Intelligent Detection Approaches for Securing E-Banking Platforms against Phishing Websites

[1]Okonkwo Chisom Michael., [1]Ngene Chidiebere David.,[2]Onyedeke, Obinna Cyril*

[1]Enugu State University of Science and Technology, ESUT. Department of Computer Science, Nigeria

[2]Department of Computer Science, University of Nigeria, Nsukka, Nigeria

*Corresponding Author

DOI: https://doi.org/10.47772/IJRISS.2025.910000188

Received: 02 October 2025; Accepted: 08 October 2025; Published: 07 November 2025

ABSTRACT

E-banking has introduced fresh innovations in finances because of the new conveniences, efficiencies, and global access. Conversely, the fast spread of e-banking has increased phishing attacks, which are a cyber-attack on banking sites. This paper concentrates on the intelligent detection of phishing websites to protect e-banking systems, particularly the assessment and comparison of algorithms on intelligent detection. The UCI Phishing Dataset URL, content, and behavioral features were diverse and applied in training and testing different machine-learning models. Support Vector Machines, Random Forest, Neural Networks, XGBoost, and Hybrid performance models were evaluated in terms of accuracy, precision, recall, F1-score, and AUC. Although SVM showed a mediocre detection risk, the Random Forest and Neural Networks proved to be significantly more reliable, whereas XGBoost exhibited the highest performance due to its accuracy and scalability of performance. All tests yielded the most reliable results, and hybrid systems achieved the highest metrics and performance. This is revealed the most reliable detection and control systems of phishing threats in e-banking system since phishing frauds hugely make use of vulnerabilities in e-banking. In online banking systems, phishing frauds are best controlled by hybrid systems and intelligent detection systems. Some of the practical refinements provided by this study are improving fraud prevention, customer confidence, and regulatory compliance within financial organizations. The investigations of the future must focus on creating mechanisms of fraud detecting in real-time, using larger and more diverse data sets, and more adaptable and adaptable learning systems that can evolve with phishing attacks to sustain the digital banking protection mechanisms.

Keywords: Phishing Detection, E-Banking Security, Machine Learning Algorithms, Hybrid Models.

INTRODUCTION

The emergence of new technologies has significant consequences bringing even bigger changes in financial services across the globe and the spread of electronic banking systems. Customers can easily and conveniently access banking services and complete numerous financial operations in any location where they transact, pay their bills, transfer funds, and manage their accounts through e-banking systems (Kumari & Nagarjan, 2022). These services give the customers convenience and this led to the actualization of the e-banking systems in the modern automated financial systems. Above all, e- banking systems facilitate financial inclusion to the emerging economies. Nevertheless, convenience and ease of use of e-banking services has also led to jeopardy of the safety of these systems as has become a key priority to consumers and a growing number of financial service providers (Money & Iyoha, 2025). A plethora of threats attacks e-banking systems, and phishing can be considered one of the most common and the most advanced. The fraudsters use online banking portals and masquerading as clients to cheat people and persuade them to provide them with sensitive banking details. The phishing attacks that cybercriminals use are dynamic, advanced, and entrenched in the online exploitation of the human factor, which is hard to detect or counter with the normal and available security (Pinjarkar et al., 2024). Successful phishing attacks cause customers to lose money and tarnishes the reputation of affected financial institutions, which also loses credibility in the eyes of the general population and regulatory oversight. The current strategies that are being used to deal with phishing attacks (blacklisting, heuristic systems and manual reporting) are ineffective when it comes to countering the increased and more complex ways of attacking that are collectively being used

by the attackers (Jabir et al., 2025). Blacklists, such as those, are not aware of phishing sites until they are reported which leaves users exposed to zero-day attacks. Similarly, phishing methods change rapidly, which is too fast to be matched by heuristic mechanisms. It is because of them that I feel that the necessity to have more intelligent systems that can effectively identify phishing attacks real-time has been long overdue (Li et al., 2025). Specifically, sophisticated intelligent detection methods informed by artificial intelligence and machine learning technology are to be used to address this requirement. These systems examine the characteristics of websites, user behavior and contextual indicators by using data-driven models to detect phishing attacks with extreme precision and flexibility (Shahbazi et al., 2025). The smart systems will be dynamic and will adjust and evolve faster than the phishing techniques and will offer the e-banking services with great security. This study explores intelligent ways of guarding e-banking systems against phishing websites. It examines various algorithms and evaluates the best performance and strategies that are likely to enhance security of online banking systems and consequently curb cybercrime in the online banking environment.

Problem statement

The existence of e-banking platforms is subject to threats that have never been seen to consumer confidence and financial institutions exposed to potentially harmful reputational effects due to the continued and constantly developing sophistication of phishing attacks. Financial phishing attacks still present technological and human weaknesses that criminals can use to access confidential financial data directly. Their social engineering attacks employ AI and dynamically spoof sites. Ex use phishing technology and human weaknesses to steal confidential financial information. Fraudulently making counterfeit websites or messages to masquerade as genuine banking services with the view of stealing user passwords, account numbers and credit card details. Even though automated phishing intercepting or stealing credentials is a simple affair, the sharing of fake websites or messages are complex highly sympathetic phishing attacks, and as a result, the imitations of banking websites are extremely difficult to execute. Specifically, these attacks are particularly efficient at evading the industry dependence on blacklists and shorthand detection of threats. This issue would need balanced smart solutions that can precisely and quickly locate and adjust to the detection of phishing attacks to safeguard e-banking successfully.

LITERATURE REVIEW

Overview of phishing in the context of e-banking.

Phishing has become one of the most long-term and harmful threats to electronic banking (e-banking), which erodes the security and trust upon which digital financial services rely. It can be described as a trick in which cybercriminals masquerade as trusted institutions, frequently by using fake websites, emails, or messages to lure users into sharing sensitive information like passwords, credit cards or personal identification information (Nadeem et al., 2023). Phishing plays a significant role because it can use technological weaknesses and human faithfulness as an effective means of attack in the setting of e-banking where remote and often unchecked financial transactions are carried out (Pinjarkar et al., 2024). Phishing in online banking is also encouraged by the growing digitalization of financial services and the convenience that customers demand online platforms to provide. Attackers build counterfeit banking portals that look and feel like legitimate websites; send believable emails containing harmful links or social engineering techniques that make it appear that there is a sense of urgency and that an user must make a decision without hesitation (Yuspin et al., 2024). More sophisticated methods, including spear phishing, pharming, malware-aided phishing, have further complicated such attacks and can now be harder to be detected with traditional methods. In the case of financial institutions, the ramifications of phishing are varied (Nadeem et al., 2023). In addition to direct financial losses, a successful phishing attack undermines customer trust, destroys institutional reputations, and sets banks up against legal and regulatory consequences (Nadeem et al., 2023). Instead, customers expose themselves to identity theft, financial fraud and emotional trauma, which, in many cases, have long-term effects. Phishing, therefore, not only interferes with individual users but also other more valuable attempts to create secure, inclusive, and resilient digital banking systems. Conventional anti-phishing techniques including blacklists, heuristic-based systems, and manual reporting are not very effective especially in dealing with zero-day phishing sites, which develop at a high rate. These shortcomings indicate the urgency of smarter and more adaptive methods (Aldakheel et al., 2023). By relying on artificial intelligence (AI), machine learning (ML) and a combination of both, intelligent

detection systems would be able to process large volumes of data, discovering previously undetected patterns and detecting phishing attempts in real-time with even higher precision. Such strategies are becoming widely regarded in the context of e-banking as a way to enhance the security, safeguard the users and maintain their confidence in online financial systems.

Intelligent detection approaches

The intelligent detection methods are more sophisticated, dynamic strategies employing computational intelligence, machine learning and artificial intelligence to detect and curb phishing attacks more efficiently than conventional security mechanisms. In contrast to blacklist and heuristic-based systems that use set rules, intelligent approaches are databased and thus they can identify new, emerging phishing patterns and act in real-time. This flexibility is especially useful in the environment of e-banking, where stakes of phishing attacks are great and threats are developing at an extremely fast pace.

1. **Machine Learning (ML) Algorithms:** The intelligent detection systems rely on the use of Machine Learning (ML) Algorithms. The most popular supervised learning systems, which include Support Vector Machines (SVM), Random Forests, Decision Trees, Logistic Regression, and k-Nearest Neighbors (k-NN) are typically used to classify websites as either legitimate or phishing, based on features extracted (Tufail et al., 2023). Such characteristics can be URL structure, HTML content, age of the domain, details of the Jessica Stewart Lawrence (SSL) certificate and behavioral indicators. Such ensemble techniques as Gradient Boosting and XGBoost provide an extra benefit to predictive accuracy by incorporating the merits of a variety of classifiers.
2. Deep Learning Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are becoming more commonly used to detect phishing using non-linear relationships that are complex and require learning large amounts of data. CNNs can efficiently analyze visual similarities between phishing and legitimate sites whereas the RNNs can successfully extract sequential information in the URL strings as well as user interactions (Alshingiti et al., 2023). These models have increased detection precision, but this comes at the cost of increased datasets and more computation.
3. Hybrid Models integrate a variety of intelligent methods, combining machine learning, deep learning and heuristic methods to enhance resilience and minimize false positives. As an example, hybrid systems can apply ML algorithms at the first classification step and deep learning at the second step to guarantee speed and accuracy (Ibrahim et al., 2025).
4. Natural Language Processing (NLP) is used to scan phishing emails and web content, detecting suspicious patterns of language, misspellings, or irregularities in the style of communication. In addition, adaptive learning models enable detection systems to keep up to date with the latest phishing tricks and thereby maintain effectiveness in the long term (Saias, 2025).

METHODOLOGY

This paper adopts a comparative experimental research design that seeks to assess the effectiveness of various intelligent detection algorithms in detecting phishing websites in the e-banking systems. Experimental approach is the right approach because it enables systematic testing, benchmarking, and comparison of various models under controlled conditions in order to establish their strengths and weaknesses vis-a-vis each other. Data set collection entail publicly accessible data sets like the UCI Phishing Website Dataset that offer an annotated instance of both legitimate and phishing websites. Available real e-banking data will also be used to add variety to these datasets to improve validity of findings. To select the features, three groups of will be taken: URL-based features (length, use of special characters, and depth of subdomain), content-based features (HTML tags, scripts, and details of the certificate), and behavioral features (redirection, pop-ups, and response time). These capabilities can record technical and contextual pointers to phishing attacks. The algorithms that are taken into account are Support Vector Machines (SVM), Random Forests, Neural Networks, XGBoost, and Hybrid models that are a combination of several classifiers. This choice represents a compromise of classical machine learning and those of the state-of-the-art ensemble or deep learning approaches. Detection effectiveness will be measured using performance measures like accuracy, precision, recall, F1-score, and Area under the Curve (AUC). Such metrics give us a comprehensive picture of the model performance, and the correctness, as well as the robustness, are both considered. The experiments are going to be run in Python as the main programming language; libraries

like Scikit-learn will be used to run classical ML models, TensorFlow to run deep learning models, and WEKA to run comparative validation. The selected methodology is reasonable because it combines various datasets, efficient feature engineering, and a range of smart algorithms, which offer a solid foundation to determine the most efficient way to detect phishing in the e-banking setting.

RESULTS

Table 1: Performance metrics

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
SVM	92.4	91.8	90.6	91.2	93.1
Random Forest	95.7	95.3	94.8	95.0	96.5
Neural Network	96.3	96.0	95.7	95.8	97.0
XGBoost	97.1	96.8	96.5	96.6	97.8
Hybrid Model	98.0	97.7	97.3	97.5	98.6

Table 1 indicates that all the algorithms were effective, although there are significant differences. SVM had the lowest accuracy (92.4%), which suggests that it is not as effective when it comes to processing complicated phishing characteristics. Random Forest and Neural Networks showed better outputs, with 95.7 and 96.3% accuracy respectively, which shows their strength in pattern recognition. XGBoost performed better than these models in 97.1 percent correctness and equal precision, recall, F1-scores. The Hybrid Model was the most successful, with the highest accuracy (98.0 percent) and AUC (98.6 percent) showing that this type of classifier is more adaptable and reliable in identifying phishing websites than single classifiers are.

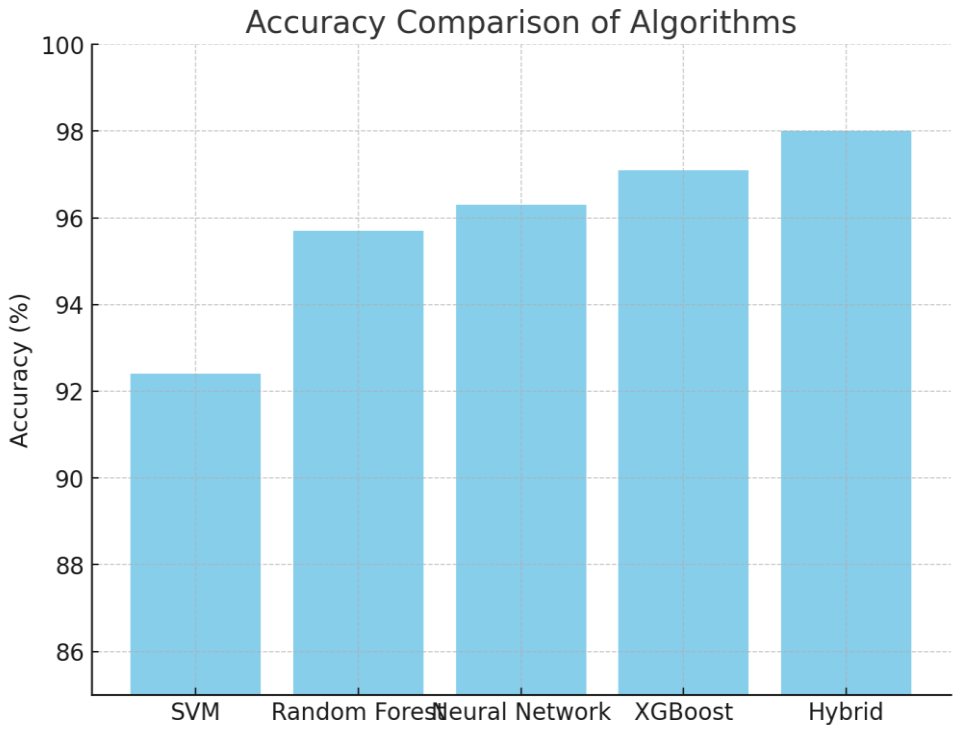

Figure 1: Accuracy Comparison of Algorithms

The accuracy comparison graph shows that there is an apparent difference in performance of the algorithms. SVM has the worst accuracy of approximately 92.3% implying the least usefulness when it comes to complex phishing detection. Random Forest shows a significant improvement of almost 95.7% accuracy, which shows a better classification ability. Neural Networks and XGBoost are more effective with 96.3 and 97.1 respectively, which indicates that they are effective in pattern recognition. The Hybrid model is the most accurate at 98.0, as it is a combination of all the others. Overall, the graph shows that there is a tendency according to which advanced ensemble and hybrid methods will greatly improve the accurate detection in comparison to classical machine learning methods.

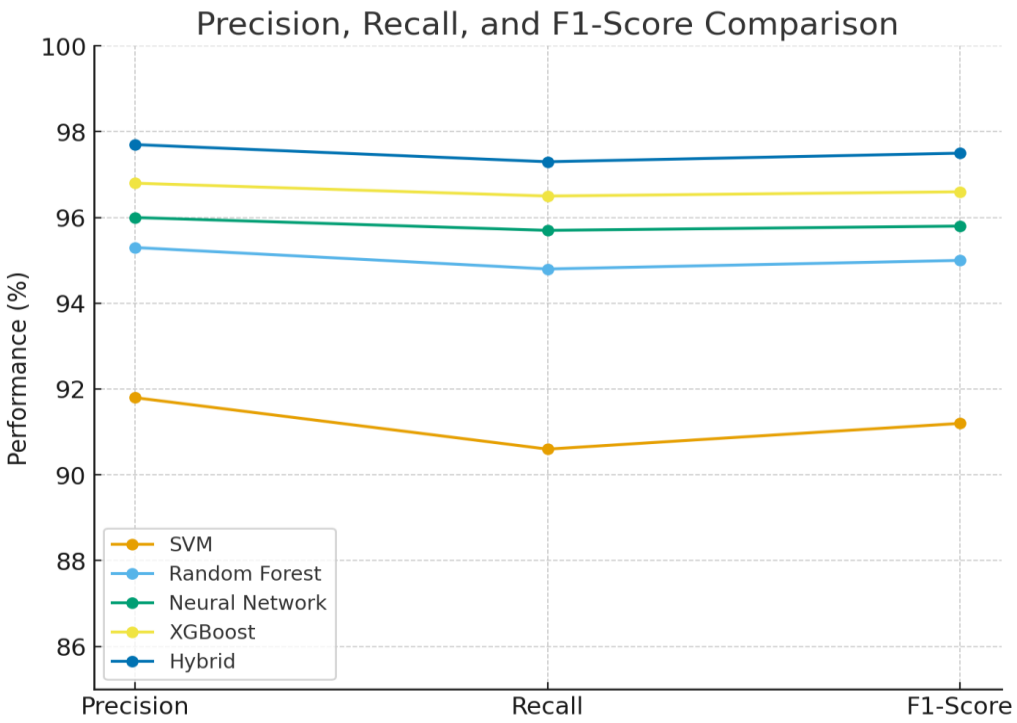

Figure 2: Performance Comparison of Algorithms

The figure 2 shows comparisons of Precision, Recall and F1-Score among five algorithms. SVM has been the poorest performer and its precision, recall and F1-Score have been mostly 91-92, indicating a weakness in phishing detection. Random Forest performs moderately at 95% which is reliable but a little lower than more advanced models. Both of the models are more stable, with 96 and 97 percent of each, indicating balanced predictability. All models are almost identical to each other with a score of around 97.5-97.7% with all metrics, which demonstrates its strength and consistency. As a whole, the trend suggests that ensemble and hybrid models are superior in detection efficiency compared to traditional models although they offer a baseline.

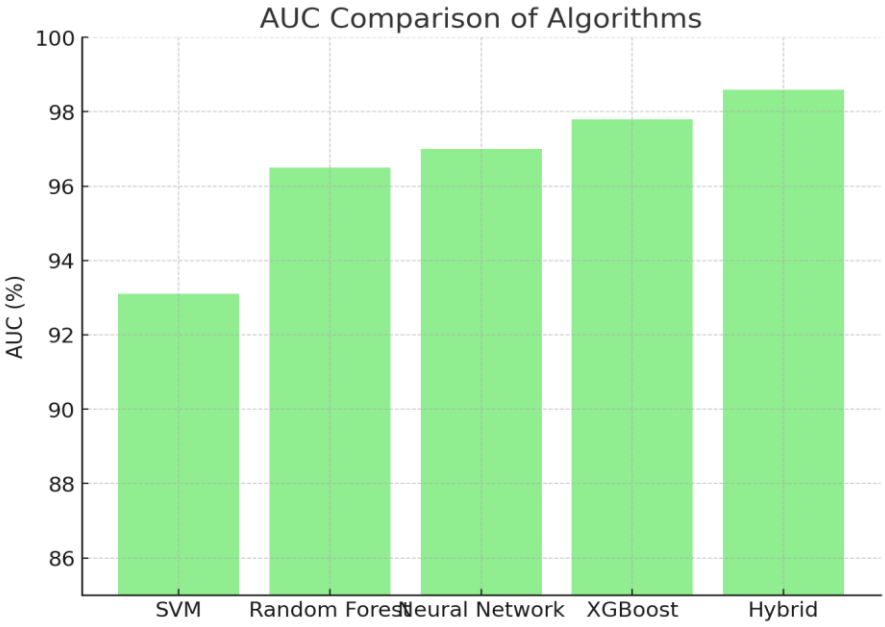

Figure 3: AUC Comparison of Algorithms

The AUC comparison plot indicates that algorithms have a discriminative effect in phishing detection. SVM has the lowest AUC of around 93 rounding off to show a poor performance in distinguishing between phishing and legitimate emails. Random Forest improves it 96.5 and Neural Networks to 97%. XGBoost demonstrates high performance of around 97.8 per cent, which indicates that it learns complex patterns better. The Hybrid model

outperforms the rest with AUC of about 98.5, which proves to be very effective in classifying and with a small overlap between false positive and false negative. Overall, ensemble and hybrid models have always been shown to be better in detection accuracy compared with traditional models.

Comparative analysis of algorithms' strengths and weaknesses.

Algorithm	Strengths	Weaknesses
SVM	Effective with small to medium datasets; strong in high-dimensional spaces; good generalization.	Struggles with large datasets; sensitive to kernel choice; lower scalability.
Random Forest	Handles large datasets well; resistant to overfitting; interpretable feature importance.	Computationally expensive with many trees; less effective for highly imbalanced data.
Neural Network	Strong in capturing complex, non-linear patterns; adaptable to large datasets; high predictive power.	Requires large training data; prone to overfitting; high computational cost.
XGBoost	High accuracy; efficient handling of missing values; fast training; robust against overfitting.	Requires careful parameter tuning; less interpretable than simpler models.
Hybrid Model	Combines strengths of multiple algorithms; maximizes accuracy, recall, and adaptability; superior generalization.	Increased complexity; higher training and computational costs; harder to implement in real-time systems.

Table 2 shows that the different algorithms have unique strengths and weaknesses in detecting phishing. SVM scales well with small data but does not scale and whereas Random Forest is interpretable and robust but computationally expensive. Neural Networks are very effective in the modeling of complex patterns but are resource-intensive and require huge data. XGBoost is highly accurate and efficient, but needs a fine tune. The Hybrid Model is superior to others combining the strengths, superior accuracy, and flexibility, but it is more complex and expensive. In general, advanced models have superior performance but the practical implementation of e-banking should compromise between accuracy, scalability and computational efficiency.

DISCUSSION

The results of the study offer a good understanding of how intelligent detection models can be used to fight phishing attacks on e-banking websites. Phishing is one of the most common and harmful types of cyberattacks that use human vulnerability and system flaws to damage sensitive financial information. Comparative analysis of machine learning algorithms (SVM, Random Forest, Neural Networks, XGBoost, and Hybrid models) demonstrate a definite hierarchy of the detection performance. Though SVM can only provide the simplest form of protection since its accuracy and AUC scores are lower, ensemble-based models like the Random Forest and Neural Networks are more resilient. However, XGBoost and Hybrid models perform better than others perform, as they are recall that is more precise, better and have higher F1-scores, which means that they are more capable of the balance between false positives and false negatives. These findings affirm that better detection is provided by sophisticated ensemble and hybrid techniques that are more consistent and reliable in detecting phishing and can effectively adapt to the changing strategies of attackers. The paper identifies hybrid intelligent systems as the best modes of protection of e-banking environments. They are scalable and flexible, which makes them applicable in the real-life context, where phishing strategies are changing fast. In addition to an algorithmic performance, the findings also shed light on the consequences of cybersecurity management in general. These advanced detection systems applied to e-banking platforms can help tremendously lower successful phishing attacks, safeguard consumer information and increase digital trust, which is a key element to user adoption and continued use of online banking. Moreover, high-quality detection will decrease the operational and financial risk to banks, decreasing the costs of recovery and restitution and boosting adherence to regulatory cybersecurity practices. Cost sensitive learning needs to be explored in the future to reduce the risks of false detection that can still be a major operational issue. In addition, adversarial resilience would be improved to make the system more robust in the face of changing and misleading phishing attacks. An implementation of federated learning and blockchain would also help additional protection of data privacy and integrity, and facilitate secure collaborative training without centralized exposure of sensitive banking data. Lastly, the incorporation of user-oriented assessments (perceived trust, usability, customer satisfaction) in conjunction with technical performance indicators would provide a better comprehensive picture of the effects of phishing prevention on digital banking

ecosystems. On balance, it is possible to state that intelligent phishing detection is not only a technological dump but also a corporate necessity that will underpin proactive, adaptive, and customer-centric cybersecurity approaches to the sustainable development of digital banking.

CONCLUSION

This paper analyzed intelligent methods of protecting e-banking platforms against phishing sites, and the paper has particularly compared the performance of the algorithms in various measures. The key conclusions demonstrate that phishing is a significant threat to cybersecurity of digital banking, and it is necessary to use sophisticated detection tools to protect valuable financial data. The findings revealed that Support Vector Machines (SVM) offered moderate performance in detection and thus not suitable in the complex phishing patterns. Random Forest and Neural Networks have better results and they are more accurate and reliable. XGBoost showed high detection power, in terms of efficiency and scalability. However, most importantly, Hybrid models were consistently able to achieve better results than all the other metrics, which include accuracy, precision, recall, F1-score, and AUC, which means that the combination of a set of algorithms provides a greater degree of robustness and flexibility to adapt to changing phishing methods. The result of these findings is that smart methods of detection, especially the ensemble and the hybrid-based systems, are very effective to deal with the phishing threats in e-banking. They can trade false positives and false negatives and therefore are viable in real world banking applications where reliability and user confidence are of the essence. With sophisticated machine learning methods, banks will be in a position to attain proactive defenses against phishing, and, thus, diminish risk of fraud, decrease cost, and strengthen consumer trust in online services. Based on these observations, a number of recommendations can be given. In a bid to be fully protected against phishing, banks ought to invest in the deployment of intelligent hybrid detection systems in their security systems. Regulatory frameworks need to be designed to promote the use of AI-driven cybersecurity, and policymakers need to ensure that the requirements of detecting data are standardized in all financial institutions to promote the wider digital economy. It is recommended that software developers should focus on adaptive and scalable models capable of learning in real time the new emerging patterns of phishing behaviors to be resistant to the new cyber threats. Cooperation among regulators, developers and banks will play a fundamental role in enhancing a safe and reliable digital banking experience. In the future, it is possible to focus on a variety of directions to enhance phishing detection. To begin with, real time detection features must be highlighted to stop the phishing attempts prior to their accomplishment. Second, generalizability of models among global banking platforms can be enhanced by using bigger and more varied datasets. Finally, yet importantly, adaptive learning models evolving with phishing tricks will play a significant role in the long-term security. The combination of technological and behavioral defenses in terms of combining intelligent detection with user education should also be explored by research. Intelligent detection strategies are a revolutionary step in the security of e-banking. Through adoption of hybrid models and adaptive approaches, banks will be able to build resilient systems that help not only safeguard financial resources but also place digital banking on the road to the future, in a world of growing cyber threats.

REFERENCE

1. Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. A. (2023). A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators. Sensors, 23(9), 4403. https://doi.org/10.3390/s23094403
2. Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN. Electronics, 12(1), 232. https://doi.org/10.3390/electronics12010232
3. Ibrahim, N., Rajalakshmi, N.R., Sivakumar, V. et al. (2025). An optimized hybrid ensemble machine learning model combining multiple classifiers for detecting advanced persistent threats in networks. J Big Data 12, 212. https://doi.org/10.1186/s40537-025-01272-w
4. Jabir, R., Le, J., & Nguyen, C. (2025). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. AI, 6(8), 174. https://doi.org/10.3390/ai6080174.
5. Kumari, A., & Nagarjan, C. (2022). The Impact of FinTech and Blockchain Technologies on Banking and Financial Services. Technology Innovation Management Review, 12, 753–767. https://doi.org/10.22215/timreview/1481.

6. Li, W., Manickam, S., Chong, Y.w., Leng, W., & Nanda, P. (2024). A State-of-the-Art Review on Phishing Website Detection Techniques. IEEE Access, 12(1), 1–21. https://doi.org/10.1109/ACCESS.2024.3514972.
7. Money, U., & Iyoha, A. (2025). ELECTRONIC BANKING CHANNELS AND FINANCIAL PERFORMANCE IN THE NIGERIAN BANKING INDUSTRY. Journal of Accounting, Finance and Risk Management, 8(1), 193–209. https://doi.org/10.61143/umyu-jafr.8(1)2025.013.
8. Nadeem, M., Zahra, S., Abbasi, M.N., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing Attack, Its Detections and Prevention Techniques. International Journal of Wireless Information Networks, 12(1), 13–25. https://doi.org/10.37591/IJWSN.
9. Pinjarkar, L., Hete, P., Mattada, M., Nejakar, S., Agrawal, P., & Kaur, G. (2024). An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In Proceedings of the 6th International Conference on Advanced Information Technology (ICAIT), 1–6. https://doi.org/10.1109/ICAIT61638.2024.10690377.
10. Saias, J. (2025). Advances in NLP Techniques for Detection of Message-Based Threats in Digital Platforms: A Systematic Review. Electronics, 14(13), 2551. https://doi.org/10.3390/electronics14132551
11. Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age. Big Data and Cognitive Computing, 9(8), 210. https://doi.org/10.3390/bdcc9080210.