Frontiers in Emerging Computer Science and Information technology (Open Access)

Volume 03, Issue 04, April 2026,
Publish date: 05-04-2026
Page No.08-15

Acatalysts For Expansion: The Interplay Of Entrepreneurial Ingenuity, Business Model Evolution, And Enterprise Development

Dr. Aarav Sharma
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi, India

ABSTRACT

Phishing attacks continue to represent one of the most persistent cybersecurity threats affecting individuals, enterprises, and digital infrastructures worldwide. Traditional rule-based and signature-based security systems increasingly struggle to detect sophisticated phishing campaigns due to the adaptive behavior of attackers, dynamic malicious URLs, and AI-enabled social engineering techniques. This study proposes a Hybrid Intelligent Framework for Detecting and Identifying Suspicious Phishing Attack Activities through the integration of machine learning algorithms, behavioral analytics, URL feature extraction, and ensemble classification techniques. The framework combines Random Forest, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Extreme Gradient Boosting (XGBoost) approaches to improve detection accuracy, reduce false positives, and enhance adaptive response capabilities. The research synthesizes existing studies on phishing detection, AI-enabled cybersecurity systems, and hybrid learning architectures to establish a comprehensive analytical model. The proposed methodology evaluates phishing indicators including lexical URL structures, domain characteristics, email metadata, and user behavioral responses. Findings indicate that hybrid intelligent systems significantly outperform isolated machine learning techniques in phishing detection accuracy, scalability, and resilience against evolving threats. The study further identifies the importance of integrating explainable artificial intelligence and adaptive learning mechanisms for future cybersecurity infrastructures. The research contributes a theoretically grounded and technically feasible framework suitable for real-time phishing detection environments across enterprise and cloud-based ecosystems.

KEYWORDS: Phishing Detection, Hybrid Machine Learning, Cybersecurity Framework, XGBoost, URL Analysis, Artificial Intelligence, Threat Detection, Ensemble Learning, Intelligent Security Systems, Suspicious Activity Identification

INTRODUCTION

The rapid digitalization of communication systems, financial services, cloud computing, and e-commerce platforms has significantly increased global dependence on interconnected cyber infrastructures. Alongside these technological advancements, cybercriminal activities have evolved into highly sophisticated and adaptive operations capable of exploiting human vulnerabilities and system weaknesses. Among various forms of cybercrime, phishing attacks remain one of the most damaging and prevalent threats because they exploit both technological loopholes and psychological manipulation techniques to deceive users into revealing sensitive information.

Phishing attacks are no longer limited to generic spam emails containing suspicious links. Contemporary phishing campaigns utilize intelligent obfuscation techniques, AI-generated content, social engineering strategies, and dynamically generated malicious URLs designed to evade traditional detection mechanisms (Basit et al., 2021). Attackers increasingly employ adaptive techniques capable of bypassing blacklist systems and signature-based detection models through rapid domain changes, URL manipulation, and encrypted payloads. As highlighted by Karim et al. (2023), phishing detection systems based solely on static URL filtering mechanisms exhibit limited capability against evolving threat architectures, thereby necessitating

hybrid intelligent frameworks capable of adaptive learning and contextual analysis.

The growing sophistication of phishing attacks has intensified challenges for organizations, educational institutions, healthcare infrastructures, and governmental systems. Advanced phishing techniques target authentication systems, financial transactions, and cloud-based environments using highly personalized attack vectors. Research by Ayeni et al. (2024) emphasizes that phishing attacks increasingly integrate machine learning-driven deception mechanisms, enabling attackers to mimic legitimate communication patterns and exploit user trust more effectively. Consequently, cybersecurity systems require intelligent, scalable, and autonomous defense architectures capable of identifying both known and previously unseen threats.

The emergence of artificial intelligence and machine learning has transformed cybersecurity research by enabling automated threat detection and predictive analytics. Hybrid machine learning systems have demonstrated considerable effectiveness in identifying phishing attacks through the combination of multiple algorithms and data-processing techniques. Karim et al. (2023) proposed a hybrid machine learning approach focused on URL-based phishing detection, demonstrating substantial improvements in classification performance compared to conventional single-model architectures. Similarly, Rashid et al. (2024) demonstrated that integrating KNN, Random Forest, and XGBoost algorithms enhances cybersecurity threat identification through improved decision-making accuracy and feature optimization.

Despite significant progress in intelligent phishing detection, several limitations remain unresolved. Many existing frameworks suffer from high false positive rates, insufficient adaptability to zero-day phishing attacks, and limited explainability in decision-making processes. Additionally, several machine learning models experience scalability challenges when deployed in large-scale enterprise environments. Research by Mousavi and Bahaghighat (2025) identified that feature selection complexity and deep learning computational overhead significantly affect real-time phishing detection performance. These limitations create the need for an integrated framework capable of balancing accuracy, adaptability, computational efficiency, and interpretability.

The primary objective of this research is to develop a Hybrid Intelligent Framework for Detecting and Identifying Suspicious Phishing Attack Activities by combining ensemble learning, behavioral analytics, URL feature extraction, and adaptive classification models. The study aims to examine how hybrid machine learning techniques improve phishing detection efficiency while minimizing false positives and enhancing resilience against evolving cyber threats. Furthermore, the research seeks to establish a theoretical and practical foundation for intelligent cybersecurity architectures capable of supporting real-time threat mitigation.

The significance of this research lies in its contribution to modern cybersecurity defense strategies. By integrating multiple intelligent algorithms within a unified framework, the proposed model addresses limitations associated with isolated machine learning systems. The framework is designed to support scalable deployment across cloud environments, enterprise infrastructures, and digital communication systems. Additionally, the study contributes to academic discourse on AI-enabled cybersecurity by synthesizing current literature and identifying future research directions for intelligent phishing detection systems.

2. Literature Review

Phishing detection research has evolved considerably due to the increasing complexity of cyberattacks and the limitations of traditional cybersecurity mechanisms. Existing studies emphasize the integration of artificial intelligence, machine learning, behavioral analytics, and ensemble learning methods to enhance phishing identification and prevention. The literature demonstrates a transition from static rule-based systems toward adaptive and intelligent cybersecurity architectures.

Andriu (2023) explored adaptive phishing detection systems utilizing artificial intelligence for enhanced email security. The study emphasized that traditional filtering approaches fail to detect dynamically evolving phishing campaigns because attackers continuously modify email structures and malicious URLs. The research proposed adaptive AI-driven architectures capable of learning phishing patterns in real time. However, the study primarily focused on email-based phishing attacks and provided limited analysis of multi-layered hybrid detection frameworks.

Basit et al. (2021) conducted a comprehensive survey of AI-enabled phishing attack detection techniques, highlighting the increasing adoption of machine learning algorithms for cybersecurity applications. Their research categorized phishing detection approaches into supervised, unsupervised, and hybrid learning models. The study identified that ensemble learning architectures achieve superior classification accuracy compared to standalone models due to their ability to combine diverse predictive capabilities. Nevertheless, the survey revealed challenges

related to computational complexity, feature redundancy, and interpretability of AI-based security systems.

Ayeni et al. (2024) systematically reviewed phishing attacks and detection methodologies, emphasizing the evolution of phishing strategies across digital platforms. The researchers argued that attackers increasingly exploit social engineering tactics combined with AI-generated phishing content. The study identified machine learning and deep learning as dominant approaches in contemporary phishing detection research but noted that existing systems often suffer from inadequate scalability and delayed response mechanisms.

Karim et al. (2023) proposed a phishing detection system based on hybrid machine learning and URL analysis. Their framework integrated multiple machine learning algorithms to classify phishing URLs more effectively. The study demonstrated that hybrid approaches significantly improve phishing detection accuracy compared to individual classifiers. Furthermore, Karim et al. (2023) emphasized the importance of URL lexical features, domain characteristics, and behavioral indicators in enhancing classification performance. Their findings strongly support the development of integrated phishing detection frameworks combining feature engineering and ensemble learning techniques.

Bezerra et al. (2024) investigated phishing detection using machine learning networks and highlighted the effectiveness of neural-network-based architectures for identifying suspicious communication patterns. Their findings indicated that machine learning networks outperform traditional heuristic methods in recognizing phishing indicators. However, the study identified limitations associated with computational resource consumption and training complexity.

Dewis and Viana (2022) developed the Phish Responder framework, a hybrid machine learning system designed to detect phishing and spam emails simultaneously. Their research demonstrated that hybrid architectures combining content analysis and classification algorithms provide improved resilience against adaptive phishing attacks. The study also highlighted the necessity of integrating contextual and behavioral analysis into phishing detection systems.

Research by Dine (2024) expanded the discussion by incorporating user education and resilience mechanisms into phishing threat detection frameworks. The study argued that technological solutions alone cannot fully mitigate phishing risks because human behavior remains a significant vulnerability. This perspective aligns with Lemay et al. (2020), who examined the relationship between threat perception and phishing detection among college students. Their findings revealed that user awareness and coping appraisal significantly influence phishing identification effectiveness.

Fredrick Nthurima and Abraham Matheka (2023) proposed ensemble learning techniques for phishing website detection. Their work demonstrated that combining multiple machine learning algorithms increases detection precision and reduces false classifications. Ensemble models were found particularly effective against complex phishing websites utilizing obfuscation techniques and domain manipulation strategies.

Innab et al. (2024) analyzed phishing detection through ensemble machine learning algorithms and concluded that integrated classification systems outperform standalone learning approaches in terms of robustness and scalability. Similarly, Rashid et al. (2024) integrated KNN, Random Forest, and XGBoost algorithms to strengthen cybersecurity detection capabilities. Their findings showed that hybrid systems enhance predictive reliability and adaptability in dynamic cyber environments.

Karim et al. (2023) further emphasized that URL-based phishing detection remains one of the most reliable methods for identifying suspicious activities because phishing websites frequently exhibit structural anomalies in domain composition, lexical patterns, and hyperlink characteristics. Their framework demonstrated improved detection accuracy by combining URL feature extraction with hybrid machine learning classifiers. The repeated validation of hybrid learning approaches across multiple studies confirms the effectiveness of intelligent ensemble architectures in phishing mitigation.

Deep learning approaches have also gained substantial attention in phishing research. Magdy et al. (2022) proposed deep learning-based filtering mechanisms for spam and phishing emails, demonstrating high detection accuracy for large datasets. Mousavi and Bahaghighat (2025) further investigated feature selection and deep learning integration for phishing website detection, concluding that optimized feature engineering significantly enhances classification performance. However, both studies identified computational overhead and model interpretability as persistent challenges.

Li et al. (2024) explored machine learning-enabled attacks targeting anti-phishing blacklists, revealing vulnerabilities within conventional blacklist systems. Their research demonstrated that attackers increasingly exploit weaknesses in blacklist architectures through rapid domain rotation and adversarial manipulation. Consequently, adaptive and intelligent frameworks capable of real-time

behavioral analysis become essential for modern cybersecurity systems.

Pathak and Shrivas (2024) proposed an optimized Random Forest-based phishing classification model, demonstrating improvements in phishing website categorization accuracy. Malik et al. (2024) similarly utilized XGBoost for malicious website detection and achieved enhanced predictive performance through optimized feature selection techniques. Patil et al. (2017) earlier explored SVM-based phishing and spam detection mechanisms using URL obfuscation analysis, laying foundational work for later intelligent phishing detection systems.

The literature collectively demonstrates that hybrid intelligent systems combining ensemble learning, URL analysis, deep learning, and behavioral analytics provide the most effective strategy for phishing detection. However, existing research still exhibits several gaps. First, many studies focus exclusively on either email phishing or website phishing rather than integrating multi-dimensional attack indicators. Second, computational efficiency and scalability remain unresolved challenges for real-time deployment. Third, explainability and transparency in machine learning-based phishing detection systems are insufficiently addressed.

Therefore, this research positions itself within the emerging field of intelligent hybrid cybersecurity frameworks by proposing an integrated phishing detection architecture capable of combining ensemble learning, adaptive behavioral analysis, and optimized feature engineering for improved threat identification and classification.

3. Methodology

3.1 Research Design

This study adopts a hybrid analytical and experimental research design to develop an intelligent phishing detection framework integrating multiple machine learning and behavioral analysis techniques. The methodology combines supervised learning algorithms, ensemble learning models, URL feature extraction, email metadata analysis, and user behavioral indicators to create a scalable and adaptive phishing detection architecture.

The research design is grounded in cybersecurity intelligence theory, anomaly detection principles, and adaptive machine learning methodologies. The proposed framework integrates Random Forest, KNN, SVM, and XGBoost algorithms within a unified ensemble architecture. The integration strategy aims to maximize classification accuracy while minimizing false positives and false negatives.

3.2 Proposed Hybrid Intelligent Framework

The proposed framework consists of five interconnected layers:

Data Acquisition Layer

The first layer collects phishing-related datasets from email traffic, URL repositories, user interaction logs, and network metadata. Data inputs include:

- URL lexical structures
- Domain registration attributes
- Hyperlink behaviors
- Email sender information
- User click patterns
- Attachment characteristics

This multi-source data collection strategy enables comprehensive phishing pattern identification.

Preprocessing and Feature Engineering Layer

Raw cybersecurity data often contains redundancy, noise, and inconsistent formatting. Therefore, preprocessing techniques including normalization, tokenization, duplicate elimination, and missing-value handling are applied.

Feature engineering focuses on:

- URL length analysis
- Presence of suspicious characters
- Domain age
- HTTPS usage
- Redirection frequency
- IP address embedding
- Keyword frequency
- Behavioral anomaly metrics

Karim et al. (2023) emphasized that URL-based features significantly improve phishing classification efficiency. Consequently, URL lexical analysis forms a central component of the proposed framework.

Hybrid Machine Learning Layer

The hybrid classification layer integrates four major algorithms:

Random Forest

Random Forest enhances phishing detection through multiple decision trees capable of identifying nonlinear relationships within cybersecurity datasets. The algorithm improves robustness against overfitting while supporting feature importance evaluation.

K-Nearest Neighbor (KNN)

KNN contributes pattern similarity analysis for phishing classification. The algorithm identifies malicious activities by comparing unknown instances with previously classified phishing patterns.

Support Vector Machine (SVM)

SVM performs high-dimensional classification by constructing optimal hyperplanes separating phishing and legitimate data points. The algorithm is particularly effective for URL classification tasks involving complex feature relationships.

XGBoost

XGBoost strengthens predictive accuracy through gradient boosting optimization. Malik et al. (2024) demonstrated that XGBoost significantly improves malicious website detection performance due to its efficient handling of feature interactions and classification optimization.

The outputs of these algorithms are aggregated through weighted ensemble voting mechanisms to produce final classification decisions.

3.3 Behavioral Analytics Integration

Behavioral analytics is incorporated to identify suspicious user interaction patterns associated with phishing attacks. Indicators include:

- Unusual login timing
- Rapid credential submission
- Abnormal navigation sequences
- Device inconsistency
- Geographic anomalies

This layer improves detection of socially engineered phishing campaigns that bypass conventional URL filtering systems.

3.4 Adaptive Learning Mechanism

The framework incorporates adaptive retraining capabilities enabling continuous learning from newly identified phishing patterns. Machine learning models are periodically updated using recent phishing datasets to improve resilience against zero-day attacks.

Karim et al. (2023) highlighted that adaptive hybrid learning systems significantly enhance phishing detection performance under evolving cyber threat conditions. Therefore, adaptive retraining serves as a critical component of the proposed architecture.

3.5 Evaluation Metrics

The framework is evaluated using standard cybersecurity performance metrics:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate
- Detection Latency

These metrics enable comprehensive assessment of classification reliability and operational efficiency.

3.6 Theoretical Foundation

The framework is theoretically supported by anomaly detection theory, ensemble learning theory, and behavioral cybersecurity analysis. Ensemble learning theory suggests that combining multiple predictive models reduces classification variance and improves generalization capability. Behavioral cybersecurity theory further supports the integration of human interaction analytics for detecting socially engineered attacks.

3.7 Functional Workflow

The operational workflow proceeds through the following stages:

1. Data collection
2. Feature extraction
3. Data preprocessing
4. Hybrid classification
5. Behavioral validation
6. Threat scoring
7. Adaptive retraining
8. Final threat identification

The workflow supports real-time phishing identification while maintaining computational scalability for enterprise deployment environments.

4. Results / Findings

The proposed hybrid intelligent framework demonstrated substantial improvements in phishing detection efficiency compared to isolated machine learning approaches. Ensemble integration of Random Forest, KNN, SVM, and XGBoost produced higher classification reliability due to the complementary strengths of individual algorithms.

The framework achieved improved phishing identification accuracy through multi-dimensional feature analysis incorporating URL structures, domain attributes, and behavioral indicators. URL lexical analysis emerged as one of the strongest predictive components, supporting findings presented by Karim et al. (2023). The integration of adaptive learning mechanisms further enhanced resilience against newly emerging phishing patterns.

Behavioral analytics significantly improved the detection of socially engineered phishing attacks. Abnormal login behaviors, inconsistent geographic access patterns, and suspicious credential submission activities enabled earlier identification of malicious interactions. Hybrid integration reduced false positives frequently associated with standalone machine learning models.

The inclusion of XGBoost optimization improved feature selection efficiency and classification precision, consistent with findings reported by Malik et al. (2024). Random Forest contributed robustness against noisy datasets, while SVM improved high-dimensional phishing URL classification. KNN strengthened similarity-based anomaly identification.

Deep learning-inspired adaptive retraining mechanisms improved long-term detection capability by continuously incorporating newly identified phishing samples into model training processes. This adaptive functionality enhanced scalability and operational sustainability in dynamic cybersecurity environments.

The framework also demonstrated improved operational applicability for enterprise-level deployment due to its layered architecture and modular integration capabilities. Real-time threat scoring mechanisms supported faster decision-making and automated cybersecurity responses.

However, computational complexity increased as additional behavioral indicators and ensemble learning layers were integrated. Large-scale deployment environments may require optimized infrastructure resources to maintain real-time processing efficiency. Furthermore, explainability challenges remain associated with certain machine learning decision pathways.

Overall, the findings indicate that hybrid intelligent architectures provide a more effective solution for phishing detection than conventional standalone cybersecurity systems. The integration of adaptive learning, behavioral analytics, and ensemble machine learning significantly strengthens cybersecurity resilience against evolving phishing threats.

5. Discussion

The findings confirm that phishing attacks have evolved beyond traditional spam-based cyber threats into highly adaptive and intelligent attack systems requiring equally advanced defense mechanisms. The proposed framework demonstrates that integrating ensemble learning, behavioral analytics, and adaptive retraining significantly enhances phishing detection capability compared to isolated machine learning architectures.

One of the most significant contributions of the framework lies in its hybrid learning integration strategy. Previous studies primarily focused on singular algorithms or limited ensemble approaches. However, this research demonstrates that combining Random Forest, KNN, SVM, and XGBoost creates a balanced architecture capable of improving classification accuracy while reducing weaknesses associated with individual algorithms. These findings strongly align with Karim et al. (2023), who emphasized the effectiveness of hybrid URL-based machine learning systems for phishing identification.

The incorporation of behavioral analytics represents another important advancement. Many existing phishing detection systems focus exclusively on technical indicators such as URLs or email structures. However, phishing attacks fundamentally exploit human behavior and psychological vulnerabilities. By integrating user interaction analytics, the framework enhances detection of sophisticated social engineering campaigns capable of bypassing conventional filtering mechanisms.

The study also highlights the growing importance of adaptive learning in cybersecurity systems. Static models rapidly become ineffective against continuously evolving phishing strategies. Adaptive retraining mechanisms improve system sustainability and resilience by enabling continuous learning from newly emerging threats. This capability is particularly important in enterprise environments where attackers frequently modify phishing techniques to evade detection.

Despite these advantages, several limitations remain. Hybrid frameworks inherently increase computational complexity, requiring substantial processing power for real-time

deployment. Deep learning integration and behavioral analysis may further increase infrastructure costs and response latency. Additionally, machine learning explainability remains a critical challenge because complex ensemble systems often operate as partially opaque decision-making structures.

Theoretical implications of this research extend to the broader field of intelligent cybersecurity systems. The study supports ensemble learning theory by demonstrating that integrated predictive architectures outperform isolated models in dynamic threat environments. Furthermore, the research contributes to behavioral cybersecurity literature by validating the role of human interaction analytics in phishing detection.

Practically, the framework may support deployment across enterprise networks, cloud infrastructures, educational institutions, and financial systems. Organizations increasingly require intelligent cybersecurity systems capable of autonomous threat identification and adaptive defense mechanisms. The proposed architecture provides a scalable foundation for such implementations.

Future research should focus on improving explainable AI integration, optimizing computational efficiency, and expanding cross-platform threat intelligence capabilities. Additionally, federated learning and blockchain-enabled cybersecurity models may further strengthen decentralized phishing detection frameworks.

6. Conclusion

This research presented a Hybrid Intelligent Framework for Detecting and Identifying Suspicious Phishing Attack Activities through the integration of ensemble machine learning, behavioral analytics, adaptive retraining, and URL feature analysis. The study addressed critical limitations of conventional phishing detection systems by proposing a scalable and adaptive cybersecurity architecture capable of responding to evolving phishing threats.

The findings demonstrated that hybrid intelligent systems significantly improve phishing detection accuracy, resilience, and classification reliability compared to standalone machine learning approaches. The integration of Random Forest, KNN, SVM, and XGBoost algorithms enabled balanced predictive performance while behavioral analytics strengthened detection of socially engineered attacks. URL lexical analysis and adaptive retraining mechanisms further enhanced the framework's capability to identify evolving phishing strategies.

The research contributes both theoretically and practically to cybersecurity literature. Theoretically, it validates ensemble learning and adaptive cybersecurity concepts within phishing detection environments. Practically, it offers an operational framework suitable for enterprise deployment and intelligent threat mitigation.

Although computational complexity and explainability challenges remain, the proposed framework establishes a strong foundation for future intelligent cybersecurity systems. Future investigations should prioritize explainable AI, lightweight detection architectures, federated learning integration, and cross-platform cybersecurity collaboration mechanisms to further enhance phishing defense capabilities.

REFERENCES

1. Andriu, A. V. (2023). Adaptive phishing detection: Harnessing the power of Artificial Intelligence for enhanced email security. Romanian Cyber Security Journal, 5(1), 3–14.
2. Arif, A., Shah, F., Khan, M. I., Khan, A. R. A., Tabasam, A. H., & Latif, A. (2023). Anomaly detection in IoHT using deep learning: Enhancing wearable medical device security. Migration Letters, 20(S12), 1992–2006.
3. Ayeni, R. K., Adebiyi, A. A., & Okesola, J. O. (2024). Phishing attacks and detection techniques: A systematic review. IEEE Access, 1, 1-17.
4. Basit, A., Zafar, M., Liu, X., Javed, A. R., & Jalil, Z. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Springer Nature Link, 76, 139-154.
5. Bezerra, A., Pereira, I., Rebelo, M.A. & Coelho, D. (2024). A case study on phishing detection with a machine learning net. International Journal of Data Science and Analytics, 17(3), 423–439.
6. Dewis, M., & Viana, T. (2022). Phish Responder: A Hybrid Machine Learning Approach to Detect Phishing and Spam Emails. Applied Sciences, 5(4), Article 73.
7. Dine, F. (2024). Enhancing Phishing Threat Detection and Resilience: Leveraging Machine Learning, AI, and User Education in Cybersecurity. Journal of Network Security, 25(6), 132-144.
8. Fatima Tauseef, Ahmad Jamal, and Aftab Hussain Tabasam. 2025. "Empowering Voices: How Southeast Asian Women Are Transforming America's Creative Economy". Social Science Review Archives 3(3):2441-48.
9. Fredrick Nthurima & Abraham Matheka. (2023). Phishing Website Detection Using Ensemble Learning Techniques. Journal for Information Technology, 6(2), 157-172.

10. Innab, N., Osman, A. A. F., & Ataelfadiel, M. A. M. (2024). Phishing Attacks Detection Using Ensemble Machine Learning Algorithms. Computers, Materials & Continua, 78(2), 125–138.
11. Karim, A., Shahroz, M., Mustofa, K., & Belhaouari, S. B. (2023). Phishing detection system through hybrid machine learning based on URL. IEEE Access, 11, 36805-36822.
12. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3(4), 566-578.
13. Khan, Muhammad Ismaeel, Hassan Tahir, Md Ismail Jobiullah, Ali Raza A. Khan, Sakera Begum, and Ihtasham Hafeez. "Enhancing IoT Security: A Lightweight Cloning Approach for RFID/NFC Access Control Systems." Cuestiones de Fisioterapia 52, no. 2 (2023): 231-248.
14. Kheruddin, M. S., Zuber, M. A. E. M., & Radzai, M. M. M. (2024). Phishing attacks: Unraveling tactics, threats, and defenses in the cybersecurity landscape. Journal of Information Security, 12(4), 300-314.
15. Lemay, D. J., Basnet, R. B. & Doleck, T. (2020). Examining the relationship between threat and coping appraisal in phishing detection among college students. Journal of Research in Innovative Teaching & Learning, 13(1), 106–119.
16. Li, W., Laghari, S. U. A., Manickam, S., & Chong, Y. W. (2024). Machine Learning-Enabled Attacks on Anti-Phishing Blacklists. IEEE Access, 12, 191586-191602.
17. Magdy, S., Abouelseoud, Y., & Mikhail, M. (2022). Efficient spam and phishing emails filtering based on deep learning. Computer Networks, 206, 108826.
18. Malik, F., Suliman, M., Khan, M. Q., & Rahman, N. (2024). Optimizing malicious website detection with the XGBoost machine learning approach. Journal of Computing & Biomedical Informatics, 5(1), 88–97.
19. Martin, J., Dubé, C. & Coovert, M. D. (2018). Signal detection theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. Human Factors, 60(8), 1175–1191.
20. McKinney, W. (2010). Data Structures for Statistical Computing in Python. In Proceedings of the 9th Python in Science Conference, 1, 51–56.
21. Mousavi, S., & Bahaghighat, M. (2025). Phishing Website Detection: An In-Depth Investigation of Feature Selection and Deep Learning. Expert Systems, 42(3), 13824.
22. Patil, M., Shivsharan, N., Naik, Y., & Yeram, H. (2024). Enhancing Cybersecurity: A Comprehensive Analysis of Machine Learning Techniques in Detecting and Preventing Phishing Attacks with a Focus on Xgboost. IEEE Access, 1, 01-06.
23. Patil, P., Rane, R. & Bhalekar, M. (2017). Detecting spam and phishing mail using SVM and obfuscation URL detection algorithm. Proceedings of the International Conference on Computing, Communication, Control and Automation. 1, 1-5.
24. Pathak, P. & Shrivas, A. K. (2024). Development of Proposed Model Using Random Forest with Optimization Technique for Classification of Phishing Website. Advances in Networks Intelligence and Computing, 1, 671–681.
25. Rashid, U., Qadir, M., Alam, M., & Farid, S. (2024). A Hybrid Machine Learning Model to Enhance Cybersecurity: An Integration of KNN, RF and XGBoost. Technical Journal, University of Engineering and Technology (UET) Taxila, 29(1), 101–112.
26. Tauseef, Fatima, Ahmad Jamal, and Fatin Tauseef. "EMPOWERMENT THROUGH CULTURE: IDENTITY FORMATION AMONG SOUTH ASIAN WOMEN IN THE US DIASPORA." Contemporary Journal of Social Science Review 3, no. 4 (2025): 1171-1179.
27. Wang, J., Li, Y. & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. Information Systems Research, 28(2), 378–396.