Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine Learning Models for Cybersecurity Risk Analysis in U.S. Critical Infrastructure Systems

Md Habibul Arif[1*], Habibor Rahman Rabby[2], Nusrat Yasmin Nadia[3], Md Zahid Hassan[4], and Rasel Hossain Babu[5]

[1]Department of Computer Science, University of the Potomac, 1401 H Street NW, Suite 100, Washington, DC 20005, USA

[2]Department of Computer Science, Campbellsville University, 2300 Greene Way #100, Louisville, KY 40220, USA

[3]Department of Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA 22314, USA

[4]Department of Information Management Systems, Bay Atlantic University, 1510 H St NW, Washington, DC 20005, USA

[5]Department of Cybersecurity, Bay Atlantic University, 1510 H St NW, Washington, DC 20005, USA

Corresponding Author: habibularif2233@gmail.com

ARTICLE INFO

Received: 08 Dec 2025

Revised: 16 Jan 2026

Accepted: 24 Jan 2026

ABSTRACT

The growing sophistication and frequency of cyber attacks on critical infrastructure in the United States make it increasingly important for robust cybersecurity tools to be put into place. In this paper, we study Artificial Intelligence (AI) for the protection of critical infrastructure, focusing on the use of machine learning (ML) models for attack detection. The analysis is based on a data set that contains network session attributes such as network packet size (mean: 500.43, standard deviation: 198.38), login (mean: 4.03, standard deviation: 1.96), session duration (mean: 792.75, standard deviation: 786.56), IP reputation score (mean: 0.33, standard deviation: 0.18), failed logins (mean: 1.52, standard deviation: 1.03), and odd time access (mean: 0.15, standard deviation: 0.36). Logistic Regression, Random Forest, Support Vector Machine (SVM), and XG Boost were the four machine learning models to use for the evaluation of the dataset. Model performance was measured through various evaluation metrics such as accuracy, precision, recall, F1 score, and Area Under the Curve (AUC). The final results demonstrated that XG Boost realized the best performance, with a maximum test accuracy of 88.52% and an AUC value of 0.88 compared to the other models. Random Forest obtained the second maximum test accuracy of 88.41% and an AUC of 0.88. Logistic Regression had the worst performance testing accuracy 73.11%, AUC 0.79. Furthermore, model calibration analysis using calibration curves showed that XG Boost overconfidently predictions for attacks, and the SVM and Logistic Regression were well-calibrated, albeit slightly underestimating attacks. From the feature distribution analysis, it was found that login attempts and session duration were the most important factors for the separation of attack and non-attack cases. This research shows that machine-learning-capable AI-driven cybersecurity solutions are very effective in protecting critical infrastructure, and insights are provided to help improve cybersecurity resilience using machine learning solutions. In the future, deploying more advanced technologies and tackling the regulatory barriers to adopting AI should be the focus of further research.

Keywords: AI-based cybersecurity, machine learning, critical infrastructure, reinforcement learning, privacy protection.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. Introduction

Critical infrastructure is a set of systems or assets whose disablement or damage would cause grave effects on national security, economy, and public health. The critical infrastructure in the United States cuts across various sectors, including energy, transport, the healthcare sector, water supply, and communications [1-4]. The more interconnected such systems are, as well as the more dependent on digital technologies, the more susceptible to cyber threats they are going to be, which is why their security will require the most effective measures [5]. Attacks on these infrastructures have caused immense disruptions in cyberattacks, and hence, the need to ensure the security of the infrastructure through cybersecurity. The importance of cybersecurity in enhancing national security is preventing cyberattacks and other data breaches and system collapse of important infrastructures affecting the nation [6]. As the use of digital technologies is gaining ground in crucial segments, conventional cybersecurity practices tend not to be as adequate to manage the sophistication or volume of contemporary threats. This has necessitated the cybersecurity function not only to act as a protective measure but also as a way of ensuring resilience, along with the continuously developing threats. The potential impact of AI on the field of cybersecurity has become one of the game-changing technologies that provide unprecedented opportunities to detect, respond to, and prevent cyber-related threats [7, 8]. Using machine learning (ML), deep learning (DL), natural language processing (NLP), and anomaly detection, AI-driven solutions read large quantities of data in real-time and determine trends that indicate unsafe developments [9, 10]. Applied to the domain of critical infrastructure, AI might help increase the probability of cyberattack detection, foresee the next attack according to past observations, and even react to the new wave of security threats automatically [11]. Scalability, adaptability, and efficiency characteristics of AI technologies also introduce a potential area in the protection of critical infrastructure against advanced and long-standing cyber risks. Fig. 1 shows small and medium-scale enterprise categories to mitigate cyber threats.**[5]**

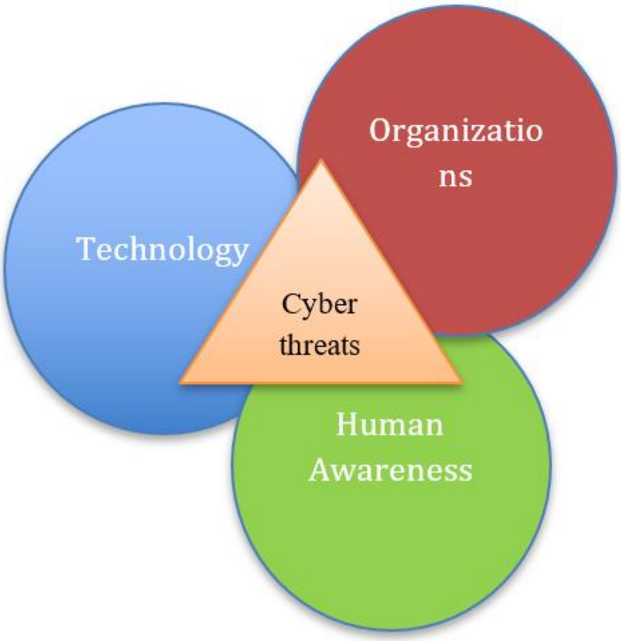


Fig. 1. Small and medium-scale enterprise categories to mitigate cyber threats.

1.1 Goal of the Paper

This paper aims to discuss AI-based cybersecurity solutions that can provide security to the critical assets in the US [12]. The paper will give a brief on the existing AI technologies, determine their ability to protect the critical sectors, and review the case studies in which AI has been successfully incorporated into cybersecurity systems. Moreover, the paper will discuss the problems and opportunities in the implementation of AI to provide protection to critical infrastructure and provide suggestions to the policymakers, security experts and industry stakeholders to enhance defence [13].

Although lots of progress was made in the field of AI-based cybersecurity tools, there is an insufficient amount of in-depth investigations that can specifically deal with the use of AI to protect its critical facilities of various fields within the United States. There has been a body of literature that has looked at single industries to study, with hardly anything done concerning how to leverage existing cybersecurity systems that won't have to be changed to fit specific infrastructures. Also, most research does not consider the scientific, legal, and logistical nuances that surround the decision to implement AI to protect infrastructure at scale [14, 15].

The proposed research can help address the identified gap in relevant literature by delivering a detailed discussion of the ways to use AI-based cybersecurity systems to mitigate threats to critical infrastructure in the United States [16-18]. It discusses the use of AI in various industries, such as energy, medical, and transportation, and evaluates the possibility to use such solutions in the current security system. The research paper also analyses the possible challenges and impediments to adoption of AI, including ethical impact, regulatory constraints, and operational viability and provides concise recommendation on how to deal with such challenges. Uniting theory and practice, the paper is going to present recommendations to implement to improve the resilience of the U.S. critical infrastructure with the help of AI-powered algorithms in cybersecurity [19-21].

2. Literature Review

2.1 Present-day Threats to Hyper-Critical Infrastructure

An alarming number of cybersecurity threats is on the rise in the critical infrastructure of the United States, which comprises energy, water, healthcare, transportation and telecommunications sectors [22-24]. These threats include old-school hacking to more advanced types of attacks, including advanced persistent threats (APTs), ransomware, and insider [25, 26]. Malicious cyberoperations may impair critical functions, which may result in economic losses, national security, as well as endanger community health [27, 28]. The complex and interconnected nature of the critical infrastructure has further complicated the challenges about identifying and mitigating these threats [29, 30]. Most of these infrastructures can therefore be said to have little security, even though there may be some form of security being applied to them; due to the dynamic nature and the complexities involved in the framework of these evil attacks, there is a necessity to have better and adaptive security systems [6, 31].

2.2 Cybersecurity AI technologies overview

Artificial Intelligence (AI) has been a game-changer as far as cybersecurity is concerned, since it is delivering dynamic solutions that are capable of keeping pace with the ever-shifting security environment [32]. The main AI technologies are: machine learning (ML) and deep learning (DL), natural language processing (NLP), and anomaly detection, which increase threat detection and decrease response times [33]. The possibility to examine large volumes of data in real-time enables AI to establish patterns, forecast possible vulnerability, and eliminate the risk before it is produced. Fig. 2 shows key technologies of Artificial Intelligence in Cybersecurity [34, 35].

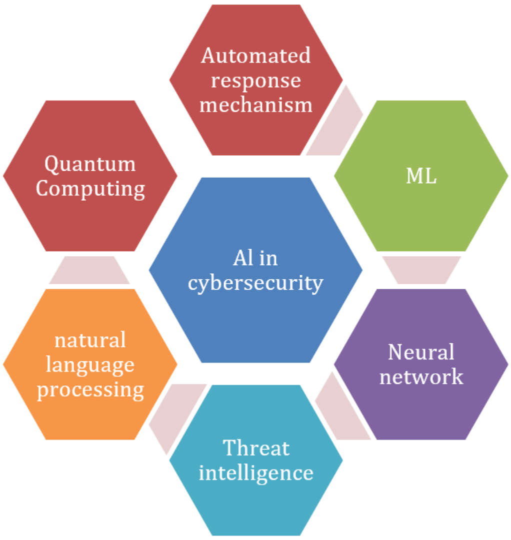


Fig. 2. Key technologies of Artificial Intelligence in Cybersecurity

2.3 AI to Detect and Prevent Threats

AI-based systems offer superior powers to insinuate online threats. The machine learning models, more so the supervised learning models, are fed with past attack data to train them to recognize patterns to predict probable future attacks [17, 36, 37]. With an AI system such as an intrusion detection system (IDS), network traffic is perpetually tracked and irregularities recognized and marked as possible threats, which will help in averting data discard and attacks [38-40].

2.4 AI-Driven Cybersecurity Solutions Case Studies

The fields of several industries have adopted AI-powered cybersecurity and achieved some good results [41, 42]. The energy industry has taken advantage of AI in real-time monitoring of power grids to detect abnormal activities, including cyber-attacks through the power grid cyber-attacks that may jeopardise the national power supply [43, 44]. The technology of AI in the medical market has led to a significant increase in security over sensitive patient information against malicious hackers. Moreover, it is possible to say that AI-based security features have gained successful implementation in transportation systems, especially in the security of autonomous vehicles and transportation networks [45]. As reflected in these case studies, AI has been shown to be very useful in safeguarding the critical infrastructure due to its capacity to decrease response time, enhance the accuracy of identification of the threats, and undertake proactive cybersecurity interventions [46, 47].

3. The necessity of Cybersecurity AI Software.

3.1 The Estrangement of Cyber Threats to Critical Infrastructure

Cyber threats have become more advanced and are now more targeted attacks on critical infrastructure rather than the basic opportunistic attacks they were before [21]. Now, it is revealed that hackers resort to even smarter methods, such as AI-enhanced malware and APTs that are harder to track and handle with conventional cybersecurity tools. The more the critical infrastructure is digitized and networked, the greater the attack surface becomes and thus a higher chance of security breaches [23, 48].

3.2 Challenges of the Conventional Cybersecurity Solutions

The classic methods of dealing with threats to cybersecurity, such as firewalls, signature-based detection, and antivirus software, are reactive and unable to handle contemporary threats [49]. Their drawbacks are associated with the fact that they are based on known attack signatures, which is why they cannot be applied to zero-day attacks and any significantly new, advanced threats [50-52]. They also fail to scale to the big data and complex systems in nowadays critical infrastructure [53]. The inadequacies of traditional cybersecurity tools and their inflexibility regarding changes in the nature and scope of attacks have necessitated the search for modern tools and services. Research has made its impact on the emergence of AI-based cybersecurity tools [8, 54].

3.3 The Benefits of AI to Work on These Limitations

There are multiple benefits of AI when compared to conventional cybersecurity systems. Machine learning algorithms will be able to analyze enormous amounts of incoming data in real-time, providing the detection of anomalies and the subsequent forecasting of threats [54, 55]. Whereas in conventional systems, the systems can only respond to predetermined patterns of threats, the AI systems can incorporate new information, which enables them to be flexible to changing threats [52, 56]. Furthermore, with AI, it will be possible to automate most of the threat detection and response cycle, thus lessening the need to rely on human involvement and increasing responsiveness. The AI-based cybersecurity systems are more efficient than the traditional ones, but also scalable and therefore more effective when it comes to protecting large critical infrastructures, which are widely interconnected [57-59].

4. Artificial Intelligence to be Used in Cybersecurity

4.1 Deep Learning and Machine Learning

The AI-driven cybersecurity is based on machine learning and deep learning [60]. The systems can be programmed (these technologies make it possible) to learn from large volumes of data, and they become better at revealing new threats that have never been encountered before. In machine learning, anomaly detection is possible through machine learning algorithms applied in cybersecurity: it finds patterns in network traffic that do not follow regular behavior [61, 62]. Machine learning is further subdivided into deep learning, which is capable of processing advanced data and providing predictions on a high level about the possible vulnerabilities and threats in real-time.

4.2 Threat Detection with Natural Language Processing

Natural language processing (NLP) enables artificial intelligence (AI) to read and understand human language, which may be of great benefit in cybersecurity [63]. As an example, we can state that NLP may help to detect phishing emails by noticing suspicious patterns in the text or using the threat intelligence reports to infer new threats. NLP also has applicability in the prevention of social engineering attacks, where it is used to identify manipulative language in a communication to exploit a vulnerable person [64, 65].

4.3 Behavioral Analysis and Anomaly Detection, and AI

With the help of behavioral analysis enabled by AI, the activity of users and systems can be monitored to identify abnormalities in their patterns [66]. This may be especially useful in detecting insider threats or zero-day exploits. With the help of AI, the systems are capable of scrutinising the user behaviour and interaction with the system indefinitely and raising red flags in the case of any abnormal activity being present as a possible threat. AI systems will be able to resolve the problem instantly and prevent worse complications by identifying the anomalies in real-time [67].

5. AI applications in securing the Critical Infrastructure

5.1 Protection of the Smart Grid

The type of protection needed is AI-driven cybersecurity that can aid in securing smart grids, which keep getting exposed to cyber threats because of their interconnectedness [52]. AI models would be able to monitor grid traffic and anticipate the vulnerabilities in the system that may disrupt it, and thus limit the disruption before it commences. Moreover, AI has the capability of automating the search and response to threats, thereby ensuring the robustness of the critical elements of the energy infrastructure [68].

5.2 Network Security AI in Critical Systems

AI technologies may be used to monitor the traffic on the network through healthcare and transportation essential systems, and find the weak points of the network to avoid any cyberattacks [28]. To illustrate, AI may examine the cycles of information passing through the system in real time, as well as identify anomalies such as unauthorized access or abnormalities in communication patterns, which may indicate an attack. The use of AI-integrated network security systems is more flexible, and they will help in safeguarding critical infrastructure against advanced and dynamic dangerous patterns [69].

5.3 Threat Intelligence and real-time response

AI can be used to improve threat intelligence systems, including gathering data across several sources, including threat feeds, system logs, and external databases [67]. This data can be used by AI to detect threats in the making, pre-warn cybersecurity teams of the possible vectors of attack, and offer real-time visualization of the same. Moreover, AI may be used to automate responses to quickly reduce threats with the minimum time between detecting a threat and responding [70].

5.4 Industrial Applications

With the cybersecurity threat rising, there are a number of industries that have already managed to implement AI into their cybersecurity system, such as the energy industry, the healthcare industry, or the telecommunications industry [71]. In the energy sector, artificial intelligence has been applied to defend power systems against cyberattacks [68]. AI helps healthcare organisations to protect patient data and secure the safety of medical devices. Telecommunications is an area where AI has already been used to detect network traffic to keep the information secure. These case studies show how efficient AI can work in safeguarding the critical infrastructure of various industries [72, 73]. Fig. 3 shows AI in cybersecurity research.

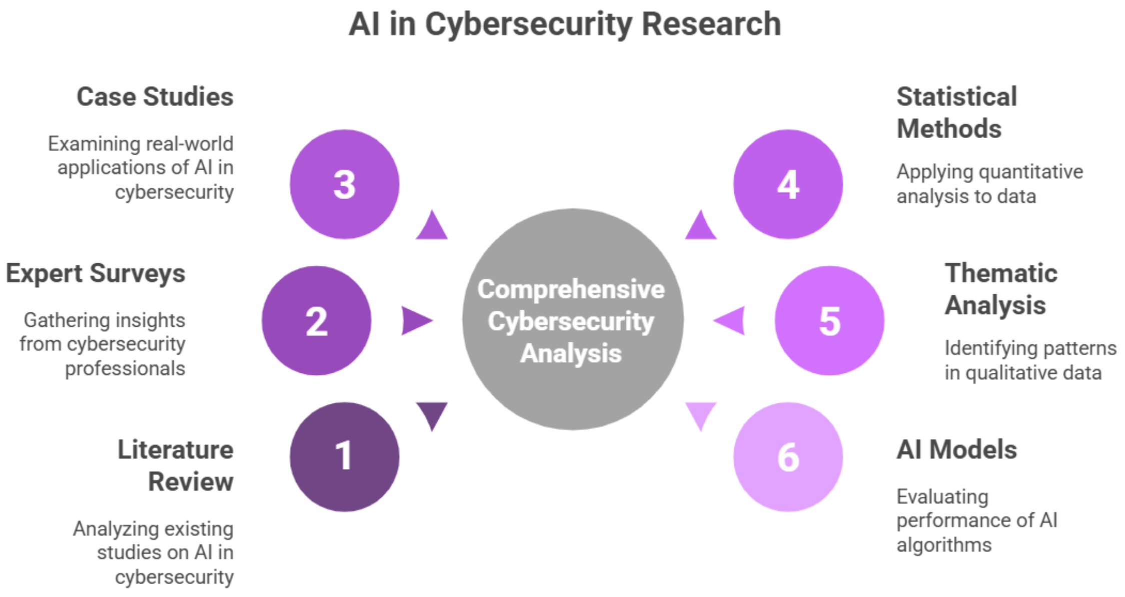

AI in Cybersecurity Research
Case Studies
Examining real-world applications of AI in cybersecurity
3
Statistical Methods
Applying quantitative analysis to data
4
Expert Surveys
Gathering insights from cybersecurity professionals
2
Comprehensive Cybersecurity Analysis
5
Thematic Analysis
Identifying patterns in qualitative data
Literature Review
Analyzing existing studies on AI in cybersecurity
1
6
AI Models
Evaluating performance of AI algorithms

Fig. 3. AI in cybersecurity research

6. Methodology

6.1 Design and Method of Research

The research is considered mixed-methods because it has both qualitative and quantitative elements of the mixed case study and data analysis, respectively. An in-depth analysis of current literature available on AI in the field of cybersecurity shall be made, and following this examination, the employment of AI in the areas of critical infrastructure shall be carried out.

6.2 Collection of data

Information will be gathered by means of surveys and interviews among cybersecurity experts and stakeholders. Further, secondary data regarding case studies, industry research, as well as academic studies will be analyzed to get a perspective with regard to the present scenario of AI-led cybersecurity solutions. Table 1 shows a Statistical report.

Table 1. Statistical report

Feature	Count	Mean	Std Dev	Min	25%	50%	75%	Max
network_packet_size	9537	500.43	198.38	64.00	365.00	499.00	635.00	1285.00
login_attempts	9537	4.03	1.96	1.00	3.00	4.00	5.00	13.00
session_duration	9537	792.75	786.56	0.50	231.95	556.28	1105.38	7190.39
ip_reputation_score	9537	0.33	0.18	0.00	0.19	0.31	0.45	0.92
failed_logins	9537	1.52	1.03	0.00	1.00	1.00	2.00	5.00
unusual_time_access	9537	0.15	0.36	0.00	0.00	0.00	0.00	1.00
attack_detected	9537	0.45	0.50	0.00	0.00	0.00	1.00	1.00

6.3 Methods of Data Analysis

Statistical methods will be used to analyze the quantitative data, whereas the qualitative data will be analyzed by conducting thematic analysis. Another evaluation criterion of the machine learning models will be their performance on real-life case studies to examine how accurate they are, what is their detection rate and their adaptability.

6.4 Models

SVM: SVM is a supervised learning method which is applied to classification. This is achieved by searching for the hyperplane that maximizes the margin between two classes. SVMs are strong in high-dimensional spaces and features, and are especially useful for finding non-linear patterns among data, like finding an intrusive attack on network traffic. It is also easy to generalize for the usage of regression [74, 75]. Fig. 4 shows the SVM model buildup.

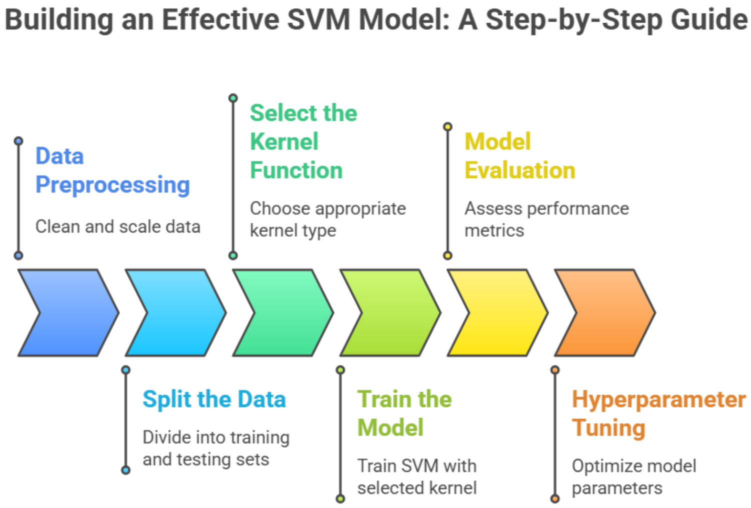

Building an Effective SVM Model: A Step-by-Step Guide
Data Preprocessing
Clean and scale data
Select the Kernel Function
Choose appropriate kernel type
Model Evaluation
Assess performance metrics
Split the Data
Divide into training and testing sets
Train the Model
Train SVM with selected kernel
Hyperparameter Tuning
Optimize model parameters

Fig. 4. SVM model build up.

XG Boost (Extreme Gradient Boosting): XG-Boost is a feature-rich, scalable and efficient machine learning algorithm that is a variant of Gradient Boosting [76]. It is famous for its high performance, scalability, and accuracy, particularly with large-scale datasets. XG-Boost trains an ensemble of decision trees sequentially, and each tree in the ensemble corrects the errors of previously trained trees. It's widely applied to classification problems and more, as well as regression problems, such as cybersecurity use cases for predicting threats [77]. Fig. 5 shows XG Boost ML steps.

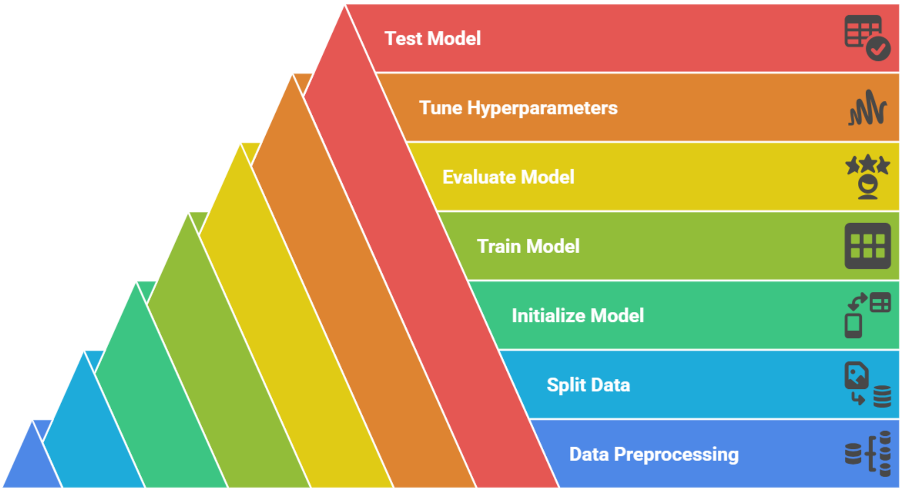


Fig. 5. XG Boost ML steps.

Logistic Regression: Logistic regression is a statistical machine learning algorithm in binary classification problems. It is used to predict the likelihood of a certain class (yes/no) given a set of input features. It is easy to understand and interpretable, but may not be able to catch intricate structures as well as other models, such as SVM or XG-Boost, when dealing with non-linear problems [78]. Fig. 6 shows Logistic Regression model development cycle.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

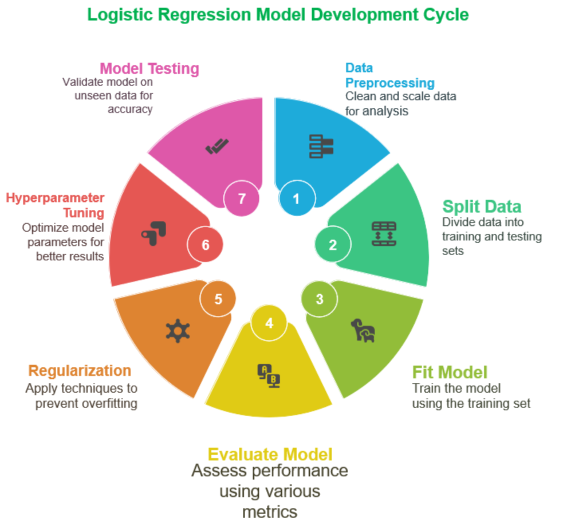

Logistic Regression Model Development Cycle
Model Testing
Validate model on unseen data for accuracy
Data Preprocessing
Clean and scale data for analysis
Hyperparameter Tuning
Optimize model parameters for better results
Split Data
Divide data into training and testing sets
Regularization
Apply techniques to prevent overfitting
Fit Model
Train the model using the training set
Evaluate Model
Assess performance using various metrics
1
2
3
4
5
6
7

Fig. 6. Logistic Regression model development cycle.

Random Forest: A Random Forest is an ensemble learning technique that constructs a forest of decision trees during the training phase and returns the mode of the classes for a classification type of problem [79, 80]. It is flexible, intrinsically mitigates overfitting by averaging tree outputs, and performs well on a variety of data types [75]. Fig. 7 shows the RF model development process.

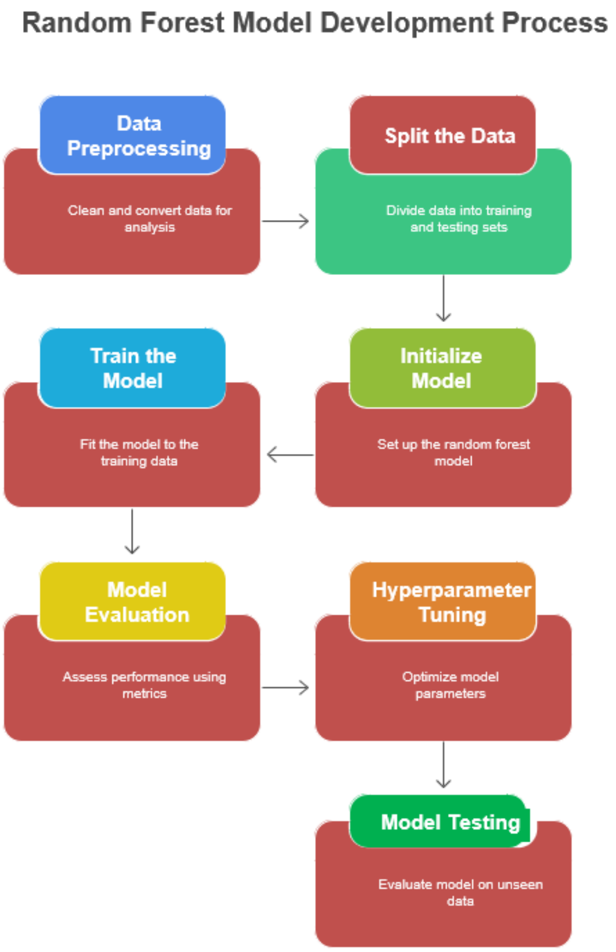

Random Forest Model Development Process
Data Preprocessing
Clean and convert data for analysis
Split the Data
Divide data into training and testing sets
Train the Model
Fit the model to the training data
Initialize Model
Set up the random forest model
Model Evaluation
Assess performance using metrics
Hyperparameter Tuning
Optimize model parameters
Model Testing
Evaluate model on unseen data

Fig. 7. RF model development process.

6.5 Measures of Evaluation of AI Models

The performance of the models will be evaluated based on important assessment metrics that provide details on the outcomes of using AI models in the identification and prevention of cyber threats. These include:

Accuracy: It is a metric that determines the percentage of correct (both true positives and negatives) predictions made by AI based on the total number of all predictions. Although accuracy is a relevant factor, it is not always enough since it can sometimes give only incomplete results, particularly when concerned with an imbalanced dataset (e.g., when there are very many benign activities and only a few actual threats) [81].

Precision: Precision is the ratio of true positive predictions (identification of threats correctly) to all of the times that the model labels something as positive (threats). A large value of precision means that in cases where the model predicts a cyber attack, the probability is high that it will be right, and reduce false positives.

Recall: Recall is also called sensitivity or true positive rate, and it is used to measure the percentage of real threats to which the model responds accurately. In the context of cybersecurity, a high score in the area of recall is also vital since it guarantees the effectiveness of the AI model in identifying as many threats as possible to reduce instances of false negatives.

F1 Score: F1 score is a harmonic mean of the precision and recall that gives an overall weighting between precision and recall. It also has the advantage of being very helpful when the data is not balanced, because it assists in reviewing the overall capability of the model to succeed in identifying both threats and benign functions [82].

Area under the curve (AUC): AUC is the area located under the Receiver Operating Characteristic (ROC) curve, which is plotted as true positive rate (sensitivity) versus false positive rate. The higher the value of AUC is the greater the chance that the model can differentiate between the positive and the negative cases. the value of AUC is very important in determining the general discrimination ability of the model [83-85]. Fig. 8 shows AL model evaluation metrics.

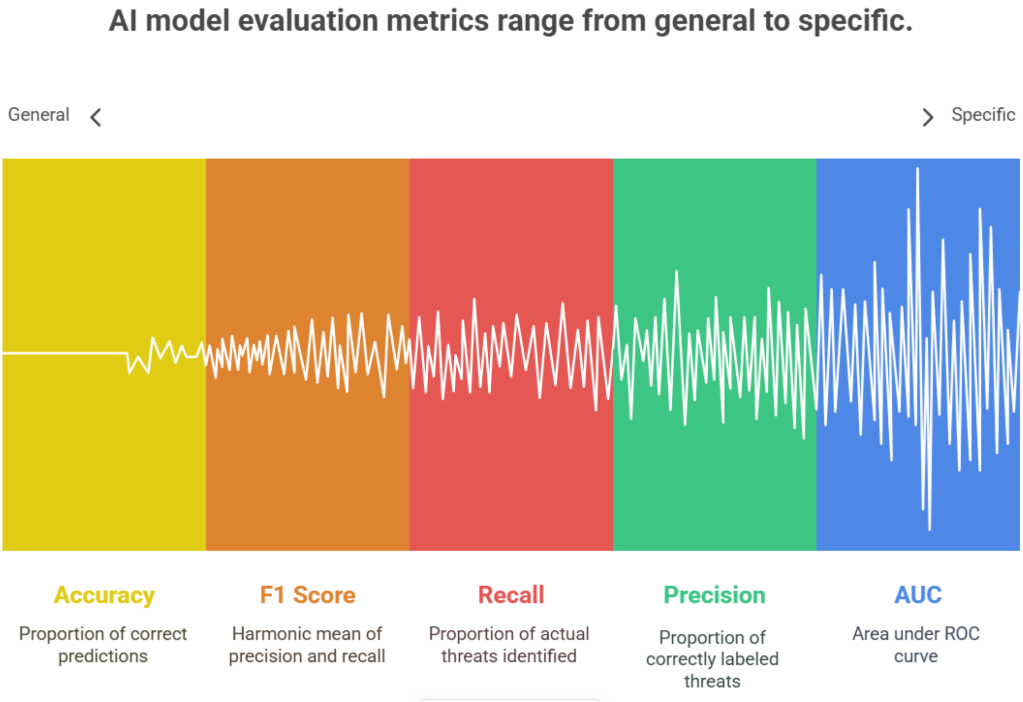

AI model evaluation metrics range from general to specific.
General
Specific
Accuracy
Proportion of correct predictions
F1 Score
Harmonic mean of precision and recall
Recall
Proportion of actual threats identified
Precision
Proportion of correctly labeled threats
AUC
Area under ROC curve

Fig. 8. AL model evaluation metrics.

7. Results and discussion

7.1 Distribution of Log-Transformed Numerical Features in Network Security Data

The Fig.9 shows the log-transformed distributions of the six major network measures. One of its common usages is for creating plots for different network features like network_packet_size, login_attempts, session_duration, ip_reputation_score, failed_logins, and unusual_time_access, among others. From the density plots for network_packet_size, we can see that it has a single peak located close to 0 which seems to support the claim that network_packet_size has many small packets in the network, whereas other features like login_attempts and failed_logins have multiple peaks indicating different sorts of login behavior in certain periods with occasional heavy spiking. Out of these features, I can see 'network_packet_size' to have the highest impact on the distribution as it seems more concentrated towards low values, indicating the traffic is dominated by small packets. It suggest that the dataset more often contains many but small transactions for cases and larger but rarer packages for controls, which may have some potential in the detection and resistance to cyber threats.

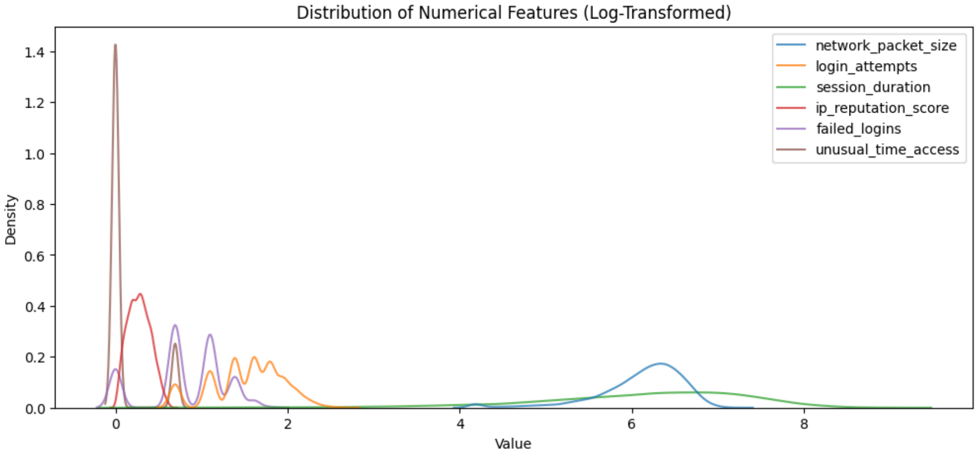
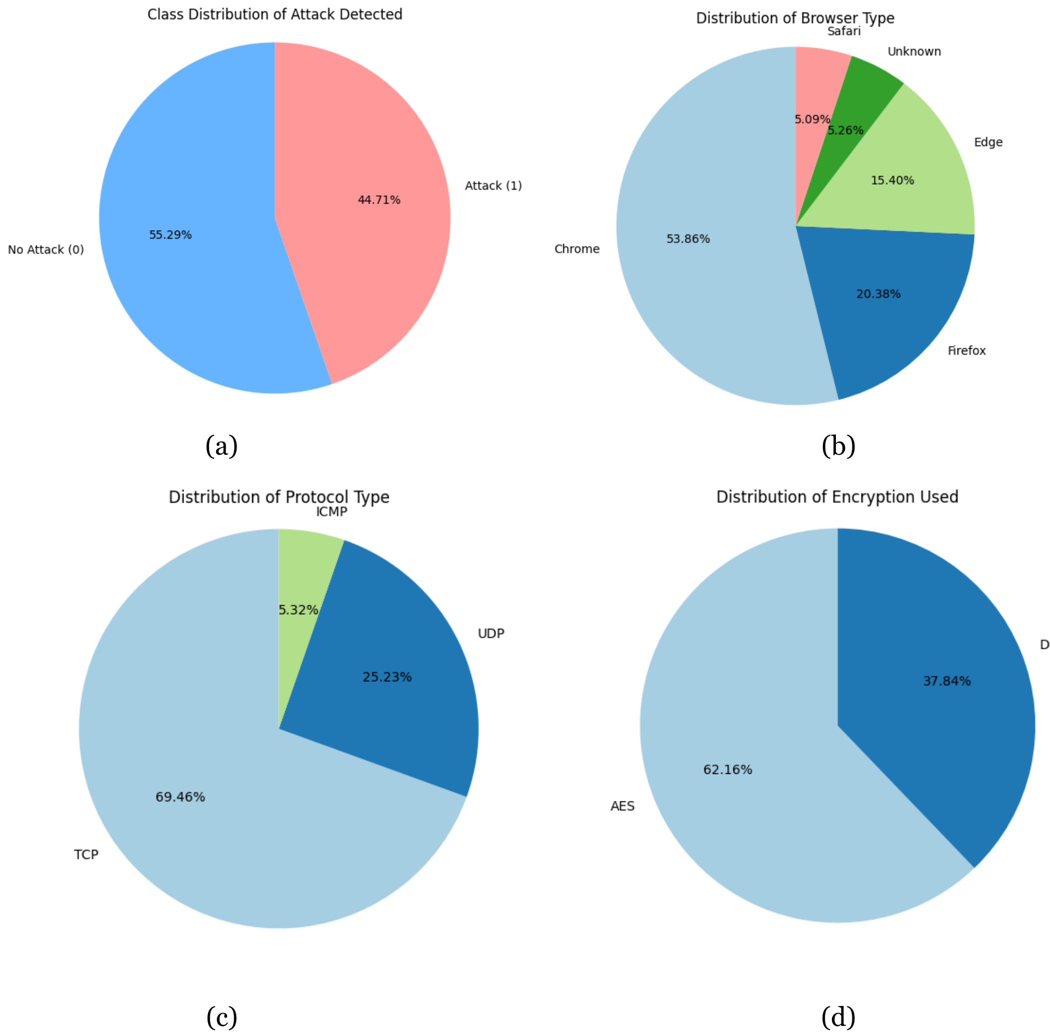


Fig. 9. Comparison of Log-Transformed Distributions for Key Network Metrics

7.2 Distribution of Attack Classes and Browser Usage in Network Traffic

Fig. 10(a) and Fig. 10(b) show different distribution analyses for network and browser data. Fig. 10(a) depicts the Class Distribution of Attack Detected, 55.29% of the data is "No Attack" (0), and 44.71% is "Attack" (1). This indicates slightly more than the no-attacks attack frequency. In Fig. 10(b), Browser Type. Not surprisingly, the Distribution of Browser types shown in Table 1 says that Chrome is the most popular browser, holding 53.86%, then Firefox holds 20.38%, Safari holds 5.09%, Edge holds 15.40%, and Unknown has 5.26%. These percentages demonstrate that Chrome has conquered the browser market, and some others have taken a bite for themselves. Additionally, Fig. 10(c) presents the Distribution of Protocol Type, which shows TCP with 69.46%, UDP with 25.23% and ICMP with 5.32%, meaning much preference towards TCP instead of other protocols. Lastly, Fig. 10(d) depicts the Distribution of Encryption Used, and it is observed that the AES encryption (62.16%) is much widely used than the DES encryption (37.84%). These numbers give valuable information about traffic on networks, how often attacks occur, and which browsers and encryption techniques are favored.



(a) (b)

(c) (d)

Fig. 10. Class and Protocol Distribution Analysis in Network Data

7.3 Model performance analysis

In this table 2 performances for 4 machine learning models (Logistic Regression, Random Forest, SVM, and XG Boost) are compared using several metrics. Random Forest has the best test accuracy (0.8841) and R² (0.6048), and then XG Boost with a test accuracy of 0.8852 and R² of 0.6198. Logistic Regression has the lowest test accuracy (0.73113) and the R² (0.26042), SVM has the test accuracy of 0.8710 and an R² of 0.5532.

Table 2. Model performance:

Model	Train Accuracy	Test Accuracy	Train MAE	Test MAE	Train MSE	Test MSE	Train RMSE	Test RMSE	Train R²	Test R²
Logistic Regression	0.74387	0.73113	0.34822	0.36085	0.17330	0.18282	0.41630	0.42757	0.29892	0.26042
Random	0.8964	0.8841	0.1995	0.2193	0.082	0.097	0.287	0.312	0.6661	0.604

Forest					5	6	2	5		8
SVM	0.8897	0.8710	0.1975	0.2152	0.095 1	0.1104	0.308 4	0.332 3	0.6152	0.5532
XG Boost	0.8948	0.8852	0.169 8	0.1853	0.081 1	0.095 5	0.284 9	0.309 1	0.6713	0.6198

7.3.1 Evaluating Model Performance: A Comparison of Train and Test Metrics Across Logistic Regression, Random Forest, SVM, and XG Boost

Fig. 11 evaluated machine learning in terms of 6 metrics. Logistic Regression has also somewhat higher errors, with a Train MSE of 0.173 and Test MSE of 0.183, and RMSE of 0.416 (Train) and 0.428 (Test), suggesting some inaccuracy in the predictions. Random Forest has a great fit with the train data (Train MSE = 0.098 and Test MSE = 0.200) but gains a bit of test error, which can also be seen in RMSE (0.287 for Train and 0.313 for Test). The right middle column indicates SVM is the middle performance-wise, it is decent, it performs uniformly, provides trade-off sample sizes relative middle performances with low errors, and the Train MSE and Test MSE are 0.095 and 0.110, respectively and RMSE for Train and Close 0.198 and 0.215, respectively. XG Boost is the best performing model with minimum Train MSE (0.081), Train RMSE (0.170), Test MSE (0.096) and Test RMSE (0.185), indicating the least errors and best predictive accuracy. From this experiment, it can be concluded that XG Boost is the best model and SVM is the second best one, whereas Logistic Regression has the worst errors.

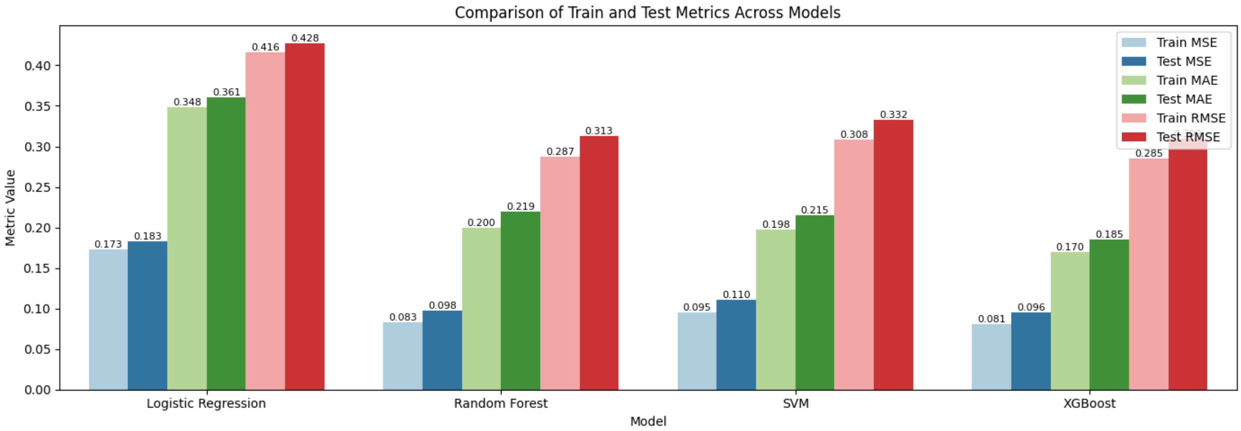


Fig. 11. Performance Comparison of Machine Learning Models: Train vs. Test Metrics for Attack Detection

7.3.2 Comparison of Train and Test Accuracy, and R² Metrics Across Machine Learning Models for Attack Prediction

Fig. 12 compares the performance of four machine models with Accuracy and R² metrics. Logistic Regression Train Accuracy: 0.744 Test Accuracy: 0.731Decent and very slight drop in test accuracy. The Train R² is 0.299 and Test R² is 0.260, which indicates that the fitting isn't bad. Random Forest - Train R²: 0.666 > Test R²: 0.605 > Train Accuracy: 0.896 > Test Accuracy: 0.884 (train: good fit & slightly overfitting) > For Random Forest, we found a good performance, including a high R², good fit and just a little overfitting. SVM is comparable to that with a Train Accuracy = 0.890, Test Accuracy = 0.871, Train R² = 0.615 and Test R² = 0.553, indicative of a good fit of the voting result. XG Boost model surpasses all models with Train Accuracy: 0.895, Test Accuracy: 0.871, Train R²: 0.672, Test R²: 0.613, demonstrating the best predictive and generalization capacity. In general, XG Boost is the best model, and Logistic Regression has the worst efficiency in accuracy and R².

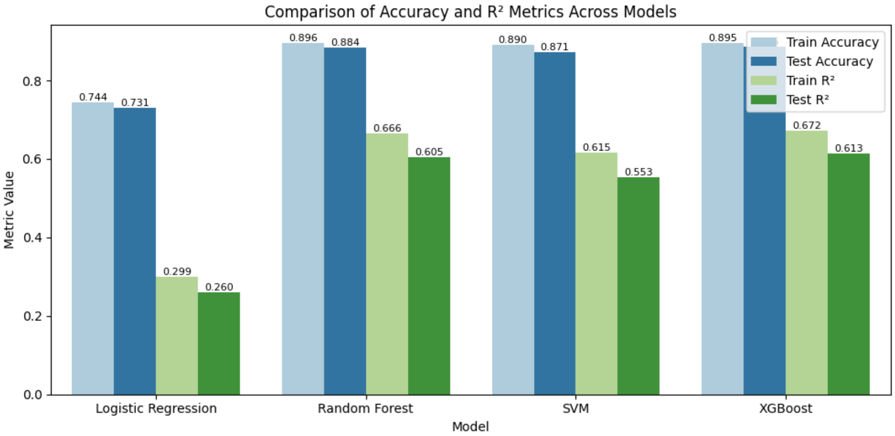


Fig. 12. Evaluating the Performance of Logistic Regression, Random Forest, SVM, and XG Boost: Accuracy and R² Metrics Analysis

7.3.3 Radar Chart Analysis of Model Performance: Comparing Train and Test Metrics Across Logistic Regression, Random Forest, XG Boost, and SVM

Fig. 13 is a radar chart that shows the performance of different machine learning models in Train Accuracy, Test Accuracy, Train R², Test R², Train MSE, Test MSE, Train MAE, and Test MAE. The figure helps in understanding not only each model's performance but also its performance on training data and testing data (distance from the center is the metric) visualized for comparison. The more words a model can cover, the higher its performance on all the metrics. XG Boost is great, achieving good coverage over the metrics for both train and test. Random Forest performs well, with Logistic Regression and SVM performing considerably weaker, especially in the Train MSE and Test MSE metrics. This radar graph permits an easy comparative analysis of the performance of models in generalizing to unseen data and fitting to the training set, thereby serving as a useful model evaluation tool.

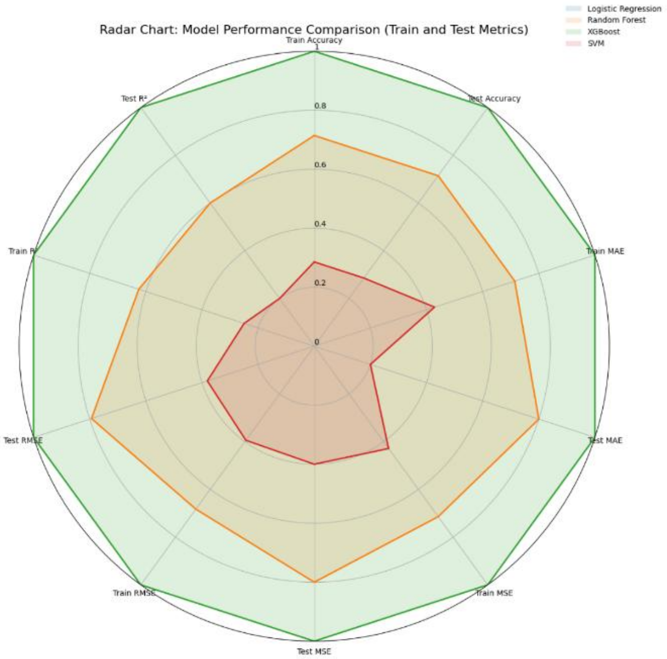


Fig. 13. Visual Comparison of Machine Learning Models: Radar Chart Analysis of Train and Test Metrics.

7.74 Exploring Feature Relationships in Attack Detection: Lower Triangle Correlation Heatmap of Numerical Features

Fig. 14: lower triangle correlation heatmap for numerical features associated with attack detection. The relationship between the different network variables: network_packet_size, login_attempts, session_duration, ip_reputation_score, failed_logins, unusual_time_access, and attack_detected, is depicted in the heatmap. The values can be between -1 and 1, and the larger the value, the larger the correlation. The Attack_detected feature has the highest correlation with failed_logins (0.36) and login_attempts (0.28), indicating a slightly strong dependence between failed_logins/login_attempts and the appearance of attacks. In addition, attack_detected is also weakly dependent on ip_reputation_score (0.21) and session_duration (0.04). Other features like network_packet_size, unusual_time_access and failed_logins have weak correlation with attack_detected of −0.01, 0.01 and 0.02, respectively. This heatmap offers an interpretation as to how various features are correlated and may assist in the comprehension of which features are most influential signs in the detection of attacks.

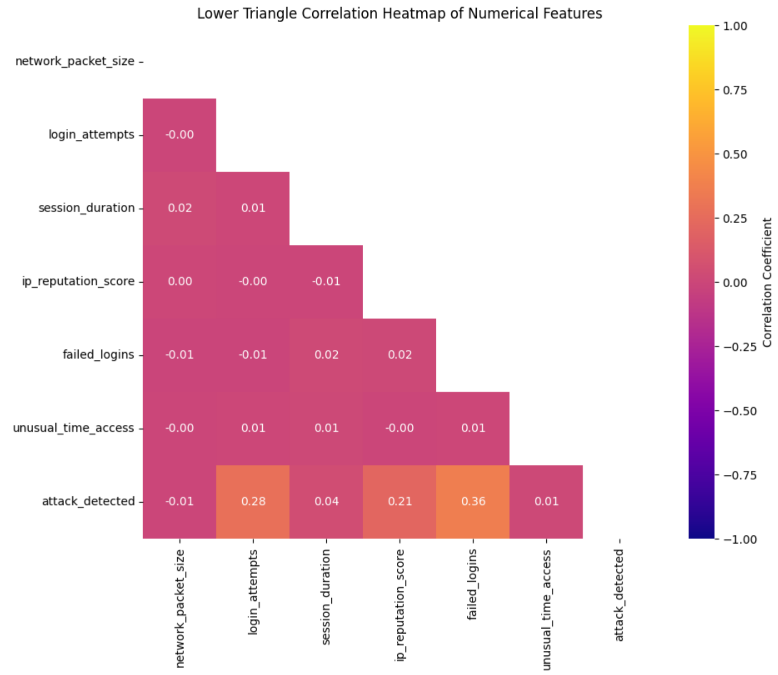
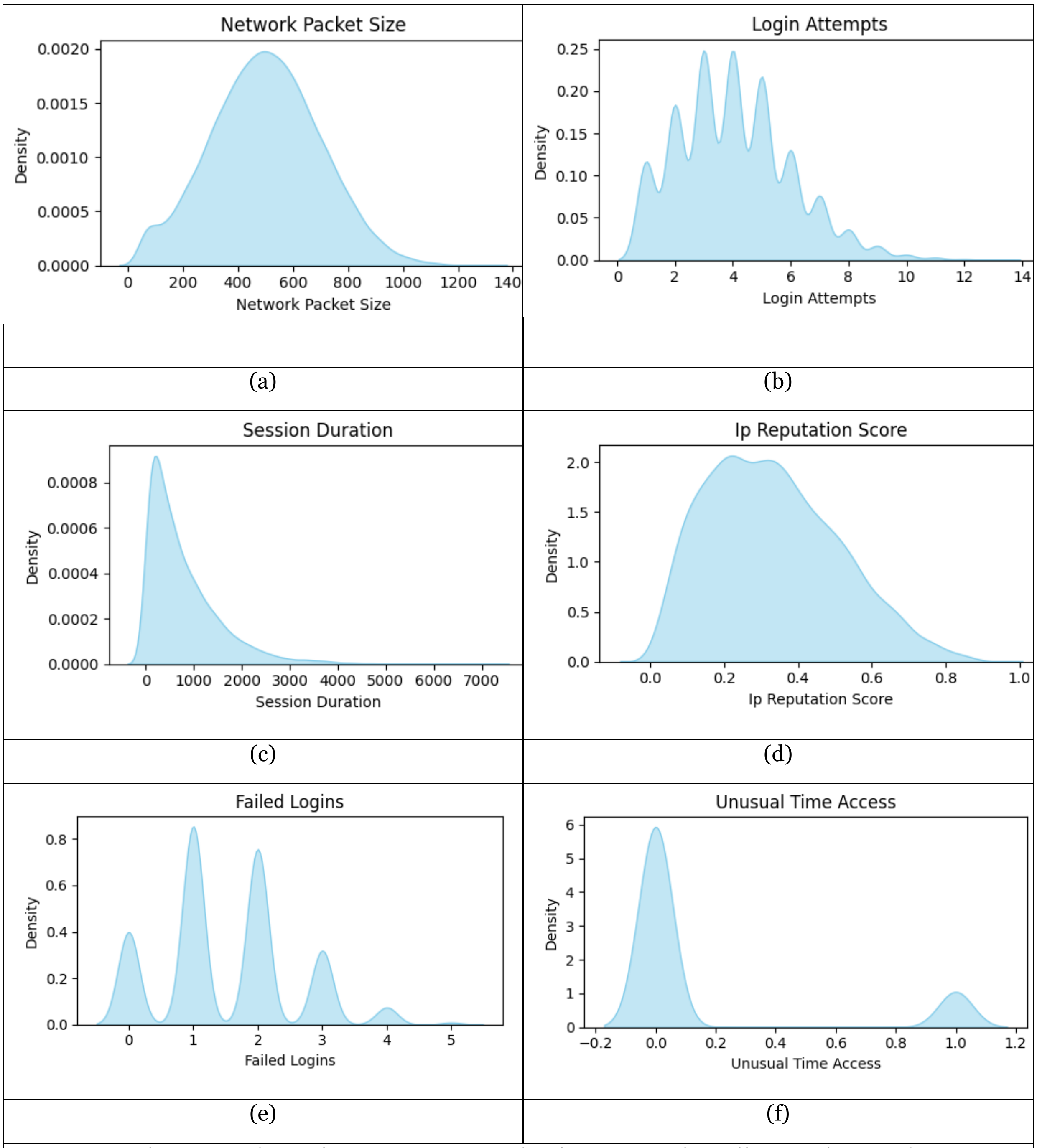


Fig. 14. Correlation Analysis of Numerical Features in Attack Detection: A Heatmap of Key Variables

7.5 Feature-wise Density Distributions: A Comparative Study of Network Traffic Metrics for Attack Detection

Fig. 15 presents a distribution-based analysis of important attributes on the network traffic data for attack detection. The panels display the density of the respective quantities. The network packet size (a) is distributed around a normal distribution, most packets are between 300 and 900 bytes in size, with a peak around 600 and a decreasing tendency for packet sizes larger than 1000. (b) Multimodal distribution in login attempts, common login attempts are seen at 1,3 and 5 attempts, while the density decreases beyond 7 attempts. The session length (Fig. C) is also skewed: most sessions are short (around 500 seconds), while a few sessions last as long as 5000 seconds, which suggests the presence of long-duration sessions. IP reputation score (d) is close to a normal distribution whose peak ranges from 0.2 to 0.5, and a higher density is located between 0.0 and 0.3, showing that the majority of the dataset's IP addresses have moderate reputation scores. We have a bimodal distribution failed logins with peaks at 0 and 1 failures, and a lower second peak at 3, the rest of the attempts being almost marginal. Unusual day access (f) exhibits a well-skewed distribution with a maximum close to zero (at 0.0), suggesting that most of the access is done at regular times, and few access times are unusual (the peak being approximately 1.2). These distributions are useful for understanding the behaviour of a network and gaining insights into network traffic in the context of attack detection.



(a) (b)

(c) (d)

(e) (f)

Fig. 15. Distribution Analysis of Key Features: Insights from Network Traffic Data for Attack Detection

7.6 Density Distribution of Key Features: A Comparative Analysis Between Attack and No Attack Cases

Fig. 16 analyses the distribution of network traffic data features for “No Attack” and “Attack” samples. The density distributions of network_packet_size, login_attempts, session_duration, ip_reputation_score, failed_logins, and unusual_time_access for these two classes are shown in the figure. "No Attack" in the network_packet_size distribution has a peak at 500, while "Attack" has a similar shape but higher density around larger packet sizes (1000), which indicates that the larger value has a higher probability during attacks. The difference is also visible in the log-in attempts, and we have “no attack” having one of the highest peak at small log-in attempts (0-3) and “attack” having a more spread distribution with its peak extending up to 12, implying that attacks happen at higher number trials of log-ins. Session_ duration shows the same trend, where “No Attack” has a distinct peak around 1000 seconds, while “Attack” presents a wider distribution reaching up to 7000 seconds, indicating longer sessions during attacks. The distribution of ip_ reputation_ score indicates a remarkable position change, i.e., "No Attack" mainly lies between 0.0 and 0.3, while "Attack" is uniformly distributed along the range (symmetric distribution) and the peak is around 0.5, so it suggests that lower reputation scores are associated with an attack. failed_ logins No Attack has a greater density at 0 and 1 failed logins, while Attack has more density at 2-4, indicating that attacks have multiple failed logins associated with them. From unusual_ time_ access, we see the Distribution is somewhat similar between the classes, but the condition "Attack" becomes denser for values above 0, showing that attacks tend to happen during unusual time intervals. This can help to get an idea of how individual features behave with or without attacks and highlight patterns that might be able to help you detect attacks.

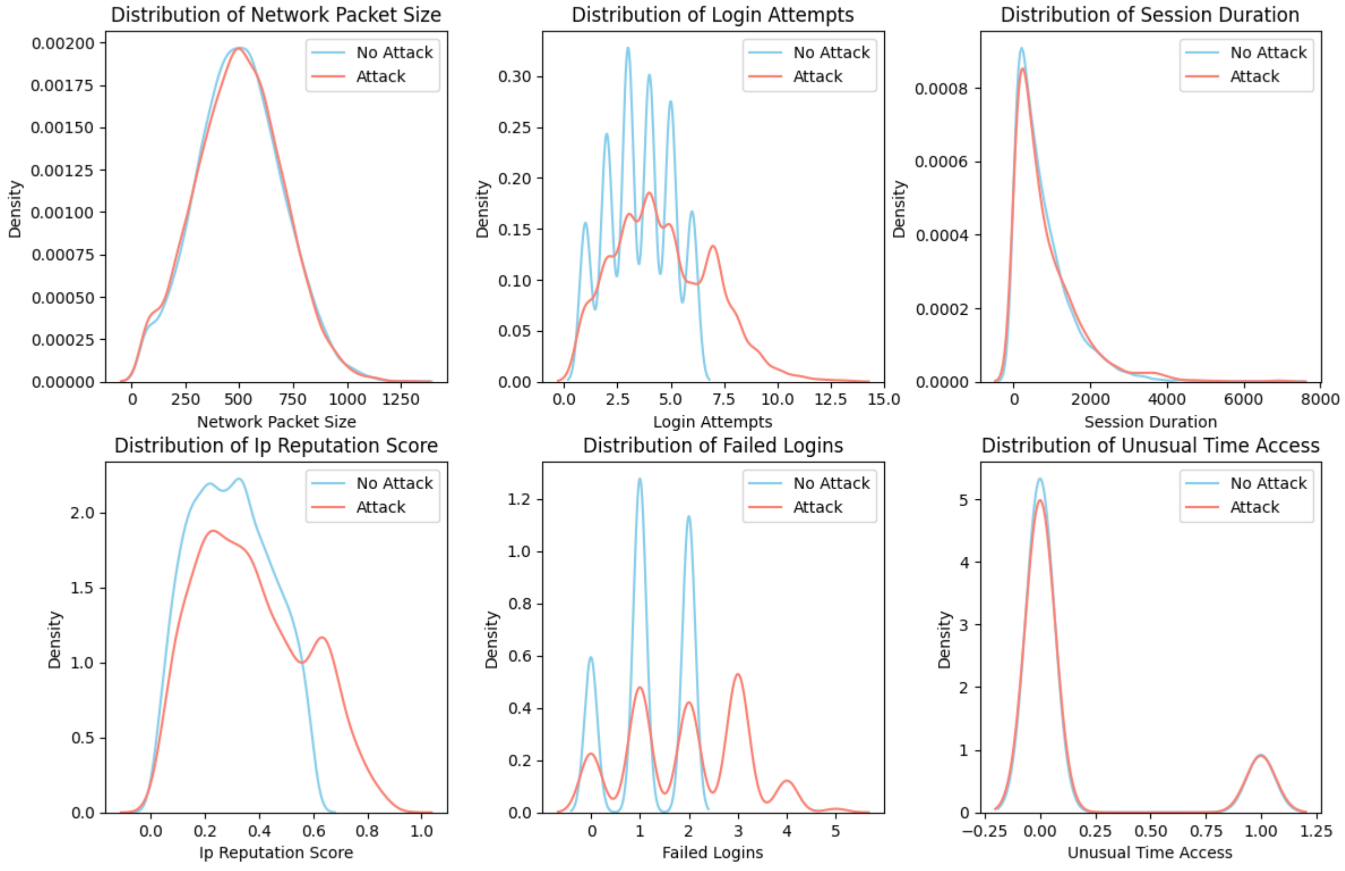


Fig. 16. Exploring Feature Distributions: Comparing 'No Attack' vs. 'Attack' in Network Traffic Data

7.7 Evaluating Model Performance for Attack Detection: ROC Curve Analysis Across Logistic Regression, Random Forest, SVM, and XG Boost

Fig. 17 investigated the discriminative capacity of various machine learning algorithms in terms of ROC curves and AUC scores. On the other hand, the chart of True Positive Rate (TPR) and False Positive Rate (FPR) from the generalization model of Logistic Regression, Random Forest, SVM and XG Boost algorithms. The AUC scores reflect the general capacity of the models to discriminate classes; Logistic Regression presented with AUC 0.79 and Random Forest and XG Boost obtained the highest AUC (0.88) while SVM´s AUC was 0.87. The curves show how well the models perform, and the Random Forest and XG Boost obtain the best performance, as seen from the highest AUC values. The diagonal dashed line is a random classifier is a baseline for comparison. Models have to be above that line to do better than random guessing; those farther from the diagonal are better discriminators.

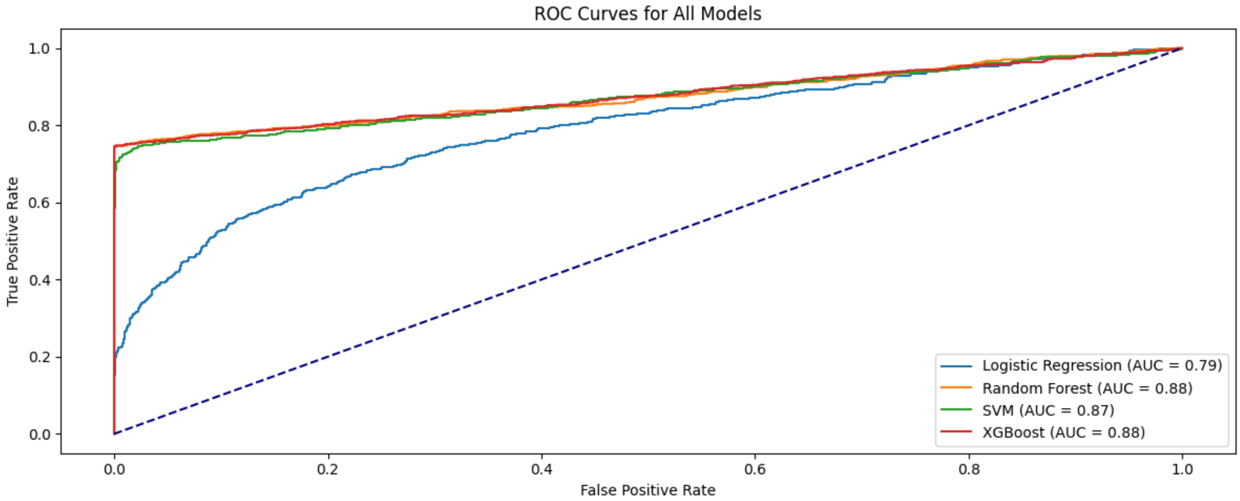


Fig. 17. Comparing Model Discriminative Power: ROC Curves and AUC for Logistic Regression, Random Forest, SVM, and XG Boost

7.8 Evaluating Model Calibration for Attack Prediction: A Comparison of Logistic Regression, Random Forest, XG Boost, and SVM

Fig. 18, presented the calibration curves for different attack detection models as a function of the actual vs. the predicted attack probabilities. On the x-axis is the average, predicted probability of attack and on the y-axis is the proportion of actual attacks. The calibration curves for Logistic Regression (blue), Random Forest (green), XG Boost (orange) and SVM (red) are indicated in the figure. The dashed blue line is the model that would be perfectly calibrated (predicted odds equal actual odds). From the graph, we observe that Logistic Regression and SVM are both quite well-calibrated but are both slightly underestimating the proportion of true attacks around higher probabilities (for example, LR gets around 0.4 at a Predicted Probability of 0.8 and SVM gets 0.5 at the same probability). XG Boost predictions exhibit a strongly overconfident model that is particularly overconfident at high probabilities, overestimating the predicted attacks and coming to nearly 1.0 at predicted probability 1.0. The Random Forest departs from the perfectly calibrated line most dramatically, especially at lower values (where there are more predicted probabilities, as it overestimates the fraction of attacks). For instance, at 0.3 predicted probability fraction is about 0.2, indicating it's giving larger weights at lower cut-offs too. These calibration curves yield information about how good the models are and how the predicted probabilities are estimated, to match the attack occurrences.

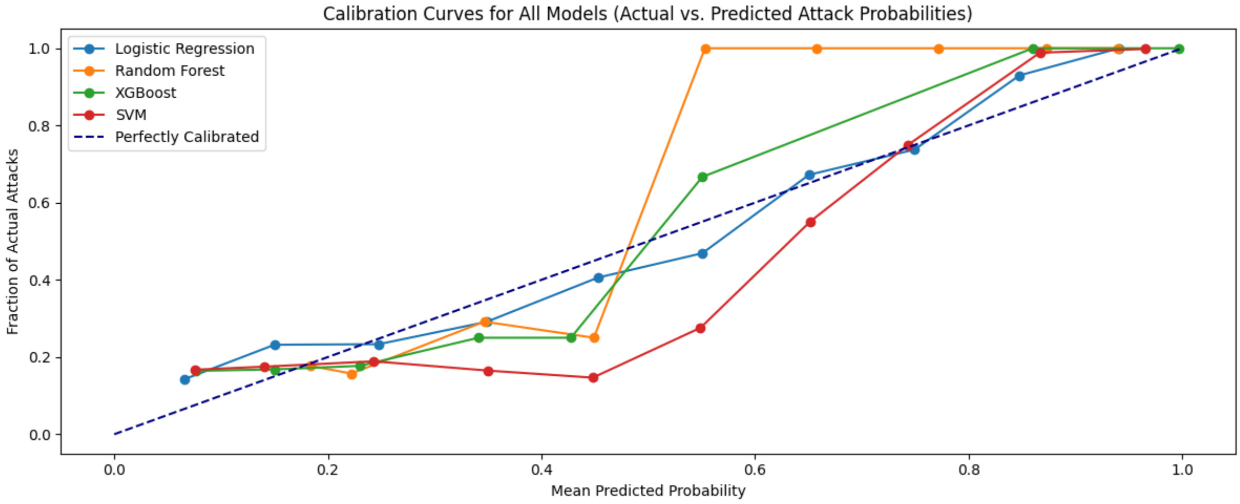


Fig. 18. Calibration of Attack Detection Models: Comparing Actual vs. Predicted Probabilities

7.9 Comparative Analysis of Model Predictions for Attack Detection: A Probability Distribution Approach

Fig. 19 shows the expected probability distribution of attack detection for a few machine learning models (Logistic Regression, Random Forest, XG Boost and SVM). The plot is of the predicted probability of attack by beast1 on the x-axis and the density on the y-axis. All models have different colors - Logistic Regression is blue, Random Forest is green, XG Boost is orange, and SVM is red. The plot illustrates how both models disperse the predicted probabilities, but with the SVM model peaking around a density of 3.5 at a predicted probability of 0.9, which implies greater confidence in the prediction that an attack is about to occur. XG Boost displays pressure around 3 in the value of 0.7, also presenting high confidence and some dispersion. The Logistic Regression has a peak density close to 2 along 0.3; this test doubts its predictions. For Random Forest, the highest density is 2.5 at 0.5, which would mean a more equitable confidence across all predicted probabilities. It allows us to observe how each model behaves and performs in predicting attack Probabilities.

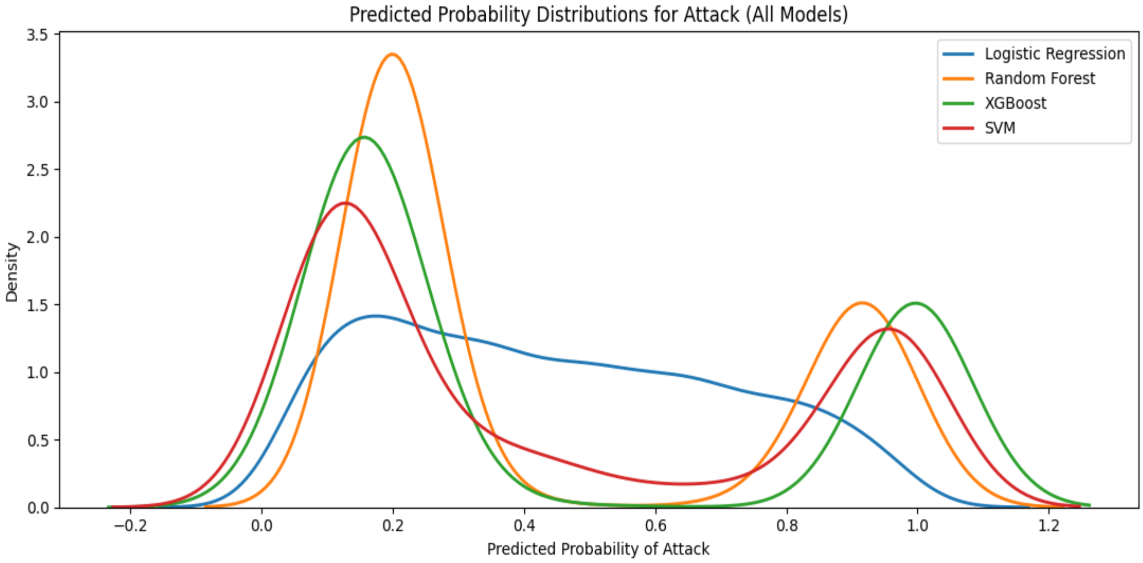


Fig. 19. Evaluating Model Performance for Attack Detection: Predicted Probability Distributions Across Multiple Algorithms

7.10 SHAP Analysis

7.10.1 Interpreting Model Predictions Using SHAP: Feature Importance Analysis for Anomaly Detection

Fig. 20) provides a SHAP Bees warm Plot to help interpret feature contributions in predictive modelling. The XGB model feature importance (measured by SHAP value, the saliency of a feature value on the model output) reveals the most informative features. Attributes such as failed_logins, login_attempts and ip_reputation_score are features that have the biggest impact on output and have SHAP scores in the largest positive or negative values that show the drastic shifts in prediction. It is worth mentioning that failed_logins and login_attempts present a higher density of values at the extremes of the histogram, indicating that they have a high impact on the predictions of security. There is also a considerable variation in session_ duration and network_ packet_ size, making them significant for prediction accuracy. The features related to the encryption technique used, such as encryption_ used_ DES, and pandemic_ Udp, and the browser type, such as Unknown, and browser type_ Firefox, their influence is also between moderate and small. The color gradient indicates feature values: larger values (red) have a larger positive effect on the output, while lower values (blue) have a negative effect. This bee's warm plot does well in depicting the impact of the features on the predicting results of the network flow-based model.

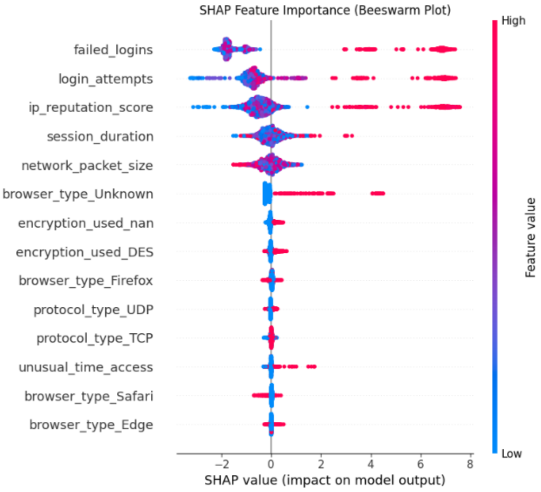


Fig. 20. Understanding Feature Contribution with SHAP: A Bees warm Plot Analysis for Predictive Modelling

7.10.2 Exploratory Data Analysis of Network Traffic Features: A Correlation Study of Session Duration, Login Attempts, and Protocol Types

Fig. 21 illustrates the relationships between various network data features, such as protocol types, encryption used, and browser types, regarding security metrics. The scatter plots demonstrate the distribution and correlation of these features. Among the factors, Login Attempts (with Failed Logins) and Session Duration exhibit strong variability across different features like protocol types (TCP and UDP), encryption types (AES, DES), and browser types (Chrome, Safari, Firefox, etc.). For example, the distribution of Login Attempts shows marked differences between Failed Logins and successful logins, with data points clustering at extreme values for failed attempts. Similarly, Session Duration shows significant changes, especially concerning the Protocol Type UDP and Encryption Used DES, which have distinct distributions. IP Reputation Score also shows a direct impact, particularly with TCP Protocol, while browser types like Firefox and Safari show consistent distributions, indicating their role in influencing the session's security-related characteristics. These findings indicate that

Login Attempts and Session Duration have the most significant influence on the data's variability due to their correlation with attack patterns, protocol choices, and encryption preferences.

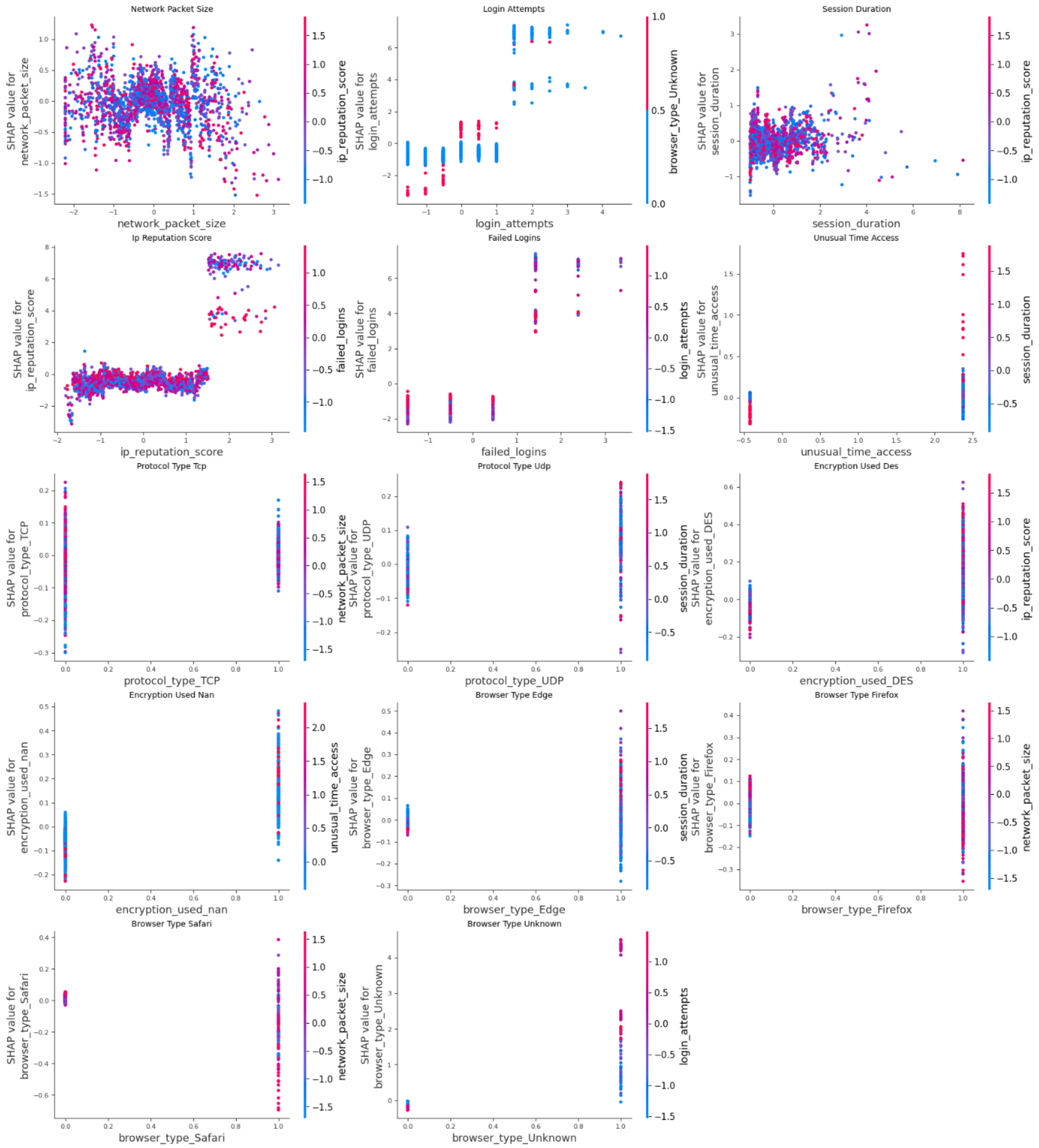


Fig. 21. Visualizing Feature Relationships in Network Data: Impacts of Protocol Types, Encryption, and Browser Usage on Security Metrics

8. Conclusion:

Growing threats to U.S.CI from cyber attacks demand an advanced cybersecurity infrastructure. This paper investigates the capacities of AI-driven systems in protecting critical infrastructures such as energy, health, and transportation from threats that benefit from traditional cybersecurity tools.

Key Findings:

- Attack detection was strongly correlated with features such as the number of failed logins (0.36) and the number of login attempts (0.28). Attack detection had a poor correlation with IP reputation score (0.21) and session duration (0.04).
- The distribution experiment showed that network packets are mostly within a size range of 300-900 bytes, with peaks at around 600 bytes, which implied that small packets dominate network traffic.
- Of the models tested, XG Boost scored the highest in terms of test accuracy 88.52% and test R^2 0.6198, outperforming the Random Forest (test accuracy: 88.41%, R^2: 0.6048), in contrast, the Logistic Regression was by far the worst (test accuracy: 73.11%, R^2: 0.2604).
- ROC curve analysis verified that XG Boost and Random Forest obtained the maximum AUC scores (0.88) and performed better than SVM (0.87) and Logistic Regression (0.79) in attack detection.
- XG Boost had an overestimation in predicting attack probabilities, whereas SVM and Logistic Regression were well-calibrated but slightly underestimated actual attack at higher probabilities.

9. Limitations and Future Directions

The research focused on a limited number of models and may not sufficiently cover the possible approaches that can be undertaken to solve the problem of cybersecurity in critical infrastructures. The dataset may not cover all forms of real-world attacks, including new ones. Further research efforts are required in the areas of reinforcement learning, transfer learning, and dataset enrichment tasks to enhance AI-driven cybersecurity. Attacking ethics and regulations is the most crucial to our privacy and system security. This paper shows the feasibility of AI in the protection of critical infrastructure.

References

[1] Moteff, J.D., S. Resources, and I. Division. *Critical infrastructures: Background, policy, and implementation*. 2007. Congressional Research Service, Library of Congress.

[2] Lewis, T.G., *Critical infrastructure protection in homeland security: defending a networked nation*. 2019: John Wiley & Sons.

[3] Berkeley, A.R., M. Wallace, and C. Coo, *A framework for establishing critical infrastructure resilience goals*. Final report and recommendations by the council, national infrastructure advisory council, 2010. **26**.

[4] Hossain, M.F. and M.M. Uddin, *AI in Precision Oncology: Revolutionizing Cancer Treatment Through Personalized Drug Discovery*. Journal of Computer Science and Technology Studies, 2025. **7**(2): p. 276-283.

[5] Rahul Reddy Bandhela, RamMohan Reddy Kundavaram, Abhishake Reddy Onteddu. (2023). Ensuring Security and Verification of Graduate Credentials Using Blockchain Technology . Journal of Computational Analysis and Applications (JoCAAA), 31(3), 601–608. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/3032

[6] Arafat, Y., et al., *Big Data Analytics in Information Systems Research: Current Landscape and Future Prospects Focus: Data science, cloud platforms, real-time analytics in IS*. Emerging Frontiers Library for The American Journal of Engineering and Technology, 2025. **7**(8): p. 177-201.

[7] Basak, B., *The Impact of Cybersecurity Threats on National Security: Strategies*. International Journal of Humanities Social Science and Management (IJHSSM), 2024. **4**(2): p. 1361-1382.

[8] Seet, P.-S., et al., *Expanding Australia's defence capabilities for technological asymmetric advantage in information, cyber and space in the context of accelerating regional military modernisation: A systemic design approach*. 2024.

[9] Khatun, M. and M.S. Oyshi, *Advanced Machine Learning Techniques for Cybersecurity: Enhancing Threat Detection in US Firms*. Journal of Computer Science and Technology Studies, 2025. **7**(2): p. 305-315.

[10] Mondal, K.K., M.S. Uddin, and T. Mahmud, *From Pandemic to Persistence: Obesity, Immunity, and Next-Gen COVID-19 Vaccines*. 2025.

[11] Masud, S.B., et al., *AI-Driven Predictive Maintenance in Infrastructure and Facilities Management*. 2025.

[12] Hossain, M.I., et al., *Zero-ETL Analytics: Transforming operational data into actionable insights*. 2025.

[13] Rahman, M.B., et al., *Appraising the historical and projected spatiotemporal changes in the heat index in Bangladesh*. Theoretical and Applied climatology, 2021. **146**(1-2): p. 125.

[14] Roy, K.K., et al., *Leveraging artificial intelligence for strategic decision-making in healthcare organizations: a business it perspective*. The American Journal of Applied Sciences, 2025. **7**(8): p. 74-93.

[15] Saeed, M., *Data-Driven Healthcare: The Role of Business Intelligence Tools in Optimizing Clinical and Operational Performance*. The American Journal of Applied Sciences, 2025. **7**(8): p. 50-73.

[16] Shaker, A.S.M., et al., *TACS-Net: Temporal-Aware Customer Segmentation Network*. IEEE Open Journal of the Computer Society, 2025.

[17] Siyam, O.F., et al., *Interpretable Deep Learning for Symptom-Based Lung Cancer Prediction Using a 1D CNN Framework*.

[18] Islam, I., et al., *The Future of Banking Fraud Detection: Emerging AI Technologies and Trends*. Well Testing Journal, 2025. **34**(S3): p. 102-120.

[19] Alim, M.A., et al., *Enhancing fraud detection and security in banking and E-Commerce with AI-powered identity verification systems*. 2020.

[20] Mandal, N.C., et al., *A Case Report of Middle Aortic Syndrome: A Rare Vascular Disorder*. Cardiovascular Journal, 2013. **6**(1): p. 60-62.

[21] Mir, M.N.H., et al., *ABMF-Net: An Attentive Bayesian Multi-Stage Deep Learning Model for Robust Forecasting of Electricity Price and Demand*. IEEE Open Journal of the Computer Society, 2025.

[22] Masud, S.B., et al., *The revolution of AI in enhancing infrastructure and facilities management*. Cuestiones de Fisioterapia, 2025. **54**(4): p. 5605-5624.

[23] Djenna, A., S. Harous, and D.E. Saidouni, *Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure*. Applied Sciences, 2021. **11**(10): p. 4580.

[24] George, A.S., T. Baskar, and P.B. Srikaanth, *Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors*. Partners Universal International Innovation Journal, 2024. **2**(1): p. 51-75.

[25] Hoque, A., et al., *Reshaping Fintech: Unveiling Recent Developments on Fintech Integration*. Well Testing Journal, 2025. **34**(S3): p. 121-148.

[26] Cole, E., *Advanced persistent threat: understanding the danger and how to protect your organization*. 2012: Newnes.

[27] Uddin, M.K., et al., *A greener approach to cotton pre-treatment using bentonite clay*. The Journal of The Textile Institute, 2022. **113**(9): p. 1775-1784.

[28] Hüsch, P. and H. Lahmann, *Societal Risks and Potential Humanitarian Impact of Cyber Operations*. Geneva Academy Working. Papergeneva-academy. chgeneva-academy. ch, 2022.

[29] Arif, M.H., et al., *AI-Driven Risk Assessment in National Security Projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects*. Journal of Computer Science and Technology Studies, 2025. **7**(2): p. 71-85.

[30] Md Abdul Alim, M.R.R., Md Shakhawat Hossen, Mamunur Rahman, Md Habibul Arif, Iftekhar Rasul, *Zero-Trust Security Models in Multi-Cloud Environments: Scalability, Challenges, and Implementation Strategies*. Journal of Advanced Research in Applied Sciences and Engineering Technology,, 2025. **56**(282–29).

[31] Mahmud, T. and S.S.M. Naim, *Predicting polycystic ovary syndrome using SVM*. International Journal of Science and Research Archive, 2024. **13**(02): p. 4400-4408.

[32] Lehto, M., *Cyber-attacks against critical infrastructure*, in *Cyber security: Critical infrastructure protection*. 2022, Springer. p. 3-42.

[33] Akhtar, Z.B. and A.T. Rawol, *Enhancing cybersecurity through AI-powered security mechanisms*. IT Journal Research and Development, 2024. **9**(1): p. 50-67.

[34] Ismail, W.S., *Threat Detection and Response Using AI and NLP in Cybersecurity*. J. Internet Serv. Inf. Secur., 2024. **14**(1): p. 195-205.

[35] Hoque, A., et al., *AI and Machine learning in Banking: Driving Efficiency and Innovation*. Well Testing Journal, 2025. **34**(S3): p. 80-101.

[36] Md Habibul Arif, I.R., Md Abdul Alim, Md Reduanur Rahman, Md Shakhawat Hossen, Mamunur Rahman, *AI-Powered DDoS Detection and Mitigation: Developing Adaptive Machine Learning Frameworks to Predict and Block Next-Generation Attacks*. Journal of Advanced Research in Applied Sciences and Engineering Technology, 2025. **56**(231–243).

[37] Ajala, O.A., et al., *Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time*. Magna Scientia Advanced Research and Reviews, 2024. **10**(1): p. 312-320.

[38] Mahmud, T. and S. Mohosin Naim, *Skin Cancer Classification Using VGG-16*. International Journal of Innovative Science and Research Technology, 2025. **10**(7): p. 457-463.

[39] Prince, N.U., et al. *Deep Transfer Learning Approach to Detect Dragon Tree Disease*. in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. 2024. IEEE.

[40] Islam, M.T., et al. *FinGraphRisk: A Graph Neural Network-Based Framework for Sentiment-Driven Financial Risk Assessment*. in *2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*. 2025. IEEE.

[41] Islam, R., et al., *Integrating Blockchain Innovation: A Sustainable Adoption Model for Business*. Journal of Computer and Communications, 2024. **12**(11): p. 141-161.

[42] Kovler, K. and N. Roussel, *Properties of fresh and hardened concrete*. Cement and Concrete Research, 2011. **41**(7): p. 775-792.

[43] Uddin, M.B., et al. *Blockchain Integration in IoMT for Secure Healthcare: Challenges, Integration, and Solutions*. in *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)*. 2025. IEEE.

[44] Alam, K., et al., *Cyber Attacks Detection And Mitigation Using Machine Learning In Smart Grid Systems*. Journal of Science and Engineering Research, 2024. **1**(01): p. 38-55.

[45] S A Mohaiminul Islam Nusrat Yasmin Nadia, M.S.B., Mohammed Majid Bakhsh, Ankur Sarkar, *AI-Driven Test Data Management for Large-Scale BI Applications*. International Journal of Innovative Science and Research Technology (IJISRT), 2025/2/15. **10**(1): p. 11.

[46] Rahman, M., et al., *Quantum Machine Learning Integration: A Novel Approach to Business and Economic Data Analysis*. 2021.

[47] Tatipatri, N. and S. Arun, *A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security*. IEEE Access, 2024. **12**: p. 18147-18167.

[48] Bellal, R.B., et al., *The Economic Impact of AI-Driven Carbon Emission Reduction Strategies in Large-Scale Industrial and Office Settings*. Cuestiones de Fisioterapia, 2023. **52**(3): p. 717-736.

[49] Stellios, I., et al., *A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services*. IEEE Communications Surveys & Tutorials, 2018. **20**(4): p. 3453-3495.

[50] Okoli, U.I., et al., *Machine learning in cybersecurity: A review of threat detection and defense mechanisms*. World Journal of Advanced Research and Reviews, 2024. **21**(1): p. 2286-2295.

[51] Sufia Zareen, N.A.T., Md Abdul Alim, Md Reduanur Rahman, Md Habibul Arif, Iftekhar Rasul Md Shakhawat Hossen, *To Secure the Digital Age: The application of Quantum Computing, and Ethical Frameworks*. 2023. **8**(6).

[52] Basak, S., M.D.H. Gazi, and S. Mazharul Hoque Chowdhury. *A Review Paper on Comparison of different algorithm used in Text Summarization*. in *International Conference on Intelligent Data Communication Technologies and Internet of Things*. 2019. Springer.

[53] Mahmud, T., S. Ibtisum, and S.S. Hossain, *A Comprehensive Survey on SmartNIC*. International Journal of Computer Applications. **975**: p. 8887.

[54] Islam, M.T., et al., *LaplaceSalesNet: A Neural Laplace-Transformer Framework for Continuous-Time Sales Forecasting*. IEEE Open Journal of the Computer Society, 2025.

[55] Sozib, H.M., et al., *Cloud Computing in Business: Leveraging SaaS, IaaS, and PaaS for Growth*. Journal of Applied Research: p. 38.

[56] Ofoegbu, K.D.O., et al., *Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach*. Computer Science & IT Research Journal, 2024. **4**(3).

[57] Mohammed Majid Bakhsh, M.S.A.J., Sazzadul Islam, Nusrat Yeasmin Nadia, Ankur Sarkar, Md Shadikul Bari, SA Islam, *From Compliance to Code: An NLP-Based QA Automation Framework For HRM Software in the US Healthcare Sector*. Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/Journal of Tianjin University Science and Technology, ISSN (Online), 2024/3/11: p. 0493-2137.

[58] Abokifa, A.A., et al., *Real-time identification of cyber-physical attacks on water distribution systems via machine learning–based anomaly detection techniques*. Journal of Water Resources Planning and Management, 2019. **145**(1): p. 04018089.

[59] Bhattacharyya, D.K. and J.K. Kalita, *Network anomaly detection: A machine learning perspective*. 2013: Crc Press.

[60] Khan, R., et al., *Technology-Assisted Parent Training Programs for Autism Management*. Technology, 2024. **1**(1).

[61] Biswas, A.K., et al., *A Dual Output Temporal Convolutional Network With Attention Architecture for Stock Price Prediction and Risk Assessment*. IEEE Access, 2025.

[62] Pankaj Kumar Sarker, S.C.S., Santanu Palit, Abdullah Al Naseeh Chowdhury, Mst Sanjida Alam, Mohammad Delowar Hossain Gazi, Mahabubur Rahman, *Machine learning applications in predicting structural failures and earthquake damage.*

[63] Sizan, M.M.H., *Machine Learning-Based Unsupervised Ensemble Approach for Detecting New Money Laundering Typologies in Transaction Graphs*. International Journal of Applied Mathematics, 2025. **38**(2s): p. 351-374.

[64] Alam, G.T., et al., *Predictive Analytics in QA Automation:: Redefining Defect Prevention for US Enterprises*. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2025. **4**(2): p. 55-66.

[65] Sharma, S. and T. Arjunan, *Natural language processing for detecting anomalies and intrusions in unstructured cybersecurity data*. International Journal of Information and Cybersecurity, 2023. **7**(12): p. 1-24.

[66] Sarker, I.H., M.H. Furhad, and R. Nowrozy, *Ai-driven cybersecurity: an overview, security intelligence modeling and research directions*. SN Computer Science, 2021. **2**(3): p. 173.

[67] Samia Ara Chowdhury, A.H., Md Sajedul Karim Chy, Mohammad Delowar Hossain Gazi, *Next Generation Financial Security: Leveraging AI for Fraud Detection, Compliance and Adaptive Risk Management*. Well Testing Journal, 2025/7/25. **34**(S3): p. 61-79.

[68] Sazzadul, I., et al., *Designing a Real-Time Human-AI Decision Support Framework for US Healthcare Providers Using Big Data Analytics*. Journal of Computer Science and Technology Studies, 2025. **7**(8): p. 716-723.

[69] Begum, S., *Artificial Intelligence and Economic Resilience: A Review of Predictive Financial Modelling for Post-Pandemic Recovery in the United States SME Sector*. International Journal of Innovative Science and Research Technology, 2025. **10**(7): p. 3620-3627.

[70] Bakhsh, M.M., G.T. Alam, and N.Y. Nadia, *Adapting Agile Methodologies to Incorporate Digital Twins in Sprint Planning, Backlog Refinement, and QA Validation*. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2025. **4**(2): p. 67-79.

[71] Bari, M., et al., *Toward an Adaptive AI/ML-Based QA Framework with HRM Integration for Inclusive and Secure Healthcare Solutions in Edge Environments*. Journal of Neonatal Surgery, 2025. **14**(32S): p. 7612-7620.

[72] Mahmud, T., *Applications for the Internet of Medical Things*. International Journal of Science and Research Archive, 2023. **10**(02): p. 1247-1254.

[73] Jada, I. and T.O. Mayayise, *The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review*. Data and Information Management, 2024. **8**(2): p. 100063.

[74] Raimundo, R. and A. Rosário, *The impact of artificial intelligence on data system security: A literature review*. Sensors, 2021. **21**(21): p. 7029.

[75] Abdullah, D.M. and A.M. Abdulazeez, *Machine learning applications based on SVM classification a review*. Qubahan Academic Journal, 2021. **1**(2): p. 81-90.

[76] Sobuz, M.H.R., et al., *An explainable machine learning model for encompassing the mechanical strength of polymer-modified concrete*. Asian Journal of Civil Engineering, 2025. **26**(2): p. 931-954.

[77] Mehortra, R., et al. *Comparative Analysis of Multinomial Naïve Bayes and XG Boost for Sentiment Analysis*. in *2024 International Conference on Signal Processing and Advance Research in Computing (SPARC)*. 2024. IEEE.

[78] Sobuz, M.H.R., et al., *Microstructural assessment and supervised machine learning-aided modeling to explore the potential of quartz powder as an alternate binding material in concrete*. Case Studies in Construction Materials, 2025. **22**: p. e04568.

[79] De Menezes, F.S., et al., *Data classification with binary response through the Boosting algorithm and logistic regression*. Expert Systems with Applications, 2017. **69**: p. 62-73.

[80] Shaik, A.B. and S. Srinivasan. *A brief survey on random forest ensembles in classification model*. in *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 2*. 2019. Springer.

[81] Mahmud, T., *ML-driven resource management in cloud computing*. World Journal of Advanced Research and Reviews, 2022. **16**(03): p. 1230-1238.

[82] Mahmud, T., *AUTONOMOUS BOUNDARY ALERT SYSTEM FOR CHILD/CRIMINAL MONITORING. 2020*. DAFFODIL INTERNATIONAL UNIVERSITY.

[83] Chicco, D. and G. Jurman, *The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation*. BMC genomics, 2020. **21**: p. 1-13.

[84] Carter, J.V., et al., *ROC-ing along: Evaluation and interpretation of receiver operating characteristic curves*. Surgery, 2016. **159**(6): p. 1638-1645.

[85] Obuchowski, N.A. and J.A. Bullen, *Receiver operating characteristic (ROC) curves: review of methods with applications in diagnostic medicine*. Physics in Medicine & Biology, 2018. **63**(7): p. 07TR01.

[86] Billah, M.M., et al., *Skin Cancer Classification using NasNet*. 2023.