# Development of a Predictive Model for Phishing and Ransomware Detection in Financial Institution Using a Random Forest Classifier and Outlier Technique

**K.C. PAUL**[1]
Department of Computer Science,
Rivers State University, Port Harcourt, Nigeria.
paul.kanu@ust.edu.ng

**V. T. EMMAH**[2]
Department of Computer Science,
Rivers State University, Port Harcourt, Nigeria.
victor.emmah@ust.edu.ng
DOI: 10.56201/ijcsmt.v11.no1.2025.pg84.96

***Abstract***
*Phishing and ransomware attacks are significant cyber threats that target financial institutions, aiming to deceive users and exploit vulnerabilities for malicious gains. Phishing attacks often involve fraudulent emails or websites that trick users into revealing sensitive information, while ransomware encrypts a victim's data and demands payment for its release. Both types of attacks pose severe risks to financial institutions, potentially leading to data breaches, financial losses, and reputational damage. To combat these threats, this paper proposed an advanced detection system using machine learning techniques. The proposed system focused on feature engineering and training a Random Forest classifier to detect phishing and ransomware attacks based on key attributes like URL structure and file characteristics. For phishing detection, features such as URL length, subdomains, and the presence of secure HTTPS protocols were extracted, while for ransomware detection, file name length, the presence of executable extensions, and suspicious keywords were analyzed. The results of the proposed system showed a significant improvement over existing systems, achieving an accuracy of 99.61%.*

***Keywords:*** *Phishing, ransomware, attacks, cyber, institutions, detection, techniques.*

## 1.0 Introduction

Cybersecurity risk in financial institutions is a critical concern due to the potential for significant financial and reputational damage. Machine learning (ML) has emerged as a promising approach to enhance cybersecurity measures in such institutions. ML can be vulnerable to cyber-attacks, particularly when dealing with large sets of challenge-response pairs, making it essential to address these vulnerabilities. Moreover, the application of Generative Adversarial Network (GAN) technologies in computer vision and artificial intelligence presents broad prospects for enhancing cybersecurity in financial institutions. GANs, when combined with unsupervised learning algorithms, can be applied to forecasting problems and target detection, including anomaly detection of data, which is vital for cybersecurity management. The prediction of cybersecurity risk in financial institutions using

machine learning is a multifaceted Endeavor that involves evaluating risk assessment, understanding user behaviour, addressing faults, and leveraging the concepts of predictive, preventive, and personalized medicine. These aspects are crucial for enhancing cybersecurity measures and predicting potential risks within financial institutions.

## 2.0 Review Of Related Literatures

Harish (2017) discussed different machine-learning algorithms that can be used in detecting fraudulent transactions. The machine learning algorithms used are Support Vector Machine, Logistic Regress, Genetic Algorithm, and Random Forest Classifier. The authors concluded by saying that the most popular techniques used in carrying out fraudulent transactions or stealing credit card information are phishing and Trojans. Therefore, this can be prevented by developing a machine-learning model to prevent this attack.

Rimpal and Jayesh (2018) proposed both deep learning and machine learning algorithms to secure credit card transactions; So, people can use e-banking safely and easily. The deep learning algorithms used are based on Deep learning, Logistic Regression, Naïve Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, K Nearest Neighbour, Data Mining, Decision Tree, Fuzzy logic-based System, and Genetic Algorithm. Their experimental result shows that the machine learning algorithms
show a better accuracy result.

Gao *et al.* (2021) enhance enterprise capabilities in addressing financial risks, reducing labour costs, minimizing financial losses, and bolstering investor confidence by establishing a comprehensive financial risk evaluation index system using deep learning technology and data mining methods in an artificial intelligence environment. The proposed financial risk prevention analysis method, grounded in interactive mining, involves creating a specialized risk analysis model to identify key factors related to various financial risks faced by listed companies. Through empirical analysis of 21 listed companies, the study identifies high-trust index evaluation model in this exploration exhibits superior performance, with an average detection accuracy of 90.27%, a 30% improvement in accuracy, and successful consistency testing for variable weights. The model proves rational and accurate, showcasing the effectiveness of the financial risk prevention model based on deep learning and data mining technology as a theoretical foundation for enterprise financial risk prevention research.

Roy and Prabhakaran (2022) delve into the various types of insider-led cyber frauds that have gained widespread attention in recent large-scale fraud events involving prominent Indian banking institutions. The focus is on identifying and classifying these cyber frauds while mapping them on a severity scale to facilitate optimal mitigation planning. The methodology employed includes a detailed literature review, a focus group discussion with risk and vigilance officers, and cyber cell experts, along with the analysis of secondary data on cyber fraud losses. Utilizing machine learning-based random forest, the authors predict the future landscape of insider-led cyber frauds in the Indian banking sector, prioritizing and forecasting potential threats. The projected scenarios highlight the prevalence of specific cyber frauds, providing a foundation for the development of a fraud mitigation model with a victim-centric approach. The paper concludes by presenting a conceptual framework that establishes a sustainable cyber fraud mitigation ecosystem within the study's scope. Policymakers and fraud investigators can leverage these findings to enhance the resilience of banking environments by enabling timely detection and prevention of cyber fraud.

Islam *et al*. (2022) presented a model that utilizes the Random Forest algorithm to identify phishing sites through URL detection. The result of the paper consists of three distinct stages: Parsing, Heuristic Classification of data, and Performance Analysis. Parsing is employed to analyse a set of features. The dataset was collected from a Phishtank. Only 8 out of the 31 features are selected for parsing. The random forest algorithm achieved an accuracy rate of 95%.

**3.0 Analysis of The Proposed System**

The proposed system in figure 1 is for analysing cyber-attack incidents targeting financial institutions demonstrates a comprehensive and methodical approach to addressing the complex challenges posed by such threats. The dataset, meticulously sourced from cybersecurity agencies, financial institutions, and research reports, offers a rich and structured repository of information on ransomware and phishing attacks. With variables spanning from timestamp to impact severity, the dataset facilitates diverse analytical use cases, including exploratory analysis, predictive modelling, and cybersecurity strategy enhancement. Prioritizing adherence to ethical guidelines and legal regulations, the dataset ensures responsible and informed usage of sensitive cybersecurity data. Moreover, the data preprocessing steps of cleaning and normalization ensure the integrity and uniformity of the dataset, laying a solid foundation for subsequent analysis.

Utilizing advanced techniques such as feature selection using Principal Component Analysis (PCA) and threat detection employing outlier analysis and Random Forest, the proposed system demonstrates a sophisticated approach to cyber threat mitigation. By identifying significant features through PCA and eliminating less relevant ones, the system enhances model performance and mitigates overfitting, particularly in datasets with high dimensions like credit risk assessments. Furthermore, integrating outlier detection with Random Forest classification enhances the accuracy and speed of cyber threat detection, fortifying the resilience of financial institutions against evolving attacks. This synergistic approach not only empowers proactive threat mitigation but also ensures the integrity and protection of critical financial assets, thereby underscoring the significance of the proposed system in bolstering cybersecurity defences within the financial sector.

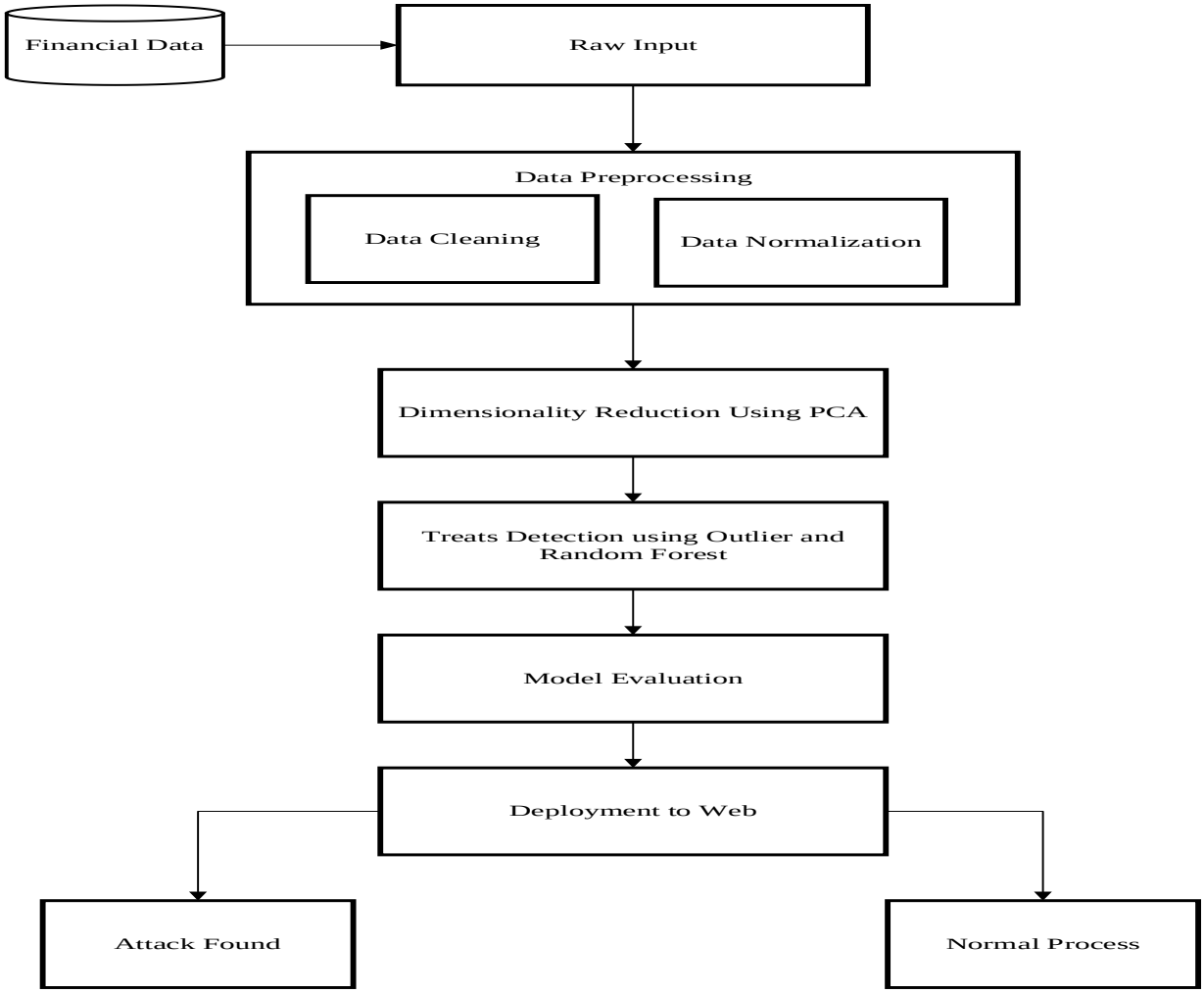


Figure 1: Architecture of the Proposed System

**Dataset:** The dataset comprises cyber-attack incidents targeting financial institutions, focusing specifically on ransomware and phishing attacks. Sourced from various cybersecurity agencies, financial institutions, and research reports, each entry in the structured dataset represents a unique attack event, detailing variables such as timestamp, institution name, attack type, vector, duration, impact severity, financial losses, data compromised, remediation actions, and optionally geographical location. With potential use cases including exploratory analysis, predictive modelling, and cybersecurity strategy enhancement, the dataset serves as a valuable resource for understanding trends, patterns, and mitigation strategies in cyber-attacks on financial institutions while ensuring adherence to ethical guidelines and legal regulations regarding sensitive cybersecurity data usage.

**Data Cleaning:** cleaning the raw credit risk dataset includes addressing missing numbers, outliers, and discrepancies. It guarantees that the data is in an appropriate format for analysis. Typical methods in data cleaning are imputation, deduplication, managing categorical variables, and rectifying data mistakes.

**Data Normalization:** During this stage, the data is scaled or normalized to provide a uniform scale across all characteristics. Normalization enhances model convergence during training and

prevents features with bigger sizes from overpowering the learning process. Methods like min-max scaling and standardization are frequently employed for data normalization.

**Feature Selection Using Principal Component Analysis:** Feature selection is essential for enhancing model performance and mitigating overfitting, particularly in datasets with many dimensions such as credit risk assessments. The Random Forest Classifier is utilized to assess the significance of features by evaluating their impact on the prediction. aspects with greater relevance scores are chosen for additional study, while less significant aspects are eliminated.

**Threats Detection Using Outlier and Random Forest:** Employing outlier detection techniques, anomalies indicative of potential cyber threats, such as unusual transaction patterns or unauthorized access attempts, can be swiftly identified within vast streams of financial data. Intertwining this with Random Forest, renowned for its prowess in classifying complex data patterns, fortifies the system's ability to discern between benign activities and malicious intrusions. This integrated approach not only bolsters the accuracy and speed of cyber threat detection but also enhances the resilience of financial institutions against evolving cyber threats, thereby ensuring the integrity of financial systems and the protection of sensitive assets.

**Model Evaluation:** Evaluation using classification reports and confusion matrix is a critical step in assessing the performance of machine learning models, particularly in classification tasks. The classification report provides a comprehensive summary of various performance metrics, including precision, recall, F1-score, and support, for each class in the dataset.

**Deployment to Web:** Deployment to the web, particularly for real-time testing purposes, entails the strategic integration of the Bootstrap framework with Python Flask. Bootstrap, renowned for its responsive design components and pre-built CSS and JavaScript utilities, serves as the cornerstone for creating visually appealing and user-friendly web interfaces. When coupled with Flask, a lightweight and versatile web framework for Python, seamless integration and deployment of web applications become achievable. Leveraging Flask's capabilities for handling HTTP requests and routing, coupled with Bootstrap's robust front-end design elements, developers can efficiently create dynamic and interactive real-time testing platforms. This amalgamation facilitates the creation of intuitive user interfaces, while Flask manages the back-end functionality, enabling real-time data processing and interaction. Through this synergistic approach, deployment to the web becomes not only streamlined but also empowers developers to deliver sophisticated real-time testing solutions with ease.

**Algorithm 4.1: Cyber Attack Detection in Financial Institutions**

**Start**

**Input:** Financial Data (structured dataset comprising cyber-attack incidents)

**Output:** Detected Cyber Attacks (Ransomware and Phishing)

1. Preprocess FinancialData to clean and normalize the dataset
2. Extract relevant features from the dataset
3. Initialize Random Forest classifier for cyber-attack detection
4. Initialize threshold for outlier detection
5. for each entry in FinancialData do
6. features = ExtractFeatures(entry)
7. prediction = RandomForestClassifier(features)
8. anomaly_score = CalculateOutlierScore(features)
9. threshold = Mean(anomaly_score)

10. if anomaly_score ≥ threshold then
11. AlertUser(CyberAttackDetected)
12. else
13. continue
14. Endif
15. endFor

## 4.0 Results and Discussion

Figure 2 and Figure 3 show the feature engineering applied to both phishing and ransomware datasets. The results indicate that the selected features, such as url_length, num_subdomains, and has_https, are crucial in differentiating phishing URLs from legitimate ones. For the botnet dataset, the use of features like name_length, has_exe_extension, and has_suspicious_keyword effectively captured attributes commonly found in malicious file names. These engineered features reflect the patterns phishing and botnet attacks utilize to deceive users and evade detection, respectively.

| | url_length | num_dots | num_slashes | has_https | num_subdomains | has_at_symbol | label |
|---|---|---|---|---|---|---|---|
| **0** | 39 | 2 | 3 | 0 | 1 | 0 | 1 |
| **1** | 26 | 1 | 2 | 0 | 0 | 0 | 1 |
| **2** | 25 | 1 | 2 | 0 | 0 | 0 | 1 |
| **3** | 35 | 2 | 3 | 0 | 1 | 0 | 1 |
| **4** | 39 | 2 | 3 | 0 | 1 | 0 | 1 |
| **...** | ... | ... | ... | ... | ... | ... | ... |
| **6995** | 17 | 1 | 2 | 0 | 0 | 0 | 0 |
| **6996** | 24 | 1 | 2 | 0 | 0 | 0 | 0 |
| **6997** | 24 | 1 | 2 | 0 | 0 | 0 | 0 |
| **6998** | 17 | 1 | 2 | 0 | 0 | 0 | 0 |
| **6999** | 17 | 1 | 2 | 0 | 0 | 0 | 0 |

7000 rows × 7 columns

Figure 2: Feature engineering of phishing dataset (Extracted Features)

| | name_length | has_exe_extension | has_suspicious_keyword | num_digits | label |
|---|---|---|---|---|---|
| **0** | 11 | 0 | 1 | 0 | 1 |
| **1** | 12 | 0 | 0 | 0 | 1 |
| **2** | 13 | 0 | 0 | 0 | 1 |
| **3** | 11 | 0 | 0 | 0 | 1 |
| **4** | 11 | 0 | 0 | 0 | 1 |
| **...** | ... | ... | ... | ... | ... |
| **6995** | 16 | 0 | 0 | 0 | 0 |
| **6996** | 12 | 0 | 0 | 0 | 0 |
| **6997** | 16 | 0 | 0 | 0 | 0 |
| **6998** | 12 | 0 | 0 | 0 | 0 |
| **6999** | 16 | 0 | 0 | 0 | 0 |

7000 rows × 5 columns

Figure 3: Feature engineering of Ransomware dataset (Extracted Features)

Additionally, the correlation matrices displayed in Figure 4 and Figure 5 highlight important relationships between features, indicating that some features are strongly correlated. For instance, url_length and num_subdomains show significant correlations in the phishing dataset, and similarly, name_length and has_exe_extension demonstrate correlations in the botnet dataset. These correlations guided the feature selection process by identifying redundant features that could be removed to enhance model performance.

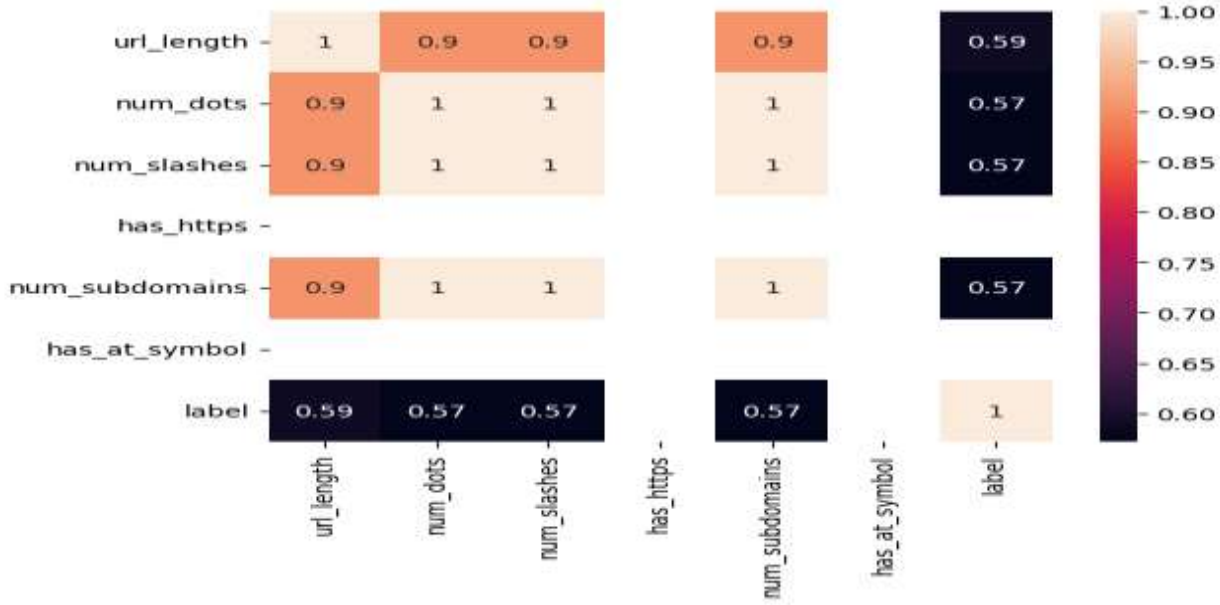


Figure 4: Correction Matrix of Phishing dataset

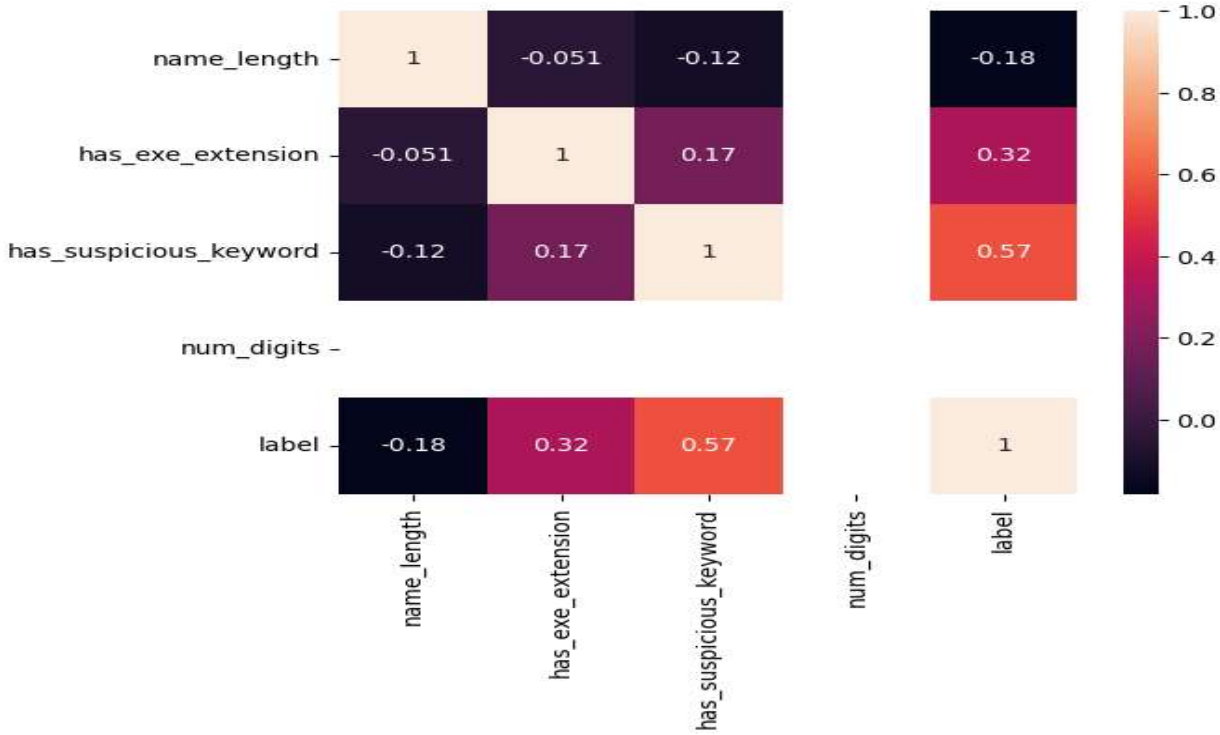


Figure 5: Correction Matrix of Botnet dataset

The performance of the Random Forest model for phishing detection, as depicted in Figure 5 and Figure 4, is promising. The classification report in Figure 5 highlights strong precision and recall for detecting phishing URLs, indicating that the model successfully identifies phishing attempts while minimizing false positives. The F1-score further underscores the model's robustness in handling the phishing dataset, despite its imbalanced nature. The confusion matrix in Figure 6 provides a detailed breakdown of the model's performance, showing a high number of true positives and true negatives, which is a positive outcome. However, there are still instances of false negatives, where phishing URLs are misclassified as legitimate, suggesting room for improvement in refining the model's sensitivity.

**Classification Report:**

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Legitimate (0) | 0.98 | 1.00 | 0.99 | 689 |
| Phishing (1) | 1.00 | 0.98 | 0.98 | 711 |
| accuracy | | | 0.99 | 1400 |
| macro avg | 0.99 | 0.99 | 0.99 | 1400 |
| weighted avg | 0.99 | 0.99 | 0.99 | 1400 |

Figure 6. Classification Report of the Phishing Dataset

**Classification Report:**

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Normal file (0) | 0.97 | 1.00 | 0.99 | 689 |
| Ransomware (1) | 1.00 | 0.97 | 0.98 | 711 |
| accuracy | | | 0.99 | 1400 |
| macro avg | 0.99 | 0.99 | 0.99 | 1400 |
| weighted avg | 0.99 | 0.99 | 0.99 | 1400 |

Figure 7 Classification Report of the Botnet Dataset

The integration of these models into a real-time simulation environment, as shown in Figure 9 and Figure 10, demonstrates the practical application of the trained Random Forest models in cybersecurity. The real-time phishing and ransomware detection system provides an interactive platform for users, simulating real-world scenarios. This implementation not only highlights the practicality of machine learning in detecting cyber threats but also emphasizes the

importance of continuous model retraining. As phishing techniques and ransomware attacks evolve, the models will need to adapt by incorporating new data to maintain high accuracy levels.

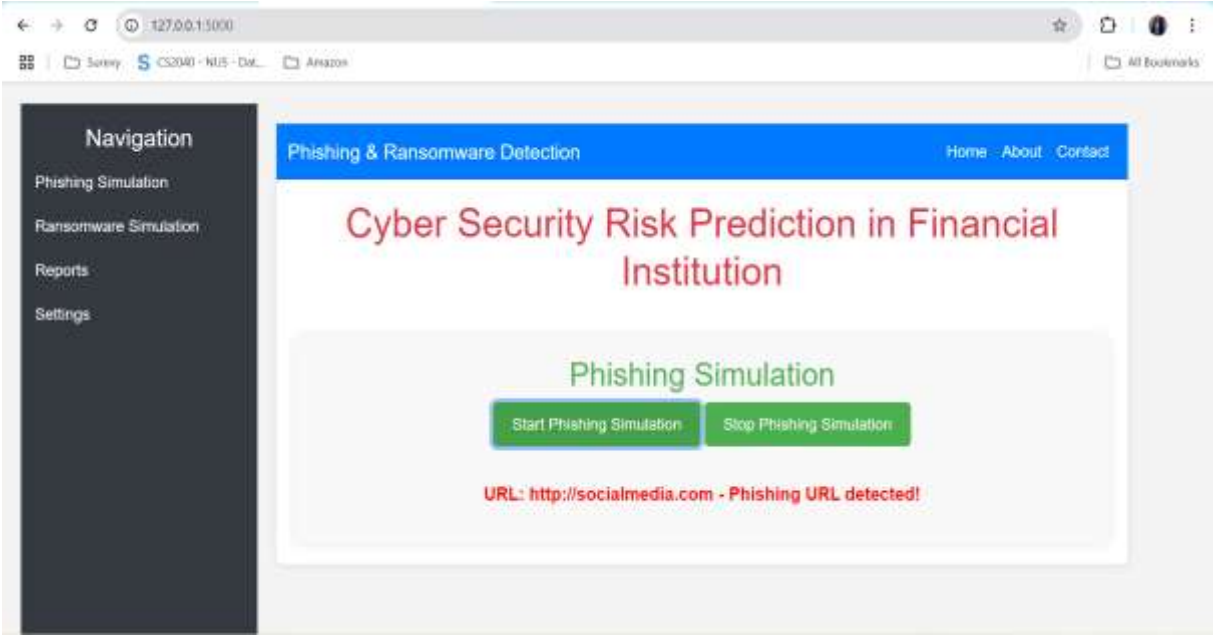


Figure 8: Simulated results of phishing website

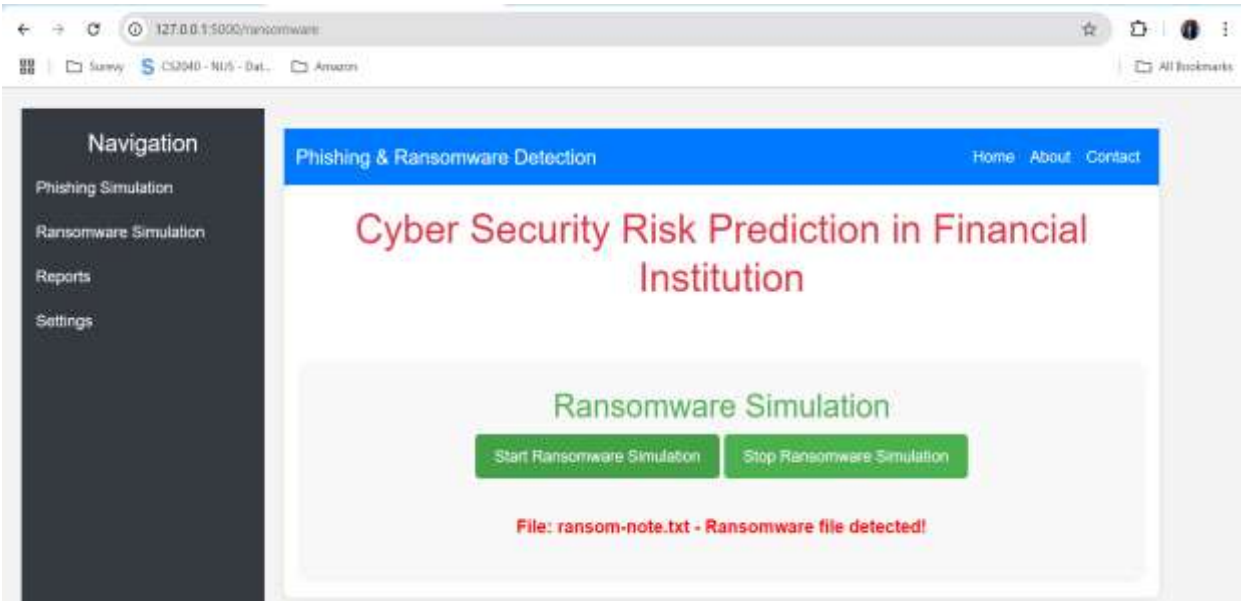


Figure 9: Ransomware Detected

## 5.0 Conclusion

This paper successfully achieved the objective of developing a technique for detecting dynamic cyber threats, specifically phishing attacks, using the Random Forest classifier. The performance metrics from the confusion matrix and classification report indicate that the Random Forest model performed exceptionally well, achieving a 99% accuracy in distinguishing between phishing and legitimate emails. The model demonstrated high precision (1.00 for phishing and 0.98 for legitimate emails) and

excellent recall for legitimate emails (1.00) and phishing emails (0.98), with an F1-score nearing perfect values. These results confirm the effectiveness of Random Forest in identifying phishing threats, making it a robust tool for dynamic cyber threat detection.

In addition to the model's accuracy, dimensionality reduction using Principal Component Analysis (PCA) helped optimize the dataset by removing less relevant features while retaining the most informative ones. This process improved computational efficiency and enhanced the model's performance by focusing on key attributes such as suspicious keywords and executable file extensions. The correlation matrix highlighted these features as having the strongest positive correlations with phishing threats, validating the choice of features selected through PCA. Reducing dimensionality not only streamlined the dataset but also increased the clarity of detecting phishing patterns.

Furthermore, the system incorporated outlier detection techniques to analyse patterns and identify potential threats more effectively. The detection of outliers played a crucial role in identifying unusual behaviours and patterns that could signify emerging or sophisticated phishing attacks. By incorporating outlier detection within the Random Forest framework, the system could enhance its capability in recognizing both common and rare phishing instances, thus broadening the scope of threat detection.

Finally, the system was implemented using Python, leveraging its vast libraries for machine learning and data analysis, such as sklearn for Random Forest and PCA, matplotlib and seaborn for visualization, and pandas for data manipulation. The use of Python enabled a seamless integration of the various components, from data preprocessing to model development and evaluation, culminating in an effective and flexible phishing detection system. Overall, the objectives of the research were successfully achieved, with a highly accurate and efficient model capable of identifying dynamic cyber threats with reduced dimensionality and enhanced pattern recognition.

## 6.0 Recommendation

1. Expansion of Feature Set and Domain Adaptation: Explore and integrate additional features beyond the current dataset, such as network behaviour metrics, user interactions, or behavioural analysis of email content, to enhance the model's ability to detect more sophisticated phishing attacks. Consider domain adaptation techniques to fine-tune the model for different industries or email systems, which may have unique phishing patterns and characteristics.
2. Real-Time Threat Detection and Response Integration: Develop and implement real-time detection and response mechanisms using the Random Forest model. This could involve integrating the model into an automated email filtering system that flags suspicious emails in real time and triggers immediate alerts or responses. Additionally, explore the potential for combining the Random Forest model with other machine learning models or cybersecurity tools to create a more comprehensive and adaptive threat detection system.
3. Continual Learning and Model Updating: Establish a process for continual learning and periodic model updates to ensure the phishing detection system remains effective against evolving threats. Implement mechanisms for incorporating new data, adapting to emerging phishing techniques, and retraining the model to maintain its accuracy and relevance. Consider using online learning techniques or periodic batch updates to keep the model current with the latest threat landscape.

## 7.0 Contribution to Knowledge

This dissertation uniquely advances the field of dynamic cyber threat detection by demonstrating the exceptional performance of the Random Forest classifier in identifying phishing attacks, achieving an impressive 99% accuracy. The integration of Principal Component Analysis (PCA) for dimensionality reduction and outlier detection techniques significantly enhances the model's efficiency and robustness, allowing it to detect both common and sophisticated phishing threats with high precision

and recall. The novel application of these combined methodologies within a Python-based framework not only optimizes computational efficiency but also provides a flexible and adaptive solution, setting this research apart from existing approaches by offering a comprehensive, high-accuracy tool for real-time phishing detection and response.

## 8.0 References

Abdelkader, W., Navarro, T., Parrish, R., Cotoi, C., Germini, F., Iorio, A., … & Lokker, C. (2021). Machine learning approaches to retrieve high-quality, clinically relevant evidence from the biomedical literature: systematic review. Jmir Medical Informatics, 9(9), e30401. https://doi.org/10.2196/30401

Angelopoulos, A., Michailidis, E., Νομικός, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., … & Zahariadis, T. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 20(1), 109. https://doi.org/10.3390/s20010109

Asiimwe, I., Zhang, E., Osanlou, R., Jorgensen, A., & Pirmohamed, M. (2020). Warfarin dosing algorithms: a systematic review. British Journal of Clinical Pharmacology, 87(4), 1717-1729. https://doi.org/10.1111/bcp.14608.

Vox Sanguinis, 113(8), 737-749. https://doi.org/10.1111/vox.12708

Brasil, S., Pascoal, C., Francisco, R., Ferreira, V., Videira, P., & Valadão, G. (2019). Artificial intelligence (ai) in rare diseases: is the future brighter? Genes, 10(12), 978. s

Brown, G., Ross, S., & Kirchhübel, C. (2021). Voicing concerns: the balance between data protection principles and research developments in forensic speech science. Science & Justice, 61(4), 311-318. https://doi.org/10.1016/j.scijus.2021.05.006.

Chen, C., Hasan, M., & Mohan, S. (2018). Securing real-time internet-of-things. Sensors, 18(12), 4356. https://doi.org/10.3390/s18124356.

Gai, K., Qiu, M., & Elnagdy, S. A. (2016, April). Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 197-202). IEEE.

Gao, B. (2021). The use of machine learning combined with data mining technology in financial risk prevention. Computational Economics, 1-21.

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 14(14), 8374.

Karimi, D., Dou, H., Warfield, S., & Gholipour, A. (2020). Deep learning with noisy labels: exploring techniques and remedies in medical image analysis. Medical Image Analysis, 65, 101759. https://doi.org/10.1016/j.media.2020.101759

King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00039

Mugarza, I., Flores, J., & Montero, J. (2020). Security issues and software update management in the industrial internet of things (iiot) era. Sensors, 20(24), 7160. https://doi.org/10.3390/s20247160

Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organizations: a systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227-242.

Pascarella, G., Rossi, M., Montella, E., Capasso, A., Feo, G., Botti, G., … & Morabito, A. (2021). Risk analysis in healthcare organizations: methodological framework and critical variables. Risk Management and Healthcare Policy, Volume 14, 2897-2911. https://doi.org/10.2147/rmhp.s309098

Pemmasani, S., Raman, R., Mohapatra, R., Vidyasagar, M., & Acharya, A. (2020). A review on the challenges in Indian genomics research for variant identification and interpretation. Frontiers in Genetics, 11. https://doi.org/10.3389/fgene.2020.00753

Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights Into Imaging, 9(5), 745-753. https://doi.org/10.1007/s13244-018-0645-y

Petersilge, C. (2019). The enterprise imaging value proposition. Journal of Digital Imaging, 33(1), 37-48. https://doi.org/10.1007/s10278-019-00293-1

Qayyum, A., Qadir, J., Bilal, M., & Al-Fuqaha, A. (2021). Secure and robust machine learning for healthcare: a survey. Ieee Reviews in Biomedical Engineering, 14, 156-180. https://doi.org/10.1109/rbme.2020.3013489

Radanliev, P., Roure, D., Walton, R., Kleek, M., Montalvo, R., Santos, O., … & Cannady, S. (2020). Covid-19 what have we learned? the rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive, and personalized medicine. The Epma Journal, 11(3), 311-332. https://doi.org/10.1007/s13167-020-00218-x

Roy, N. C., & Prabhakaran, S. (2022). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. Journal of Financial Crime, 30(1), 48-85.

Sarker, I. (2021). Machine learning: algorithms, real-world applications, and research directions. Sn Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00592-x