JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 3, June 2026, hlm. 477 – 484 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i3.4411
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

OPTIMIZING CYBER ATTACK SIMULATION AS A RESPONSE TO ESCALATING SECURITY THREATS USING A MACHINE LEARNING APPROACH

Rivaldi Lubis[1*], Apriyanto Halim[1], Felix Jansen Tanjaya[1], Tandri[1]
[1]Information Technology, Universitas Mikroskil
email: *rivaldi.lubis@mikroskil.ac.id

Abstract: The growing intensity of cyber attacks, marked by rapid, large-scale, automated, and adaptive execution, requires analytical methods that represent the diversity of network environments, including variations in target platforms such as IoT, traditional networks, and hybrid infrastructures. This study compares machine learning models for cyber attack classification under heterogeneous environmental conditions and formulates a conceptual optimization framework based on model performance. Four publicly available benchmark datasets were used, namely UNB CIC IoT 2023, UNB CIC IDS-2018, UNSW-NB15, and a Kaggle cyber security attacks dataset, comprising approximately 40,000 to over 3.6 million records and 25 to 80 features across IoT, conventional, and mixed network environments. Random Forest, XGBoost, Multilayer Perceptron, and Transformer were implemented within a unified pipeline involving preprocessing, feature selection, and Bayesian Optimization-based hyperparameter tuning. All models achieved F1-score and Cohen's Kappa above 96%, with XGBoost performing best (97.80%, 97.26%), followed by Random Forest (97.78%, 96.96%) and Transformer (97.44%, 96.82%), while MLP scored lowest (96.74%, 96.00%), a gap below one percentage point. Confusion matrix analysis revealed persistent misclassification in minority and overlapping attack classes, informing a proposed adaptive cyber attack simulation optimization framework.

Keywords: cyber attacks; optimization; machine learning; environmental variability.

Abstrak: Meningkatnya intensitas serangan siber yang berlangsung cepat, masif, otomatis, dan adaptif menuntut pendekatan analitis yang merepresentasikan keragaman lingkungan jaringan, termasuk perbedaan karakteristik platform sasaran seperti Internet of Things (IoT), jaringan konvensional, dan infrastruktur hibrida. Penelitian ini membandingkan model machine learning untuk klasifikasi serangan siber pada kondisi lingkungan heterogen, sekaligus menyusun kerangka optimasi konseptual berdasarkan performa model. Empat dataset benchmark publik digunakan, yaitu UNB CIC IoT 2023, UNB CIC IDS-2018, UNSW-NB15, serta dataset Kaggle cyber security attacks, dengan jumlah data berkisar 40.000 hingga lebih dari 3,6 juta rekaman dan 25 sampai 80 fitur, mewakili lingkungan IoT, konvensional, dan campuran. Random Forest, XGBoost, Multilayer Perceptron, dan Transformer diimplementasikan melalui pipeline terpadu mencakup pra-pemrosesan, seleksi fitur, dan optimasi hyperparameter berbasis Bayesian Optimization. Seluruh model mencapai F1-score dan Cohen's Kappa di atas 96%, dengan XGBoost menunjukkan performa terbaik (97,80%, 97,26%), diikuti Random Forest (97,78%, 96,96%) dan Transformer (97,44%, 96,82%), sementara MLP mencatat skor terendah (96,74%, 96,00%), dengan selisih kurang dari satu poin persentase. Analisis confusion matrix mengungkap misklasifikasi yang konsisten pada kelas minoritas dan serangan dengan karakteristik serupa, yang menjadi dasar kerangka optimasi simulasi serangan siber adaptif yang diusulkan.

Kata kunci: serangan siber; optimasi; machine learning; variabilitas lingkungan.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 3, June 2026, hlm. 477 – 484 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i3.4411
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

The rapid advancement of information and communication technologies has led to increasingly complex digital ecosystems, in which both public and private sectors rely heavily on cyber infrastructure as a core component of their operations [1], [2]. This growing dependence has been accompanied by a significant escalation of cybersecurity threats [3]. The Check Point Security Report 2024 indicates that the education and research sectors are among the most targeted, experiencing on average more than 2,000 attack attempts per institution per week [4].

This situation is further intensified by the increasing speed and automation of modern cyber attacks [5], [6]. Automated attack mechanisms enable large-scale intrusion attempts within seconds [7]. Such attack efficiency is strongly influenced by environmental variability, across heterogeneous environments such as conventional and IoT systems [8], [9], [10]. Each environment exhibits distinct vulnerability characteristics, making attack success highly dependent on the attacker's ability to adapt strategies to heterogeneous system conditions [11], [12].

These dynamics underscore the need for optimization in cyber attack simulation modeling, as non-optimized simulations may fail to represent adaptive and environment-dependent threats accurately [13]. From an academic perspective, such optimization serves to strengthen cyber defense by enabling more realistic and representative simulations [14].

Although machine learning has been extensively applied for intrusion detection, prior studies have predominantly emphasized detection accuracy under static or single-environment conditions, focusing on false negative reduction [15], temporal pattern modeling [16], ensemble classification [17], context-aware web attack detection [18], and known-attack detection via dataset integration [19], [20], while adaptive strategy optimization via deep reinforcement learning [21] remains an isolated exception.

The use of supervised learning combined with systematic hyperparameter optimization to support adaptive, environment-aware attack simulation thus remains largely unexplored. Here, optimization refers to leveraging model performance outputs, namely classification accuracy and misclassification patterns across heterogeneous environments, to refine attack simulation scenarios for greater real-world representativeness. This research addresses that gap using Random Forest, XGBoost, MLP, and Transformer models tuned via Bayesian Optimization to inform a conceptual framework for adaptive cyber attack simulation.

METHOD

This research followed a sequential methodological framework comprising literature review, data collection and analysis, preprocessing, model implementation, and evaluation.

Literature Review

The literature review establishes the study's theoretical foundation by examining recent machine learning approaches, cyberattack modeling studies, and treatment of target environment variability in reputable, recent publications. Based on this review, the study addresses three research questions: (RQ1) common ML approaches for cyberattack classifi-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 3, June 2026, hlm. 477 – 484 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i3.4411
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

cation, (RQ2) frequently used benchmark datasets, and (RQ3) the extent to which prior studies consider target environment variability.

Data Collection

The datasets used in this study were selected from publicly available and widely adopted benchmark sources in machine learning–based cybersecurity research to enable measurable performance evaluation and direct comparison with prior work. All datasets were obtained from official repositories and open platforms, covering IoT, conventional, and mixed network environments. Their characteristics are summarized in Table 1.

Table 1. Dataset Information

Dataset	Characteristics	Environment
[22]	Large-scale IoT network traffic with modern attacks (DoS, DDoS, spoofing, botnet)	Internet of Things (IoT)
[23]	IDS traffic data with controlled attack scenarios (brute force, DoS/DDoS, web attacks)	Conventional networks
[24]	Benchmark IDS dataset with flow-based and packet-based features	Conventional networks
[25]	Public dataset with heterogeneous attack types and mixed features	General / mixed environment

Data Analysis

Prior to preprocessing, dataset analysis was conducted to identify differences in scale, feature structure, and complexity. The datasets range from approximately 40,000 to over 3.6 million records, with 25 to 80 features. Datasets [22], [23], and [24] primarily consist of numerical network flow and packet-based attributes, whereas dataset [25] includes both numerical and categorical features such as attack type, protocol, and severity. This heterogeneity strengthens robustness evaluation across diverse environments.

Preprocessing Data

Preprocessing included missing value handling, duplicate removal, normalization, categorical encoding, and stratified splitting.

Model Implementation

Four supervised models were implemented in this study, namely Random Forest, XGBoost, Multilayer Perceptron (MLP), and Transformer, representing both ensemble-based and deep learning approaches for cyberattack classification under heterogeneous network environments [15], [16], [17], [19]. Hyperparameter tuning was conducted using Bayesian Optimization with the Optuna framework, employing validation data from the training set and F1-score as the objective function to address class imbalance. Optuna's pruning mechanism was applied for early stopping to enhance computational efficiency and reduce overfitting.

Evaluation

Model performance was evaluated using accuracy, precision, recall, F1-score, Cohen's Kappa, and confusion matrix analysis, since relying on a single metric under multi-class, imbalanced data may obscure class-level performance, agreement consistency, and misclassification patterns [26].

RESULT AND DISCUSSION

Based on the defined research questions, relevant studies were identified and selected using predefined crite-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 3, June 2026, hlm. 477 – 484 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i3.4411
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

ria. The findings from the literature review were subsequently synthesized and summarized in Table 2.

Table 2. Literature Review Result

Literature	Method	Key Contribution
[15]	XGB + CSO	Reduced false negatives with optimized IDS
[16]	RNN	Effective modeling of temporal attack patterns
[17]	RF, XGB	Ensemble models outperform classical ML
[18]	Transformer + NLP	Context-aware web attack detection
[19]	ML & DL	High accuracy on known attacks via dataset integration
[20]	DT + FS	High accuracy with computational efficiency
[21]	DRL (DQN)	Adaptive exploitation based on target environment

Environmental variability is implicitly reflected through differences in network communication patterns, particularly protocol types and their distributions across datasets. A summary of dataset characteristics and protocol distributions is presented in Table 3.

Table 3. Summary of Dataset and Protocol Distribution

Dataset	Records	Features
[22]	3,653,576	41
[23]	2,097,150	80
[24]	2,059,418	50
[25]	40,000	25

After preprocessing, the label distribution revealed substantial class imbalance: flooding-based attacks (TCP_FLOOD, UDP_FLOOD, and SYN_FLOOD) dominated, while several reconnaissance, exploitation, and minority classes were underrepresented.

All models were developed and evaluated using an identical pipeline, including the same datasets, preprocessing, feature selection, and data splitting. Feature selection was performed after data partitioning, using training data only to avoid information leakage, and applied feature importance from tree-based models to retain relevant attributes such as TCP flag indicators, flow and packet statistics, port and protocol information, traffic direction ratios, byte-based attributes, and time-based metrics.

The evaluation results for all models are presented in Table 4. All metrics were computed using the test dataset, which was not involved in either the training process or hyperparameter optimization.

Table 4. Model Evaluation Metrics

Model	Accuracy	Precision	Recall	F1-score	Cohen's Kappa
Random Forest	97.63%	97.96%	97.63%	97.78%	96.96%
XGBoost	97.87%	97.78%	97.87%	97.80%	97.26%
MLP	96.89%	96.82%	96.89%	96.74%	96.00%
Transformer	97.52%	97.42%	97.52%	97.44%	96.82%

All models exceeded 96% in F1-score and Cohen's Kappa, reflecting stable classification capability, with XGBoost leading overall while MLP and Transformer remained competitive despite architectural differences. To examine its classification error patterns in greater detail, the confusion matrix of XGBoost is presented in Figure 1, illustrating its classification behavior across attack categories and misclassification tendencies.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 3, June 2026, hlm. 477 – 484 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i3.4411
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

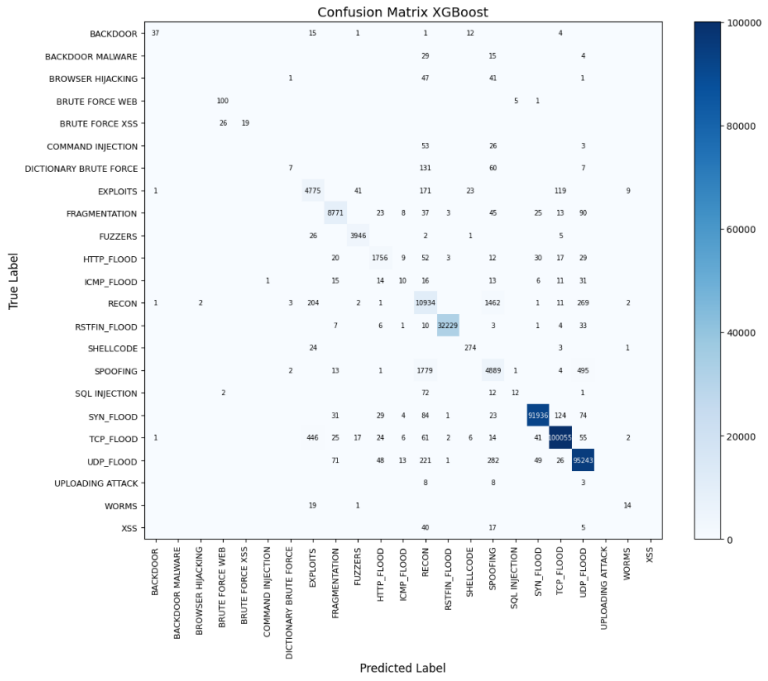

Figure 1. XGBoost Confusion Matrix

The confusion matrix shows that majority classes, particularly flooding-based attacks, were classified with high accuracy, while minority and overlapping classes exhibited higher misclassification due to class imbalance and feature similarity. These results, together with the strong and stable performance across all models, particularly XGBoost's balance of accuracy and stability, support the proposed optimization framework, which leverages model outputs and misclassification patterns to enable adaptive cyber attack simulation across heterogeneous environments, as illustrated in Figure 2. A high-resolution and complete version of Figure 2 is available at repository.

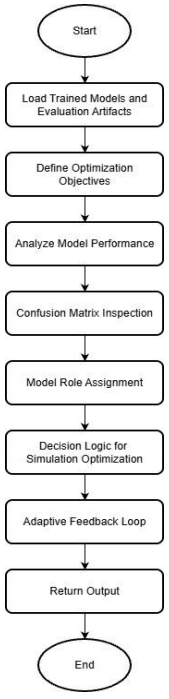

Figure 2. Model Selection Flow Optimization

CONCLUSION

This study evaluated machine

learning and deep learning models for cyber attack classification under heterogeneous network environments, with all models exceeding 96% in F1-score and Cohen's Kappa and XGBoost achieving the best accuracy-stability balance, though minority and overlapping attack classes showed greater misclassification due to class imbalance. These error patterns inform the proposed optimization framework, which assigns each model a functional role, baseline detection, minority-class anomaly reinforcement, or volumetric attack specialization, and drives environment-aware model selection during simulated traffic evaluation, with confusable attacks cross-checked via confidence-weighted voting and periodically re-evaluated to adjust model selection priority.

The framework thus shifts attack simulation from static, single-model classification toward a role-based, error-aware process adapted to observed misclassification tendencies. Future research may extend these models into an interactive cyber defense training simulation, using the best-performing models as an attack behavior engine to generate adaptive attack patterns based on network environment characteristics such as protocol type, traffic intensity, and operational context, supporting game-based training in which users assume a defensive role against dynamic, realistic scenarios whose difficulty and variation can be adaptively adjusted using model outputs and misclassification patterns without retraining.

BIBLIOGRAPHY

[1] Z. Bederna and Z. Rajnai, "Analysis of the cybersecurity ecosystem in the European Union," *International Cybersecurity Law Review*, vol. 3, no. 1, pp. 35–49, 2022, doi: 10.1365/s43439-022-00048-9.

[2] M. Czuryk, "Cybersecurity and Protection of Critical Infrastructure," *Studia Iuridica Lublinensia*, vol. 32, no. 5, pp. 43–52, 2023, doi: 10.17951/sil.2023.32.5.43-52.

[3] P. B. Rangavittal, "Cybersecurity Threats in the Age of Digital Transformation: Strategies for Mitigation and Resilience," *International Journal of Science and Research (IJSR)*, vol. 13, no. 7, pp. 1279–1285, Jul. 2024, doi: 10.21275/SR24721221003.

[4] Check Point Software Technologies, "Cyber Security Report 2024," 2024. [Online]. Available: https://www.checkpoint.com/resources/report-3854/report–cyber-security-report-2024

[5] B. Fischer, D. Meissner, R. Nyuur, and D. Sarpong, "Guest Editorial: Cyber-Attacks, Strategic Cyber-Foresight, and Security," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3660–3663, 2022, doi: 10.1109/TEM.2022.3204165.

[6] S. Sharma, S. S. Agrawal, and S. A. Kumar, "Unlocking Cybersecurity Horizons: Exploring Cutting-Edge Technologies, Strategies, and Trends in the Dynamic Cyber Threat Landscape," in *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 2024, pp. 1–6. doi: 10.1109/ICEC59683.2024.10837210.

[7] D. Chapagain, B. Aryal, D. Chhetri, B. Bastakoti, and P. Bhusal, "Botnet Technology: A Persistent Threat to Digital Infrastructure," *Preprints (Basel).*, Dec.

2024, doi: 10.20944/preprints202412.0660.v1.

[8] M. Bircan and G. Tuna, "Analysis of Windows Operating Systems in Incident Response Processes in Cyber Wars: Use of Open Source Tools," in *Handbook of Research on War Policies, Strategies, and Cyber Wars*, F. Özsungur, Ed., IGI Global Scientific Publishing, 2023, pp. 1–25. doi: 10.4018/978-1-6684-6741-1.ch001.

[9] A. Garg, A. Pandey, N. Sharma, A. Kumar, P. K. Jha, and R. K. Singhal, "An In-Depth Analysis of the Constantly Changing World of Cyber Threats and Defences: Locating the Most Recent Developments," in *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)*, 2023, pp. 181–186. doi: 10.1109/PEEIC59336.2023.10451963.

[10] D. D. Gemmer, B. H. Meyer, E. R. de Mello, M. Schwarz, M. S. Wangham, and M. Nogueira, "A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–7. doi: 10.1109/NOMS56928.2023.10154400.

[11] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *Journal of Web Engineering*, vol. 21, no. 07, pp. 2187–2208, Dec. 2022, doi: 10.13052/jwe1540-9589.2178.

[12] R. Mohammadi, M. M. Hosseini, and R. Bahrami, "Uncovering security vulnerabilities through multiplatform malware analysis," *SECURITY AND PRIVACY*, vol. 8, no. 1, p. e455, 2024, doi: https://doi.org/10.1002/spy2.455.

[13] J. Aws and L. Fritsch, "Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, L. Barolli, Ed., Cham: Springer International Publishing, 2023, pp. 249–257.

[14] Q. Bai, "A Novel Two Step Computer Network Attack and Defense Strategy," in *2024 International Conference on Inventive Computation Technologies (ICICT)*, 2024, pp. 1360–1367. doi: 10.1109/ICICT60155.2024.10544975.

[15] N. S. Abd, K. Karoui, and M. G. Abdulkareem, "Enhancing the Accuracy of Intrusion Detection Systems by Reducing the Rates of False Negatives Through Using XG-boost and Optimization Algorithm," *Security and Safety*, 2024, doi: 10.1051/sands/2024025.

[16] A. Muragodmath, A. Shaikh, N. Baraker, D. Baligar, and P. Patil, "An Efficient Network Attack Detection System Using Recurrent Neural Network Models," in *Proceedings of the 2024 5th International Conference for Emerging Technology (INCET)*, 2024, pp. 1–5. doi: 10.1109/INCET61516.2024.10593098.

[17] S. A. Ajagbe, J. B. Awotunde, and H. Florez, "Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset," *SN Comput. Sci.*,

vol. 5, no. 8, p. 1028, 2024, doi: 10.1007/s42979-024-03369-0.

[18] W. Priatna, I. Sembiring, A. Setiawan, and I. Setyawan, "Network Intrusion Detection Using Transformer Models and Natural Language Processing for Enhanced Web Application Attack Detection," *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, vol. 13, no. 3, pp. 482–493, Dec. 2024, doi: 10.23887/janapati.v13i3.82462.

[19] C. Aouiche, B. Chen, B. Shen, A. Aouiche, R. K. Singla, and S. Dhelim, "Comprehensive Detection of Known Attacks Using Integrated Datasets," in *2024 14th International Conference on Information Science and Technology (ICIST)*, 2024, pp. 924–929. doi: 10.1109/ICIST63249.2024.10805263.

[20] M. Alharby, "Evaluating machine learning approaches for multiple attack classification with improved computational efficiency in IoT networks," *Sci. Rep.*, vol. 15, no. 1, p. 39914, 2025, doi: 10.1038/s41598-025-23711-7.

[21] A. AlMajali, L. Al-Abed, K. M. Ahmad Yousef, B. J. Mohd, Z. Samamah, and A. Abu Shhadeh, "Automated Vulnerability Exploitation Using Deep Reinforcement Learning," *Applied Sciences*, vol. 14, no. 20, 2024, doi: 10.3390/app14209331.

[22] Canadian Institute for Cybersecurity University of New Brunswick, "UNB CIC IoT Dataset 2023," 2023.

[23] Canadian Institute for Cybersecurity University of New Brunswick, "UNB CIC IDS-2018 Dataset," 2018.

[24] University of New South Wales (UNSW) Canberra at ADFA, "UNSW-NB15: Intrusion Detection Evaluation Dataset," 2017.

[25] TeaminCribo, "Cyber Security Attacks Dataset," 2025. [Online]. Available: https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks

[26] R. Purba, R. Lubis, N. Sikana, and G. F. Situmorang, "BERT Model Implementation for Dynamic Sentiment Analysis of Pertamina on Social Media X," *Engineering Science Letter*, vol. 4, no. 02, pp. 77–82, Aug. 2025, doi: 10.56741/IISTR.esl.001139.