Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 11 No. 1, 2020 - www.cisdijournal.net

Development of an Anomaly Detection System for Zero-Day Attacks in Network Traffic Using Ensemble Machine Learning Algorithms

Oyeniran, B.G, Oguntunde, T. & Akinola, S.O.
Department of Computer Science
University of Ibadan
Ibadan, Nigeria.
E-mail: oyeniranblessing25@gmail.com; tantos557@yahoo.com; solom202@yahoo.co.uk
Phone: +14375569319; +2348131461570; +2348169748281

ABSTRACT

The rapid evolution of technology has heightened cybersecurity challenges, particularly zero-day attacks that exploit unknown vulnerabilities. Traditional methods like signature-based systems are inadequate due to their reliance on predefined patterns. While machine learning (ML) and deep learning (DL) show promise in anomaly detection, individual algorithms struggle with the complexity of modern network traffic. This study proposes an ensemble ML approach, combining XGBoost, Random Forest, LightGBM, and CatBoost using a voting ensemble classifier, to detect zero-day attacks effectively. The UGRansome dataset, with 149,043 observations and 14 features, was preprocessed to handle missing values, outliers, and inconsistencies. Feature engineering techniques like label encoding and scaling were applied, and the dataset was split into training (75%) and testing (25%) sets using stratified sampling. Individual models were trained and optimized, with predictions combined using a soft voting ensemble. Results showed the ensemble voting classifier outperformed individual models, achieving 99.95% accuracy, F1-score, and precision. LightGBM led individual models with 99.44% accuracy, followed by Random Forest (99.43%), XGBoost (99.41%), and CatBoost (99.41%). The ensemble approach effectively classified traffic into safe, suspicious, and attack categories, overcoming limitations of traditional methods in handling encrypted traffic and multi-class classification. The study provides a robust, scalable solution for zero-day attack detection, enhancing real-time threat identification, reducing financial losses, and protecting sensitive data. Future work should focus on real-time data integration, computational efficiency, and hybrid approaches to further improve accuracy and robustness.

Keywords: Zero-Day Attacks, Anomaly Detection, Ensemble Learning, Machine Learning, Cybersecurity, Models, Ugransome Dataset.

CISDI Journal Reference Format
Oyeniran, B.G., Oguntunde, T. & Akinola, S.O. (2020): Development of an Anomaly Detection System for Zero-Day Attacks in Network Traffic Using Ensemble Machine Learning Algorithms. Computing, Information Systems & Development Informatics Journal. Vol 11 No 1, Pp 97-104. Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V11N1P10

1. INTRODUCTION

Technology has revolutionized every aspect of our lives, offering numerous conveniences while simultaneously introducing significant challenges. One of the most pressing challenges is the increasing threat to cybersecurity as technology evolves. The rapid growth of data and the sophistication of cyberattacks have made it difficult to ensure robust security. As hackers with extensive coding skills and system knowledge may take advantage of even well protected systems, cybersecurity is a major worry [7].

While increasing productivity, dependability, and adaptability, the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) have revolutionized a number of sectors. Nevertheless, these systems' heightened interconnectedness and connection have also brought up novel and intricate security flaws. Concerns regarding the security of IIoT infrastructure have been raised by the recent spike in cyberattacks that target industrial systems. Such attacks have the ability to breach sensitive data, disrupt essential activities, and do serious harm to the environment and economy [1, 2, 8]. Network traffic has increased exponentially in volume, velocity, and diversity because of the spread of cloud computing, online services, and IoT devices. Due to this expansion, it is now more difficult to identify anomalies, which are departures from typical network behavior that might point to operational, performance, or security risks. Particularly worrisome are zeroday attacks, which take use of vulnerabilities that have not yet been discovered. These attacks remain undetected by traditional security systems, causing significant damage before they are identified and mitigated [5].

Cybersecurity has emerged as one of the most critical areas of concern in today's digital landscape. With the proliferation of interconnected systems, cloud computing, the Internet of Things (IoT), and advanced persistent threats, organizations are increasingly exposed to sophisticated cyberattacks. Among the most dangerous are zero-day attacks - exploits targeting undisclosed vulnerabilities in software or hardware systems. Because these attacks exploit unknown flaws, traditional security mechanisms such as signature-based detection are unable to identify or prevent them in real-time. This detection gap can lead to severe breaches involving data theft, financial loss, and reputational damage. Machine learning (ML) has become a powerful tool in cybersecurity, offering the capability to detect patterns, anomalies, and threats with higher accuracy and adaptability. ML algorithms learn from historical data to identify previously unknown threats, making them ideal for zero-day detection. However, individual ML models may have limitations due to bias, overfitting, or inability to generalize well across diverse data types. This has led to a growing interest in ensemble learning techniques, which combine the strengths of multiple models to improve overall detection performance

This study proposes a robust ensemble ML model that utilizes four state-of-the-art algorithms—XGBoost, Random Forest, LightGBM, and CatBoost. By employing a soft voting ensemble strategy, the model aggregates predictions from each classifier to enhance detection accuracy. The research leverages the UGRansome dataset, a modern ransomware dataset containing labeled samples categorized as safe, suspicious, or attack. The primary goal of this research is to build a real-time anomaly detection system capable of identifying and classifying zero-day attacks with high precision. The model is trained and validated using advanced preprocessing, feature engineering, and evaluation metrics. Through this work, we aim to contribute to the development of scalable and intelligent cybersecurity frameworks that proactively defend against emerging threats.

2. RELATED WORKS

Network traffic, as used in digital communication, is the movement of data packets between devices connected to a network. These packets are sent using protocols like User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). They are made up of a header with routing information and a payload with the actual contents. In order to maximize resource usage and guarantee reliable communication, the Internet uses packet switching technology, which divides data into tiny packets and routes them separately [4].

Traditional anomaly detection methods, including detection based on signatures, depend on predetermined trends of known attacks. Despite being efficient against known threats, zero-day attacks are not detected by these systems since they do not have established signatures. Anomaly-based detection systems, on the other hand, spot departures from typical behavior and may be able to discover unidentified dangers. However, these systems often have significant false positive rates and computational inefficiencies [3].

In an effort to get beyond these limitations, researchers have turned to machine learning (ML) and deep learning (DL). These methods improve the accuracy and efficacy of zero-day attack detection by analyzing large datasets to identify patterns and anomalies. Individual machine learning algorithms, however, could not be sufficient to manage the intricacy and unpredictability of contemporary network traffic. By combining many ML models, ensemble learning is a viable way to enhance detection performance by utilizing the advantages of each approach [5, 10].

Traditional security methods are no longer sufficient due to the growing complexity and frequency of cyberattacks. The average detection time for an intrusion stands at 240 days, highlighting the need for more effective solutions [7]. Traditional computer algorithms and intrusion detection systems (IDSs) that rely on signatures have not been able to detect zero-day attacks, which take use of undiscovered flaws [1]. In order to identify zero-day attacks in network flows, Touré *et al.,* [10] proposed a novel approach. By integrating online supervised learning, unsupervised learning (K-Means clustering), and supervised learning (1D-CNN), they used a hybrid learning strategy. High detection accuracy was shown by the findings, with an average online learning accuracy of 96.6% for the NSL-KDD dataset and 98.4% for the IBM dataset. The framework was able to detect abnormalities and zero-day attacks, including attack classes that had not been learnt before.

Using the CIC-AWS-2018 dataset, Zhou [11] evaluated six ML classifiers for zeroday intrusion detection: Random Forest (RF), Gaussian Naive Bayes, Decision Tree (DT), Multi-Layer Perceptron (MLP), K-Nearest Neighbors, and Quadratic Discriminant Analysis. The findings indicated that the DT classifier performed the best, achieving 100% accuracy in detecting zero-day intrusions and benign data and 96% accuracy in scrambled data. The study showed the efficacy of using flow-based statistical data for intrusion detection. Nkongolo *et al.,* [6] presented a cloud-based technique that uses ensemble learning and a genetic algorithm to identify zero-day threats. The technique combines three ML algorithms (Naive Bayes, RF, and Support Vector Machine (SVM)) and made use of a brand new anomaly detection dataset called UGRansome1819. With an accuracy rating of 99.6% before optimization and a classification ratio of 1% before and after optimization, the findings showed remarkable accuracy. By acting as a feature selector, the genetic algorithm cut down on over-fitting and computing time. The study emphasizes how well genetic algorithm optimization and ensemble learning work to identify zero-day attacks.

A Deep Neural Network (DNN)-based system for detecting anomalies in IoT network data was presented by Reddy *et al*., [9], with a focus on smart city applications. The authors used the “Distributed Smart Space Orchestration System (DS2OS) traffic traces dataset. It comprises 357,952 samples with 13 attributes, including standard and abnormal behaviors divided into seven attack categories. With an accuracy of 98.28%, the suggested DNN model outperformed conventional machine learning classifiers such as RF (98.01%), SVM (97.39%), and Gaussian Naive Bayes (89.14%). The model's efficacy in identifying irregularities and assaults in IoT networks was demonstrated by measures including accuracy, recall, F1-score, and ROC curves, which were used to assess its performance.

Machine learning (ML) algorithms have demonstrated remarkable efficacy in identifying network irregularities and zero-day attacks. While individual machine learning algorithms have demonstrated encouraging results, studies have indicated that they could not be sufficiently resilient to manage the intricacy and unpredictability of zero-day attacks in network traffic. This restriction has prompted research into ensemble learning strategies, which integrate many algorithms to increase the resilience and accuracy of detection. To the best of our knowledge, no study has combined XGBoost, RF, LightGBM, and CatBoost algorithms using a voting ensemble classifier for the classification of network traffic into safe, suspicious, and attack categories, despite the fact that several studies have used ensemble models for anomaly detection.

3. METHODOLOGY

This study utilizes a systematic approach to develop an anomaly detection model for zero-day attacks using ensemble learning. The methodology is designed to ensure high accuracy, robustness, and the ability to classify encrypted network traffic into meaningful categories. It consists of data acquisition, preprocessing, feature engineering, model training, and evaluation. The UGRansome dataset from Kaggle was chosen due to its relevance to ransomware detection. It contains 149,043 samples and 14 features, including timestamps, protocol types, IP addresses, Bitcoin transactions, and threat labels (Safe, Suspicious, Attack). These features provide a rich context for identifying malicious behavior.

Preprocessing involved cleaning the dataset by removing missing values, duplicates, and addressing inconsistencies. Outlier detection was performed using boxplots, and transformation techniques such as logarithmic scaling were applied to handle skewness. Feature engineering included label encoding for categorical variables, standard scaling, and feature selection using correlation analysis and mutual information.

For training, the data was split using stratified sampling to maintain label proportions. Models trained included Random Forest, XGBoost, LightGBM, and CatBoost. Each model was tuned for optimal performance. The final ensemble model used soft voting, which aggregates the predicted probabilities from individual classifiers to make a final decision.

Evaluation metrics included Accuracy, Precision, Recall, and F1-score. Confusion matrices were also analyzed to identify misclassifications. These steps ensured that the model could accurately detect and classify zero-day attacks in complex network environments.

The generic architecture of this research is shown in Figure 1. It commences with data extraction from the UGRansome dataset, sourced from Kaggle data repository. The extracted data undergoes preprocessing to enhance its quality, which includes handling missing values, duplicate values, outliers detection, and inconsistencies. Following preprocessing, feature engineering techniques are applied, comprising label encoding, feature scaling, feature transformation, and feature selection. The preprocessed and feature-engineered dataset is then split into training (75%) and testing sets (25%).

The training set is utilized to train individual ML algorithms, including XGBoost, Random Forest, LightGBM, and CatBoost. The trained models are then combined using a soft voting ensemble approach. The testing set is used to evaluate the models' performance using relevant ML metrics, such as accuracy, F1-score, precision, and recall. After evaluating the models with the test set, the trained models generate predictions, classifying the attacks into three categories: Safe (S), Suspicious (SS), and Attack (A), as shown in the model prediction stage.

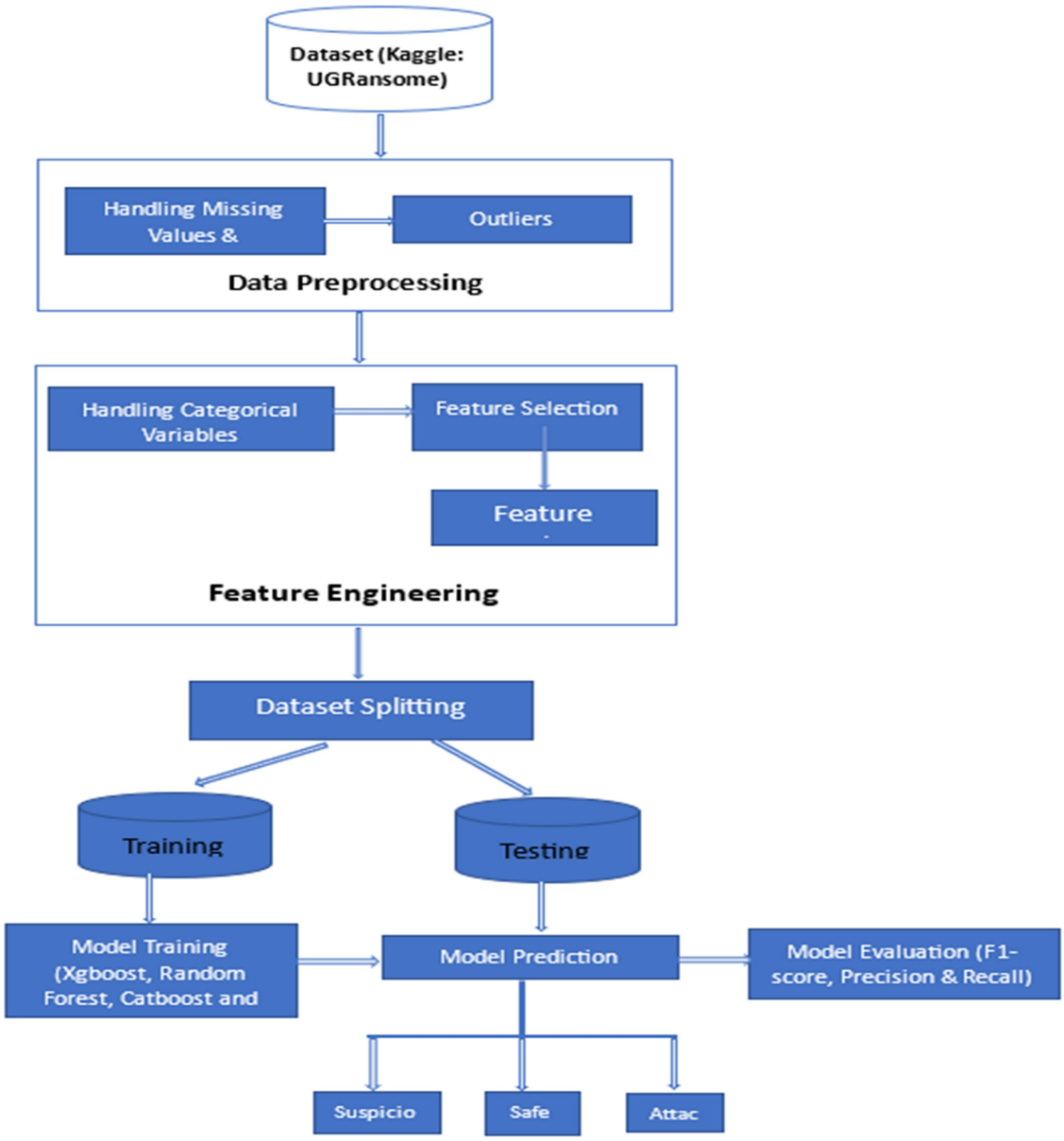

Figure 1: The generic architecture of the system

4. RESULTS AND DISCUSSION

The results of this study demonstrate the effectiveness of the ensemble voting classifier in accurately identifying zero-day threats. Each model in the ensemble - Random Forest, LightGBM, XGBoost, and CatBoost - was independently evaluated before being combined. Among them, LightGBM had the highest standalone accuracy at 99.44%, followed closely by Random Forest (99.43%), XGBoost (99.41%), and CatBoost (99.41%).

The ensemble classifier achieved an impressive accuracy of 99.95%, along with an equivalent F1-score and precision. This improvement validates the hypothesis that combining multiple models through ensemble learning enhances classification accuracy and reduces the likelihood of overfitting. The use of soft voting allowed the ensemble to consider class probabilities, leading to more balanced decisions. Further analysis showed that the ensemble model effectively handled multi-class classification, accurately distinguishing between Safe, Suspicious, and Attack categories. This is a notable improvement over traditional models, which often struggle with subtle distinctions between suspicious and malicious traffic. The model also performed well on encrypted and obfuscated traffic features, showcasing its potential for real-world deployment.

Figure 2 illustrates the Accuracy Scores of the models after hyperparameter tuning and the inclusion of the Voting Model. The results are as follows: RandomForest (Rdf_Model) achieves an accuracy of 0.998, indicating excellent performance after hyperparameter tuning. XGBoost (Xgb_Model) performs slightly lower than RandomForest, with an accuracy of 0.996, but still highly effective. CatBoost (Cat_Model) matches XGBoost's accuracy at 0.996, showing consistent performance. LGBM (Lgbm_Model) achieves an accuracy of 0.994, slightly lower than the others but still robust. The Voting Model (Voting_Model) outperforms all individual models with an accuracy of 0.9995, demonstrating the effectiveness of the ensemble approach.

Table 1: Performance Evaluation of the ML Models

ML Algorithms	F1-Score	Precision	Accuracy
RandomForest	0.9943	0.9943	0.9943
XGBoost	0.9941	0.9941	0.9941
CatBoost	0.9941	0.9941	0.9941
LGBM	0.9944	0.9944	0.9944
Voting Classifier	**0.9995**	**0.9995**	**0.9995**

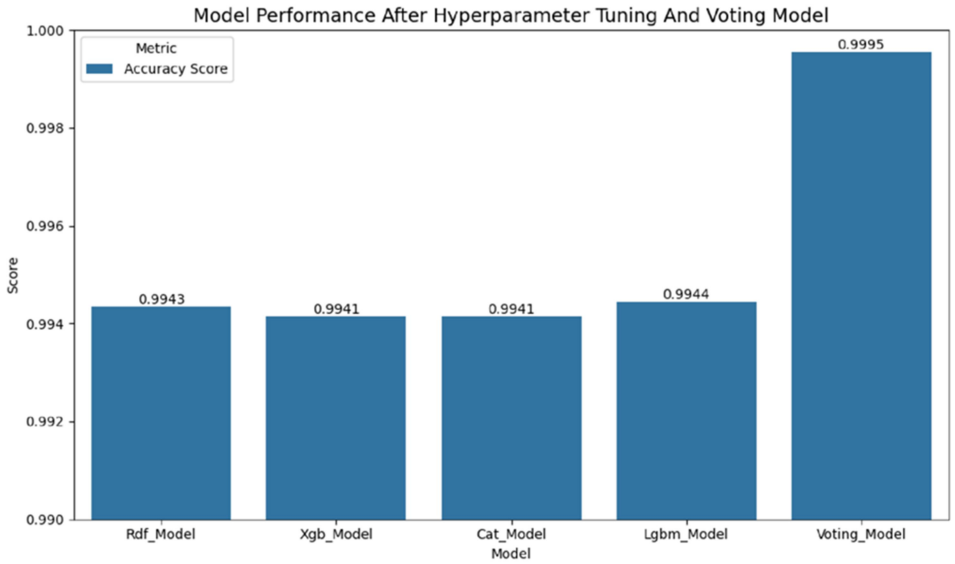

Figure 2: Bar Plot showing the Accuracy of the individual models and voting model

The results from Table 1 and Figure 2 highlight several key points. All individual models (RandomForest, XGBoost, CatBoost, and LGBM) perform exceptionally well, with accuracy scores above 0.994. This indicates that each model is highly capable of handling the classification task. LGBM slightly outperforms the other individual models, achieving the highest F1-Score and Accuracy among them (0.9944). The Voting Classifier outperforms all individual models, achieving an accuracy of 0.9995 and an F1-Score of 0.9995. This demonstrates the strength of ensemble methods in combining the predictions of multiple models to achieve higher accuracy and reliability. The voting classifier's performance is particularly notable, as it reduces misclassifications and improves overall model robustness.

Comparative analysis with previous studies highlighted the superiority of the proposed method. For instance, existing models using binary classifiers or single ML algorithms reported lower accuracy and were prone to higher false-positive rates. This research overcomes those limitations by integrating a diverse range of classifiers and comprehensive preprocessing techniques.

The study by Zhou [11] achieved high accuracies of 99.67% and 100%, respectively, using traditional datasets like CICIDS2017 and CIC-AWS2018. However, these studies did not address the challenges posed by encrypted traffic, which is a critical limitation in modern network environments. In contrast, this research utilizes the UGRansome dataset, which incorporates encrypted traffic patterns, making it more relevant for real-world applications. Additionally, while Zhou [11] achieved perfect accuracy, their approach was limited to binary classification and did not explore ensemble learning with advanced boosting algorithms.

5. CONCLUSION

This study presents a novel approach to detecting zero-day attacks using ensemble machine learning techniques. By integrating XGBoost, Random Forest, LightGBM, and CatBoost into a soft voting ensemble, the study addresses the limitations of traditional and individual ML-based intrusion detection systems. The proposed model effectively classifies network traffic into three categories: Safe, Suspicious, and Attack, achieving 99.95% accuracy. The use of the UGRansome dataset further strengthens the model's applicability, as it includes real-world encrypted traffic, ransomware indicators, and financial impact metrics. Comprehensive preprocessing, including outlier treatment, feature transformation, and label encoding, ensured data quality and model performance. Feature selection methods like mutual information and correlation analysis helped enhance learning efficiency.

The ensemble model outperformed individual classifiers and existing works in terms of precision, recall, and robustness. Its ability to generalize across encrypted traffic and handle multi-class classification makes it a valuable tool for modern cybersecurity systems. The findings of this study contribute to the growing field of intelligent threat detection and offer a scalable framework suitable for real-time implementation. Future research could explore integrating deep learning models into the ensemble or optimizing the system for real-time deployment using streaming data. Additionally, extending the dataset to include more diverse attack types and conducting cross-validation with other public datasets could further validate the model's reliability and effectiveness.

Reference

[1] Agbedanu, P. R., Yang, S. J., Musabe, R., Gatare, I., and Rwigema, J. (2025). A Scalable Approach to Internet of Things and Industrial Internet of Things Security: Evaluating Adaptive Self-Adjusting Memory K-Nearest Neighbor for Zero-Day Attack Detection. *Sensors*, *25*(1), 1–35. https://doi.org/10.3390/s25010216

[2] Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*(April), 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[3] Bridges, R. A., Oesch, S., Verma, M. E., Iannacone, M. D., Huffer, K. M. T., Jewell, B., Nichols, J. A., Weber, B., Beaver, J. M., Smith, J. M., Scofield, D., Miles, C., Plummer, T., Daniell, M., and Tall, A. M. (2020). Beyond the Hype: A Real-World Evaluation of the Impact and Cost of Machine Learning-Based Malware Detection. *Digital Threats: Research and Practice*, *1*(1), 1–23. https://doi.org/10.1145/3567432

[4] Dashevskiy, M., and Luo, Z. (2014). Network Traffic Classification and Demand Prediction. In *Conformal Prediction for Reliable Machine Learning: Theory, Adaptations and Applications*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-398537-8.00012-2

[5] Guo, Y. 2023. A review of Machine Learning-based zero-day attack detection: Challenges and future directions. *Computer Communications*, *198*, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001

[6] Nkongolo, M., van Deventer, J. P., Kasongo, S. M., Zahra, S. R., and Kipongo, J. (2022). A Cloud Based Optimization Method for Zero-Day Threats Detection Using Genetic Algorithm and Ensemble Learning. *Electronics (Switzerland)*, *11*(11). https://doi.org/10.3390/electronics11111749

[7] Ozkan-Okay, M., Akin, E., Aslan, O., Kosunalp, S., Iliev, T., Stoyanov, I., and Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*, *12*(January), 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

[8] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., and Wu, D. O. 2020. Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. *IEEE Communications Surveys and Tutorials*, *22*(4), 2462–2488. https://doi.org/10.1109/COMST.2020.3009103

[9] Reddy, D. K. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., and Singh, P. K. 2021. Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies*, *32*(7), 1–26. https://doi.org/10.1002/ett.4121

[10] Touré, A., Imine, Y., Semnont, A., Delot, T., and Gallais, A. (2024). A framework for detecting zero-day exploits in network flows. *Computer Networks*, *248*(April), 110476. https://doi.org/10.1016/j.comnet.2024.110476

[11] Zhou, Q. (2019). *Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection*. *July*. https://doi.org/10.48550/arXiv.1905.03685