

Phishing Detection Using Genetic Algorithm-Based Feature Selection and Boosting Ensemble Learning

Sulaiman Mohd Yusof*, Nazhatul Hafizah Kamarudin*, Abdul Ghafar Jaafar**

*Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

**Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

sulaiman.my@gmail.com, nazhatulhafizah@ukm.edu.my, abdulghafar@utm.my

Abstract—In line with the increasing frequency of complex cybersecurity threats such as phishing attacks, the need for accurate phishing detection has become more important. This study aims to identify the key factors that influencing the effectiveness of phishing detection, develop an enhanced phishing detection model based on these findings, and evaluate the model in terms of accuracy, precision, sensitivity, and F1-score. To build a strong foundation, the PRISMA methodology was applied to conduct a comprehensive literature review. Using KNIME and WEKA, we created a phishing detection model that blends feature selection techniques with a stacked boosting classification approach. A Genetic Algorithm (GA) was used to pinpoint the most relevant features, while Random Forest ensured their accuracy. The classification process utilizes XGBoost, AdaBoost, and RealAdaBoost, with their results integrated through majority voting. The model was tested in two phases using datasets D1 and D2 which obtained from previous studies via Mendeley website. The outcomes were very impressive where for dataset D1, the model achieved 100% marks across all metrics in both testing phases. For dataset D2, it scored 100% during validation and delivered near perfect results which is 100% precision and 99.99% for accuracy, sensitivity, and F1-score during testing. Even more remarkable, these achievements were accomplished using just 27 out of 48 features for D1 and 21 out of 54 features for D2. This study highlights how combining GA-based feature selection with a stacked boosting based model can fortify cybersecurity measures against increasingly tricky phishing threats.

Index Terms—Genetic Algorithm, Machine Learning, Network Security, Phishing Detection, Phishing Websites

I. INTRODUCTION

Phishing attacks continue to be among the most pervasive and damaging cybersecurity threats, targeting individuals, organizations, and critical infrastructure. By impersonating legitimate websites and services, attackers deceive users into revealing sensitive information such as login credentials, personal identifiers, or financial data. The sophistication of phishing schemes has increased substantially, incorporating techniques such as domain spoofing, fast-flux hosting, and URL obfuscation. According to recent threat intelligence reports, phishing attacks now account for a significant proportion of social engineering-based intrusions, with consequences ranging from data breaches to financial fraud and operational disruption.

These widespread and evolving threats have triggered a diverse array of research efforts aimed at combating phishing from multiple dimensions—including detection techniques,

user awareness initiatives, and the development of phishing-resistant authentication systems. For instance, Yusop et al. (2025) provide a systematic review of passwordless authentication technologies and identify phishing as a critical motivator for the transition away from traditional password-based mechanisms. Their review highlights how approaches such as biometric verification, physical security keys, and FIDO2-compliant protocols offer inherent resistance to phishing by eliminating the use of shared secrets—thereby removing the very element that phishing attacks most commonly exploit [1].

However, despite the potential of passwordless authentication to reduce phishing risks at the identity layer, phishing attacks remain prevalent due to the persistence of legacy systems, user behavior, and the emergence of new phishing vectors. Consequently, effective detection systems remain essential to complement authentication reforms and mitigate phishing threats in operational environments.

Traditional phishing detection mechanisms—such as blacklists, rule-based filters, and heuristic engines—have proven insufficient in countering modern phishing strategies [2]. These static approaches are not only reactive and slow to adapt, but also prone to false positives and high maintenance overhead. The dynamic and adversarial nature of phishing attacks requires more adaptive and intelligent solutions. In response, machine learning (ML) has emerged as a viable and effective approach due to its ability to learn patterns, generalize across evolving threats, and automate feature extraction. However, the adoption of ML also brings forth new challenges: class imbalance, noisy features, and overfitting can severely hinder model performance.

To mitigate phishing detection issues, this work introduces an ensemble-based system that integrates intelligent feature selection, high-performing machine learning models, and a dependable voting mechanism. The key contributions of this research are as follows:

- 1) **Optimized Feature Selection:** A Genetic Algorithm (GA) is used to identify the most relevant features by evaluating their accuracy using Random Forest (RF). This is to remove features that are redundant or unnecessary, and leave only the vital ones. It moves the model toward a less resource-intensive one, though intuitively desired, and without losing the original accuracy as much as possible.

- 2) **Boosting Ensemble Design:** The model then trains on these with AdaBoost (AdaB), RealAdaboost (RealAdaB), and XGBoost Algorithm (XGB), which are boosting algorithms that use predicted feature importance and select the best-performing features. They all learn differently, and by collaborating, they are what helps the system become more proficient as a whole at identifying phishing websites effectively and with minimal errors.
- 3) **Reliable Voting Mechanism:** To make the final decision, the system combines predictions from all three models by casting a majority vote to arrive at a final decision. It ensures that the results are more reliable and reduces the chances of unintentionally flagging a legit website as risky or declining to detect an authentic phishing email.
- 4) **Evaluated Across Multiple Datasets:** The model is quantitatively evaluated on two publicly available datasets with different sizes and structures. This further proves the ability of the system to adjust based on different types of data and real-life phishing examples.

Thus the hybrid model pushes forward the problem of phishing detection driven by better feature selection, combining different learning models and also ensuring steady performance. It provides a convenient way for making more secure digital experiences and phishing responses faster.

II. RELATED WORKS

Phishing is becoming more and more sophisticated with each passing day that it necessitates a greater than ever emphasis on identifying phishing websites. Conventional methods have laid a solid groundwork; however, breakthroughs in machine learning and deep learning have improved the field further. In spite of these advances in technology, many crucial issues linger—such as the availability of imbalanced datasets, a surplus of unnecessary or extraneous features, and malicious behavior that masks true intentions. In addition, most current methods are slow in terms of speed demands for real-time protection. In this work, we examine current methods, measure their efficacy, and clarify how our solution builds on and improves upon previous ones to address modern concerns.

A. Traditional Approaches

Traditional methods of phishing detection are largely based on blacklists, rule-based filters, and heuristic feature examination. These methods measure several features like domain name pattern, URL length, SSL certificate expiration, and the presence of suspicious keywords. While having low computational complexity, these approaches are limited by their poor adaptability and high rates of false positives, especially in the context of zero-day attacks and dynamic phishing URLs [2]. Moreover, blacklists are insufficient in handling the rapid creation of new phishing domains, and the heuristic rules lack adequate generalizability to cover emerging attack variations, making them unsuited to today's, large-scale detection efforts.

B. Machine Learning Approaches

Machine learning-based detection models have seen widespread adoption due to their flexibility and ability to learn based on historical data. RF, SVM, and Decision Trees are some of the techniques found to be extremely effective [3]. More recent work has further observed ensemble methods like AdaB and XGB to be especially good in handling feature interactions and class imbalances [4]. However, in general, most of these models are based on heavy feature engineering and might struggle with generalization when learned from datasets that involve imbalance and noise. Many models in this category are plagued by a lack of interpretability and require computational tuning to avoid overfitting or poor performance in real-world traffic conditions.

C. Deep Learning Approaches

Deep learning provides the advantage of automated feature extraction, enabling models to recognize complex and non-linear relationships in phishing datasets. CNNs and LSTMs are architectures that are found to be applicable in analyzing sequences of URLs, HTML, and webpage images [5]. Hybrid Deep Neural Network-LSTM models are found to be over 99% accurate, especially when complemented with Natural Language Processing-based tokenization and character embeddings [6]. However, while powerful, deep learning approaches are beset by challenges in deployment due to high costs of training, limited interpretability, and susceptibility to adversaries—miniscule adjustments to inputs can deceive the classifier [7].

D. Hybrid and Ensemble Models

In light of the constraints seen in individual models, recent research stresses the importance of crafting hybrid models that couple feature selection with ensemble learning strategies. Such models include PhishPrint (2021), which combines behavioral profiling with supervised classification algorithmic techniques, and BoostDroid (2023), which couples CatBoost and LightGBM with automated feature selection [8]. More recent research employs either genetic algorithms or swarm intelligence techniques to optimize feature selection before their input into ensemble classifiers [9]. A recent extensive literature review by Abdillah et al. has found ensemble learning and feature selection to be key avenues in phishing detection, showing their positive impacts on classification accuracy and the generalizability of models across a range of phishing formats, including websites, emails, and URLs [10]. While hybrid models achieve accuracy gains and false positive rate reductions, they are largely faced with increased complexity, longer training times, and limited verification on a range of phishing sources.

E. Gaps and Our Contribution

Notwithstanding considerable advances in detecting phishing attempts, many long-term challenges remain. Various models are found to be less adaptable to rapidly evolving tactics used in phishing, particularly with regard to zero-day

exploits. Also, some models are based heavily on static or hand-engineered feature sets, thus limiting their scalability and effectiveness in tackling newly emerging threats. Further, a balance between detection accuracy and computational cost remains challenging, thus compromising the usability of real-time implementations. While ensemble models are promising, they are often weak in terms of robust aggregation mechanisms, thus being prone to misclassification when the participating learners perform poorly [11]. In addition, according to Abdillah et al., the lack of standardized evaluation metrics and reporting of parameters in previous works hinders fair performance comparison and reproducibility [10].

In response, we developed a hybrid detection model that improves both performance and reliability. We start by using a Genetic Algorithm (GA) to find the most important features, with Random Forest (RF) evaluating their accuracy. These chosen features are then used in three varying boosting classifiers with differing viewpoints: XGBoost, AdaBoost, and Real AdaBoost. In order to make sure that there is consistent prediction, their predictions are aggregated via majority voting. This model was highly successful and resilient when applied to two phishing datasets of various configurations. Our work by addressing typical issues of overfitting, feature overload, and inconsistency is bringing phishing detection one step nearer to being ready for the real world.

III. METHODOLOGY

Our study introduces a hybrid machine learning framework designed to detect phishing websites more accurately by combining feature selection, ensemble learning, and majority voting. The model is built to tackle common challenges like imbalanced data, redundant features, and the ever-changing tactics used in phishing attacks. The approach follows four main phases: data preprocessing, model development, training, and evaluation—each playing a crucial role in building a strong and adaptable detection system.

A. Data Collection and Preprocessing

This research uses two publicly available datasets from Mendeley, referred to as D1 and D2. These datasets contain labeled examples of both legitimate and phishing websites. Dataset D1 includes 10,000 balanced entries—half legitimate and half phishing—with 48 features each. Dataset D2 is much larger, containing 235,795 samples with a slightly imbalanced split which consist of 57.2% legitimate and 42.8% phishing and 54 features. Together, these datasets provide a diverse and up-to-date representation of modern web-based threats.

To ensure rigorous evaluation, each dataset was partitioned using stratified random sampling with a preset random state (313) into three subsets: 70% for training, 15% for validation, and 15% for final testing. This approach maintains the original class distributions across all splits while guaranteeing reproducible results. Categorical features were processed using one-hot encoding to ensure compatibility with machine learning algorithms.

The stratified splitting strategy is particularly valuable for D2's slight class imbalance, preventing evaluation bias and ensuring all subsets contain representative examples of both classes. By preserving the natural data distribution in each partition, we maintain the reliability of performance metrics. All processed datasets were structured for efficient batch loading during model training and evaluation.

B. Model Development

The proposed model is designed to efficiently identify phishing websites by combining optimized feature selection with robust ensemble classification. The model consists of three key components.

1) *Automated Feature Selection Using GA*: This evolutionary approach outperforms traditional filter/wrapper methods by balancing exploration and exploitation of the feature space [12]–[14].

- **Stratified Data Partitioning**: The dataset was split into 70% training and 30% testing sets using stratified sampling, preserving class distribution integrity.
- **RF Evaluation**: Feature subsets were assessed using a RF learner with Gini Index split criterion (max depth=10, node size=1) and 100-tree ensembles for robust importance estimation.
- **Accuracy-Optimized Selection**: The GA was configured to maximize accuracy as the primary fitness criterion during feature space exploration.
- **Computational Efficiency**: The final output delivers an optimized feature subset that enhances detection performance while minimizing redundant computational overhead.

2) *Ensemble Classifiers*: After feature selection, the processed data is fed into three distinct boosting algorithms, each designed to capture complementary patterns in phishing detection. Unlike single-model approaches, this ensemble strategy combines diverse learning biases to improve generalization and robustness [15]–[17].

- **XGB**: A high-performance implementation of gradient boosting that incorporates regularisation and optimised tree learning for speed and accuracy. It is well-suited for high dimensional datasets and has been widely adopted in machine learning competitions..
- **AdaB**: A boosting technique that iteratively trains weak classifiers, typically decision stumps, while adjusting sample weights to focus on previously misclassified instances, thereby improving sensitivity to difficult cases.
- **RealAdaB**: An extension of AdaBoost that utilises real-valued confidence scores from weak learners rather than binary outputs. This enables more refined updates and often yields smoother decision boundaries with improved classification performance.

3) *Majority Voting*: The final stage uses majority voting to combine predictions from all three models (XGB, AdaB, and RealAdaB). When at least two models agree on whether a website is phishing or legitimate, we use that as the final answer. This simple voting system makes our final decision more

reliable than using any single model alone. The architecture of the proposed framework is illustrated in Figure 1.

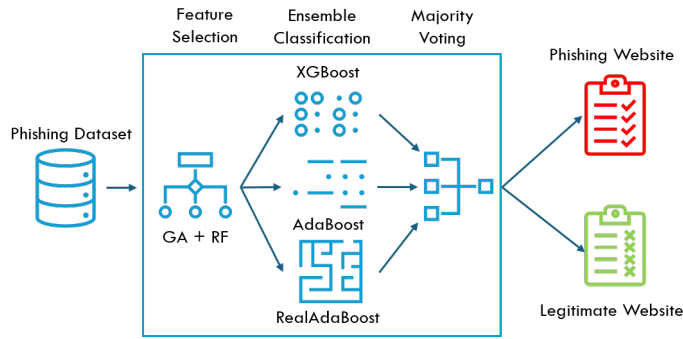


Fig. 1. Proposed model for phishing website detection.

C. Training Process

The training process was conducted using a unified dataset, which was preprocessed and split into 70% training, 15% validation, and 15% testing to ensure robust generalization and reliable performance evaluation. Each model (XGB, AdaB, and RealAdaB) independently learned from the same dataset, with their respective configurations optimized for their specific algorithms.

Each model was trained independently with its own specific settings. XGB used a learning rate of 0.3, multi-class soft probability as the loss function, and ran for 100 boosting rounds. It included L2 and L1 regularization (both set to 1.0) to prevent overfitting, a maximum tree depth of 6, and early stopping if no improvement was seen in validation loss for 10 rounds. AdaB and RealAdaB both used RF as their base classifier, with 10 trees and 10 iterations. AdaB combined weak learners into a strong learner, while RealAdaB used real-valued predictions and a shrinkage factor of 1.0 to control the learning rate.

For both AdaB and RealAdaB, the RF parameters included default feature splitting (square root of total features), a random seed of 1, and single-threaded execution. Early stopping was not applied since the number of iterations was fixed at 10 for both models. Each model's unique configuration ensured it was optimized for its specific algorithm and learning approach. To prevent overfitting and enhance generalization, several techniques were implemented across all models:

- **Dropout-like Behavior:** In XGB, column sampling acted as a form of dropout, reducing reliance on specific features.
- **Early Stopping:** Implemented in XGB to monitor validation loss and halt training if no improvement was observed for 10 consecutive rounds.
- **Fixed Iterations:** For AdaB and RealAdaB, the number of iterations was capped at 10 to avoid excessive complexity and overfitting.

D. Evaluation and Testing

The final model evaluation utilized the 15% test partition, which remained separate during the development process.

We used standard performance metrics like accuracy, precision, recall, F1-score, and confusion matrix. These gave a full picture of how reliable, sensitive, and strong the classification was. Our model did an outstanding job of detecting phishing websites on both datasets—showing either perfect or nearly perfect results. And the best part? It achieved this high level of accuracy while using fewer features, which means it's not only effective but also efficient. This makes the framework highly adaptable and well-suited for real-world use.

Figure 2 shows how the whole model is trained and tested.

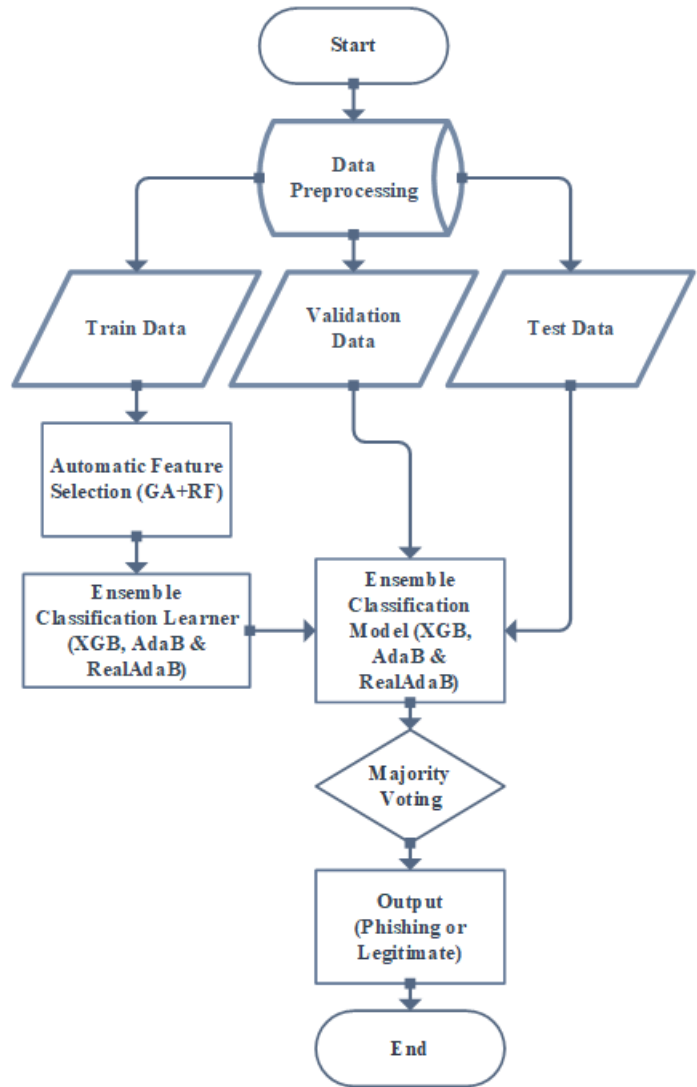


Fig. 2. Training and Evaluation Flow.

IV. RESULTS

We performed comprehensive testing to ascertain the extent to which the model is effective in predicting phishing websites. In this section, we evaluate its performance during validation

and final testing, focusing on how accurately it can tell real webpages and fake ones.

A. Training and Validation Performance

For validation, we set aside 15% of each dataset to test the model independently. In order to ensure that the results are fair and not biased, the correct labels were hidden from the model during prediction and were only used after all predictions to test performance. It helps to ensure that the validation is a reflection of how the real world works but also helps preserve evaluation accuracy and credibility.

The results showed excellent performance for both datasets, and made no mistakes in classification, hence zero false positives and false negatives. The model achieved 100% accuracy in identifying phishing websites apart from legitimate ones, which shows the strength and the reliability of the proposed model.

The results remain consistent for both balanced (D1) and imbalanced datasets (D2), indicating the robustness of the model over different styles of data. Figures 3 and 4 display the confusion matrices for D1 and D2 during validation while Figure 7 and Figure 8 show the ROC Curve, clearly demonstrating an excellent performance of the model.

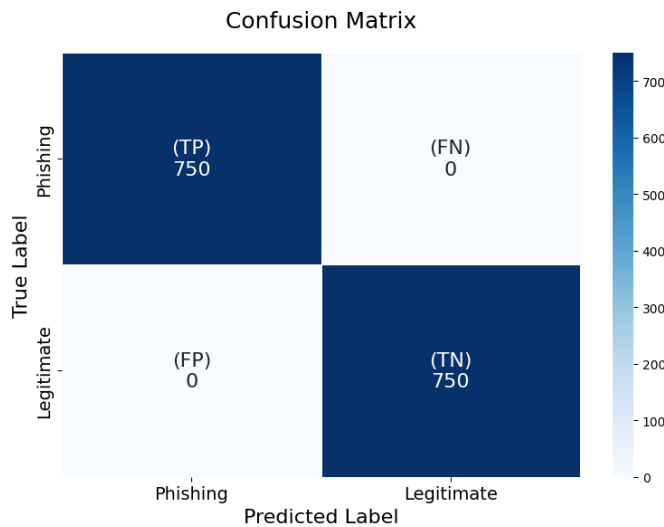


Fig. 3. Validation result for D1.

B. Model Performance Comparison

We compared our model to the previous boosting model and evaluated their properties using the same metrics. Our comparison was focused on the accuracy, precision, recall, and F1-score of each model, as well as the number of features each model used. The detailed comparison of the proposed model with the BMLSELM and MLSELM boosting-based model is shown in Table 1.

Based on Table 1, the proposed ensemble-based model outperforms traditional machine learning models in phishing detection. It obtained 100% accuracy, surpassing the 98.8% and 98.9% accuracy of the BMLSELM and MLSELM models,

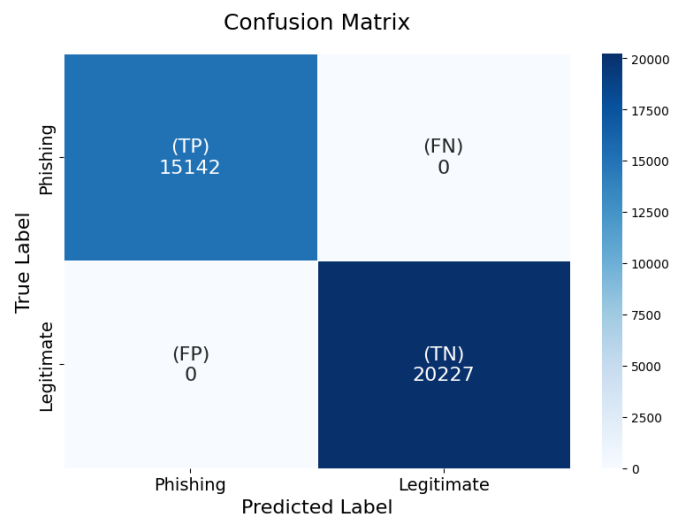


Fig. 4. Validation result for D2.

TABLE I
COMPARISON OF PROPOSED MODEL WITH BMLSELM AND MLSELM

Metric	PROPOSED	BMLSELM	MLSELM
	(D1)	(D2)	(D2)
Accuracy	1.00	0.988	0.989
Precision	1.00	0.989	0.985
Recall	1.00	0.987	0.992
F1-Score	1.00	0.988	0.989
Features Used	27	33	48

respectively. This highlights its improved ability to distinguish between phishing and legitimate URLs effectively. Additionally, the hybrid approach significantly reduced false positives and false negatives, achieving 100% precision and recall. These results underscore the model's reliability in real-world applications. In terms of computational efficiency, the proposed model demonstrated significant advantages, particularly in its ability to achieve high performance with a reduced feature set.

C. Testing Performance

The classification report further evaluates the model's predictive performance during the testing phase, summarizing precision, recall, and F1-score. The confusion matrix provides additional insights into the model's classification capabilities for both datasets. Confusion Matrix: D1 testing result:

- True Positive (TP): 750 phishing URLs correctly identified.
- False Positives (FP): 0 legitimate URLs misclassified as phishing.
- True Negatives (TN): 750 legitimate URLs correctly identified.
- False Negatives (FN): 0 phishing URLs misclassified as legitimate.

Confusion Matrix: D2 testing result:

- True Positive (TP): 15141 phishing URLs correctly identified.

- False Positives (FP): 0 legitimate URLs misclassified as phishing.
- True Negatives (TN): 20228 legitimate URLs correctly identified.
- False Negatives (FN): 1 phishing URLs misclassified as legitimate.

TABLE II
CONFUSION MATRIX SUMMARY FOR DATASET D1

Phase	TP	TN	FP	FN
Validation	750	750	0	0
Testing	750	750	0	0

TABLE III
CONFUSION MATRIX SUMMARY FOR DATASET D2

Phase	TP	TN	FP	FN
Validation	15142	20227	0	0
Testing	15141	20228	0	1

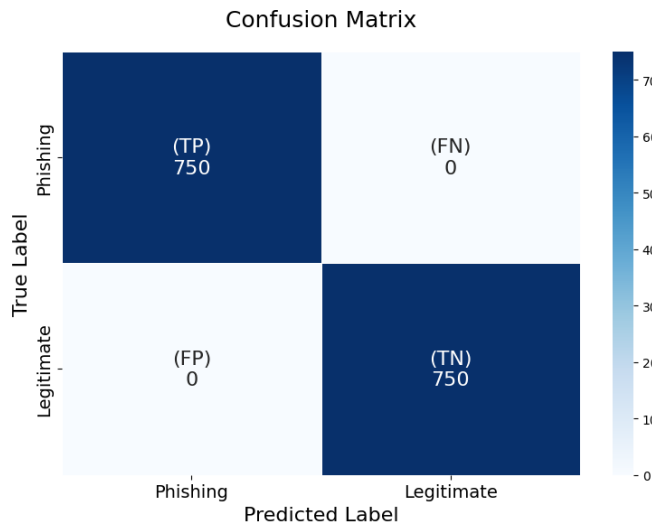


Fig. 5. Testing result for D1.

The confusion matrix for D1 shows perfect classification with no false positives or negatives, highlighting the model's strength in handling balanced datasets. For D2, the model achieves near-perfect performance with only one false negative, demonstrating its ability to manage imbalanced datasets effectively. These results confirm the model's high accuracy and reliability in detecting phishing URLs, outperforming traditional methods by leveraging ensemble learning and majority voting. The use of only 27 discriminative features ensures computational efficiency, making the model robust against class imbalance, feature redundancy, and adversarial attacks, and suitable for real-world cybersecurity applications.

V. DISCUSSION

We designed a hybrid phishing detection model in our approach with four state-of-the-art feature selection Genetic

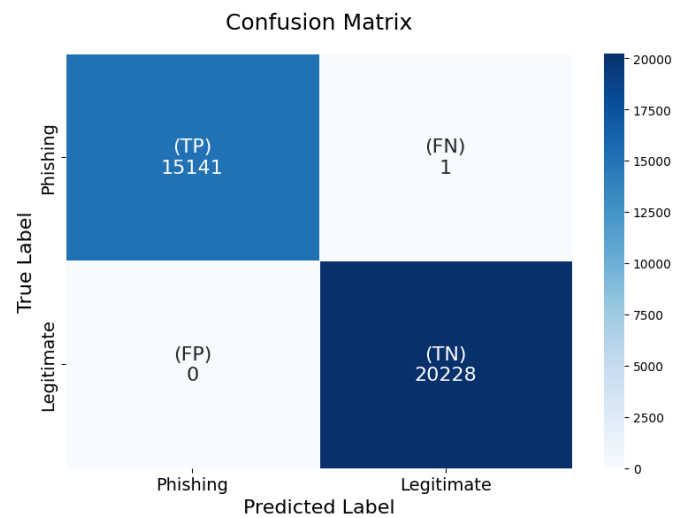


Fig. 6. Testing result for D2.

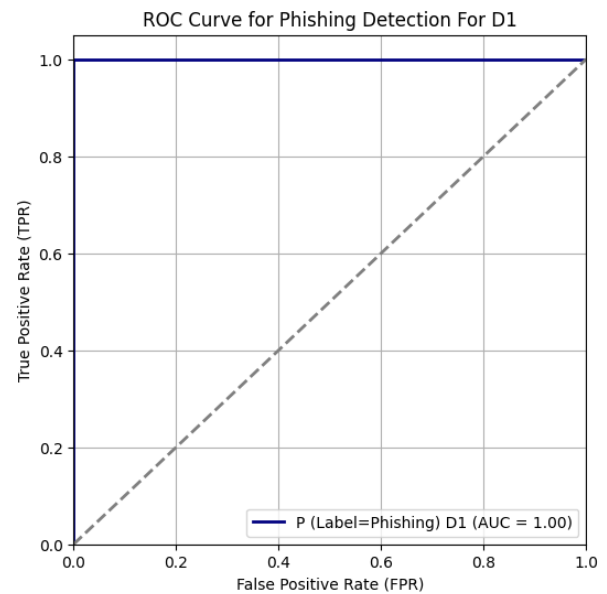


Fig. 7. ROC Curve for D1.

Algorithm (GA), and three ensemble classifiers XGBoost, AdaBoost, and RealAdaBoost using majority voting. The model performed well on two public datasets D1 and D2, exhibiting almost perfect accuracy.

Examining this feature selection, driven by a Genetic Algorithm and scored on Random Forests, the model maintained its precision with less number of features. It has surpassed well-known models like BMLSELM and MLSELM, as it achieves higher accuracy using only 27 features compared to 33 and 48 in those models.

The ensemble design of the proposed model enabled it to deal with various data challenges, such as unbalanced samples and correlated features. Its performance across datasets indicates that it is a reliable enough model to be trusted for real

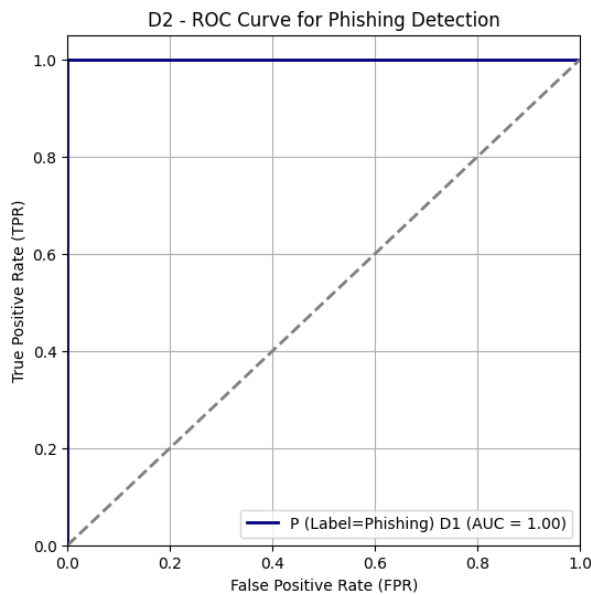


Fig. 8. ROC Curve for D2.

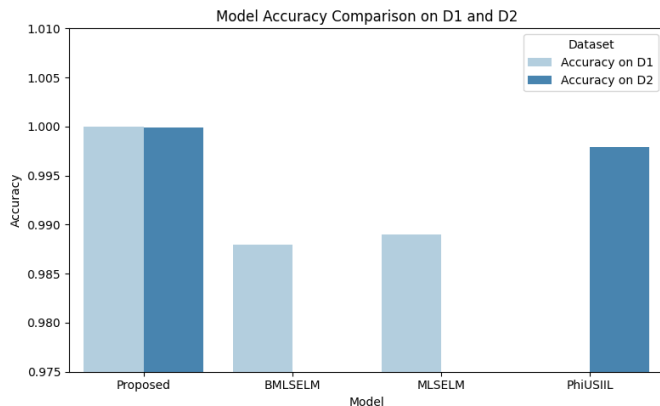


Fig. 9. Model accuracy comparison.

applications in phishing detection as well.

VI. CONCLUSION

In summary, this research has attained its goals. First, it explored the key factors that impact the performance of phishing detection models, such as feature selection, balance and data quality, algorithm, and hyperparameter tuning. Second, it proposed a machine learning technique that uses an ensemble of XGBoost, AdaBoost, and Real AdaBoost with genetic algorithm-based feature selection and majority voting. The obtained model outperformed state-of-the-art techniques in precision, recall, F1-score, and, in turn, was more accurate. These results have important implications in cybersecurity research and present practical application of the suggested model to early detection of phishing. The research, though, is limited by static data and has not been tested in real-time settings. Future research projects need to put more emphasis on real-time testing and the inclusion of explainable

artificial intelligence models like SHAP or LIME to enable transparency, trust, and usability on various platforms.

ACKNOWLEDGMENT

We would like to acknowledge the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia that supported us in this work under the grant GGPM-2023-070.

REFERENCES

- [1] M. I. M. Yusop, N. H. Kamarudin, N. H. S. Suhaimi, and M. K. Hasan, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, vol. 13, pp. 13919–13935, Jan. 2025, doi: 10.1109/ACCESS.2025.3528960.
- [2] W. Rafique, M. Humayun, M. A. Jan, R. Jurdak, and S. M. K. Khan, "An evaluation of heuristic-based phishing detection techniques," *Computers & Security*, vol. 92, p. 101768, 2020.
- [3] M. S. Islam, M. R. Asaduzzaman, and M. M. Rahman, "Phishing URL detection using ML techniques: A comparative study," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 354–372, 2021.
- [4] L. Fang, Y. Zhang, and X. Zhao, "Ensemble-based phishing URL detection using AdaBoost and XGBoost," *Information Sciences*, vol. 631, pp. 59–74, 2023.
- [5] K. L. Chiew, S. N. Sze, and W. K. Tiong, "Deep PhishNet: A CNN-LSTM framework for phishing detection," *Expert Systems with Applications*, vol. 190, p. 116229, 2022.
- [6] Y. Zhou, M. Zhang, X. Jiang, and Z. Chen, "Intelligent detection of phishing websites using deep learning," *IEEE Access*, vol. 8, pp. 11724–11733, 2020.
- [7] T. Wang, J. Chen, L. Zhou, and R. Liu, "On the robustness of deep learning for phishing detection," *Neural Computing and Applications*, vol. 35, pp. 11067–11081, 2023.
- [8] R. Kalabarige, A. R. A. Rahman, and F. Ahmad, "A boosting-based hybrid feature selection and multi-layer stacked ensemble learning model," *Journal of King Saud University – Computer and Information Sciences*, in press, 2023.
- [9] A. Jain, S. Sharma, and P. Rawat, "Genetic algorithm-optimized hybrid learning model for phishing website detection," *Applied Soft Computing*, vol. 120, p. 108675, 2022.
- [10] R. Abdillahi, Z. Shukur, M. Mohd, and T. M. Z. Murah, "Phishing classification techniques: A systematic literature review," *IEEE Access*, vol. 10, pp. 41574–41589, 2022.
- [11] M. Singh, R. Sahu, and R. Raw, "Ensemble classifier for phishing detection using voting mechanism," *Procedia Computer Science*, vol. 187, pp. 469–476, 2021.
- [12] Ş. B. Dalkılıç, A. Özgür, and H. Erdem, "Balancing exploration and exploitation in genetic algorithm optimization: a novel selection operator," *Evolutionary Intelligence*, vol. 18, Article 40, 2025.
- [13] M. G. Altarabichi, S. Nowaczyk, S. Pashami, and P. S. Mashhad, "Surrogate-assisted genetic algorithm for wrapper feature selection," *arXiv preprint arXiv:2111.09074*, 2021.
- [14] F. Amini and G. Hu, "A hybrid two-layer feature selection method using genetic algorithm and elastic net," *arXiv preprint arXiv:2001.11177*, 2020.
- [15] S. Innab, H. M. Hasan, and A. H. Jasim, "Phishing attacks detection using ensemble machine learning algorithms," *Computer Modeling in Engineering & Sciences*, vol. 139, no. 2, pp. 1689–1703, 2024.
- [16] R. Kalabarige, A. R. A. Rahman, and F. Ahmad, "PhishGuard: A multi-layer ensemble model for phishing URL detection using gradient-based boosting classifiers," *arXiv preprint arXiv:2409.19825*, 2024.
- [17] S. Akshayah, R. S. Menon, and A. Rajkumar, "A web phishing detection model using voting-based ensemble of boosting classifiers," *SSRN Electronic Journal*, 2025. [Online]. Available: <https://papers.ssrn.com/abstract=5245455>
- [18] A. Prasad and S. Chandra, "PhiUSIIL phishing URL dataset," *Mendeley Data*, V2, 2023. [Online]. Available: <https://doi.org/10.17632/shwpxsxxy2.2>
- [19] C. L. Tan, "Phishing dataset for machine learning: Feature evaluation," *Mendeley Data*, V1, 2018. [Online]. Available: <https://doi.org/10.17632/h3cgnj8hft.1>



Sulaiman Mohd Yusof received the Bachelor's degree in computer science, majoring in computer system, from Universiti Teknologi Malaysia, Skudai, Johor, Malaysia, in 2005. He obtained the Master's degree in cyber security from Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia, in 2025. His major field of study is computer systems and cybersecurity. He is currently serving as a Eksekutif Hasil Kanan II at the Seksyen Keselamatan Siber, Jabatan Digital, Inland Revenue Board of Malaysia. In this role, he is responsible for enterprise cybersecurity

operations, including network security management and Security Operations Center (SOC) oversight. His scope of work includes the administration and optimization of SIEM, IPS, and NDR platforms to enhance threat visibility, incident response readiness, and overall organizational cyber resilience. His professional interests focus on cybersecurity operations, security monitoring, and incident handling. Mr. Sulaiman is a Professional Technologist (Ts.) registered with the Malaysia Board of Technologists. He also holds the GIAC Certified Incident Handler (GCIH) certification, issued by Global Information Assurance Certification.



Nazhatul Hafizah Kamarudin is currently a Senior Lecturer at the Centre for Cybersecurity, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM). She received her Bachelor of Engineering in Electrical Engineering and Master of Engineering in Wireless Security from Stevens Institute of Technology, New Jersey, USA. In 2019, she was awarded the Ph.D. degree in Electrical Engineering, specializing in Security and Cryptography, from Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia. Her research interests

include authentication, network security, the Internet of Things (IoT), and network intrusion detection. Prior to joining UKM, she served as an Assistant Professor at UCSI University and as a Lecturer at Infrastructure University Kuala Lumpur (IUKL). She is a Certified Ethical Hacker (CEH) accredited by EC-Council and a Chartered Engineer (CEng) registered with the Institution of Engineering and Technology (IET), UK.



Abdul Ghafar Jaafar obtained his PhD in Cybersecurity from Universiti Teknologi Malaysia (UTM) in 2020. He has over 10 years of industry experience, which supports his academic and research activities. He is currently serving as a Senior Lecturer at the Faculty of Artificial Intelligence (FAI), Universiti Teknologi Malaysia. His research spans a broad spectrum of cybersecurity domains, with particular emphasis on Ethical Hacking, Network and Application Security, Intrusion Detection and Prevention Systems (IDPS), Endpoint Detection and

Response (EDR), Cyber Threat Intelligence (CTI), Malware Analysis and Mitigation, Cryptographic Systems, Digital Forensics, and the application of Artificial Intelligence in Cybersecurity. He holds professional certifications as a CompTIA PenTest+ Certified Professional and a Certified Ethical Hacker (CEH). He is a Professional Technologist (Ts.) registered with the Malaysia Board of Technologists (MBOT) with a specialization in Cybersecurity.