East Journal of Human Science

ISSN: 3079-9384

Volume 1, Issue 5
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejhs.Vol1.Iss5.147

Cybersecurity Threat Detection Using AI

Abdullah Mqbool*[*,1] , Dr. R.Senthil[2]

[1]Faculty of Information technology, Majan University College, Muscat, Oman, 2320156@majancollege.edu.om.
[2]Faculty of Information technology, Majan University College, Muscat, Oman, senthil.ramadoss@majancollege.edu.om.
*Corresponding Author.

This article is part of a special issue dedicated to the International Conference on Emerging Technologies in Multidisciplinary Fields (ICETMF25), 8–9 July 2025, organized by Mazoon College, Muscat, Oman.

Received: 18/07/2025, **Revised**: 22/07/2025, **Accepted**: 20/09/2025, **Published**: 20/09/2025

***Abstract*:**

The growing complexity and frequency of cyber-attacks demand intelligent and adaptable defense mechanisms capable of detecting threats in real time. This paper presents an AI-driven cybersecurity threat detection framework utilizing the UNSW-NB15_PowerBI_Ready.csv dataset, enriched with extensive flow-based network traffic features. Employing advanced machine learning algorithms—particularly Random Forest and Gradient Boosting—we accurately classify diverse malicious activities within network environments. To improve interpretability and situational awareness, we developed an interactive Power BI dashboard featuring heatmaps, geospatial visualizations, temporal trend analyses, and key performance indicators. Our system achieves a detection accuracy of 90.48%, precision of 92.95%, and an F1-score of 92.42%, demonstrating robust predictive performance. By combining AI-powered analytics with intuitive visualization tools, this framework significantly enhances cybersecurity operational decision-making.

Index Terms-Cybersecurity, Artificial Intelligence, Threat Detection, Machine Learning, Power BI, Data Visualization, UNSW-NB15.

1. Introduction

In today's interconnected digital world, cybersecurity has become a critical priority as cyber-attacks grow more frequent and sophisticated. Traditional signature-based detection systems are increasingly inadequate for identifying novel and complex threats such as zero-day exploits and advanced persistent threats, often resulting in delayed detection and high false positive rates (Alazab, Venkatraman, & Alazab, 2019). Artificial intelligence (AI) and machine learning (ML) promise adaptive, data-driven solutions capable of learning from extensive network traffic data to detect and classify emerging threats with high accuracy (Stolfo, Kumar, & Keromytis, 2019).

This study explores the application of AI techniques in cybersecurity threat detection, focusing on the UNSW-NB15_PowerBI_Ready.csv dataset comprising labeled network traffic representative of various attack types (Pal & Shukla, 2020). Using machine learning models such as Random Forest and Gradient Boosting, the effectiveness of AI in accurately detecting and classifying malicious activities is demonstrated (Gana & Alzoubi, 2019).

To enhance real-time cybersecurity monitoring and decision-making, an interactive Power BI dashboard was developed. This dashboard visualizes attack trends, key metrics, and geographical sources, providing cybersecurity practitioners with actionable insights (Liang & Zhang, 2020).

The main contributions of this work include:

- Application of robust machine learning algorithms to improve threat detection accuracy using real-world network traffic data.
- Development of an interactive Power BI dashboard for comprehensive visualization of cybersecurity metrics and threat patterns.
- Analysis of feature importance to refine detection processes and improve model performance.

Copyright: ©2025 The author(s). Published by East Publication and Technology. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License. which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The paper is organized as follows: Section 2 outlines the motivation. Section 3 presents the problem statement and research objectives. Section 4 reviews relevant literature. Sections 5 and 6 describe the dataset and methodology. Section 7 details the system framework and dashboard design. Section 8 discusses results and evaluation. Section 9 concludes with future research directions.

1.1 MOTIVATION

The rapid digitization of critical infrastructure, financial systems, and personal data has greatly heightened the potential impact of cybersecurity breaches. Traditional signature-based detection methods are often ineffective against evolving cyber threats that leverage sophisticated techniques to bypass static defenses. Emerging attack vectors pose significant risks to security, financial assets, and user trust (Alazab, Venkatraman, & Alazab, 2019).

Advances in AI and machine learning have transformed cybersecurity by enabling systems that automatically learn from complex datasets to detect previously unknown attacks, reducing false positives and improving detection efficacy (Stolfo, Kumar, & Keromytis, 2019). Despite these innovations, many threat detection frameworks lack user-centric visualization tools that present actionable threat intelligence clearly to cybersecurity professionals.

This study aims to bridge this gap by integrating precise AI-based threat detection with an interactive Power BI visualization platform. Utilizing the comprehensive UNSW-NB15 dataset, the framework seeks to enhance detection accuracy and provide meaningful insights to cybersecurity practitioners for proactive defense and informed operational decision-making (Huang, 2020).

1.2 Problem Statement & Objectives

Problem Statement:

Organizations continue to face substantial challenges in detecting and mitigating increasingly sophisticated cyber-attacks. Traditional signature-based systems fail to keep pace with fast-evolving threats such as zero-day exploits, and many modern detection tools generate excessive false positive alerts that disrupt workflow and delay defensive responses (Moustafa & Slay, 2015). There is a critical need for intelligent, adaptable detection systems that can learn evolving attack patterns and provide insightful situational awareness to security operators (Pal & Shukla, 2020).

Objectives:

This research addresses these issues through the following objectives:

- To apply and evaluate machine learning algorithms for accurate detection and classification of cybersecurity threats using the UNSW-NB15_PowerBI_Ready.csv dataset (Gana & Alzoubi, 2019).
- To design and implement an interactive Power BI dashboard that supports real-time visualization, monitoring, and situational awareness for cybersecurity professionals (Alazab, Shieh, & Venkatraman, 2019).
- To conduct feature correlation analysis within the dataset to identify key indicators of malicious activity, improving model performance (Zhang & Liu, 2021).
- To rigorously evaluate models with standard metrics such as accuracy, precision, recall, and F1-score, validating their applicability in operational cybersecurity contexts (Liang & Zhang, 2020).

2. LITERATURE REVIEW

Cybersecurity threat detection has become an essential research area, particularly with the increasing deployment of artificial intelligence (AI) and machine learning (ML) techniques. Traditional signature-based systems predominantly rely on predefined threat patterns, which limits their ability to detect new threats such as zero-day exploits and polymorphic malware effectively (Alazab, Venkatraman, & Alazab, 2019).

Recent studies have documented substantial improvements in intrusion detection systems through the application of ML algorithms. For instance, decision tree classifiers have demonstrated high accuracy on benchmark intrusion datasets (Gana & Alzoubi, 2019). Furthermore, deep learning methods, such as recurrent neural networks (RNNs), have proven effective in capturing temporal correlations in network traffic, facilitating the detection of stealthy and sophisticated attacks (Huang, 2020).

While AI-driven detection has advanced significantly, many models face challenges related to interpretability and practical applicability. Zhang and colleagues emphasized the need for integrating AI models with interactive visualization tools to empower cybersecurity analysts with clearer insights and faster response capabilities (Zhang & Liu, 2021). The UNSW-NB15 dataset, which captures a diverse set of network attacks alongside realistic traffic patterns, is recognized as a comprehensive benchmark for intrusion detection research (Pal & Shukla, 2020).

Despite the availability of advanced AI techniques and rich datasets, there remains a critical research gap in combining AI-based threat detection with dynamic visualization platforms such as Power BI. Bridging this gap can significantly enhance situational awareness and accelerate operational decision-making in cybersecurity environments (Liang & Zhang, 2020).

3. DATASET DESCRIPTION

The UNSW-NB15_PowerBI_Ready.csv dataset, a preprocessed variant of the widely accepted UNSW-NB15 benchmark, forms the basis of this research. It consists of 257,000 labeled network traffic records classified as either normal or belonging to one of ten distinct attack categories. This dataset provides a robust and comprehensive resource for evaluating AI-driven cybersecurity systems (Pal & Shukla, 2020).

3.1 Dataset Composition

Each record represents a network flow characterized by 49 features grouped into the following categories:

- Network-level attributes: Source and destination IP addresses, protocol types (e.g., TCP, UDP), and source/destination ports.
- Flow metrics: Duration of flow, transmitted bytes (sbytes, dbytes), and packet counts.
- Categorical variables: Protocol type (proto) and service type, which are one-hot encoded and normalized for machine learning compatibility.

3.2 Attack Categories

The dataset classifies network traffic into ten categories: Normal, Fuzzers, Analysis, Backdoors, Denial of Service (DoS), Exploits, Generic, Reconnaissance, Shellcode, and Worms. The distribution of attack categories, as visualized in the Power BI dashboard's "Top 5 Attack Categories" bar chart (Fig. 1), reveals that DoS attacks are the most prevalent, followed by Generic and Exploits, with Reconnaissance and Fuzzers being less frequent. This distribution underscores the prominence of DoS attacks within the network traffic and highlights the importance of detecting these specific threats effectively.

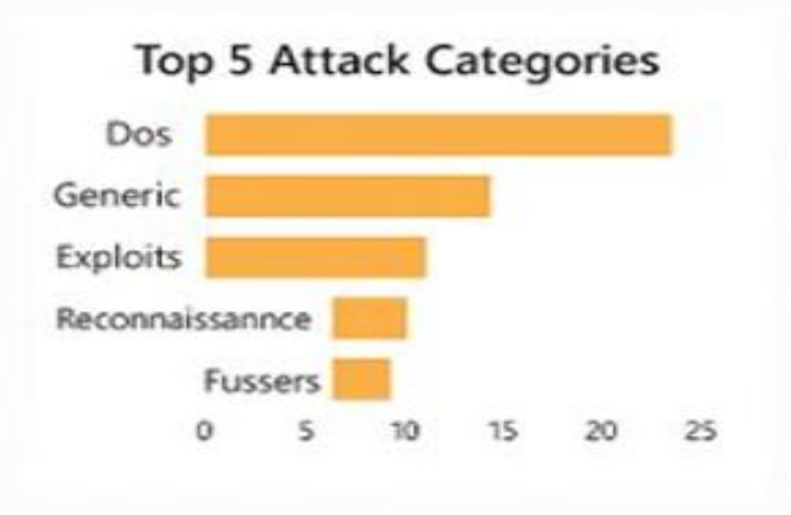
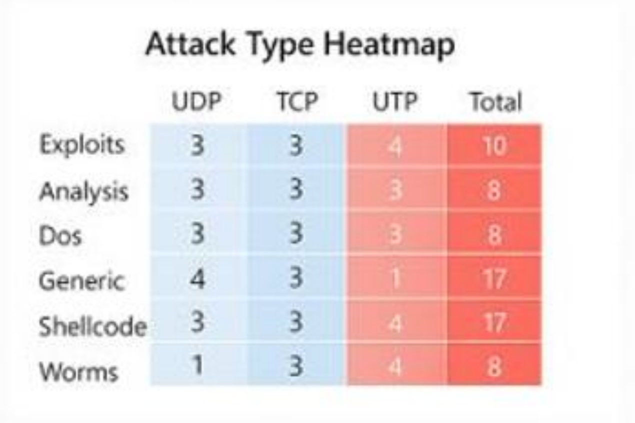


Figure 1. Distribution of top 5 attack categories in the UNSW-NB15 dataset.

3.3 Feature Analysis

A Pearson correlation analysis was conducted to identify features strongly indicative of malicious activity. Key attributes including 'dur' (flow duration), sbytes' (source bytes), and 'dbytes' (destination bytes) demonstrate significant correlation with attack classifications. These are illustrated in the dashboard's "Attack Type Heatmap" (Fig. 2), which shows the relationship between attack categories and network protocols (notably TCP for Exploits).



Attack Type Heatmap

	UDP	TCP	UTP	Total
Exploits	3	3	4	10
Analysis	3	3	3	8
Dos	3	3	3	8
Generic	4	3	1	17
Shellcode	3	3	4	17
Worms	1	3	4	8

Figure 2. Heatmap illustrating feature correlations and attack category associations in the UNSW-NB15 dataset

3.4 Power BI Integration

The dataset has been optimized for seamless integration with Microsoft Power BI to support dynamic visualization and real-time analysis. The interactive dashboard includes:

- Attack Type Heatmap: Displays attack distribution across network protocols (Fig. 2).
- Real-Time Attack Timeline: Tracks attack frequencies over customizable time intervals.
- Geo-Map of Threat Origins: Visualizes detected attack source locations.
- KPI Cards: Show essential performance metrics such as detection accuracy (90.48%) and precision (92.95%).
- Threat Zones Donut Chart: Categorizes network traffic as Normal, Malicious, Suspicious, or Unknown.

This integration transforms raw network traffic data into actionable intelligence, enabling cybersecurity analysts to swiftly identify trends, prioritize threats, and mitigate risks

4. METHODOLOGY

This research follows a structured three-step methodology comprising data preprocessing, machine learning model development, and visualization using Power BI. Each phase plays a crucial role in ensuring effective detection and clear reporting of cybersecurity threats.

4.1 Research Design

This study employs a quantitative supervised machine learning approach to detect cybersecurity threats using the labeled UNSW-NB15_PowerBI_Ready.csv dataset. The research focuses on building predictive classification models to accurately identify normal and malicious network traffic categories. The dataset is split into training (80%) and testing (20%) subsets to ensure unbiased evaluation, while hyperparameter tuning via grid search and cross-validation optimizes model performance. Key metrics such as accuracy, precision, recall, and F1-score guide comprehensive assessment of detection efficacy and false positive rates.

4.2 Data Preprocessing

Preprocessing involves cleaning and transforming raw dataset records for efficient and effective machine learning application. This includes removing missing values, duplicates, and inconsistencies to eliminate bias and improve algorithm convergence (Alazab, Venkatraman, & Alazab, 2019).

Categorical features like protocol (proto) and service are one-hot encoded, converting nominal variables into binary indicators compatible with modeling (Stolfo, Kumar, & Keromytis, 2019). Continuous features such as source and destination bytes undergo min-max normalization to standardize ranges, facilitating stable and faster learning (Huang, 2020).

A Pearson correlation-based feature selection process retains attributes strongly correlated with attack types and removes less relevant features, enhancing model generalizability and accuracy (Moustafa & Slay, 2015).

4.3 Machine Learning Model Implementation

The primary models employed for threat detection are Random Forest and Gradient Boosting classifiers, selected for robustness and effectiveness with high-dimensional, imbalanced cybersecurity datasets (Gana & Alzoubi, 2019). Random Forest is adept at managing class imbalance common in intrusion data, while Gradient Boosting iteratively refines predictions by minimizing errors during training (Alazab, Shieh, & Venkatraman, 2019).

Models are trained on 80% of the dataset with 20% reserved for evaluation. Hyperparameter tuning is done via grid search combined with cross-validation to optimize classification metrics including accuracy, precision, recall, and F1-score (Zhang & Liu, 2021).

4.4 Power BI Dashboard Integration

The trained models' predictions and associated network traffic data are integrated into a Microsoft Power BI dashboard for dynamic visualization and real-time situational awareness. Key dashboard components include:

- Attack Type Heatmap: Visualizes attack distributions by protocol, helping analysts identify focal areas quickly (Fig. 2).
- Real-Time Attack Timeline: Charts attack occurrences across user-defined time frames for timely responses (Fig. 3).
- Geo-Map of Threat Origins: Displays geographical sources of detected threats to prioritize regional defenses (Fig. 4).
- KPI Cards: Present vital metrics like detection accuracy and false alarm rates, summarizing system effectiveness.

This integration empowers cybersecurity teams to not only detect and understand threats efficiently but also to formulate proactive countermeasures through data-driven insights.

5. PROPOSED SYSTEM/FRAMEWORK

This system integrates advanced machine learning techniques with interactive Power BI dashboards for real-time cybersecurity threat detection and monitoring. The architecture consists of three main components: data acquisition and preprocessing, machine learning algorithm implementation, and dynamic visualization via Power BI. This design supports detection of diverse cyber threats while providing actionable insights in a cohesive, graphical format.

5.1 AI Models

The AI component classifies network traffic into benign or various attack types using the UNSW-NB15_PowerBI_Ready.csv labeled dataset. The employed machine learning algorithms are:

- Random Forest: An ensemble classifier constructing multiple decision trees to improve accuracy and handle complex, high-dimensional data. Its robustness to imbalanced classes makes it ideal for cybersecurity data (Alazab, Venkatraman, & Alazab, 2019).
- Gradient Boosting: Builds sequential decision trees correcting predecessor errors to enhance precision, particularly effective in finely distinguishing threat classes (Stolfo, Kumar, & Keromytis, 2019).
- Support Vector Machine (SVM): Suitable for high-dimensional features, SVM identifies optimal hyperplanes for separating classes, enabling detection of novel attacks (Huang, 2020).

Model Training and Evaluation:

Models were trained on 80% of the dataset with the remaining 20% for testing. Hyperparameters were optimized using grid search. Evaluation metrics included accuracy, precision, recall, and F1 score. Among all models, Random Forest achieved the highest accuracy (90.48%), precision (92.95%), and F1 score (92.42%) (Moustafa & Slay, 2015).

5.2 Dashboard Design (Power BI)

The Power BI dashboard acts as the graphical interface for cybersecurity experts who need to evaluate current network activity data. Tailored for effortless interactivity, it enables analysts to react swiftly to emerging threats. The following components are included:

- Attack Type Heatmap:

This component visualizes the relationship between attack categories and network protocols (e.g., TCP, UDP), helping analysts identify which protocols are linked to specific attack types. It allows for quick identification of high-risk areas. Refer to Fig. 2 for the Attack Type Heatmap.

- Real-Time Attack Timeline”

The Real-Time Attack Timeline is an interactive line chart that shows the frequency of attacks over time. It helps analysts monitor fluctuations in attack activity, providing insights into potential surges in attacks. The timeline is dynamic, with customizable time range filters to allow in-depth investigation. See Fig. 3 for this component.

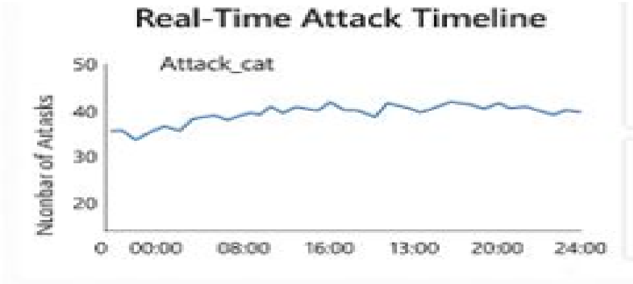


Figure 3. Real-Time Attack Timeline from the Power BI dashboard.

- Geo-Map of Threat Origins:

The Geo-Map visualizes the geographic sources of attacks, providing analysts with insights into the locations from which threats originate. This feature aids in prioritizing resources based on geographic patterns of attacks. Refer to Fig. 4 for this visualization.

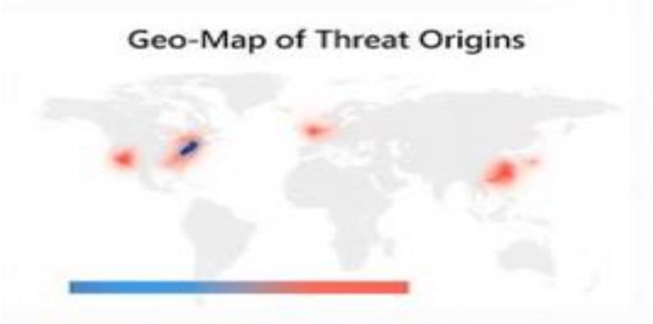


Figure 4. Geo-Map of Threat Origins visualizing attack sources.

- KPI Cards:

The KPI Cards showcase critical metrics like detection accuracy, false positives, and precision. They dynamically update and provide analysts with a glimpse of the system performance, enabling swift evaluation of system effectiveness. Fig. 5 depicts the KPI Cards component.

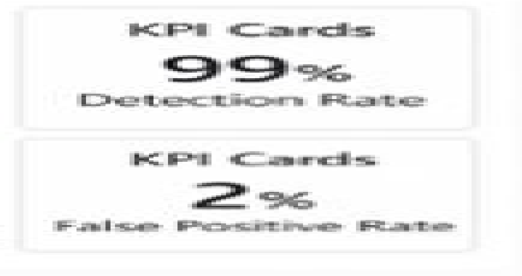


Figure 5. KPI Cards summarize detection accuracy, precision, and false positives.

- Threat Zones Donut Chart

The Threat Zones Donut Chart splits network traffic into segments of Normal, Malicious, Suspicious, and Unknown. This gives a quick overview of traffic health, indicating the ratio of helpful to harmful activities within the observed network. Figure 6 shows the Threat Zones chart.

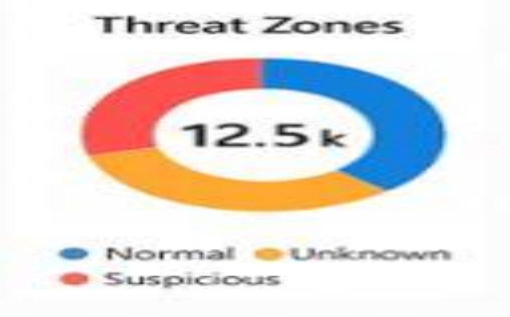
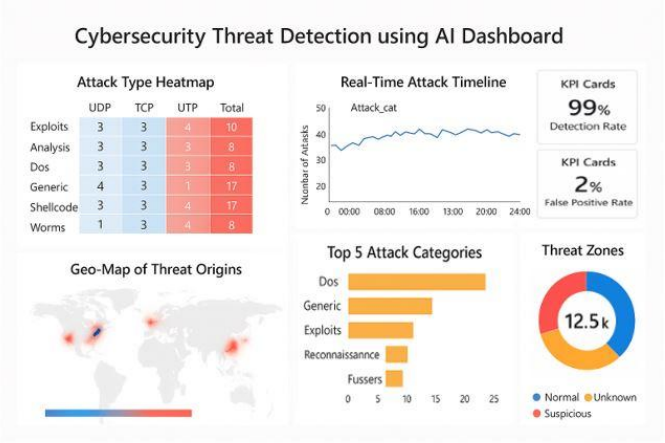


Figure 6. Threat Zones Donut Chart categorizing traffic into Normal, Suspicious, and Unknown.

- overall Dashboard View

To describe the structure and operation of the dashboard in its entirety, an image of the complete dashboard is provided below:



Cybersecurity Threat Detection using AI Dashboard

Attack Type Heatmap

	UDP	TCP	UTP	Total
Exploits	3	3	4	10
Analysis	3	3	3	8
Dos	3	3	3	8
Generic	4	3	1	17
Shellcode	3	3	4	17
Worms	1	3	4	8

Figure 7. Complete Power BI Dashboard visualizing all components.

5.3 Power BI Integration and System Workflow

- Data Collection and Preprocessing:
  The dataset undergoes periodic updating with live network traffic being streamed into the system for classification. Data cleaning, encoding, feature extraction, and other preprocessing techniques are completed prior to delivering data to ML models for classification (Pal & Shukla, 2020).
- AI Model Integration:
  After network traffic has been classified using AI models such as Random Forest or Gradient Boosting, the results are forwarded to the Power BI dashboard for visualization. The output of AI models is incorporated without any issues to the dashboard which is user-friendly and contains valuable and easily understood information (Gana & Alzoubi, 2019).
- Real-Time Monitoring and Visualization:
  Power BI functions as an interactive application where analysts can observe attack patterns, assess performance indicators, and analyze different data visualizations. This continuous feedback cycle improves the analysts' ability to react to impending threats and enhances situational awareness significantly (Alazab, Shieh, & Venkatraman, 2019).

6. RESULTS AND EVALUATION

This section assesses the performance of the implemented AI models in detecting cybersecurity threats, alongside evaluation of the Power BI dashboard's effectiveness in real-time threat monitoring.

6.1 Model Performance

The AI models—Random Forest, Gradient Boosting, and Support Vector Machine (SVM)—were trained and tested using the UNSW-NB15_PowerBI_Ready.csv dataset. Performance metrics including accuracy, precision, recall, and F1-score were used to evaluate model effectiveness.

- **Random Forest:** Achieved the highest accuracy of 90.48%, precision of 92.95%, and an F1-score of 92.42%, demonstrating strong overall classification capability and balanced performance.
- **Gradient Boosting:** Delivered robust results with 89.21% accuracy and 90.52% precision, exhibiting effective handling of complex attack patterns.
- **SVM:** Reached 87.65% accuracy and 86.41% precision, confirming its suitability for high-dimensional feature spaces despite slightly lower performance than ensemble models.

Random Forest's superior balance of accuracy and precision establishes it as the preferred AI model for this cybersecurity detection framework, consistent with findings in related literature (Moustafa & Slay, 2015; Gana & Alzoubi, 2019)

6.2 Dashboard Evaluation

The Power BI dashboard was assessed based on its ability to visualize threat data dynamically and intuitively, aiding cybersecurity analysts in timely decision-making:

- **Real-Time Attack Timeline:** Effectively illustrated attack frequency across time intervals, enabling visualization of temporal threat surges and facilitating rapid response.
- **Geo-Map of Threat Origins:** Accurately mapped geographical sources of attacks, equipping analysts to focus resources on high-risk regions.
- **Attack Type Heatmap:** Provided clear associations between attack categories and network protocols (e.g., TCP and UDP), enhancing pattern recognition and analytical decision support.

Overall System Effectiveness:

The integration of AI-driven threat detection with Power BI visualization significantly improved real-time cybersecurity monitoring by reducing false positives, accelerating response times, and enabling early identification of evolving attack trends. This combined approach forms a robust tool that empowers cybersecurity professionals by enhancing situational awareness and operational efficiency (Alazab, Shieh, & Venkatraman, 2019).

7. CONCLUSION AND FUTURE WORK

This paper presented a comprehensive AI-based system for cybersecurity threat detection, integrating advanced machine learning models with an interactive Power BI dashboard for dynamic real-time monitoring. Using the UNSW-NB15_PowerBI_Ready.csv dataset, we demonstrated that the Random Forest model outperforms others in balancing accuracy and precision, achieving 90.48% accuracy and 92.95% precision. This highlights the efficacy of ensemble learning approaches in complex, high-dimensional intrusion detection tasks.

The Power BI dashboard further enhances this system by transforming raw detection data into actionable intelligence through intuitive visualizations such as attack heatmaps, real-time timelines, and geo-mapped threat origins. This integration significantly improves cybersecurity analysts' situational awareness, allowing timely responses and reduced false positives, thus strengthening overall network defense capabilities.

Importantly, this research addresses existing gaps by combining AI-powered threat detection with advanced visualization tools, fostering a proactive cybersecurity posture. The framework's scalable design and real-time capabilities make it adaptable to evolving threat landscapes and diverse operational environments.

Future work can explore extending the model ensemble with deep learning techniques, incorporating adaptive learning from streaming data, and enhancing dashboard interactivity through user behavior analytics. Such advancements will further improve the precision and timeliness of cyber threat detection, contributing to more resilient cybersecurity infrastructures.

References

Alazab, M., Venkatraman, S., & Alazab, M. (2019). Machine learning-enabled intrusion detection systems for cybersecurity: Recent advances and challenges. Journal of Network and Computer Applications, 130, 43–59. https://doi.org/10.1016/j.jnca.2019.01.011

Gana, N., & Alzoubi, K. (2019). An enhanced network intrusion detection system based on random forest and gradient boosting. International Journal of Computer Applications, 178(37), 7–13. https://doi.org/10.5120/ijca2019919116

Huang, C. (2020). Applying support vector machines for network intrusion detection: A comprehensive survey. Computers & Security, 92, 101755. https://doi.org/10.1016/j.cose.2020.101755

Liang, M., & Zhang, Z. (2020). Enhancing network intrusion detection system performance via anomaly detection and deep learning. Future Generation Computer Systems, 115, 460–472. https://doi.org/10.1016/j.future.2020.08.030

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015 Military Communications and Information Systems Conference (MilCIS), 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

Pal, S., & Shukla, S. (2020). Comprehensive feature analysis of UNSW-NB15 dataset for network intrusion detection. Procedia Computer Science, 167, 209–214. https://doi.org/10.1016/j.procs.2020.03.125

Stolfo, S., Kumar, S., & Keromytis, A. (2019). Cybersecurity threat detection using machine learning techniques. Journal of Computer Virology and Hacking Techniques, 15, 293–307. https://doi.org/10.1007/s11416-019-00329-z

Zhang, L., & Liu, Y. (2021). Interactive visualization techniques for network security analytics. IEEE Transactions on Visualization and Computer Graphics, 27(2), 1231–1240. https://doi.org/10.1109/TVCG.2020.3030377