International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Optimized Machine Learning for Cyber Security Applications

Mrs. V.R. Jayashree , *Assistant Professor in Computer Science,*
Siva Sivani Degree College, NH-44, Kompally, Secunderabad-500100, Telangana, India.
E-mail Id: jayashree9000@gmail.com

Abstract: Machine learning plays crucial role in cyber-attack detection from different platforms like IOT (Internet of things), from network or from different ecommerce as well as banking sector. In this study different traditional machine learning and optimized machine learning algorithms are used for performance analysis. It is observed that optimized machine learning algorithms are performing better than traditional machine learning classifiers giving better performance metrics. The dataset of BOTNET attackers is used which has two labels as 'Normal' or 'Attack'. The dataset is highly imbalanced so to avoid the training issues from highly imbalanced dataset in proposed method SMOTE algorithm is used which makes both normal user and attackers data equally available for training. The classifiers used in this proposed method are SVM (support vector machine) classifier , decision tree classifier , BOGP Optimized Decision tree and advance deep learning algorithm CNN (Convolution Neural Networks). Out of these four classifiers CNN is performing superior than other traditional classifiers.

Keywords: Attackers , Machine Learning , Cyber Attack Prediction , Optimized Machine Learning , CNN (Convolution Neural Networks)

Received: 24-10-2025 Accepted: 09-12-2025 Published: 16-12-2025

I. Introduction

The fast pace of digitalization in all industries has greatly contributed to dependence on interdependent systems, digital infrastructures and online services, which leads to a drastic escalation of cyber threats. With attackers becoming increasingly sophisticated with their techniques, e.g. polymorphic malware, zero-day exploits, botnet-driven attacks, or AI-driven intrusion, standard security systems tend to be unable to find and respond to new threat patterns. Thus, smart, automated, and adaptive technology is a growing trend in current cybersecurity as it allows studying large volumes of data in real-time and identifying oddities to provide strong security to digital ecosystems.

A number of sources emphasize the increasing role of artificial intelligence (AI) and machine learning (ML) in the provision of better cybersecurity. Mehta and Dave focused on the idea that AI-powered personalization approaches have a major impact on individual behavior in online platforms, and how intelligent algorithms can examine the intricate user patterns on a massive scale [1]. Aneja showed that AI algorithms that involve clustering give profound understanding of the customer and user behavior that can be also utilized to trace abnormal or malicious behavior in the network settings [2]. Martins also discussed AI-based behavioral analytics used in operation systems, demonstrating that pattern-mining algorithms can identify deviations that can be viewed as signs of cyber threats [3]. Onifade et al. also affirmed that the predictive AI models are capable of predicting the future state of the system which is a very important feature of early attack detection [4].

Researchers have demonstrated that AI-based systems of recommendation and analysis rely on the foundation of the strong data mining, anomaly detection, and predictive modeling in the domain of online systems and e-commerce. Necula and Păvăloaia have reviewed AI integration with recent computing solutions, including blockchain and VR, and the significance of reliable and secure digital ecosystems [5]. Agboola et al. emphasized the importance of AI-driven data integration to generate real-time insights, which is in line with current cybersecurity systems that are developed to identify intrusions in real-time with the least delay [6]. Radhakrishnan wrote about how AI can be used to predict behavior and detect suspicious trends, which is why predictive analytics have to be integrated into cyber defense systems [7].

The use of machine learning in behavior prediction, and anomaly detection also shows a

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

high level of applicability to intrusion detection systems (IDS). Sharma and Singh demonstrated that online behaviors could be predicted with the help of ML, which directly implies detection of suspicious cyber activities [8]. Kim et al. introduced AI-based recommendation models that have the ability to filter and classify large streams of data, akin to ML-based IDS which process network packets in real time [9]. Gupta and Arora talked about behavioral analysis with the use of big data where scalable ML algorithms should be used to process large cybersecurity datasets [10]. Correspondingly, Zhang et al. outlined deep learning methods that are capable of learning complicated nonlinear trends which is necessary to detect stealthy cyberattacks [11].

Anomaly and suspicious behavior have also been detected using data mining approaches. Patel and Desai showed the role of data mining in the visualization-based setting to identify trends in behaviors, which contributes to creating explainable IDS models [12]. Ali et al. studied the advanced recommendation systems and highlighted the fineness of accuracy, personalization, and anomaly detection, which reflected similar peculiarities of cybersecurity requirements of accurate intrusion detection [13]. Wang and Zhao suggested the hybrid ML solutions to predicting behaviors, which improves the detection rate in complicated cyber space [14]. Lin and Zhang proposed clustering and deep learning methods to segment the data and analyze the behavior, which subsequently justify the intelligent methods of detection of malicious users or compromised systems [15].

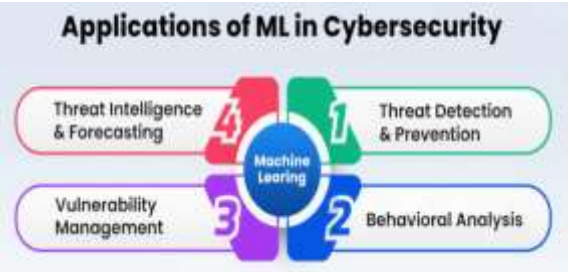

Fig. 1.1 Applications of ML in Cyber Security

As per the above figure , cybersecurity uses ML in different applications such as detection and prevention of cyber threats , Analysis of the behaviour of cyber attacker , management of vulnerability , forecasting of threat action in different domains including banking , clouds and internet.

This paper will suggest a full-scale cyberattack detection framework based on optimized machine learning models. The system makes use of data preprocessing, SMOTE-based balancing, conventional ML classifiers, optimized ML, and deep learning models that detect diverse cyber threats. Our solution is more accurate in terms of detecting, more robust in terms of modeling, and offers a valid cybersecurity solution that will meet the requirements of the contemporary digital infrastructures.

II. LITERATURE SURVEY

Aledhari et al. have carried out an extensive empirical research on machine learning applications to network application security by analyzing a variety of ML algorithms in diverse attack cases to determine the most effective setting classifier. Their work focuses on optimization techniques of models (spinning of hyperparameters and calibration of performance) to improve the accuracy of detection on a real network traffic. Although it includes powerful practical considerations, the study is less inclined on addressing the issue of algorithms comparison and does not prioritize the issue of dealing with highly disequilibrium datasets, which is a major issue in cybersecurity detection systems [1].

Hussen et al. came up with a full streaming big-data based cybersecurity structure that is constructed using optimized deep learning models that are relevant in processing extensive network traffic in real time. They are based on their system, which uses distributed architectures and streaming analytics to identify attacks with the lowest latency, is more scalable and responsive. This framework works well in a real-time setting, but it needs much computing power and provides little analysis of interpretability and imbalance of data typical of cyber-attack data [2].

Veerasamy et al. proposed an optimized cybersecurity framework to network applications based on highly developed machine learning methods. Their methodology combines several optimization techniques to attain better performance of classification besides guaranteeing system level applicability to real life network

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

scenarios. Although an integrated framework is tough, it does not go into a great depth of multi-class attack datasets and superior feature-balancing algorithms like SMOTE, which constrains the generalization capabilities across the various attack classes [3].

Markkandeyan et al. came up with an innovative hybrid deep learning model that is integrated with an optimization algorithm in order to enhance the accuracy of cyber-threat detection. The hybrid architecture is based on the advantages of deep neural networks and the metaheuristic optimization, which helps to improve the model parameters. The results of their analysis demonstrate significant performance improvement particularly in complex types of attacks. Nevertheless, the further complexity of training and higher computational cost of the model make it difficult in lightweight or real-time security applications [4].

Eugene Prince, et al. suggested optimized deep learning algorithm to detect cyber-attack based on enhancing the efficiency of learning and classification accuracy. They have their model, which has integrated advanced tuning techniques to boost deep network performance in various types of attacks. Although the study gives a good accuracy improvement, it is mostly about deep learning and not the comparison between the results with the classical machine learning models so it does not cover the scope of performance benchmarking with different algorithm families [5].

Khadidos et al. have proposed a cybersecurity system to use in IoT systems with the binary HunterPrey Optimization algorithm and machine learning classifiers. The metaheuristic is better in feature selection and more accurate in detection and can be used in constrained devices of the IoT due to its lower complexity in computation. Though useful in the circumstances of the IoT, the approach might not be efficient enough to handle bigger enterprise-level data and needs to be assessed more broadly across multiple types of attacks [6].

In an insightful but early view of the use of machine learning in cybersecurity, Das and Morris identified the potential and the difficulties in the implementation of ML models to detect attacks. They write about such critical issues as feature engineering, dataset variability, adversarial threats, and model robustness. Although groundbreaking, the paper is older than most of the modern deep learning and streaming detection innovations, and it is not very relevant to the modern high-performance cybersecurity architecture [7].

III. PROPOSED METHOD

Following are the steps of proposed method,

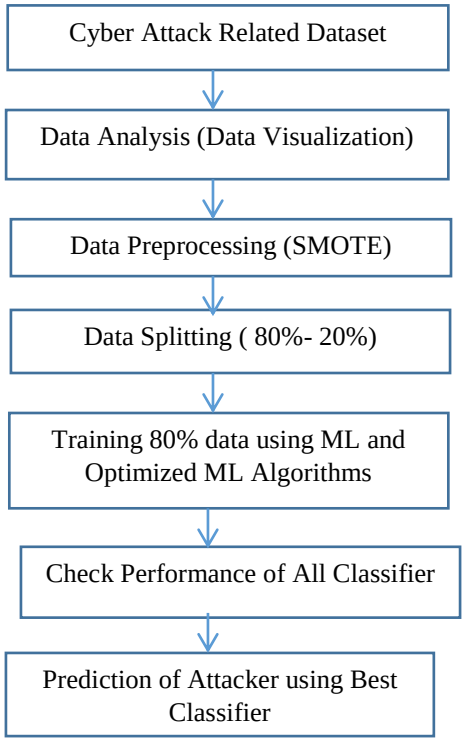

Fig. 3.1 Block Diagram of Proposed Method

3.1 Cyber-Attack Data set collection: An appropriate set of cyber-attacks data is assembled to examines the various attack patterns and develop the detection model.

3.2 Data Analysis and Visualization: The dataset is analyzed to learn pattern of features, attack distribution and correlation and it assists in finding valuable attributes.

3.3Preprocessing of Data through SMOTE: To deal with the imbalance of classes and optimize the model learning process, the SMOTE technique is used to clean, format, and balance the data.

3.4 Train–Test Splitting (80%–20%): The processed dataset is split into 80 percent of training

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

data and 20 percent of testing data as a way of ensuring impartial assessment.

3.5 ML and Optimized ML Algorithms Training Models: A series of machine learning algorithms are trained on the training data in order to acquire attack signatures and patterns.

3.6 All Classifiers Performance Evaluation: All trained models are evaluated and compared over the standard evaluation metrics in order to determine which classifier is the most accurate.

3.7 Best Classifier Selection: The final detection model is selected as the classifier that has the best performance.

3.8Prediction of Cyber-Attacks: The chosen classifier helps forecast and categories cyber-attacks on new or unknown information with a better precision.

IV. Results Analysis

The dataset (BOTNET2018 dataset) is collected from below link,

https://cloudstor.aarnet.edu.au/plus/s/umT99TnxvbpkkoE?path=%2FCSV%2FTraning%20and%20Testing%20Tets%20(5%25%20of%20the%20entier%20dataset)%2FAll%20features in the existing different machine learning classifiers such as SVM classifier , decision tree classifier are used which has lower accuracy than proposed optimized classifiers.

In proposed method we tested performance of BOGP Optimized Decision tree and advance deep learning algorithm CNN (Convolution Neural Networks) which are outperforming the cyber security domain by giving superior performance compared to traditional machine learning algorithms.

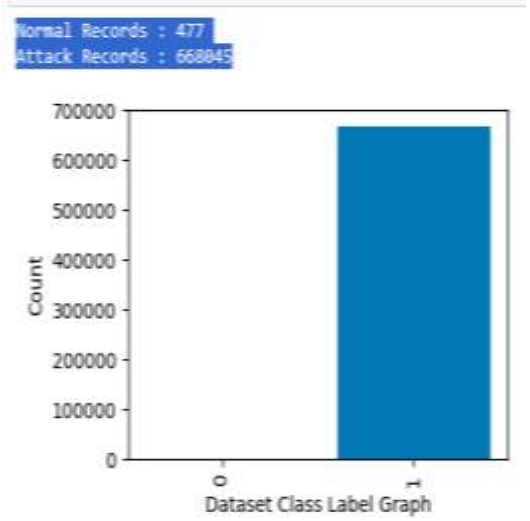

Fig.4.1 Bar Graph for Representing total types of data with count

It is observed that attacked users' data is more so dataset is highly imbalanced to make dataset balanced SMOTE technique is used.

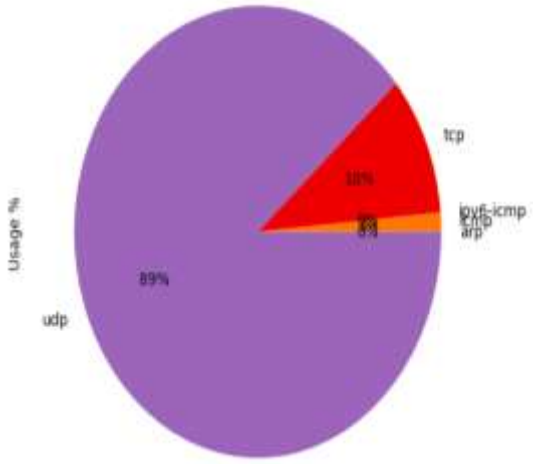

Fig.4.2 Different Communication Protocols used by different Users (Normal User and Attackers)

In the above graph different users which communication protocol they used is plotted using pie chart. Almost 89% users have used UDP protocol and remaining protocols and users in percentage is shown.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

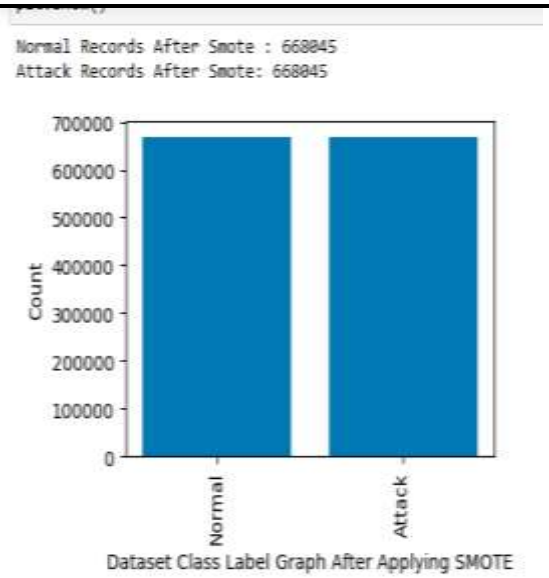

Fig.4.3 Bar Graph Representing Users After SMOTE

Both users have equal data after applying the SMOTE technique for data balancing.

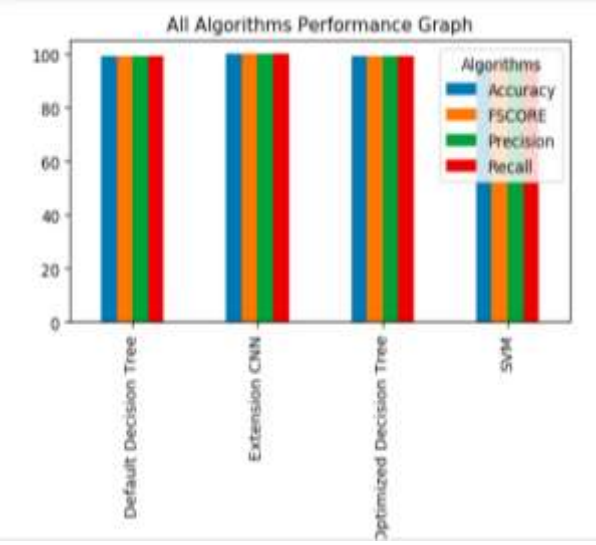

Fig. 4.4 Performance of Different Machine Learning and optimized machine learning algorithms

In the above graph there is performance graph of different machine learning and optimized machine learning algorithms are used for detection of cyber-attacks.

	Algorithm Name	Accuracy	Precision	Recall	FSCORE
0	Default Decision Tree	99.232836	99.242247	99.231364	99.232778
1	Optimized Decision Tree	99.306559	99.315312	99.305145	99.306509
2	SVM	96.496119	96.496291	96.495960	96.496089
3	Extension CNN	99.996258	99.996267	99.996249	99.996258

Fig.4.5 Table of performance of different Machine Learning and Optimized Machine Learning Algorithms

Tabular format performance analysis of different machine learning and optimized machine learning algorithms is represented which shows that optimized CNN algorithm has better performance than other machine learning algorithms.

I. CONCLUSION

The swift development of cyber threats requires sophisticated and dynamic security systems with the ability to examine vast information and identify complex attack patterns. This paper has created an efficient machine learning system that is used to detect cyberattacks based on the BOTNET2018 data. The proposed system combines the data balancing based on SMOTE, the classical ML classifier, the optimized model of a ML classifier, and the advanced deep learning method. As it can be seen, experimental findings indicate that optimized methods are more effective than conventional classifier in terms of accuracy, precision, recall, and overall detection ability. Out of the tested algorithms, including SVM, Decision Tree, BOGP-Optimized Decision Tree, and CNN, the last model, based on deep learning, demonstrated the best results and showed to be more effective in learning complicated attack patterns and detecting harmful traffic. The results confirm that optimization and deep learning play an important role in predicting cyber threats and could become even more suitable to protect the modern digital infrastructures. In general, the suggested framework will be an efficient and scalable tool in real-time cyberattack recognition and can be used as a powerful basis to apply future cybersecurity solutions related to large and dynamic data.

REFERENCES

[1] Aledhari, M., Razzak, R., & Parizi, R. M. (2021). Machine learning for network application

security: Empirical evaluation and optimization. *Computers & Electrical Engineering*, *91*, 107052.

[2] Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I. (2023). A fully streaming big data framework for cyber security based on optimized deep learning algorithm. *IEEE Access*, *11*, 65675-65688.

[3] Veerasamy, B., Nageswari, D., Kumar, S. N., Shirgire, A., Sitharthan, R., & Jasmine Gnana Malar, A. (2023, April). An optimized cyber security framework for network applications. In *International Conference on Frontiers of Intelligent Computing: Theory and Applications* (pp. 511-518). Singapore: Springer Nature Singapore

[4] Markkandeyan, S., Ananth, A. D., Rajakumaran, M., Gokila, R. G., Venkatesan, R., & Lakshmi, B. (2025). Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. *Cyber Security and Applications*, *3*, 100075.

[5] Eugine Prince, M., Josephin Shermila, P., Sajithra Varun, S., Anna Devi, E., Sujatha Therese, P., Ahilan, A., & Jasmine Gnana Malar, A. (2023, April). An optimized deep learning algorithm for cyber-attack detection. In *International Conference on Frontiers of Intelligent Computing: Theory and Applications* (pp. 465-472). Singapore: Springer Nature Singapore.

[6] Khadidos, A. O., AlKubaisy, Z. M., Khadidos, A. O., Alyoubi, K. H., Alshareef, A. M., & Ragab, M. (2023). Binary Hunter–Prey optimization with machine learning—Based cybersecurity solution on Internet of Things environment. *Sensors*, *23*(16), 7207.

[7] Das, R., & Morris, T. H. (2017, December). Machine learning and cyber security. In *2017 international conference on computer, electrical & communication engineering (ICCECE)* (pp. 1-7). IEEE.

[8] Omer, N., Samak, A. H., Taloba, A. I., & Abd El-Aziz, R. M. (2024). Cybersecurity Threats Detection Using Optimized Machine Learning Frameworks. *Computer Systems Science & Engineering*, *48*(1).

[9] Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In *Proceedings of the 27th international conference on computer applications in industry and engineering* (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore.

[10] Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., & Aljaaf, A. J. (2019). Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks. In *Nature-inspired computation in data mining and machine learning* (pp. 47-76). Cham: Springer International Publishing.

[11] Nayak, J., Meher, S. K., Souri, A., Naik, B., & Vimal, S. (2022). Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *The Journal of Supercomputing*, *78*(13), 14866-14891.

[12] Mahmood, R. K., Mahameed, A. I., Lateef, N. Q., Jasim, H. M., Radhi, A. D., Ahmed, S. R., & Tupe-Waghmare, P. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. *Journal of Robotics and Control (JRC)*, *5*(5), 1502-1524.

[13] Kulkarni, A. J., & Satapathy, S. C. (Eds.). (2020). *Optimization in machine learning and applications* (pp. 51-68). Heidelberg: Springer.

[14] Alemerien, K., Al-Suhemat, S., & Almahadin, M. (2024). Towards optimized machine-learning-driven intrusion detection for Internet of Things applications. *International Journal of Information Technology*, *16*(8), 4981-4994.

[15] Mishra, S. (2022). An optimized gradient boost decision tree using enhanced African buffalo optimization method for cyber security intrusion detection. *Applied Sciences*, *12*(24), 12591.