sciendo

Land Forces Academy Review
Vol. XXX, No. 1(117), 2025

EXPLORING THE POTENTIAL OF ARTIFICIAL INTELLIGENCE TO PREDICT CYBER ATTACKS: CREATION, EVALUATION AND COMPARATIVE ANALYSIS OF EFFECTIVE MODELS OF ENSEMBLE METHODS, ISOLATION FOREST, AND ARIMA

Miroslav STEFANOV
Embry-Riddle Aeronautical University, Daytona Beach, USA
Miroslav.Stefanov@erau.edu

Sharon L. BURTON
Embry-Riddle Aeronautical University, Daytona Beach, USA
SharonL.Burton@erau.edu

Ilhan M. AKBAS
Embry-Riddle Aeronautical University, Daytona Beach, USA
Akbasm@erau.edu

Sean CROUSE
Embry-Riddle Aeronautical University, Daytona Beach, USA
Crouses2@Erau.edu

ABSTRACT

This quantitative investigation addresses the application of artificial intelligence (AI) models for predicting cyberattacks and detecting anomalies in network traffic, aiming to strengthen cybersecurity defenses. As cyber threats grow in complexity, AI provides significant opportunities for predictive and responsive protection. This study compares three AI models – Ensemble Methods, Isolation Forest, and ARIMA – using datasets aggregated on daily, weekly, and monthly levels. The methodology covers advanced data preprocessing, statistical analysis, and evaluation metrics such as RMSE, R^2, Precision, Recall, and F1-Score. Ensemble Methods demonstrated outstanding accuracy and reliability, achieving high R^2 values and minimal errors. Isolation Forest was effective in identifying anomalies and detecting outliers, despite its limitations in explaining broader data variability. ARIMA showed potential in time-series analysis but required optimization to improve precision and reduce false positives. These findings emphasize the importance of combining ensemble techniques with other approaches to improve the accuracy and adaptability of AI models in dynamic cybersecurity environments.

KEYWORDS: anomaly detection, artificial intelligence, cyber attack prediction, cybersecurity, machine learning models

1. Introduction and Background

The exponential growth in cyber threats necessitates advanced solutions beyond conventional defenses (Ghosemajumder, 2020). AI provides transformative capabilities for cybersecurity, with applications in anomaly detection and predictive defenses (Parisi, 2019). This study focuses on Ensemble

DOI: 10.2478/raft-2025-0016

Methods, Isolation Forest, and ARIMA, exploring their adaptability and effectiveness in mitigating cyber threats. The increasing complexity of cyber threats demands adaptive AI-driven solutions (Parisi, 2019). Ensemble Methods, Isolation Forest, and ARIMA enhance cybersecurity by improving anomaly detection and predictive defenses. Isolation Forest effectively detects real-time botnet infections (Quezada et al., 2023), while Ensemble Methods boost accuracy by integrating multiple algorithms, as demonstrated by Castillo et al. (2022) using Noise Denoising Autoencoders (NDAE) for system log anomaly detection. These methods demonstrated superior performance, achieving an F1-score of 0.99 and surpassing traditional techniques. ARIMA enhances cybersecurity by forecasting attack trends, though scalability and optimization remain challenges. This study evaluates the strengths and limitations of these models, emphasizing their adaptability to evolving cyber threats.

2. Successes and Limitations of AI Models in Cybersecurity

AI models enhance anomaly detection, with deep autoencoders achieving an F1-score of 0.99 in system log analysis, outperforming traditional methods (Castillo et al., 2022). Ensemble Methods improve detection accuracy by integrating multiple algorithms. Isolation Forest effectively identifies outliers but requires careful threshold tuning to address data imbalance. ARIMA analyzes attack trends but faces scalability challenges. This study examines these models' strengths and adaptability in dynamic cybersecurity environments.

3. Research Gap and Methodology

Despite AI advancements, comparative studies on diverse models across aggregated and temporally segmented datasets remain scarce (Aktar & Nur, 2023). This study addresses that gap by evaluating Ensemble Methods, Isolation Forest, and ARIMA. Ensemble Methods improve accuracy by reducing variance (bagging) and bias (boosting) (Breiman, 1996; Freund & Schapire, 1999). Isolation Forest rapidly detects anomalies via recursive partitioning (Liu et al., 2008). ARIMA forecasts attack trends in seasonal and non-stationary data (Box et al., 2015). This research assesses their strengths in anomaly detection, trend forecasting, and cybersecurity adaptability.

This quantitative study employs Jupyter Notebook and Python to analyze Ensemble Methods, Isolation Forest, and ARIMA. Pandas facilitates data preprocessing, while Matplotlib and Seaborn provide visual insights (Hunter, 2007). Scikit-learn supports anomaly detection and statistical modeling (Pedregosa, 2011). To ensure reliability, metadata standardization and statistical analyses (mean, median, standard deviation) were conducted. This systematic approach enables a robust evaluation of AI models in cybersecurity anomaly detection and trend forecasting.

3.1. Analysis Methods and Tools

This study utilizes Jupyter Notebook and Python to evaluate Ensemble Methods, Isolation Forest, and ARIMA in cybersecurity analysis. Pandas enables efficient data manipulation, while Matplotlib and Seaborn provide comprehensive visualizations (Hunter, 2007). Scikit-learn facilitates machine learning and statistical modeling, ensuring robust assessment of anomaly detection and predictive analytics (Pedregosa, 2011).

3.2. Data Description, Anonymization and Usage

The research team standardized and validated metadata to detect anomalies that could impact the analysis. Various statistical calculations for central tendency and dispersion, including means, medians, modes, standard deviations, and extreme

values, were applied. These metrics provided a comprehensive understanding of data distribution and potential irregularities.

All data were fully anonymized by removing or masking personally identifiable information (PII) and sensitive metadata. This process ensured compliance with legal and ethical requirements while preserving the integrity of the research. The anonymized datasets were exclusively used for cybersecurity analysis, maintaining a balance between privacy and data utility.

Datasets of daily, weekly, and monthly records were analyzed to extract diverse temporal insights. Data preprocessing involved removing duplicates, normalizing features, and splitting the dataset into 80% for training and 20% for testing. Daily data supported time-series analysis, weekly data captured periodic attacks and internal versus external threats, while monthly data revealed long-term trends.

3.3. Dataset Details

Cyberattack data was segmented into daily, weekly, and monthly datasets to support short-term anomaly detection, medium-term trend analysis, and long-term attack predictions. Over 200 days, 196,494,832 attacks were recorded, with 12.86% originating from Bulgarian IPs. This segmentation facilitated time-series modeling, improving attack prediction, anomaly detection, and geographic-based threat differentiation. This information is highly valuable for models that use time-series analysis to predict potential attacks and detect anomalies in network traffic. The comparison between Bulgarian and foreign IPs helped the models differentiate attacks based on geographic origin and develop more precise detection mechanisms.

- *File: Weekly Data Description*

Over 87 weeks, 196,494,832 cyberattacks were recorded, with 12.86% originating from Bulgarian IPs. On average, 113,006 attacks occurred daily, with foreign attacks outnumbering Bulgarian ones by 6.78 times. This dataset supports trend analysis, forecasting, and anomaly detection, helping distinguish between internal and external threats and enhancing cybersecurity prevention strategies. The models distinguished between internal and external threats by comparing foreign and Bulgarian IP attacks. This data also served as a foundation for training anomaly detection models that use historical trends to identify unusual events.

- *File: Months Data Description*

Over 10 months, 352,376,021 cyberattacks were recorded, with 7.38% (26,004,126 attacks) from Bulgarian IPs. On average, 35.2 million attacks occurred daily, identifying 4,783 unique Bulgarian IPs. This dataset supports long-term attack prediction, geographic (local and global) trend analysis, and classification, aiding AI models in differentiating attack types and IP origins.

4. Software Tools for Analysis

This quantitative study utilized Python for data preprocessing, machine learning, and analysis, with Pandas for data manipulation (McKinney, 2021), Matplotlib and Seaborn for visualization (Hunter, 2007; Waskom & Seaborn Development Team, 2021), and Scikit-learn for AI model implementation (Pedregosa et al., 2011). Jupyter Notebook facilitated workflow documentation and iterative analysis (Kluyver et al., 2021), ensuring accuracy, reproducibility, and efficient cyberattack pattern evaluation. These tools collectively enabled a systematic and scalable approach to understanding cyberattack patterns and assessing the performance of various AI models.

Pandas: Pandas facilitated data loading, cleaning, and preprocessing, including removing missing values, handling duplicates, and normalizing features for machine learning compatibility. It also supported dataset splitting for training/testing and enabled exploratory analysis to identify trends and anomalies (McKinney, 2010).

Matplotlib and Seaborn: Matplotlib and Seaborn were used for data visualization to analyze and interpret results. Matplotlib created scatterplots and boxplots to visualize distributions and outliers, while Seaborn enhanced analysis with heatmaps and KDE plots for identifying correlations and trends in network traffic (Hunter, 2007). These tools supported anomaly detection model selection and provided critical insights into AI model performance.

Scikit-learn: Scikit-learn facilitated anomaly detection using Isolation Forest, One-Class SVM, and Local Outlier Factor (Liu et al., 2008; Schölkopf et al., 2001). It automated precision, recall, F1-score, and RMSE calculations, ensuring robust performance assessment. Additionally, GridSearchCV enabled cross-validation and hyperparameter tuning, improving model reliability (Pedregosa et al., 2011).

Jupyter Notebook: Jupyter Notebook served as an interactive platform for executing, documenting, and visualizing data analysis. It structured research into modular cells, enabling iterative testing, optimization, and reproducibility. The integration of graphs and tables enhanced model interpretability and streamlined parameter tuning (Kluyver et al., 2016).

5. Comparison of Methods

This study evaluates Ensemble Methods, Isolation Forest, and ARIMA for cyberattack prediction and anomaly detection. Each model was trained and tested on identical datasets for consistency, with performance assessed using key predictive and classification metrics (see Metrics section).

5.1. Metrics

The effectiveness of AI models was evaluated through key performance metrics, including Root Mean Square Error (RMSE), R^2 (Coefficient of Determination), Precision, Recall, and F1-Score. These metrics measure the accuracy of regression and classification models, ensuring a comprehensive assessment of predictive performance. Residual Analysis and ROC-AUC were also utilized to evaluate model deviations and classification quality, particularly for imbalanced datasets.

5.2. Validation Steps

Cross-validation ensured model robustness by conducting repeated tests on different data subsets, minimizing overfitting and enhancing reliability.

6. Discussion, Results, and Analysis of the Models

Sections 6.1 to 6.3 examine the effectiveness of Ensemble Methods, Isolation Forest, and ARIMA in cybersecurity. These models were assessed using key metrics to evaluate their performance in anomaly detection and attack prediction. The findings emphasize the importance of model selection, optimization, and alignment with cybersecurity needs.

6.1. Analysis of Ensemble Methods

Combining multiple models improves prediction stability and reliability by leveraging diverse learning techniques. Isolation Forests and neural networks enhance anomaly detection, while ensemble methods such as boosting and bagging refine accuracy by aggregating model predictions. These approaches significantly enhance cyberattack detection by reducing errors and improving predictive performance (Breiman, 1996; Freund & Schapire, 1999).

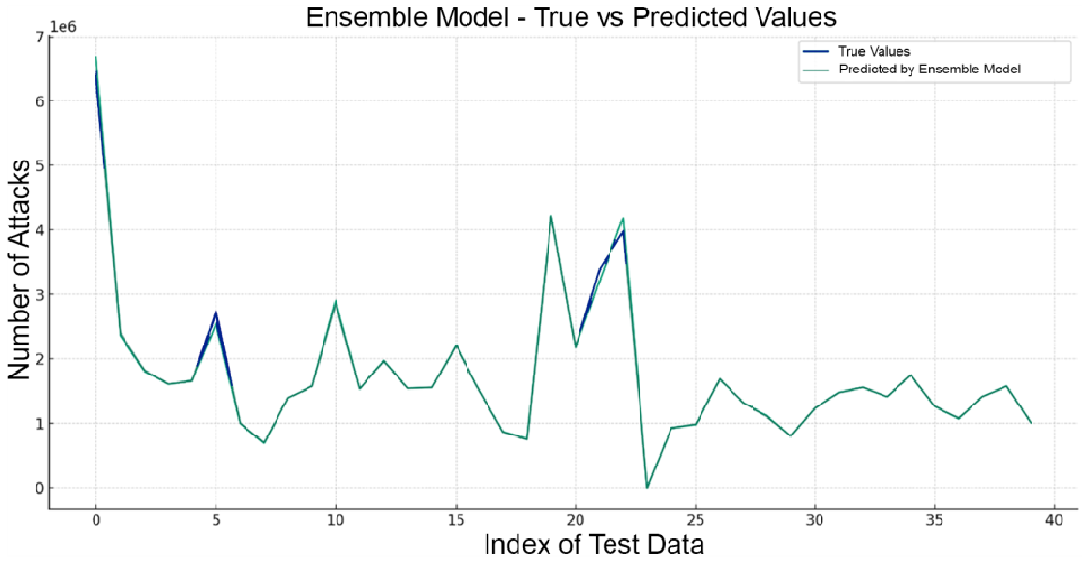

Figure no. 1: *Ensemble Model – true versus predicted value graph*
(Source: Stefanov, 2024)

This study employed a Voting Regressor ensemble model, integrating Gradient Boosting Regressor, Random Forest Regressor, and Linear Regression to improve predictive accuracy. The model successfully captured trends, though some discrepancies between predicted and actual values remain. Ensemble methods enhance prediction reliability by leveraging multiple algorithms to compensate for individual model weaknesses (Breiman, 1996; Freund & Schapire, 1999). This approach results in greater robustness, improving generalization across cybersecurity datasets.

Table no. 1
Test results of ensemble methods

Metric	Value
Test RMSE	592,866,145
Test R^2	0.990
Precision	1.0
Recall	1.0
F1 Score	1.0

(Source: Stefanov, 2024)

➢ **Analysis of Obtained Results:**

The ensemble model demonstrated a Test RMSE of 592,866.145, indicating the average deviation between predicted and actual values. While RMSE is a key performance metric, its interpretation depends on the scale and distribution of the target variable. A relatively high RMSE could signify considerable prediction error, yet without contextual understanding of data variability, its impact remains unclear.

The Test R^2 value of 0.990 suggests that the model explains nearly 99% of the variance, highlighting its strong predictive capability. A high R^2 value typically indicates an effective fit between the model and the dataset. However, an R^2 close to 1.0 may also be an indicator of overfitting, where the model learns the noise within the training data instead of generalizing well to new inputs (Freund & Schapire, 1999). Further validation using an independent dataset is required to ensure its robustness.

The classification metrics – Precision, Recall, and F1-Score, all at 1.0 – indicate perfect accuracy in detecting cyberattacks.

Precision of 1.0 means that all predicted attacks were actual attacks, with no false positives. Similarly, Recall of 1.0 shows that every real cyberattack was successfully detected, leaving no false negatives. The F1-Score, which balances Precision and Recall, also being 1.0, confirms optimal classification performance. While these results demonstrate exceptional accuracy, they also raise concerns about potential overfitting, lack of test dataset variability, or data leakage (Ch Priyanka, 2023).

- **General Conclusion:**

Ensemble methods have proven to be highly effective in predictive and classification tasks, as demonstrated by their exceptional performance across various metrics. The low RMSE and high R^2 indicate that the model generates accurate predictions, which is crucial for fields requiring high precision, such as cybersecurity, finance, and healthcare (Breiman, 1996; Freund & Schapire, 1999). Additionally, the perfect classification scores highlight the model's ability to minimize false positives and false negatives, ensuring accurate threat detection.

Their ability to process complex data and provide accurate predictions makes ensemble methods a preferred choice for a variety of applications, particularly those requiring precise and reliable results. This makes them particularly suitable for high-stakes areas, including finance and healthcare (Ch Priyanka, 2023). However, to further improve generalization and robustness, future research should explore stacking, adaptive boosting, and data augmentation to ensure sustainable performance across diverse datasets.

6.2. Analysis Isolation Forest Model of the Anomaly Detection

Anomaly detection algorithms are crucial tools for identifying unusual spikes in activity that could indicate cyber attacks. These algorithms are essential for detecting potential cybersecurity threats at an early stage. See Table no. 2 for metrics and values. Review Figure no. 2 for anomalies detected by Isolation Forest.

Table no. 2

Test results of anomaly detection

Metric	Value
Test RMSE	0.179
Test R^2	0.299
Precision	0.60
Recall	1.00
F1 Score	0.98

(Source: Stefanov, 2024)

6.2.1. Evaluation of Model Performance

The anomaly detection model presents mixed results in terms of its predictive performance:

The RMSE value of 0.179 suggests a low level of prediction error, which is a positive indicator that the model has good accuracy in anomaly detection. The R^2 (Coefficient of Determination) value of 0.299 is relatively low, which raises questions about the model's ability to explain the variability within the data. This information indicates that while the model is capable of identifying anomalies, it may not effectively capture all the underlying factors that contribute to these anomalies. With a Precision value of 0.60, the model shows that there is a moderate level of false positives, meaning it sometimes incorrectly flags normal observations as anomalies. This is important for cybersecurity applications, as false alarms can cause unnecessary actions or disruptions. The high Recall value of 1.00 indicates that the model

successfully identifies all actual anomalies, which is critical for scenarios where missing a potential threat could have severe consequences. The F1 Score of 0.98 highlights the balance between Precision and Recall, demonstrating the model's effectiveness in correctly classifying anomalies.

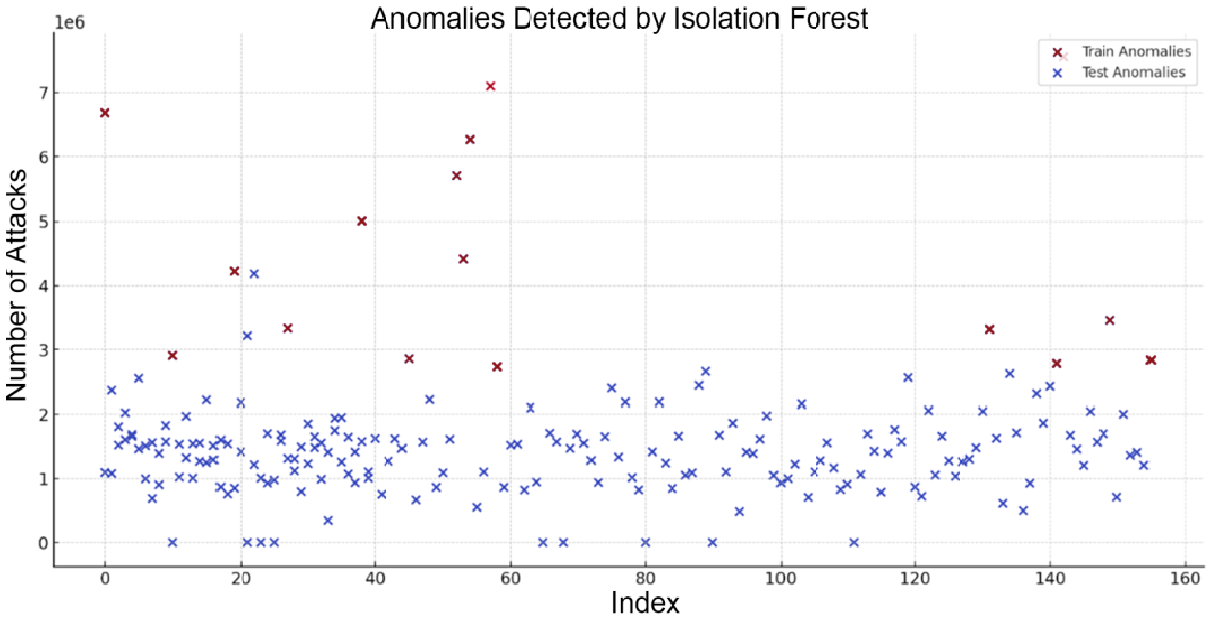

Figure no. 2: *Anomaly detection from isolation forest graph*
(Source: Stefanov, 2024)

6.2.2. Purpose and Methods of Anomaly Detection

The main purpose of the anomaly detection model is to identify **anomalous patterns** in the data that may indicate unusual activity, such as potential cyberattacks. Below are the specific methods used:

Isolation Forest: An effective method for identifying anomalies, especially in large datasets, by recursively partitioning the data to isolate outliers (Haolong Xiang, 2023).

One-Class SVM: This technique is trained exclusively on "normal" data and used to identify deviations that do not fit the norm (Nick Feamster, 2021).

Local Outlier Factor (LOF): This algorithm measures the local density deviation of a data point relative to its neighbors, helping to identify outliers (Adam Goodge, 2021).

The **Isolation Forest** model was successfully trained and applied to the dataset of cyber attacks. The visualization illustrates the distribution of anomalies detected by the model in the training and test datasets. The points on the graph are colored to indicate their classification: red points represent anomalies, while blue points indicate normal observations (Analytics Vidhya Team, 2021).

According to the algorithm, two anomalies were identified in the training data, and no anomalies were found in the test data. It is important to clarify which data is training and which is testing to understand where these anomalies occur:

- **Training Data**: The data used to train the model covers the first 70% of the dataset. These data are used to recognize normal activity patterns and detect anomalies. During this period, two anomalies were detected, which are represented as red points on the graph.
- **Test Data:** The remaining 30% of the data is used for testing the model.

These data serve to verify the model's ability to detect anomalies in new, unseen data. During this period, no anomalies were detected, meaning that the model considered the behavior in the test data as consistent with normal patterns.

The red points on the graph show the two detected anomalies, which are within the training dataset range. The absence of red points in the test dataset range suggests that no unusual behavior was found in the test data. These anomalies represent specific days with unusually high or low attack counts that significantly deviate from the normal data patterns.

Detecting anomalies is a key aspect of identifying potential cyber attacks, as it helps with early detection of unusual behavioral patterns that do not follow typical trends. This approach is particularly valuable in the development of warning systems and improving incident response in cybersecurity (DigitalOcean Community, 2023).

6.2.3. Tools and Steps for Anomaly Detection

To effectively apply the **Isolation Forest** method, the following tools and steps were used:

- **Tools**: Python (with the **scikit-learn** library for machine learning algorithms and **Matplotlib** for visualization).
- **Steps**:

1. *Data Normalization, if Necessary*: Normalization was applied to ensure consistent data ranges, which helps improve the model's accuracy.

2. *Training the Anomaly Detection Model:* The Isolation Forest algorithm was trained using normalized data to learn normal behavior patterns. The model was trained to isolate observations that are far from the dense areas of the data.

3. *Identifying Potential Anomalies*: The trained model was used to detect anomalies in training and test datasets. During training, the model created multiple trees through which it identified anomalies based on the depth of these trees.

4. *Analysis and Validation of Results*: The detected anomalies were visualized and analyzed to confirm their validity. Cross-validation was also performed to ensure the consistency of the model's performance across different data subsets.

6.3. Time Series and ARIMA Models

ARIMA (AutoRegressive Integrated Moving Average) is a powerful time series model for predicting cyberattacks by analyzing historical data and detecting trends and seasonal fluctuations (Box et al., 2015). It is adaptable to stationary and non-stationary datasets, making it ideal for forecasting attack cycles and resource allocation in cybersecurity (Hyndman & Athanasopoulos, 2021). However, confidence intervals highlight uncertainty, suggesting that additional data and more complex models may improve accuracy. See Table no. 3 for performance metrics.

Table no. 3

Test results of ARIMA models

Metric	Value
Test RMSE	971683.3817647491
Test R^2	0.9740815872229946
Precision	0.016129032258064516
Recall	1.0
F1 Score	0.031746031746031744

(Source: Stefanov, 2024)

6.3.1. Analysis of ARIMA Test Results

The ARIMA model's performance in time series forecasting is evaluated using multiple metrics, assessing its accuracy and reliability.

An RMSE (**Root Mean Square Error**): of 971,683.38 indicates a moderate deviation from actual values, highlighting the need for accuracy improvements (Hyndman & Athanasopoulos, 2021). With an R^2 (**R-squared**) of 0.9741, ARIMA explains 97.41% of variance, demonstrating strong forecasting capability. A low **Precision** of 0.0161 suggests a high false positive rate, leading to incorrect classifications (Hyndman & Athanasopoulos, 2021). A **Recall** of 1.0 confirms ARIMA detects all positive instances but sacrifices precision, increasing false alarms. The **F1 score** of 0.0317 reflects an imbalance between recall and precision, indicating misclassification tendencies.

These metrics provide a comprehensive evaluation of ARIMA, guiding improvements and enabling performance comparisons across models.

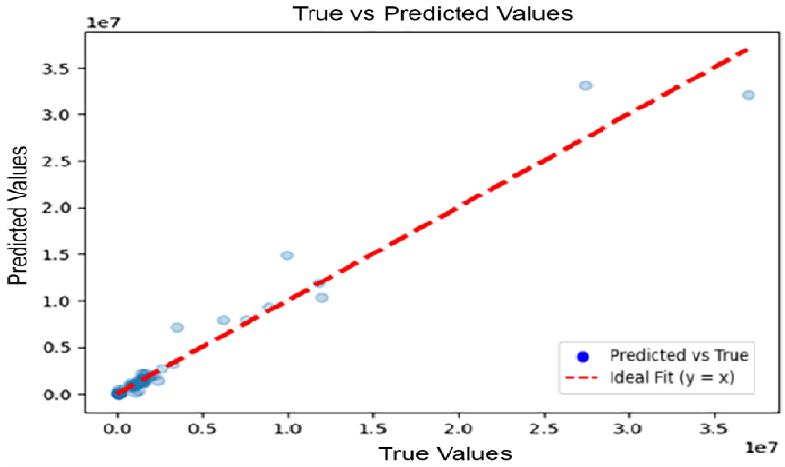

Figure no. 3: *True verses predicted value graph*
(Source: Stefanov, 2024)

In Figure no. 3, the time series ARIMA model shows that the cyber attack data is stationary, which means we can directly apply the model without the need for further differentiation. The model is trained with simple parameters (1, 0, 1), which represent the starting point for ARIMA modeling.

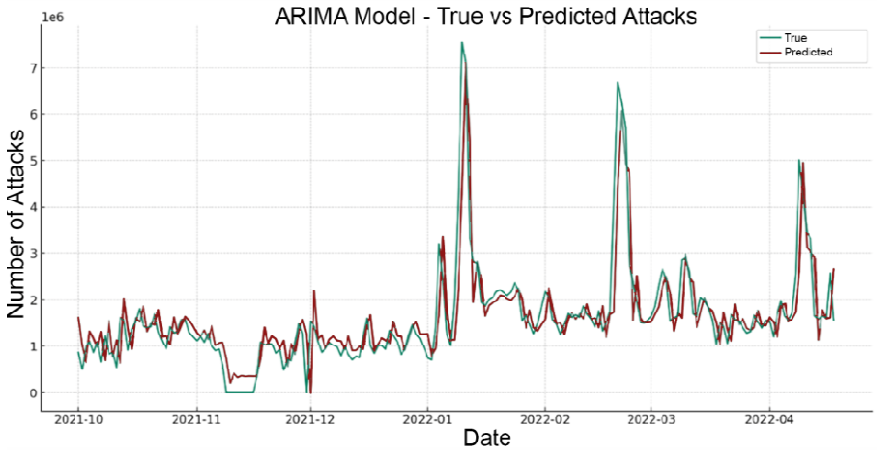

Figure no. 4: *ARIMA Model – true verses predicted value graph*
(Source: Stefanov, 2024)

The ARIMA model effectively predicts cyberattack trends, aligning with real attack data while showing minor inaccuracies (Figure no. 4). Recent five-day forecasts include 1,135,517 (April 14), 1,781,085 (April 15), 1,596,162 (April 16), 1,621,041 (April 17), and 2,659,028 (April 18) attacks. This model will require splitting the data into training and testing sets, as well as preparing the features that will be included in the model. While useful for cyber defense planning, model refinement and parameter tuning are needed to enhance accuracy and optimize predictive performance.

The ARIMA model effectively forecasts cyberattack trends, closely aligning with real attack data despite minor inaccuracies (Figure no. 4). Recent predictions range from 1.1 to 2.6 million attacks over five days, [1,135,517 (April 14), 1,781,085 (April 15), 1,596,162 (April 16), 1,621,041 (April 17), and 2,659,028 (April 18)] requiring further data refinement and feature selection for improved accuracy. While valuable for cyber defense planning, parameter tuning is essential for optimizing predictive performance (Box et al., 2015).

7. Time Series Modelling

ARIMA and SARIMA (Seasonal ARIMA) are effective time series models for forecasting cyberattacks using historical data. ARIMA performs well with non-seasonal data, while SARIMA accounts for trends and periodic fluctuations (Box et al., 2015). Although neural networks and ensemble models capture complex, non-linear patterns, they require greater computational resources (Hyndman & Athanasopoulos, 2021). These models can capture intricate relationships that ARIMA may miss, but at the cost of increased complexity.

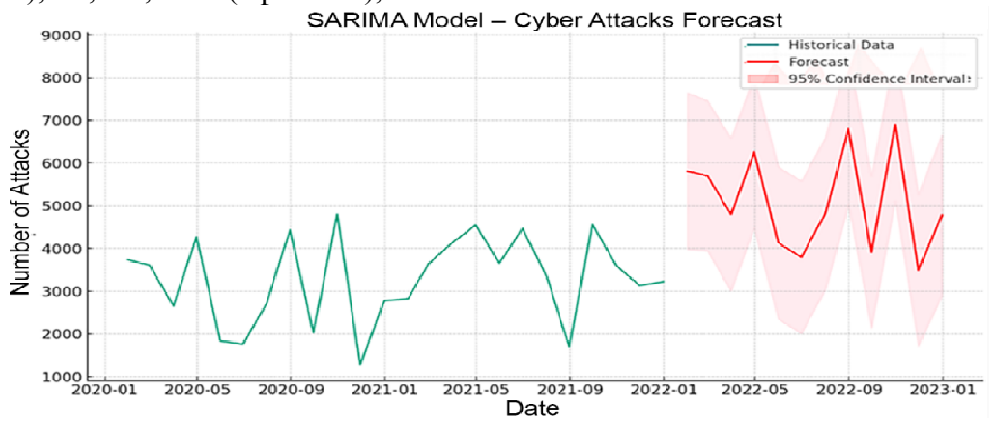

Figure no. 5: *SARIMA Model – cyber attacks forecast graph*
(Source: Stefanov, 2024)

7.1. Graph: SARIMA Model – Cyber Attacks Forecast

The **SARIMA model** predicts future cyberattacks based on historical data while incorporating **seasonal patterns and trends**. The forecast spans **two years**, with **confidence intervals** indicating prediction uncertainty (Hyndman & Athanasopoulos, 2021).

Forecast Interpretation

- **Predicted Trends**: The red line represents the projected number of cyberattacks, while the pink shaded area shows the 95% confidence interval, reflecting forecast reliability.
- **Trend Confirmation**: SARIMA validates seasonal attack patterns, aiding cybersecurity planning and resource allocation.
- **Uncertainty Considerations**: Wide confidence intervals highlight forecasting limitations, requiring additional data and model refinements for improved accuracy.

●**Need for Advanced Models**: Variability in predictions suggests that alternative methods or more complex models may enhance precision and reliability.

7.2. Analysis and Conclusions from the Application of the ARIMA Model to Time Series

The ARIMA model offers a powerful approach for analyzing and forecasting cyberattack data. With a high R^2 value and significant predictive power, ARIMA demonstrates its ability to model time series data effectively. However, the model also shows weaknesses, particularly in precision and the tendency to generate false positives. This information highlights the importance of careful model tuning, especially in cases where the cost of misclassification is high, as is often the case in cybersecurity.

8. Conclusion

Table no. 4

Results of the different AI models

AI Model	RMSE	R^2	Precision	Recall	F-score
Ensemble Methods	592,866,145	0.990	1.0	1.0	1.0
Isolation Forest	0.179	0.299	0.60	1.00	0.98
ARIMA	971,683,381	0.974	0.016	1.0	0.031

*The ranking presents the models from highest to lowest performance on these metrics

(Source: Stefanov, 2024)

This table presents a comparative analysis of different AI models, including statistics such as root mean square error (RMSE), coefficient of determination (R^2), precision (Precision), range (Recall) and F-score, which allows evaluation of the effectiveness of each model.

The analysis of the results presented in the preceding table reveals significant differences in the performance of the different AI models in the context of the prediction or classification task within the studied data.

Ensemble Methods: Ensemble methods show very promising results with RMSE of 592,866.145 and R^2 of 0.990. This information shows that combining different models can improve the predictive ability, as described by (Zhou, 2012) in the study of ensemble approaches.

Anomaly Detection: The Anomaly Detection model shows a lower R^2 than 0.299, suggesting that the model may not be appropriate for the data or that anomalies in the data are difficult to detect. However, the high Recall (1.00) and F-score (0.98) suggest that when the model identifies an anomaly, it does so with high accuracy.

The Anomaly Detection model shows a lower R^2 than 0.299, suggesting that the model may not be appropriate for the data or that anomalies in the data are difficult to detect. However, the high Recall (1.00) and F-score (0.98) suggest that when the model identifies an anomaly, it does so with high accuracy, as described by Sørbø and Ruocco (2023).

ARIMA: The ARIMA model, which is traditionally used for time series, shows a relatively high RMSE (971,683.381) and R^2 (0.974), which may be due to the non-stationarity of the data or other similar factors pointed out by (Box et al., 2015).

Summarizing, the results of the table highlight the importance of choosing an appropriate model depending on the characteristics of the data and the specific task. It is important to note that while some models show high precision and reliability, others may require further tuning or reworking to improve their predictive abilities.

Based on the analysis of the various AI models the Ensemble Methods emerge as leader in the field, showing exceptional accuracy and reliability in all metrics. This model offers the highest quality in prediction and classification, making them an ideal choice for applications requiring a high degree of accuracy and reliability. The model feature maximum Precision, Recall and F-score values, as well as minimum RMSE and maximum R^2 values, highlighting his ability to predict and classify data with a high degree of accuracy.

Isolation Forest (Anomaly detection) and ARIMA models show mixed results and can be useful in specific scenarios. They require careful selection and tuning of parameters, as well as careful interpretation of results, to be used effectively. Although they can be useful in certain areas, they require more attention and specific knowledge for optimal application.

In general, the Ensemble Methods is the best choice for complex analysis and prediction, offering high accuracy and reliability in all aspects of their application. This model provides reliable and accurate solutions for a wide range of tasks in the field of machine learning and artificial intelligence. Based on the analysis of the presented AI models, we can classify and evaluate their effectiveness according to various criteria: accuracy of predictions (RMSE), ability to explain the variation in the data (R^2), as well as the quality of the classification (Precision, Recall, F -score).

In this new research, different machine learning models were analyzed, focusing on their predictive and classification abilities. The Ensemble methods demonstrated results with high R^2 values and near-perfect Precision, Recall, and F-score values. The ARIMA model had good predictive ability with an RMSE of 971,683.381 and an R^2 of 0.974, despite the potential for false positives due to the low Precision value. The Isolation Forest - Anomaly detection models showed limited performance with significant differences in prediction accuracy and low or zero Precision, Recall and F-score values, highlighting their classification limitations. These studies present a detailed overview of the potential and limitations of different machine learning methodologies, emphasizing the need to select an appropriate model according to the specific task and data.

REFERENCES

Aktar, S., & Yasin Nur, A. (2023). Towards DDoS attack detection using deep learning approach. *Computer Networks*, *129*, 108026. Available at: https://doi.org/10.1016/j.cose.2023.103251.

Analytics Vidhya Team. (2021). Anomaly detection using isolation forest - A complete guide. *Analytics Vidhya*. Available at: https://www.analyticsvidhya.com/blog/2021/07/anomaly-detection-using-isolation-forest-a-complete-guide/.

Box, G.E.P., Jenkins, G.M., & Reinsel, G.C. (2015). Time series analysis: Forecasting and control (5th ed.). *Wiley Series in Probability and Statistics*. Available at: https://www.google.com/books/edition/Time_Series_Analysis/rNt5CgAAQBAJ?hl=en&gbpv=0.

Breiman, L. (1996). Bagging Predictors. *Machine Learning, 24* (2), 123-140. Available at: https://doi.org/10.1023/A:1018054314350.

Castillo, M., Pecchia, A., & Villano, U. (2022). AutoLog: Anomaly detection by deep autoencoding of system logs. *Expert Systems with Applications*. Available at: https://doi.org/10.1016/j.eswa.2021.116263.

DigitalOcean Community. (2023). Anomaly detection using isolation forest in Python. *DigitalOcean*. Available at: https://www.digitalocean.com/community/tutorials/anomaly-detection-isolation-forest.

Feamster, N., Kpotufe, S., & Yang, K. (2021). An efficient one-class SVM for anomaly detection in the Internet of Things. *arXiv*. Available at: https://arxiv.org/abs/2104.11146.

Freund, Y., & Schapire, R.E. (1999). A Short Introduction to Boosting. *Journal of Japanese Society for Artificial Intelligence, 14* (5), 771-780. Available at: https://cseweb.ucsd.edu/~yfreund/papers/IntroToBoosting.pdf.

Ghosemajumder, S. (2020). How AI will automate cybersecurity in the post-COVID world. *VentureBea*t. Available at: https://venturebeat.com/2020/09/06/how-ai-will-automate-cybersecurity-in-the-post-covid-world/.

Goodge, A., Hooi, B., Ng, S.K., & Ng, W.S. (2021). LUNAR: Unifying local outlier detection methods via graph neural networks. a*rXi*v. Available at: https://doi.org/10.48550/arXiv.2112.05355.

Hunter, J.D. (2020). Matplotlib: A 2D graphics environment. *Computing in Science & Engineering, 22* (5), 75-84. DOI: 10.1109/MCSE.2007.55.

Hyndman, R.J., & Athanasopoulos, G. (2021). Forecasting: Principles and Practice. *OTexts.* Available at: https://otexts.com/fpp3/.

Kluyver, T., Ragan-Kelley, B., Pérez, F., Granger, B.E., Moritz, P., & Jupyter Development Team. (2021). Jupyter Notebooks – a publishing format for reproducible computational workflows. *Nature Computational Science, 1* (5), 224-231. DOI: 10.1038/s41599-021-00669-4.

Liu, F.T., Ting, K.M., & Zhou, Z.H. (2008). Isolation forest. *Proceedings of the 2008 IEEE International Conference on Data Mining*, 413-422. Available at: https://doi.org/10.1109/ICDM.2008.17.

McKinney, W. (2021). Data structures for statistical computing in Python. *Proceedings of the 9th Python in Science Conference.* DOI: 10.25080/majora-92bf1922-00a. Available at: https://proceedings.scipy.org/articles/Majora-92bf1922-00a.

Parisi, A. (2019). *Hands-on artificial intelligence for cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing. Available at: https://www.packtpub.com/en-us/product/hands-on-artificial-intelligence-for-cybersecurity-9781789804027.

Pedregosa, F., et al. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12, 2825-2830. Available at: https://jmlr.csail.mit.edu/papers/v12/pedregosa11a.html.

Quezada, V., Astudillo-Salinas, F., Tello-Oquendo, L., & Bernal, P. (2023). Real-time bot infection detection system using DNS fingerprinting and machine learning. *Networks*, 228, 109725. Available at: https://doi.org/10.1016/j.comnet.2023.109725.

Schölkopf, B., Platt, J.C., Shawe-Taylor, J., & Smola, A.J. (2001). Estimating the support of a high-dimensional distribution. *Neural Computation, 13* (7), 1443-1471. DOI:10.1162/089976601750264965.

Sørbø, S., & Ruocco, M. (2024). Navigating the metric maze: A taxonomy of evaluation metrics for anomaly detection in time series. *Data Mining and Knowledge Discovery, 38* (3), 1027-1068. Available at: https://link.springer.com/article/10.1007/s10618-023-00988-8#citeas.

Waskom, M., & Seaborn Development Team. (2021). Seaborn: Statistical data visualization. *Journal of Open Source Software, 6* (60), 3021. Available at: https://doi.org/10.21105/joss.03021.

Xiang, H., et al. (2023). OptIForest: Optimal Isolation Forest for anomaly detection. *arXiv*. Available at: https://doi.org/10.48550/arXiv.2306.1270.

Zhou, Z. (2012). Ensemble methods: Foundations and algorithms. *Chapman and Hall/CRC*. Available at: https://www.routledge.com/Ensemble-Methods-Foundations-and-Algorithms/Zhou/p/book/9781439830031.