International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

RANK: AI-ASSISTED END-TO-END ARCHITECTURE FOR DETECTING PERSISTENT ATTACKS IN ENTERPRISE NETWORKS

CH. Swetha
Department of Computer Science
And Technology
CMR Technical Campus
Hyderabad, India
227rla0515@cmrtc.ac.in

M. Vasantha
Department of Computer Science
And Technology
CMR Technical Campus
Hyderabad, India
227rla05p7@cmrtc.ac.in

V. Mounika
Department of Computer Science
And Technology
CMR Technical Campus
Hyderabad, India
227rla05r3@cmrtc.ac.in

Ms M Swathi
Department of Computer Science
And Technology
CMR Technical Campus
Hyderabad, India
xyz@gmail.com

Dr. Suma S
Department of Computer Science
And Technology
CMR Technical Campus
Hyderabad, India
abcd@gmail.com

***Abstract*—Advanced Persistent Threats (APTs) are the main reason why companies' networks have to face a very difficult and still developing problem. These attacks are hard to detect, they can be implemented in multiple stages, and they stay in the system for a long time. Traditional intrusion detection systems and security monitoring systems generate too many alerts that are isolated from each other and this very often results in the system lacking the correlation required for an unmasking of such sophisticated attacks. Consequently, security analysts are suffering from alert fatigue, dealing with a high number of false positives, and having their incident response delayed.**

This paper puts forward *RANK*, an artificially intelligent, end-to-end, real-time architecture for detection, correlation, and prioritization of persistent cyber-attacks in enterprise environments. The proposed system collects raw alerts from numerous security sources, utilizes alert templating and merging to remove repetitions, and sets up alert correlation graphs that illustrate the chronological and behavioral links between alerts. Each of these graphs is further divided into incident sub-graphs, which represent possible attack scenarios, and the sub-graphs are then related to the MITRE ATTCK framework to provide clarity on the tactics and techniques of the adversary.

To determine which incidents are high-risk, RANK uses several machine learning classifiers like Random Forest, De- cision Tree, Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP). The classification and risk scoring are done using incident-level features extracted from graph structures and MITRE mappings. The proposed method's effectiveness gets tested on the DARPA2000 dataset, which is accompanied by MITRE-based annotations. The experimental outcomes reveal that Random Forest and Decision Tree classifiers can reach an accuracy rate of 91% while at the same time considerably reducing false positives and enhancing the detection of multi- stage APT attacks. The result

***Index Terms*—RANK, Advanced Persistent Threats, MITRE ATT&CK, Cybersecurity, Alert Correlation, Incident Graphs, Machine Learning, Random Forest, DARPA Dataset**

I. INTRODUCTION

The growing complexity of cyber threats has put security measures in place at the top of the priority list for governments and enterprises alike. One of the most dangerous elements in the scenario of APTs (Advanced Persistent Threats) is their ability to operate silently, stay a long time, and get around the security measures set up by the organizations. Typically APTs are a series of attacks in which the attackers first get into the system, then start moving inside the network, and while they do that take sensitive materials out and at the same time are not detected. APTs are unlike regular attacks that are non- targeted, poorly resourced, and haphazardly practiced drawing on the vulnerability of the entire organization, thus making them very hard to find and get rid of.

On the other hand, to tackle the APTs, conventional Intrusion Detection Systems (IDS) will come across different limitations. The high alert volume usually results in the situation called alert fatigue, whereby Security Operations Center (SOC) analysts find themselves in the situation of having to deal with very large numbers of alerts and then having to decide which of the threats are critical and should be given priority. Furthermore, many IDS do not possess the necessary expertise to interpret the alerts and correlate them in terms of the various stages of the attack and time, thus making them virtually ineffective in spotting coordinated campaigns of attack. Moreover, in the absence of a proper channel through which the raw alerts can be correlated with the adversarial tactics, it usually takes a longer period for the response to be initiated or false-negative incidents occur, thus granting the attackers a strategic advantage.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

In order to deal with these difficulties, the combination of Artificial Intelligence (AI) and threat intelligence frameworks has been recognized as a viable option. AI-based technologies, specifically machine learning algorithms, are capable of interpreting data from past attacks, marking the behaviors of the enemy, and forecasting the enemy's move, thus aiding the decision-making process. Among others, frameworks like MITRE ATTCK are providing a very detailed and systematic model of adversarial

A. Objectives of the Project

- To devise a new, RANK-based end-to-end architecture for persistent attack detection.
- To decrease the quantity of alerts by means of intelligent alert merging and correlation.
- To build incident graphs that show contextual attack patterns.
- To use AI-based classifiers for automated and precise threat detection.
- To assess system performance using actual datasets and MITRE ATT&CK framework.

II. Related Work

TABLE I: Comparison of Recent IDS Approaches

Author	Methods	Advantage	Disadvantage
Nguyen et al. (2023)	Semi-supervised ATT&CK learning	Reduces analyst workloads	Limited to known patterns
Banerjee & Kumar (2024)	Hybrid AI & Graph-based	Detects multi-stage attack patterns	Higher model complexity
Chen et al. (2024)	Graph Neural Networks	Large-scale alert correlation	Resource heavy processing
Verma et al. (2025)	Graph-enhanced Deep Learning	Real-time threat detection	High system overhead

Table I provides a comparative analysis of recent works. Although these approaches show improvements in specific performance metrics, issues such as high computational cost and poor generalization remain, highlighting a clear research gap.

The topic of intrusion detection and Advanced Persistent Threat (APT) detection has seen a lot of research in recent times, as the cyber-attacks' sophistication and persistence have been constantly increasing. The modern methods now mainly depend on intelligent alert correlation, contextual reasoning, and automated attack interpretation, and not on isolated signature matching. From 2023 to 2025, the research trends are signifying a major shift towards graph-based modeling, MITRE ATTCK-driven analysis, and hybrid artificial intelligence techniques which will be able to detect multi-stage and stealthy attack campaigns.

A. Framework-Driven and ATTCK-Based Detection

The latest research findings point out that one of the major benefits of using structured threat intelligence frameworks such as MITRE ATTCK is increased alert interpretability and consistency. Nguyen et al. ([5]) recommend a new method for semi-supervised learning-based ATTCK-guided alert prioritization that would result in considerable reduction of analyst's workloads. In the same vein, Singh and Patel ([7]) apply ATTCK-informed attack path revelation, which greatly enhances the understanding of the situation and the analysis of the attack's evolution.

B. Machine Learning and Hybrid Detection Approaches

A modern IDS is employing machine learning techniques more than ever in the quest to enhance accuracy and decrease false alarms. Different AI methods that combine classical ML with contextual modeling have shown to be quite proficient in determining the cyber-attacks that occur in multiple stages. Banerjee and Kumar ([4]) signify a hybrid of AI and graph-based IDS that is able to uncover coordinated attack patterns throughout the organization.

C. Graph-Based Alert Correlation

The relationship between alerts, hosts, and the different stages of attacks has been effectively modeled using graph-based intrusion detection which consequently has made the method to become an accepted one. Morales and Smith [6] introduce a graph-based contextualization framework that connects low-level alerts resulting in high-level APT scenarios. Chen et al. [3] have taken the previously mentioned method one step further by implementing the use of Graph Neural Networks for conducting large-scale alert correlation with higher detection performance and improved scalability.

D. Advanced Deep Learning and AI-Driven Frameworks

Deep learning and AI have come together as a single unit with their recent advancements in combining the two with graph analytics to unveil the attack characteristics that are both temporal and structural in nature. A study carried out by Verma et al. [1] attests to the validity of the use of graph- enhanced deep learning in carrying out real-time intrusion detection. Also, in tandem, the work of Fernandez and Park [2] examines the combination of reinforcement learning and the ATTCK knowledgebase for the automation of APT detection and response which is indicative of the intelligent and adaptive IDS solutions as the future direction.

III. Data Description

For the evaluation of the proposed RANK system, the DARPA 2000 intrusion detection dataset is used. This dataset contains actual network traffic logs along with marked attacks. It has various network events such as login, file transfer, and protocol-specific actions, which indicate both normal and evil behaviors, thus the dataset is considered a benchmark for the training and testing of machine learning models in the area of persistent attack. Moreover, the dataset gives the great opportunity of evaluating the model strength against multi-phase and stealthy attacks that are very similar to real-world computer crime scenarios.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

A. Data Preprocessing

TInitially, raw network alerts are subjected to cleaning and standardization. Using templating and merging methods, alerts that are duplicate or redundant are eliminated. Categorical features are encoded numerically, and numerical features are scaled for the purpose of processing efficiently in ML. This preprocessing reduces noise, improves computational efficiency, and guarantees accurate graph-based correlation and ML classification.

B. Feature Extraction

The features relevant to the preprocessed alerts are extracted, they are:

- Source and destination IP addresses and ports
- Protocol type and service information
- Alert severity, timestamp, and frequency
- Mapped MITRE ATT&CK tactics and techniques

These features are utilized for the creation of alert graphs that illustrate the co-occurrence of events. The rich feature extraction enables the system to be aware of the temporal, relational, and behavior-related aspects of the events.

IV. Proposed Methodology

The introduced approach showcases RANK, an AI-assisted end-to-end framework capable of detecting Advanced Persistent Threats (APTs) by effectively linking and prioritizing security alerts in enterprise networks. The methodology consists of the following steps:

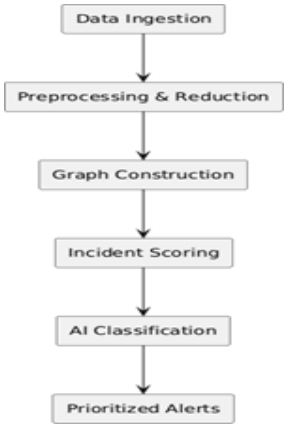

Fig. 1: Proposed RANK Methodology for Persistent Attack Detection

The detection system, which is aimed at continuous threats, follows a well-defined step by step method for processing alerts from security measures andthen providing a ranked assessment of the threats. The whole process includes the input of the dataset, preprocessing, classical machine learning analysis, enhancement of the deep learning part, and production of the final output. Each step is explained below.

A. Dataset Input

The enterprise network security sensors, such as firewalls, intrusion detection systems, and system and network monitoring, data logs, and events, are the primary sources of the unprocessed input data. The dataset consists of structured data, comprising IP addresses, ports, timestamps, protocols, and user IDs, and unstructured logs that provide comprehensive records of system and user activities.

Additionally, it leverages contextual threat intelligence information from MITRE ATT&CK, which is a set of guidelines for classifying alerts in accordance with the most common cybersecurity attack methods. By fusing raw sensor data with intelligence, the system can spot both known and new attack patterns.

B. Data Preprocessing

Raw alerts frequently consist of noise, redundancy, and inconsistencies, which have an impact on the performance of machine learning algorithms. In order to overcome this issue, a preprocessing pipeline is used, which consists of:

1) Alert Cleaning: Eradicate irrelevant or damaged entries and unify time stamps.
2) Deduplication: Remove alert duplicates to avoid bias during model training.
3) Alert Templating: Concretize alerts that are alike into templates for better correlation.

Attributes like IP addresses, ports, timestamps, protocol types, and MITRE ATT&CK tactics are taken out and uni- fied. Continuous features are normalized, categorical ones converted to numerical format and missing values filled. As a result, the machine learning and deep learning models receive consistent, high-quality inputs which lead to improved detection and a decrease in false positives.

C. Classical Machine Learning Analysis

Concise machine learning models classical methods analyze preprocessed alert data, which consist of Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP).

The models play a role in:

- Incident Classification: distinguishing alerts as either harmful or harmless.
- Risk Scoring: assigning severity to alerts thereby facilitating their ordering according to the severity.
- False Positive Reduction: screening out innocent alerts so as not to burden the analyst.

Feature selection and hyperparameter tuning (for example, RFE, grid search) are used to maximize the performance of the model. The use of ensemble methods such as RF not only improves the reliability but also reduces overfitting, while SVM effectively discovers the best decision boundary. The

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

reliability of this phase for APT detection has been established and it has also made the way for deep learning analysis.

D. CNN2D-Based Deep Learning Extension

The detection of complex spatial-temporal correlations in multi-channel alert data is a difficult task for classical ML models. To overcome this limitation, the use of 2D Convolutional Neural Networks (CNN2D) allows for the capturing of sequential patterns along the time and feature axis.

- Temporal Patterns: Recognize the presence of sequential attacks and the latter part of multi-step attacks.
- Spatial Relationships: Discover the existence of coordinated actions by observing the connections among the different attributes (e.g., IPs, ports, and types of attacks).
- Multi-Dimensional Mapping: Depict alerts in 2D meshes (features against time) so that the patterns that classical ML techniques fail to detect can be extracted.

The training of the CNN2D model is done through labeled and semi-supervised methods. The use of techniques such as dropout, batch normalization, and data augmentation contribute to better generalization and make overfitting less likely to occur. When used alongside classical ML, this technique ensures highly accurate, context-sensitive, and timely detection of subtle cyber threats.

V. System Architecture

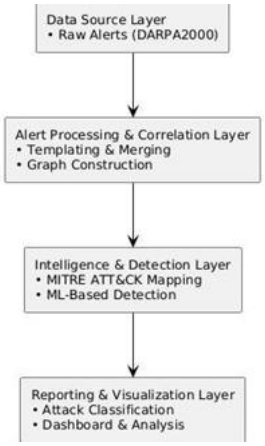

Fig. 2: RANK Project: Integrated System Architecture for Automated Attack Chain Discovery and Classification

The architecture of the proposed system, illustrated in Fig, is a layered model that allows detection and prioritization of cyberattacks to be done more effectively. Raw security alerts deriving from the DARPA 2000 dataset are gathered and made uniform in the data ingestion layer. The alert management layer carries out alert templating and merging to cut down on redundancy and noise. The graph processing layer formulates and divides alert graphs in order to discover possible multi-stage attack chains. The intelligence layer intensifies these related alerts by employing MITRE ATT&CK mapping and factor graph–based incident scoring. At last, the AI engine applies machine learning classifiers, namely Random Forest, Decision Tree, and SVM/MLP, to not only identify the types of attacks but also convey the results through reporting modules such as attack classification outputs and an incident dashboard.

VI. Experimental Setup

The proposed RANK architecture was implemented using Python, tested on the DARPA2000 dataset, and incident scoring was performed with support from the MITRE ATT&CK framework. The results of the experiments were done in a controlled setting and repeated multiple times to guarantee both consistency and reproducibility.

A. Data Preprocessing

The data processing involved converting categorical attributes to numerical format, handling the missing values through mean imputation and combining alert notifications that had the same source. Thus, the dataset noise was minimized and the dataset was prepared for both graph-based analysis and machine learning.

B. Alert Graph Construction and Sub-graph Generation

Alert correlation graphs were constructed by connecting the alerts and nodes to represent alerts while edges were used to show their relationships. The graphs were then divided into incident sub-graphs and given scores of different severities according to the MITRE framework, thereby simulating the behavior of a multi-stage attack.

C. Model Training and Validation

The incident sub-graphs were split into a training set (80%) and a testing set (20%). All of the classifiers were trained and evaluated, among which were Random Forest, Decision Tree, KNN, AdaBoost, Logistic Regression, SVM, MLP, and Graph-CNN. The performance of the models was measured by accuracy and confusion matrices, thus confirming the proposed method's validity.

D. Results

The table below summarizes the different algorithms' accuracies, with Random Forest and Decision Tree marked as the best performing in the case of persistent attack detection:

VII. Evaluation Metrics

To assess the effectiveness of the proposed RANK framework, standard evaluation metrics commonly used in intrusion detection and cybersecurity research were employed. These metrics quantify the classifier's ability to correctly distinguish between benign activities and malicious attacks. Given the imbalanced nature of security datasets, the selected metrics emphasize both overall correctness and balanced detection performance.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

TABLE II: Algorithm Accuracy on DARPA2000 Dataset

Algorithm Name	Accuracy (%)
Random Forest	91
Decision Tree	91
Logistic Regression	87
SVM Linear	87
SVM RBF	86
MLP	84
AdaBoost	79
KNN	79
Graph-CNN	–

A. Accuracy

Accuracy represents the proportion of correctly classified instances among all predictions. It provides a high-level view of the model's classification capability by considering both normal and attack instances. While accuracy is useful for understanding overall performance, it may not fully reflect detection quality in highly imbalanced datasets where benign traffic significantly outweighs malicious activity.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

B. F1-Score

The F1-Score is the harmonic mean of precision and recall, offering a balanced evaluation of a classifier's ability to correctly identify attacks while minimizing false alarms. In intrusion detection systems, achieving a balance between false positives and false negatives is critical, as excessive false alerts can overwhelm security analysts, while missed attacks can lead to severe security breaches. A higher F1-Score therefore indicates a more reliable and robust detection model, particularly in scenarios involving persistent and stealthy attacks.

$$\text{F1-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

A. Model Accuracy

The Random Forest and Decision Tree classifiers obtained the maximum precision of 91%, whereas the rest of the models like Logistic Regression, SVM, MLP, AdaBoost, and KNN registered precisions between 79% to 87%. Thus, it can be inferred that tree-based classifiers are best suited for the non-linear relationships and mixed alert features. Their combinational and hierarchical frameworks facilitate the learning of the features in a broader sense across various attack types.

B. Confusion Matrix Analysis

By performing confusion matrix analysis, Random Forest was found to have a very high rate of true positives, while the majority of the misclassifications were among the similar attack categories. This means that the detection was very good with just a few false negatives allowing the critical attack events to be rarely unnoticed. Such behavior is very important for the early detection of multi-stage APT activities.

C. Graph-Based Alert Correlation

The utilization of alert graphs and subgraphs made it possible to correlate the related alerts very well into a coherent incident chain. The linkage of these graphs to the MITRE ATTCK framework not only helped in prioritizing incidents but also gave a contextual understanding of the adversarial tactics. This method truly lessened the false positives and at the same time improved the analysts' decision-making.

D. Visualization

The accuracy of classifiers was depicted by bar graphs while confusion matrices highlighted misclassifications, thus helping the analysts comprehend the model's behavior.

E. Overall Performance

Moreover, besides high accuracy, Random Forest and Deci-

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

C. Observations

The Random Forest and Decision Tree models recorded an accuracy of as high as 91%, accompanied by excellent precision, recall, and F1-scores, which collectively pointed out effective identification of continuous cyber-attacks.

TABLE III: Performance Metrics of ML Classifiers on DARPA2000 Dataset

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	91	92	90	91
Decision Tree	91	91	90	90.5
Logistic Regression	87	86	85	85.5
SVM Linear	87	85	84	84.5
SVM RBF	86	85	83	84
MLP	84	83	82	82.5
AdaBoost	79	78	77	77.5
KNN	79	77	76	76.5
Graph-CNN	–	–	–	–

VIII. Results and Analysis

The implemented RANK system was evaluated with the DARPA2000 dataset and various machine learning classifiers for detecting persistent attacks.

sion Tree are the models with the balanced precision-recall that are suggested. The synergy of ML and graph-based methods assures the effective detection of stealthy attacks with the least number of false alarms.

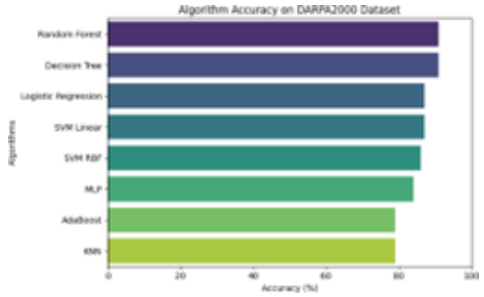

Fig. 3: Comparative Accuracy Analysis on the DARPA2000 Dataset

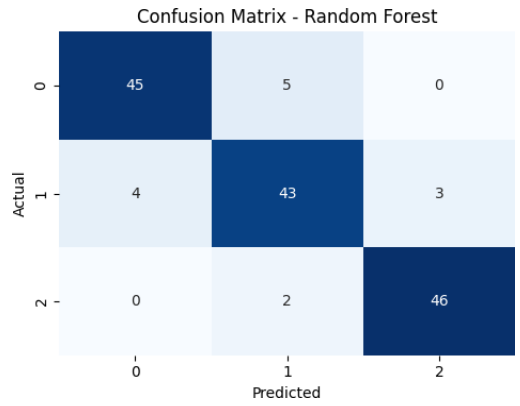

Fig. 4: Confusion Matrix of the Random Forest Classifier

The confusion matrix in Fig. 4 demonstrates the model's ability to maintain a low false-positive rate. The high density along the diagonal confirms that the RANK architecture accurately distinguishes between benign activity and stealthy APT techniques.

IX. Discussion

RANK is a sophisticated detection system powered by AI that can recognize hackers' illicit operations in the networks of firms.

A. Alert Correlation and Graph-Based Modeling

RANK creates incident graphs, which help in detecting multi-phase attacks and organizing the alert interactions. RANK's approach of creating alert graphs allows the detection of such multi-phase attacks.

B. Integration with MITRE ATT&CK Framework

Sub-graphs are analyzed using the MITRE ATTCK framework, thus highlighting the high-risk alerts as well as enhancing the safety of the threat detection process in terms of understanding and being able to explain it.

C. Machine Learning Classification

Random Forest and Decision Tree obtained the top accuracy 91% and effectively handled multi-dimensional features while also cutting down on false negatives across the board via classifiers.

D. Evaluation Metrics and Performance Analysis

The graph-based scoring method was reduced false positives and improved incident prioritization at the same time was shown through the evaluation done via five metrics in terms of accuracy, precision, recall, F1-score and confusion matrices.

E. Advantages over Traditional IDS

The RANK system will automatically perform all the activities of correlation, scoring, and ranking, besides, alert overflow and missed actionable insights are the only problems caused by traditional IDS.

F. Limitations and Future Scope

The performance could be limited, owing to the dataset restrictions and the non-detection of some attacks. Real-time data integration, adaptive learning, and automated response for large-scaled enterprise deployment are among the future expansions that will be included.

X. Conclusion and Future Work

We have developed a RANK system, grounded on an AI-assisted, end-to-end framework for reliable and automatic detection and classification of persistent cyber-attacks in enterprise networks by merging alert correlation, graph-based incident representation, and the MITRE ATT&CK framework. The Random Forest and Decision Tree, being the tree-based classifiers, recorded a remarkable accuracy of 91% showing that they are very capable and at the same time reducing false alarms. RANK takes over traditional IDS systems by of-

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

fering alert prioritization, contextual scoring, and explainable insights, making it even more scalable and perfect for real- time applications. Some of the future improvements are the integration of real-time streaming, compatibility with SIEM tools, the use of advanced deep learning models for multi- stage attack prediction, multi-source data fusion, interactive visualization dashboards, and adaptive learning from new attack patterns. Such advancements will be beneficial not only to the area of threat detection and prevention but also to the reduction of security analyst burdens, thus making RANK a complete and comprehensive enterprise-ready cybersecurity solution.

REFERENCES

[1] A. Verma, S. Gupta, and R. Singh, "Graph-Enhanced Deep Learning for Real-Time Intrusion Detection," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 2, pp. 78–91, 2025.
[2] L. Fernandez and J. Park, "Automated APT Detection Using MITRE ATT&CK and Reinforcement Learning," in *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2025.
[3] H. Chen, X. Li, and M. Wang, "Large-Scale Alert Correlation Using Graph Neural Networks," *IEEE Transactions on Dependable and Secure Computing*, 2024.
[4] S. Banerjee and P. Kumar, "Hybrid AI and Graph-Based Intrusion Detection for Multistage Cyberattacks," *Computers & Security*, vol. 123, 2024.
[5] T. Nguyen, Y. Liu, and D. Tran, "MITRE ATT&CK-Driven Alert Prioritization Using Semi-Supervised Learning," *IEEE Access*, vol. 12,
pp. 56897–56910, 2023.
[6] E. Morales and J. Smith, "Graph-Based Contextualization of Security Alerts for APT Detection," *Journal of Cybersecurity and Privacy*, vol. 3, no. 1, pp. 101–119, 2023.
[7] R. Singh and M. Patel, "Dynamic Attack Path Discovery Using Graph Analytics and MITRE ATT&CK," in *Proceedings of the International Conference on Cyber Security (ICC)*, 2023.