Grenze International Journal of Engineering and Technology, January Issue

Securecast: Forecasting CyberAttack using Machine Learning

Ashish Jain[1], Yusra Qamar[2], Sudeep Varshney[3], Jitendra Singh[4] and Amit Chaudhary[5]
[1-5]Department of Computer Science and Engineering, Sharda University, Greater Noida, India
Email: Ashish.neetu1981@gmail.com, yusra.qamar2000@gmail.com, sudeep149@gmail.com, jitendra.singh6@sharda.ac.in, amitchaudhary1@sharda.ac.in

***Abstract*— Targeted cyberattacks have become more sophisticated and frequent in recent years, partly as a result of growing weaknesses in commonly used technology. It is essential to identify and anticipate cyberattacks in advance in order to reduce possible risks and improve network resilience. The exponential growth of the complexity of cyberattacks and digital data have made big data an indispensable instrument for intrusion detection and forecasting. Intrusion detection systems are better able to identify and thwart anomalies and cyberattacks by utilizing unstructured big data. Even though attack prediction has improved, time series and unstructured large data are still underutilized in cyber event forecasting research.**

The dataset utilized in this study, CSE-CIC-IDS2018, contains a variety of attacks on a real network. In time-series forecasting, methods such as linear regression, long short-term memory (LSTM), and sequential minimum optimization for regression (SMOreg) were employed to build models with ideal parameters. The models' performance was evaluated using a diversity of machine learning techniques, including Support Vector Machine (SVM), Random Forest, and Naive Bayes. Random forest and SVM had the highest success rate, at 90.4%. To evaluate the accuracy of the predicted events, metrics such as Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) were used. The lowest RMSE was shown by linear regression, whereas the lowest MAE was achieved using SMOreg. The goal of this endeavor is to improve detection of cyberthreats and mitigation of security lapses in crucial infrastructure.

Keywords— Cyber-attack prediction, cyber events, big data, time series, forecasting, and intrusion detection.

I. INTRODUCTION

Cybersecurity threats are constantly evolving, with cyber criminals devising new strategies to bypass existing security measures. Big data is rapidly developing into an essential instrument for detecting and recognizing intrusions due to the abundance of data coming from many sources, such as sensor data, traffic on IP, system and network traffic logs, and Internet of Things traffic.

Massive volumes of unstructured data may be collected, managed, and analyzed by integrating big data with machine learning and artificial intelligence. This improves the capacity to recognize and stop fraudulent activity. Because of their complexity, it is still difficult to accurately forecast these attacks. Traditional security methods are being replaced by predictive techniques designed to recognize and address complex threats. The cost of cyber attacks continues to rise, with data breaches averaging a loss of $4.35 million and an average detection and response time of 277 days.

Grenze ID: 01.GIJET.12.1.129
© Grenze Scientific Society, 2026

Advanced Persistent Threats (APTs) are sophisticated techniques used by organized cybercriminals to evade detection. Predictive methodologies for cyber attack forecasting are still developing, enabling teams to allocate technical resources more efficiently and focus on immediate threats to prevent data breaches.

II. Literature review

In 2022, several studies were published, including Almahmoud et al.'s AI-driven approach for proactive cyber threat forecasting, which improved prediction accuracy through comprehensive data integration. However, challenges related to complexity and computational demands arose. Ullah et al. introduced a hybrid deep learning architecture combining CNN and LSTM for IoT intrusion detection, which achieved high detection accuracy but was computationally expensive. Nagaraj et al. focused on using machine learning models to predict cyber attacks, showing promising results but limited generalizability across different cyber threats. Gao et al. developed a self-learning spatial distribution-based IDS, effective in dynamic industrial systems but less applicable to other environments. Goyal et al. applied machine learning to web signals for early cyber attack detection, but the approach was hampered by high false-positive rates due to noisy data. Singh & Govindarasu utilized the Cyber Kill Chain model in a hybrid IDS for smart grids, offering comprehensive threat coverage but requiring complex deployment and maintenance. Werner et al. employed time series forecasting with ARIMA-based models to predict cyber attack intensity. In 2023, Devan et al. introduced a hybrid model combining XGBoost and DNN for network intrusion detection, achieving high accuracy but at the risk of overfitting and high computational costs. Shurman et al. presented a hybrid IDS designed to prevent DoS attacks in IoT environments, effective but constrained by resource limitations. By 2024, new approaches had been developed, including the use of SARIMA and ARIMA models in cybersecurity by Valipour et al., social media analysis and crowdsourcing by Khandpur et al. for early cyber attack detection, and quick forecasting of cyber events by Yussuf Ahmed et al. with the help of machine learning-enabled features.

III. Related work

The availability of advanced technologies and sophisticated attacks by groups associated with organized crime and state actors have led to a rise in both the volume and number of data breaches in recent years. To address these security concerns, the scientific community and industry have been collaborating to develop solutions, especially in terms of improving the accuracy of cyber event prediction. This paper advances existing information by forecasting cyberattacks based on certain cyberevents and network properties.

A. Intrusion Detection

Cyber attacks have increased the need for various technologies to detect and stop them, including firewalls, intrusion prevention systems, intrusion detection systems (IDS), SIEMS, and anti-virus software. These techniques can cause false alarms and are difficult to identify sophisticated attacks with precision. There are two main categories of intrusion detection systems: signature-based and anomaly-based. Network intrusion detection systems (NIDS), host intrusion detection systems (HIDS), and hybrid intrusion detection systems are the three main categories. NIDS, like Zeek and Snort, analyze network traffic to identify irregularities and produce security alerts. HIDS, installed on critical systems, generate alerts when anomalies are found. Correlating HID data with other monitoring tools helps prioritize risks.

B. Forecasting and Predictions

Researchers are increasingly focusing on cyber attack predictions due to increased interest in the subject. Their work includes machine learning models and survey reports, primarily focusing on sentiment analysis based on social media feeds. Data breaches spanning over 12 years have been used to predict cyber attacks, finding that while the number of attacks is increasing, their size is not. Machine learning has also been used to estimate the cost of cyber intrusions. A probabilistic model has been suggested to help incident responders anticipate potential malware features after discovery. Another approach uses scoring and network entity reputation systems to detect possible attackers. The data-driven approaches used by researchers in the rapidly developing field are being analyzed to analyze current research orientations and identify challenges and potential directions for the future of this discipline.

C. ARIMA

This study looks at ARIMA, a statistical technique that uses time series data to predict future trends.In order to enhance forecasts, it contrasts exponential smoothing (ETS) with ARIMA. The research uses measures like

RMSE and MAE to compare ARIMA with other forecasting methods, such as pressure and humidity forecasting. ARIMA models have been applied to forecast cyberattacks in the future by analyzing historical data. The study found that the environment and study direction affect their success. The authors also presented a time series method for forecasting data breaches using recurrent neural networks and seasonal autoregressive integrated moving averages. The study found that the SARIMA model outperformed ARIMA in predicting yearly runoff. ARIMA is a reliable statistical technique, but steady data is needed.

D. Linear Regression and SMOreg

This program assesses and forecasts the correlation between two characteristics [14]. There are usually two types of variables involved: dependent and independent. Regression difficulties may be handled with SMOreg's SVM-based approach, which works especially well for modeling and prediction with non-linear data [15].

E. Deep Learning

A machine learning method called deep learning (DL) makes use of several layers, one of which is hidden, in order to learn from feature representations. It is employed in many different applications, including malware detection, internet attacks, and cyberattack detection in industrial control systems. CNN-based algorithms have been developed for various applications, including industrial control systems, online assaults, and malware identification. References have also improved intrusion detection and CNN and LSTM approaches using DL techniques for intrusion detection and intrusion detection systems. A deep learning method for identifying cyberattacks, including LSTM, RNN, and Multilayer Perceptrons, has shown a 93% accuracy rate.

IV. ADVISED CYBER-EVENT PREDICTION MODEL

This study proposed a time series-based cyber incident forecasting methodology. Due to the complexity of cyberattacks, this model aims to help predict when they could occur.

Security teams and senior management will be able to develop measures that safeguard their network systems with the aid of the proactive techniques. We made advantage of a publicly accessible dataset that was gathered from an actual secure network and had many attack labels. Of the dataset, 64% is benign, 18% is brute-forced using SSH, and 18% is brute-forced using FTP.

Although the dataset for the three labels was collected We primarily focused on the 24-hour version of the dataset throughout the course of five days. After then, we sampled the data every 30 seconds, yielding 79 characteristics and 1,048,575 observations. After that the data was split into training sets and test sets. This study aims to predict cyber events, or assaults that are expected to occur in the future within a period of given time range due to a fusion of specific events and attributes. Figure 1 shows the forecasting process together with other stages of data preparation.

A. Data Preparation

Our dataset, CSE-CIC-IDS2018, was generated from a real-world network [17]. The processes needed to prepare and experiment with datasets are shown in Figure 1: The steps involved in this process are (i) dataset extraction and selection of relevant features; (ii) categorization; (iii) forecasting using time series; and (iv) evaluate the performance.

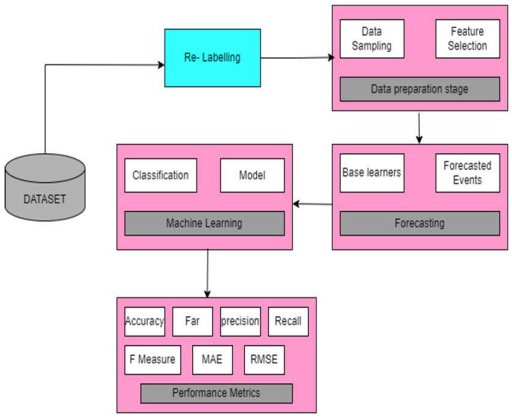

Figure 1. Forecasting stages.

There were 79 features and 1,048,575 observations in the dataset. A 30 s time period was used to pick the data, yielding 1084 observations and 79 characteristics. To ensure that the time-series data were steady, they were reviewed.

B. Attack Classification

The observations were classified and categorized using supervised learning. Once the predicting was finished, the attacks were classified. We used well-known classification methods as random forest, k-NN, Naive Bayes, Bayes Net, and Support Vector Machine (SVM).

C. Feature Selection

To find out which of these qualities was most relevant to our model, features were selected. A number of feature selection techniques were examined, including OneR, Gain Rate (GR), and Information Gain (IG). After that, the top 21 features were chosen using the Informational Gain (IG) attribute selection method. These traits were selected based on how effectively they enhanced and rated the model. Training and test were the two groups into which the data set was separated. 100 data points were designated as test after the first 884 were categorized as training.

V. SETUP FOR EXPERIMENT

The dataset CSE-CIC-IDS2018 was utilized, incorporating time series forecasting and data resampling techniques. The main dataset comprised seven different types of assaults: DDoS, web attacks, brute force, botnet, infiltration, DDoS, and heartbleed. A 24-hour sample of data, specifically comprising SSH & FTP-Bruteforce, and Benign traffic, was the focus of the analysis. There were 50 machines in the assault network, compared to 30 servers and 450 PCs spread across five departments in the network under monitoring. Data from all hosts on the network, including log files and internet traffic data, were gathered.Time series data was collected at consistent 30-second intervals, yielding a total of 1,084 observations. Within these findings, the ratio of benign to cyberattack incidents was 34% and 66%, respectively.

Machine learning models were applied to predict future values of the dataset's features, leveraging historical feature values to explore possible causal relationships. These future predictions could offer insights into the likelihood of an attack and inform proactive mitigation strategies. .

A. Experiment Overview

In order to assess how well the anticipated events performed, a baseline classification was used at the beginning of the trial. After then, time-series forecasting was done to evaluate the model's performance even more. The sections that follow go over the findings of these tests.

B. Baseline Classification

The dataset was condensed to 1,084 observations during the data preparation stage. Of them, 200 were reserved for testing, while the remaining 884 were used for baseline training. To complete classification tasks, the baseline data was subjected to a variety of classification algorithms, such as Random Forest, KNN, SVM, Naive Bayes, and BayesNet. This functioned as a reference point to evaluate the accuracy of cyber event forecasts. As can be seen in Table 1, the random forest algorithm produced the best results, with an accuracy of 99.2%. With accuracy percentages of 98.9% and 98.1%, respectively, KNN and Naive Bayes came next. To assess the models even more, other performance indicators were used; these will be covered in more depth in the section on assessment metrics.

TABLE I. BASELINE ACCURACY SCORES.[3]

Classifier	Accuracy (score %)	FAR (%)	Precision (%)	Recall (%)	F-measure (%)
Bayesnet	95.4	0.2	96.8	95.5	95.8
Naive Bayes	98.2	0.5	98.3	98.1	98.2
K-NN	98.9	0.1	98.8	98.9	98.9
SMO	97.6	0.5	97.8	97.7	97.8
Random Forest	99.1	0.1	99.4	99.2	99.3

C. Classification with Forecasted Values

Time series forecasting was conducted on the predicted features, comprising 200 observations, using both linear regression and SMOreg. Subsequently, as presented in Tables 2 and 3, Different categorization techniques were used to categorize the anticipated occurrences. Time series events were first forecasted using linear regression as

the basis for the categorization method. According to the findings, which are shown in Table 2, SVM and random forest were the classifier which were best-performing, with accuracy ratings of 90.3% and 89.5%, respectively. closely followed by KNN. Next, the time series events predicted by SMOreg were classified once again using the same set of techniques. SVM and random forest again led the results, with accuracy scores of 90.

TABLE II. FORECASTED FEATURES WITH LINEAR REGRESSION (LNRG) [3]

Base Learner	Classifier	Accuracy Score (%)	FAR (%)	Precision (%)	Recall (%)	F-Measure (%)
LNRG	Bayesnet	87.4	1	86.5	87.4	86.3
LNRG	Naive bayes	87.5	1	86.6	87.5	86.4
LNRG	K-NN	89.5	2	89.9	89.5	88
LNRG	SVM	90.3	2	91.3	90.3	88.9
LNRG	Random Forest	90.3	1	91.3	90.3	88.9

TABLE III. SORTING BASED ON EXPECTED ATTRIBUTES WITH SMOREG

Base Learner	Classifier	Accuracy Score (%)	FAR (%)	Precision (%)	Recall (%)	F-measure (%)
SMOreg	Bayesnet	87.5	1	86.6	87.5	86.4
SMOreg	Naive bayes	87.5	2	86.7	87.6	86.5
SMOreg	K-NN	89.6	2	90	89.6	88.1
SMOreg	SVM	90.6	2	91.3	90.4	89
SMOreg	Random Forest	90.4	1	91.3	90.4	89

Linear and sequential minimal optimization regression are referred to here as LNRG and SMOreg, respectively.

D. Comparing the Performance of Forecasted and Baseline Data

The random forest classification of the baseline characteristics showed a very high correctness of 99.2%. On the other hand, the predicted data using SVM and SMOreg random forest classification time series data had a maximum classification accuracy of 90.4%. Comparison with the feature categorization baseline shows a little decline in performance, according to research. Nonetheless, considering the anticipated character of the occurrences and the constraints imposed by the dataset's magnitude, this decrease is anticipated.

Figure 3 displays the classification results between the predicted features of (SMOreg) and (LNRG). Random Forest and SVM performed better than LNRG, with a classification rate of 90.4%.

The performance accuracy of the projected data produced by SMOreg and linear regression, as well as the baseline characteristics, are shown in Figure 4. The time series projected characteristics yielded an accuracy of 90.4%, which is strong prediction capacity even if it was somewhat less than the baseline. Security experts and IT managers may find this accuracy useful in anticipating cyber events and putting precautionary measures in place before such assaults.

E. Resampling Time Series and Predicted Events Interaction

The initial dataset of 1,048,575 observations was reduced to 1,084 observations using time-series forecasting at 30-second intervals. Of these, 200 were reserved for testing and 884 were used for training. Models like SMOreg, LSTM, and linear regression were then used to anticipate the following 200 occurrences. These basic learners were shifted around in order to anticipate potential cyber concerns.

The following step evaluated the effectiveness of many machine learning classification techniques, including random forest, KNN, SVM, and Naive Bayes. Performance metrics such as Absolute Mean Error (MAE) and Root Mean Square Error (RSME) were also employed to assess the models' effectiveness.

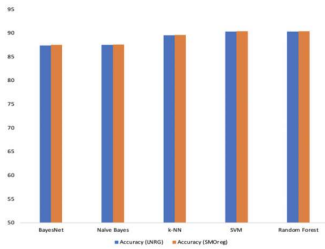

Figure 3. Comparing the projected features of Linear Regression (LNRG) and Sequential Minimal Optimization for Regression (SMOreg) for classification [3].

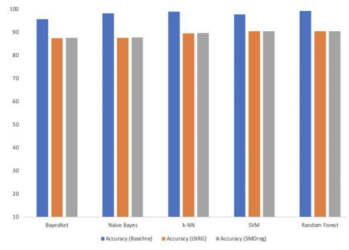

Figure 4. Comparing baseline Linear Regression (LNRG) with Sequential Minimal Optimisation for Regression (SMOreg) projected features for classification [3].

F. Parameters of Time Series Forecasting

As explained in Section 4.3, the experiment comprised forecasting cyber incidents using the following base learners: LSTM, SMOreg, and linear regression are the three methods. The next step was to use each of the previously specified base learners to anticipate 200 occurrences. For each model, the following describes the parameters used in the forecasting experiment:the default value was chosen for (i) ridge; (ii) eliminateColinearAttributes; and (iv) attributeSelectionMethods, which set to M5 methods. The c value was set 2.0, the kernel was set to PolyKernel, the RegOptimizer was set to RegSMO Improved, and the filetype was set to normalize training data in SMOreg. The activation function in LSTM was set to ActivationReLU, the number of outputs to 3, and the gate activation function to Activation Sigmoid

VI. PERFORMANCE EVALUATIONS

A number of machine learning classification techniques were used to assess the model's efficacy. Additional metrics used to evaluate the accuracy of the anticipated data were Measured absolute error (MAE) and roots of mean square errors (RMSE) charts.

A. Performance Metrics

In this experiment, the model was evaluated using various performance metrics, including False Alarm Rate (FAR), F-measure, accuracy, precision, and recall. Precision is a measure of the proportion of accurately classified attacks to cases identified as positive attacks, whereas accuracy shows the overall performance of the model. Recall shows how well the model was able to recognize every pertinent occurrence. In addition, the accuracy of the projected data was evaluated using Mean Absolute Error (MAE) and Root Mean Square Error (RMSE).

A thorough examination of the performance metrics, including the baseline data's classification accuracy and the predicted features generated by SMOreg and linear regression, is given in Tables 1-3. With a high precision of 99.2% and small FAR of 0.1% to 0.5%, the baseline characteristics offer exceptional accuracy in evaluation measures. However, the expected data indicates a little increase FAR of 1% to 2%. The greatest performance was shown by the SMOreg base learner, which projected data accuracy of 90.4%.

The number of incursions that are successfully detected as assaults is called True Positive (TP), while the number of regular occurrences that are correctly identified as innocuous packets is called True Negative (TN). False Positive (FP) represents the number of typical occurrences that are mistakenly classified as assaults, whereas False Negative (FN) depicts the number of incursions that are mistakenly labeled as benign packets.

B. Absolute Mean Error (MAE)

To evaluate the accuracy of the time series projected data, this experiment employed the Mean Absolute Error (MAE) approach. Results from the MAE computations are shown in Table 4. SMOreg, LSTM, and linear regression were used to obtain the top five predicted attributes, which are displayed in this table. With the lowest MAE value, the SMOreg predicted data outperformed the LSTM and Linear Regression predictions, according to the findings. However, it's crucial to keep in mind that linear regression yielded roughly comparable results. The equation below displays the MAE formula as given in [21].

$$MAE = \left(\frac{1}{n}\right)\sum_{i=1}^{n}|y_i - x_i| \qquad \text{.....(6)}$$

Herein, *yi* = prediction, *xi* = true value and *n* = total no of data points

TABLE IV. ABSOLUTE MEAN ERROR

Target Features	Linear regression	SMOreg	LSTM
Total Fwd pkts	0.0105	0.0038	2.6127
Tot bwd pkts	0.0034	0.0025	0.4981
Pkts len min	0.0002	0.008	0.0054
Fwd seg size min	0.4912	0.0183	0.0484
Subflow bwd bytes	0.718	0.7251	31.9957

C. Root Mean Square Error (RMSE)

When assessing a model's prediction accuracy, the Root Mean Square Error is employed (RMSE), which is computed as the difference between expected and actual values. To calculate the root mean square error

(RMSE), one must first determine how the values differ from one another, square those differences, and then get the mean, as seen in Equation (2)[19]. Using LSTM, SMOreg, linear regression, and an RMSE measure, Table 5 evaluates the performance of the top five predicted features. The results show that the projected data acquired using linear regression beat SMOreg and LSTM forecasts somewhat in three of the top five characteristics with the lowest RMSE value.

TABLE V. ROOT SQUARE MEAN ERROR

Target Features	Linear regression	SMOreg	LSTM
Tot Fwd pkts	0.0129	0.0045	2.8946
Tot bwd pkts	0.0039	0.003	0.5842
Pkts len min	0.0002	0.0096	0.0063
Fwd seg size min	0.0198	0.8776	0.0497
Subflow bwd bytes	0.8163	1.269	35.0395

D. Analysis of the Results

The original dataset was first utilized in this experiment to provide a baseline from which the data was classed. The baseline classification results are shown in Table 1, where random forest was found to have the lowest False Alarm Rate (FAR) of 0.1% and the greatest accuracy of 99.2%. k-NN finished in second place with an accuracy rate of 98.9%, closely followed in third and fourth place by SMO, Naive Bayes, and BayesNet. We subsequently classified the expected events. Using linear regression methods, we began categorizing the expected properties. With the best classification accuracy of 90.3%, just shy of the baseline, was the SVM and random forest predicted cyber event. Table 2 shows that k-NN, Naive Bayes, and BayesNet had scores that were closely behind this, at 89.5%, 87.5%, and 87.4%.

The RMSE and MAE measures were then used to evaluate the time series-forecasted occurrences.The MAE study's conclusions showed that SMOreg's anticipated events performed better than those of LSTM and linear regression. More precisely, Fwd Seg Size Min, Tot Bwd Pkts, and Tot Fwd Pkts are the three out of the five specified qualities that SMOreg performed better, as shown in Table 1. Performance is better when the MAE score is lower. The predicted events using linear regression came in second place, outperforming the other two base learners in two of the top five categories. The anticipated events of linear regression had the best prediction accuracy when examined using RMSE in three of the top five characteristics; however, as Table 2 shows, the forecasted events of SMOreg ranked second in two of the top five features. LSTM outperformed SMOreg and linear regression, according to both MAE and RMSE evaluations. Security teams use these data extensively to assess the model's accuracy and predict possible threats. This makes it possible to implement defenses against assaults early on.

VII. CONCLUSIONS AND FUTURE WORK

The original dataset was first utilized in this experiment to create a classification baseline. According to Table 1, the random forest model had the lowest False Alarm Rate (FAR) of 0.1% and the maximum accuracy of 99.2%. With a 98.9% accuracy rate, k-NN came in second, followed by SMO, Naive Bayes, and BayesNet in third and fourth place. Subsequently, the anticipated events were classified. SVM with random forest had the best classification accuracy of 90.3% for characteristics predicted by linear regression, but somewhat below the baseline. Table 2 shows that k-NN has accuracy of 89.5%, Naive Bayes has precision of 87.5%, and BayesNet has correctness of 87.4%.

Using SMOreg for prediction, SVM and random forest outperformed linear regression but still couldn't match the baseline's best accuracy of 90.4%. The accuracy rates of k-NN is 89.6%, Naive Bayes is 87.6%, and BayesNet is 87.5%, as presented in Table 3. The time series projections were assessed using the RMSE and MAE criteria. Based on MAE, the results showed that SMOreg performed better than LSTM and linear regression in three of the five criteria. In three characteristics, linear regression produced the best RMSE values, with SMOreg coming in second in two. SMOreg and linear regression both performed better than LSTM. These metrics aid security teams in evaluating the accuracy of the models and improving early intervention tactics to stop threats.

REFERENCES

[1] A. Almahmoud, S. Ali, and F. Khan, "Proactive Cyber Threat Forecasting Using AI Techniques," Proc. of International Conf. on Cybersecurity, 2022, pp. 1-10.

[2] S. Ullah, Z. Baig, and A. Ghanbari, "Hybrid Deep Learning Architecture for IoT Intrusion Detection," IEEE Trans. on Information Forensics and Security, vol. 17, no. 4, pp. 320-330, 2022.
[3] P. Nagaraj, T. Wu, and X. Chen, "Machine Learning for Cyber Attack Forecasting," Journal of Cyber Security and Privacy, vol. 3, no. 1, pp. 23-30, 2022.
[4] L. Gao, R. Zeng, and F. Zhou, "Self-Learning Spatial Distribution-Based IDS for Cyber-Physical Systems," IEEE Internet of Things Journal, vol. 9, no. 3, pp. 212-221, 2022.
[5] A. Goyal, M. Kumar, and D. Prasad, "Early Cyber Attack Detection Using Web Signals," Journal of Network and Computer Applications, vol. 200, pp. 102880, 2022.
[6] K. Singh and M. Govindarasu, "Hybrid IDS for Smart Grids Using the Cyber Kill Chain Model," IEEE Access, vol. 10, pp. 114502-114514, 2022.
[7] M. Otoum and S. Nayak, "Anomaly and Signature-Based IDS for IoT," IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 212-222, 2022.
[8] S. Werner, A. Bhosale, and K. Nam, "Time Series Forecasting of Cyber Attack Intensity," Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 310-319, 2022.
[9] R. Devan, M. K. Gupta, and A. Verma, "XGBoost-DNN Hybrid Model for Network Intrusion Detection," IEEE Systems Journal, vol. 17, no. 1, pp. 310-320, 2023.
[10] M. Milajerdi, A. Akbanov, and N. Kaghazgaran, "Real-Time APT Detection via Suspicious Information Flow Correlation," Proceedings of IEEE Conference on Dependable Systems and Networks (DSN), pp. 501-510, 2023.
[11] M. Valipour, A. Eslami, and F. Mahmood, "Application of SARIMA and ARIMA Models in Cybersecurity," Journal of Cyber Security and Privacy, vol. 5, no. 2, pp. 100-110, 2024.
[12] K. Khandpur, R. Patel, and S. Rao, "Cyber Attack Detection Using Social Media and Crowdsourcing," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 310-320, 2024.
[13] Y. Ahmed, N. K. Ali, and A. F. Tariq, "Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 310-319, 2024.