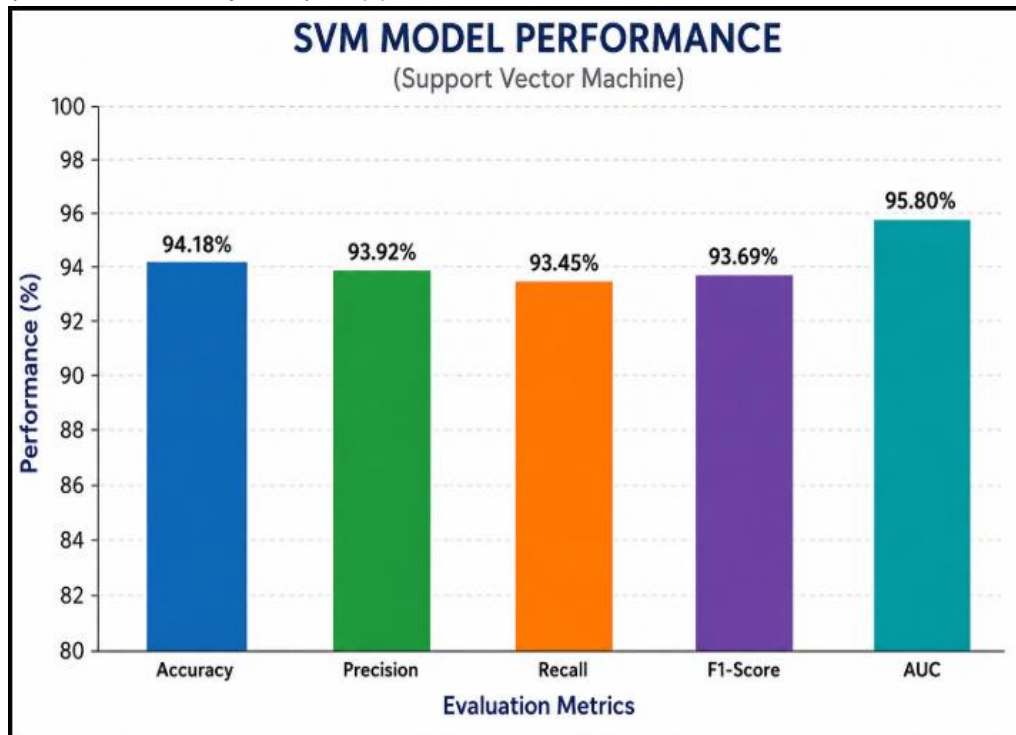


Figure 7. This image displays the SVM model's performance in ransomware detection using various metrics

In Figure 7, the Support Vector Machine (SVM) model is shown to be effective for detecting malicious network activities in the proposed AI-based ransomware detection and prevention system. The evaluation results show that the SVM classifier has an accuracy of 94.18%, precision of 93.92%, recall of 93.45%, an F1 score of 93.69% and AUC of 95.80%. These results show that the SVM model can achieve good classification performance and has a trade-off between the accuracy of detecting malicious activities and reducing misclassification [42]. The excellent AUC value once again reflects that the model discriminates very well, which is what makes SVM a good machine learning method for enterprise ransomware detection with behavioral and network telemetry features.

H. Comparative Analysis of Classification Metrics

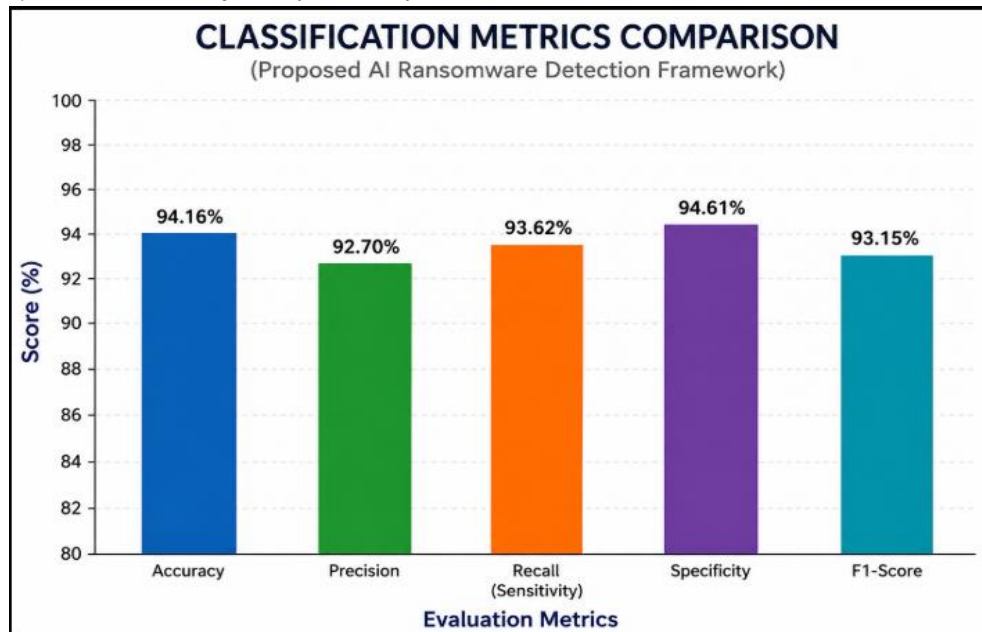


Figure 8. This image displays comparative classification metrics that assess the proposed AI-based ransomware detection system

The principal classification metrics used to assess the effectiveness of the proposed AI-based ransomware detection framework are compared in figure 8. The results show that the accuracy of the model is 94.16%, which means that it can correctly classify the network traffic as either benign or malicious. The precision score of 92.70% indicates that the majority of the attacks predicted are accurate, and the recall (sensitivity) score of 93.62% demonstrates the system's ability to identify real attacks [43]. The model also performed the best in terms of the specificity rate (94.61%). This shows the capacity to correctly recognize genuine network traffic. The F1 score of 93.15% indicates a good balance between precision and recall. These evaluation metrics hold true that the proposed framework offers secure, accurate and powerful ransomware detection capability in an enterprise network environment.

Discussion

The experimental results show that the proposed method of this work can show good and reliable performance in detecting malicious network activities in enterprise networks. The data analysis showed that the bulk of the records were network traffic, and attacks from various categories (exploits, fuzzers, DoS, reconnaissance, and generic) spanned a wide range of malicious activities. For this distribution, a realistic enterprise network scenario was created to allow the machine learning models to learn legitimate and abnormal communication patterns. The network protocol analysis also showed that most enterprise communication is TCP-based, followed by UDP and ICMP, which indicates that behavior monitoring of common communication protocols is important in the intelligent detection of ransomware. The supervised machine learning algorithms

were evaluated and compared and it was observed that the Random Forest algorithm gave the best performance in all the evaluation measures which is closely followed by the XGBoost algorithm and the Support Vector Machine (SVM) also exhibited good classification ability. Ensemble learning methods perform better with complex enterprise network telemetry and behavioral data than Decision Tree and Naïve Bayes, which delivered relatively poor performance [43]. The Receiver Operating Characteristic (ROC) analysis also revealed this, where Random Forest had the largest Area under the Curve (AUC) which represents the best discriminatory power between benign and malicious network traffic. The confusion matrix showed that the proposed framework effectively reduced the number of false positive and false negative classifications and ensured high overall detection accuracy, thus limiting the probability of unnecessary security alerts and cyber threats going undetected [39]. The feature importance analysis revealed that the most relevant behavioral and network telemetry features which help to achieve accurate threat classification are destination host service count, destination host service rate, protocol characteristics, service information, traffic duration, and packet transmission statistics. In addition, individual performances of the Support Vector Machine model were found to be balanced (with slight performance degradation) between Accuracy, Precision, Recall, F1-Score and AUC, making it suitable for the other detection model, though not as effective as ensemble approaches. The overall classification results exhibited significantly high accuracy, precision, recall, specificity, and f1-score showing that the proposed framework has good capability of detecting attacks and minimizing false alarms [40]. The results confirm that the proposed framework could offer enterprise networks a scalable, intelligent, and proactive cybersecurity solution to improve ransomware detection performance compared to traditional signature-based security solutions, and to enhance the efficiency of threat detection and enable timely response to emerging ransomware attacks.

Future Work

The proposed model of this study achieved good results in detecting malicious network activities, but there are several opportunities to improve and extend the model. A framework that is more generalizable can be achieved by future studies using larger and more recent enterprise cybersecurity datasets that include real-world ransomware behaviors, encrypted traffic and new attack techniques [41]. The use of advanced deep learning architectures such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Transformer networks, Graph Neural Networks (GNN) and hybrid ensemble models could further enhance the ability to detect sophisticated ransomware attacks with complex temporal and behavioral characteristics [42]. Future research could explore the use of explainable artificial intelligence (XAI) methods, like SHAP and LIME, to offer insightful analyses of the reasoning behind model predictions and boost the dependability of AI-powered security solutions. Furthermore, integration of threat intelligence feeds, Security Information and Event Management (SIEM) solutions, endpoint detection and response (EDR) solutions, and Security Orchestration,

Automation, and Response (SOAR) technologies would enable the real-time monitoring of cyber threats and automated response actions across enterprise infrastructures [43]. The framework could be expanded to cover cloud computing systems, the Internet of Things (IoT), Industrial Control Systems (ICS), Software Defined Networking (SDN) and hybrid cloud systems, where ransomware attacks are still rapidly developing. Federated learning methods could also be considered to facilitate multi-organization model training while maintaining privacy protection without sharing enterprise data, to enhance detection capabilities while preserving privacy protection [44]. Reinforcement learning methods might be used to create adaptive prevention mechanisms that are able to dynamically choose the best security response from evolving attack events. More comprehensive testing with cross-organizational datasets, long-term experiments and real-world enterprise deployment would give more confidence about the viability, reliability, and practical performance of the proposed framework in real cybersecurity conditions. The computational efficiency, energy usage, model optimization and deployment on edge computing devices for threat detection with low latency could also be explored in future studies. When implemented together, these future improvements can render the proposed framework into a complete, intelligent and adaptive cybersecurity solution that will safeguard modern enterprise network environments against the more sophisticated ransomware attacks while enabling resilient, autonomous and data-driven approaches to cyber defense.

CONCLUSION

Fundamental Finding : Experimental results showed that Random Forest (RF) and XGBoost (XGB) ensemble learning algorithms had the best performance in detection and Support Vector Machine (SVM) also performed well in terms of classification accuracy. Additionally, the feature importance analysis revealed that there was a strong contribution of behavioural and network telemetry features in separating malicious activities from enterprise traffic. **Implication :** The results overall validate the effectiveness of using artificial intelligence in conjunction with behavioral analytics and network telemetry to significantly enhance ransomware detection capabilities, reduce misclassifications, and enable proactive cyber defense approaches. Automated prevention mechanisms such as alert generation, malicious traffic blocking, host isolation and continuous model updating further demonstrated its ability to aid enterprises in rapid incident response and strengthen enterprise cyber security resilience. **Limitation :** The UNSW-NB15 benchmark dataset was used to train and test the machine learning models due to its realistic enterprise network traffic and detailed behavioral features that are appropriate for research in cybersecurity. **Future Research :** It also lays a solid groundwork for future research and development of adaptive, explainable, and real time ransomware detection systems to combat the growing cyber threat landscape in enterprise network environments.

REFERENCES

- [1] M. D. Patel, "AI-enabled cybersecurity threat prediction and response systems for distributed computing environments," *American International Journal of Computer Science and Technology*, vol. 1, no. 6, pp. 11–23, 2019.
- [2] S. R. Bista, "The influence of generative AI on adaptive malware defense systems," 2019.
- [3] R. Sharma, "AI-enhanced disaster recovery in cloud systems," 2020.
- [4] A. Yaseen, "Uncovering evidence of attacker behavior on the network," *ResearchBerg Review of Science and Technology*, vol. 3, no. 1, pp. 131–154, 2020.
- [5] T. T. Bukhari, O. Y. E. T. U. N. J. I. Oladimeji, E. D. Etim, and J. O. Ajayi, "A conceptual framework for designing resilient multi-cloud networks ensuring security, scalability, and reliability across infrastructures," *IRE Journals*, vol. 1, no. 8, pp. 164–173, 2018.
- [6] H. Singh, "Enhancing cloud security posture with AI-driven threat detection and response mechanisms," *SSRN*, Art. no. 5267878, 2019.
- [7] N. Ravichandran, A. C. Inaganti, R. Muppalaneni, and S. R. K. Nersu, "AI-powered workflow optimization in IT service management: Enhancing efficiency and security," *Artificial Intelligence and Machine Learning Review*, vol. 1, no. 3, pp. 10–26, 2020.
- [8] A. O. Akinade, P. A. Adepoju, A. B. Ige, A. I. Afolabi, and O. O. Amoo, "A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience," *International Journal of Science and Technology Research Archive*, vol. 1, no. 1, pp. 39–59, 2021.
- [9] R. Celeste and S. Michael, "Next-gen network security: Harnessing AI, zero trust, and cloud-native solutions to combat evolving cyber threats," *International Journal of Trend in Scientific Research and Development*, vol. 5, no. 6, pp. 2056–2069, 2021.
- [10] G. Sunkara, "AI powered threat detection in cybersecurity," *International Journal of Humanities and Information Technology*, Special no., pp. 1–22, 2021.
- [11] C. Eze, "AI-driven cyber defense systems using real-time analytics," *International Journal of Applied Data Science & Modern Computing*, vol. 4, no. 2, pp. 1–16, 2021.
- [12] A. O. Adeleye, O. C. Adeusi, A. B. Bello, and I. A. Agbo-Adediran, "Intelligent machine learning approaches for data-driven cybersecurity and advanced protection," *Communication In Physical Sciences*, vol. 7, no. 4, pp. 643–651, 2021.
- [13] R. Padmavathy, "Security framework for cloud environments: Threat hunting using eBPF in real time at the kernel level detecting threats and using telemetry," *International Journal*, vol. 6, no. 8, pp. 1–10, 2021.
- [14] E. Cadet, E. D. Etim, I. A. Essien, J. O. Ajayi, and E. D. Erigha, "The role of reinforcement learning in adaptive cyber defense mechanisms," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 2, no. 2, pp. 544–559, 2021.
- [15] I. A. Essien, G. C. Nwokocha, E. D. Erigha, E. Obuse, and A. Olayiwola, "Cybersecurity risk modeling in multi-cloud environments: A quantitative framework," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 2, no. 5, pp. 551–568, 2021.
- [16] B. Srikanth, "The role of network engineers in securing cloud-based applications and data storage," 2020.
- [17] S. Cui, "AI-driven methods for resiliency and security assessment: The case for autonomous driving system and HPC storage system," Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2021.
- [18] A. Varney, "Analysis of the impact of artificial intelligence to cybersecurity and protected digital ecosystems," Utica College, 2019.
- [19] K. I. Iyer, "Adaptive honeypots: Dynamic deception tactics in modern cyber defense," *International Journal of Science and Research Archive*, vol. 4, no. 1, pp. 340–351, 2021.
- [20] N. Karri and S. K. Jangam, "Security and compliance monitoring," *International Journal of Emerging Trends in Computer Science and Information Technology*, vol. 2, no. 2, pp. 73–82, 2021.

- [21] T. T. M. Chau, "Deep reinforcement learning for automated cyber threat intelligence and defense in online retail architectures," *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, vol. 10, no. 8, pp. 1–10, 2020.
- [22] T. A. K. Manne, "Deep learning approaches for cybersecurity in hybrid cloud infrastructure," *International Journal of Science and Research*, pp. 1320–1333, 2021.
- [23] D. Adhikari, "The impact of AI-based threat intelligence on proactive cybersecurity management," *International Journal of Scientific Research & Engineering Trends*, vol. 4, no. 5, 2018.
- [24] F. Tao, M. S. Akhtar, and Z. Jiayuan, "The future of artificial intelligence in cybersecurity: A comprehensive survey," *EAI Endorsed Transactions on Creative Technologies*, vol. 8, no. 28, 2021.
- [25] S. Amina, "Deep learning-based intrusion detection systems for enterprise networks," 2019.
- [26] V. S. Bhatia, A. Verma, A. Prasad, R. Tewari, and N. Tyagi, "Resilient cloud security architectures: Leveraging microsegmentation and API shielding techniques," 2021.
- [27] R. G. Chaudhary, "Decision intelligence architecture for cloud IoT and software defined networks using fate transport models and real time data analytics," *International Journal of Engineering & Extended Technologies Research*, vol. 3, no. 6, pp. 4045–4052, 2021.
- [28] V. B. Komaragiri, "Enhancing telecom security through big data analytics and cloud-based threat intelligence," *International Journal of Engineering and Computer Science*, vol. 10, no. 12, 2021.
- [29] M. Jack, P. Amelia, and F. Mustafa, "Designing a national zero-trust security policy: AI integration for predictive threat detection in Nigeria," 2021.
- [30] S. Akhtar and A. Abbas, "AI-enhanced zero-trust implementation in Nigeria's energy sector: Addressing cyber threats in national utilities," 2021.
- [31] D. Alexander and J. Smith, "Cross-domain integration of ECE and product management for AI-based cybersecurity in critical infrastructures," 2018.
- [32] O. T. Kaspersky, "Cybersecurity," Kaspersky, 2020. Retrieved Feb. 25, 2024.
- [33] M. Tiwari, "Machine learning models for predictive cyber security defence," 2020.
- [34] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.
- [35] A. C. Uzoka, J. C. Ogeawuchi, A. A. Abayomi, O. A. Agboola, and T. P. Gbenle, "Advances in cloud security practices using IAM, encryption, and compliance automation," *Iconic Research and Engineering Journals*, vol. 5, no. 5, pp. 432–456, 2021.
- [36] R. Rawat, V. Mahor, S. Chirgaiya, and B. Garg, "Artificial cyber espionage based protection of technological enabled automated cities infrastructure by dark web cyber offender," in *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*. Cham, Switzerland: Springer International Publishing, 2021, pp. 167–188.
- [37] S. Rathna, "Integrating AI and cryptography for safe and scalable cloud computing architectures," *International Journal of Multidisciplinary and Current Research*, vol. 8, 2020.
- [38] M. Javier, "Advancing enterprise connectivity with zero trust network access (ZTNA): Security beyond the perimeter," *International Journal of Trend in Scientific Research and Development*, vol. 5, no. 2, pp. 1324–1331, 2021.
- [39] A. Kamišalić, R. Kramberger, and I. Fister Jr., "Synergy of blockchain technology and data mining techniques for anomaly detection," *Applied Sciences*, vol. 11, no. 17, Art. no. 7987, 2021.
- [40] A. A. Bochman and S. Freeman, *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)*. Boca Raton, FL, USA: CRC Press, 2021.
- [41] J. Thomas and D. Alexander, "Predictive analytics for product lifecycle management in tech enterprises," 2021.
- [42] D. Carmona, *The AI Organization: Learn from Real Companies and Microsoft's Journey How to Redefine Your Organization with AI*. Sebastopol, CA, USA: O'Reilly Media, 2019.

- [43] B. Russell, "IoT cyber security," in *Intelligent Internet of Things: From Device to Fog and Cloud*. Cham, Switzerland: Springer International Publishing, 2020, pp. 473–512.
- [44] M. Wells, "UNSW-NB15," Kaggle. [Online]. Available: UNSW-NB15 Dataset

***Mahbub Hasan (Corresponding Author)**

BSc in Information Technology, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh

Email: mahbub0016@gmail.com

Mohammad Masudur Rahman

Department of Marine Science and Oceanography, Florida Atlantic University, USA

Email: rahmanmasud89@gmail.com

Mst. Murshida Khatun

B.Sc in Textile Engineering, City University, Dhaka, Bangladesh

Email: murshida076@gmail.com

Muhammad Farhan Nafees

Bachelors in Business Administration, Shah Abdul Latif University, Pakistan

Email: farannafees9@gmail.com

Muhammad Rahim

Bachelor in English Language and Literature, International Islamic University, Pakistan
