ISSN: 2182-2069 / E-ISSN: 2182-2077

An Innovative ML Strategy for Identifying Email Phishing Threats in Financial Cloud Infrastructure

Dr.V. Selvakumar[1*], Dr. John Yesudas Valluri[2], Dr. Takveer Singh[3], Dr.V. Haripriya[4], Dr. Shibani Borah[5], and Dr. Sachin S. Pund[6]

[1*]Assistant Professor, Department of Maths and Statistics, Bhavan's Vivekananda College of Science, Humanities and Commerce, Hyderabad, Telangana, India. drselva2022@gmail.com, https://orcid.org/0000-0003-1337-1495

[2]Associate Professor, CMS Business School, Faculty of Management Studies, Jain (Deemed-To-Be University), Bengaluru, India. dr.vy_john@cms.ac.in, https://orcid.org/0000-0002-3003-7408

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. takveer.singh.orp@chitkara.edu.in, https://orcid.org/0009-0000-7255-2507

[4]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to Be University), Bangalore, Karnataka, India. v.haripriya@jainuniversity.ac.in, https://orcid.org/0000-0003-2035-2452

[5]Assistant Professor, Department of Faculty of Commerce & Management, Assam Down Town University, Guwahati, Assam, India. shibaniborah@gmail.com, https://orcid.org/0009-0009-0828-7337

[6]Assistant Professor, Mechanical Engineering, Ramdeobaba University, Rbu, Nagpur, Maharashtra, India. pundss@rknec.edu, https://orcid.org/0000-0002-5616-2469

Received: December 15, 2024; Revised: January 22, 2025; Accepted: February 03, 2025; Published: February 28, 2025

Abstract

Phishing emails are a serious threat in financial cloud systems because they utilize deceptive information to trick users into opening unsanctioned accounts or stealing private data. To protect financial data and maintain the integrity of cloud-based financial systems. In this research, we aim to develop an innovative machine learning (ML) based strategy for identifying email phishing threats in financial cloud infrastructure. In a phished email, the sender can deceive the user into providing confidential data. Phishing emails is the primary concern while sending and receiving emails. For this, we proposed a novel Bald Eagle tuned Versatile Random Forest (BE-VRF) algorithm for identifying email phishing in a financial cloud environment. Initially, This study gathered the phish tank dataset for this study. After gathering the data we employed a stop word removal for the preprocessing method. We employed Independent Component Analysis (ICA) to extract the crucial features from the processed data. The suggested BE-VRF algorithm classifies the email texts and it can identify the abnormal mails. We implemented our suggested model in Python software. The performance evaluation phase employs various metrics such as f1 score, recall, accuracy, MAPE, and precision to examine the efficacy of suggested model. The evaluation study is done with different existing methods and the result express that the recommended model obtained

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 413-425.
DOI: *10.58346/JISIS.2025.I1.027*

*Corresponding author: Assistant Professor, Department of Maths and Statistics, Bhavan's Vivekananda College of Science, Humanities and Commerce, Hyderabad, Telangana, India.

improved outcome than other predictable methods, for identifying email phishing threats in financial cloud infrastructure.

Keywords: Email Phishing Threats, Machine Learning (ML), Bald Eagle Tuned Versatile Random Forest (BE-VRF), Financial Cloud and Security.

1 Introduction

Financial institution remains expose to serious risks starting email phishing scams as hackers are regularly changing their strategy to get around conventional defenses. Strong email protection solutions are stage more important as financial institutions shift a growing percentage of their activities in the cloud (Prasad et al., 2022). In the situation of financial cloud infrastructure, this study presents a novel machine learning (ML) approach that is particularly intended to detect and counter email phishing threats (Alnumay, 2024). Cloud computing usage in the financial production has several advantages, such as flexibility, cost-effectiveness and scalability (Abbas et al., 2021). But it also bring with new difficulty about cyber safety. Since email continues to be the major means of contact for financial institution, phishing attempt are predictable to function message (Sundararaj & Kul, 2021). These assaults frequently include relocate out fake emails that look factual in a test to deceive receiver into transfer private in revolve or moving out criminal acts (Mughaid et al., 2022). The complicated strategy used by criminal has render usual phishing recognition systems, such as rule-based filtering and signature-based scanning, which is ineffective (Alani & Tawfik, 2022). Through huge exactness, ML models can differentiate between deceiving and valid emails by using the massive volumes of data produced in financial cloud systems (Do et al., 2022). Sender reputation, email structure, verbal communication patterns and fixed address are characters. Moreover, the ML model is constantly improved via active learning, in which human analysts provide contribution on its forecasts, allowing to regulate new threats (Raman et al., 2024). The ML technique delivers a complete and flexible defense beside email phishing attacks by integrating different strategies (Vinayakumar et al., 2019). Cloud platform present the computing rule required for large-scale preparation and execution of complicated ML models (Anthony Sahaya Michael et al., 2018). Moreover, the aptitude to observe and evidence data centrally makes it easier to gather big datasets for evaluation and progress (Adebowale et al., 2020). The elective ML solution is a constructive and flexible resource of overcrowding electronic mail phishing attempt in cloud economic infrastructure. Financial organization can extensively improve their email security posture and protect sensitive data from unscrupulous actors by using cloud technologies and ML method (Alshehri et al., 2022). Financial cloud infrastructure identification of email phishing threats is complicated by factors like hackers' evolving tactics, sophisticated deception techniques, false positives that could cause failure, user knowledge, and the condition for constant update to detection algorithms, which complicates the development of functional mitigation strategies (Noor et al., 2019). This study use a novel ML method to identify email phishing risks in financial cloud connections that get better threat discovery effectiveness and precision (Sriwardany et al., 2025). It also secures the data in cyber security, defensive private financial information and reducing the threat of phishing scam (Zendehboudi et al., 2014).

2 Related Work

Barlow et al., (2020) addressed the trouble of defensive perceptive data from phishing attempt which are attractive a cyber security danger. The fact that present resolution depend on entity hazard finding is a recurring problem. The study offered a unique protection against phishing attempt that make use of ML and binary visualization. Li et al., (2020) focused on the developing risk of phishing emails in

information networks. Using an LSTM-based approach for significant email data, the system addresses complicated deception system and the increasing number of phishing emails by emphasizes model increase and difficult phases. Bountakas et al., (2021) focused on the increasing risk of phishing emails, which have been made better by the COVID-19 wave. It highlighted the need for enhanced techniques for identifying phishing emails Li et al., (2020). The study recommended and compared many ML methods like random forest (RF), decision tree (DT), logistic regression (LR), naive bayes (NB), natural language processing (NLP) approach, and term frequency-inverse document frequency (TF-IDF) for phishing email detection (Bindu et al., 2025). Fang et al., (2019) recognized the increasing danger posed by phishing emails and the lack of efficient defenses, which tackled this significant problem. To assess email association along with the header, body, character and word levels, it makes use of an improved recurrent convolution neural network (RCNN) model with multilevel vectors and an attention mechanism. The study makes use of an unbalanced dataset that depicts real-world phishing percentages. Singh et al., (2020) focused on the growing cybercrime that takes advantage of the internet's enormous reach, especially phishing. The research proposed a phishing detection system that uses deep learning (DL), in exacting a convolutional neural network (CNN), to avoid these kinds of attacks. Bansal & Sidhu, (2021); Do et al., (2022) explored the widespread problem of spam on the internet. It optional a way to avoid spam and defend private data by combine an artificial neural network (ANN) with the TFIDF approaches.

3 Methodology

In this section, the BE-VRF method is proposed to identify email phishing threats in financial cloud infrastructure. The phish tank dataset is collected. The second stage is to pre-process the data utilizing stop word removal. Then, independent component analysis (ICA) is applied for feature extraction. The study flow is shown in Figure 1.

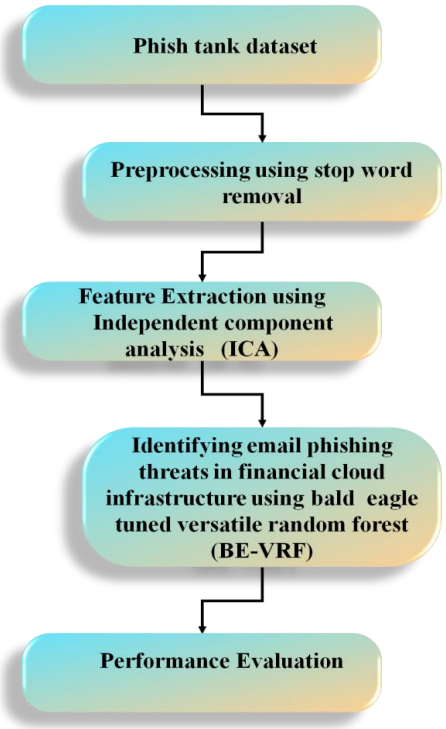

Figure 1: Flow of this Study

Dataset

For this research, the dataset consist of symmetric data (SD) metrics following by phish tank to index 10,000 authentic websites and 10,000 phishing URLs. The open, community-driven phish tank examine maintains a record of established spoof websites. Data collected from feedback usual about disputed websites is compiled by an expert team and verified directly. The phish tank data contains information on the spoofing website's URL. It is significant to use the most recent data collection since it is simplified frequently (Aldakheel et al., 2023).

Preprocessing using Stop Word Removal

Identifying email phishing threats in financial cloud architecture require parsing mail, removing stop words to remove related content and look at dispatcher hope, link location and attachment. Significant keywords that express malicious intention is decorated when stopping words like predicates and parallel connect are eliminating. After that, ML method can categorize emails according to these crucial signs, representing possible phishing attempts that need more explore or prompt response. This basic process strengthens cyber security defenses in economic cloud system by improving detection speed and exactness.

Feature Extraction Using Independent Component Analysis (ICA)

Advanced technique such as feature extraction for ICA is used in financial cloud construction to identify email phishing threats. Applying ICA makes potential to divide certain patterns and characteristics from email conversations, which can assist in identifying predictable phishing attempts. Let us believe that the random essentials of the source vector $W = [w_1, w_2, \ldots, w_K]^s$ are representing as linear combination of the element of a random vector $[t_1, t_2, \ldots, t_k]^s$. This combination can be expressed in equation (1).

$$W = Bt \tag{1}$$

Where W the vector of is observed signals, t is the vector of previously unknown independent source signals and B is the unknown matrixes of mixes of dimension $K \times K$. The combined value of X and the separation matrix $X(X = B^{-1})$ is used to get an estimate of the sources, $\hat{T}$, expressed in equation (2):

$$\hat{T} = XW = B^{-1}W \tag{2}$$

Finding a classification matrix W that could render the approximate value of the independent components $(\hat{T}_j)$as statistically independent from one another as feasible is the aim of ICA. It could be carried out by making the use of several statistical characteristics of the source signals, including temporal structure and non-Gaussianity. This technique improves detection accuracy by identifying minute differences between authentic communications and those suggestive of phishing assaults. By using ICA for feature extraction, financial institutions can improve their cyber security defenses and reduce the risks related to fake email activity in cloud environments.

Identifying Email Phishing Threats in Financial Cloud Infrastructure Using Bald Eagle Tuned Versatile Random Forest (BE-VRF)

- **Versatile Random Forest (VRF)**

Maintaining information security requires and recognize the email phishing threats in financial cloud infrastructure. One useful tool in this attempt is the VRF. Enhanced flexibility and exactness in

categorization tasks are provide by VRF, an expansion of the RF method. By using its flexibility, VRF can recognize phishing emails that are sent to cloud infrastructure in the stage. Equation (3) is used to find out the classification result.

$$D(s)\max_{O} F_s \sum_{j=l}^{L}\left(d_j(S)=O\right) \quad (3)$$

Where s is the innovative instruction dataset. The groups of data from the T gathering are denote by $D$and L. Using a random vector, the program produces L email phishing attacks for each subgroup. The classification result is shown by $D(s)$, while the classification result of the jth financial cloud infrastructure is indicated by $d_j(S)$. This time, the target category is S. To improve the model's prediction performance or accelerate the method, several random forest hyper-parameters are used. When managing high-dimensional data, VRF achieves superior performance by completing an implicit email phasing. The email phasing attacks RF can use financial cloud infrastructure as a tracking requirement to determine feature significance.

$$j(s)I - e_I^2 - e_0^2 \quad (4)$$

When using VRF, several decision trees are built, each taking into a different subset of characteristics. The predictions from these trees are combined to get a final choice. With its improved generalization and less overfitting, this method can handle a variety of phishing email patterns expressed in equation (4). In this case, every node is denoted by S and it could represent any RF node. An estimate of email assessment called the optimal split is found via email phishing. Additionally, the class is represented by $mandj = 0,1$ in equation (5), and e_i is the proportion of m_i samples relative to the total number of samples.

$$e_i = \frac{m_i}{m} \quad (5)$$

Reducing δj can be performed by dividing and sending products to two distinct sub-notes $(j_s e_r)$based on a threshold on variable Θ. The process is reflected in equation (6).

$$\delta j(s) = j(s) - e_o j(s_o) - e_r j(s_r) \quad (6)$$

Next, using all-inclusive values of Θ, which are available in the node overall thresholds, a thorough search is carried out. Equation (7) indicates email phishing identification is stored for each variable independently while taking into all nodes.

$$J_H(\Theta) = \sum_q \sum_r \delta j_\Theta(s,S) \quad (7)$$

Financial institutions can improve their cyber security defenses and lessen the risks associated with phishing attempts in cloud settings by using VRF.

- **Bald Eagle Optimization**

Protecting responsive data and avoidance economic losses depend on identifying email phishing attacks inside financial cloud architecture. A unique solution to this problem is provided by BE, which derives inspiration from the hunting habits of BE. BE effectively sorts through the enormous volumes of data to spot possible hazards by imitating the eagles' acute perception and quick reactions. The following equation (8) expresses this phase:

$$O = O_{best} + SE.s.(O_n - O) \quad (8)$$

Where SE is a variable element known as the transition factor that is used to enhance the exploration and extraction phases and O_n stands for the mean of all locations as it can be expressed in equation (9).

$$SE(j) = l\left(1 + \frac{J_{max}-j}{J_{max}+j}\right) \quad (9)$$

Where j is the current iteration, l is a gain, and J_{max} specifies the maximum number of iterations [*1.5, 2*]. BE could be used to examine communication developments, identify problems and identify insecure actions suggestive of attempted phishing. Financial institutions could enhance their safety record by detecting and eliminating phishing attacks, before they cause harm by using BE's adaptive search functions. During this stage, the eagle keeps track of its location and searches as follows in equation (10).

$$O^i = O^i + z^i.\left(O^i - O^{i+1}\right)w^i.\left(O^i - O_m\right) \tag{10}$$

The ith new location is denoted by O^i, and the directional coordinate indications w and z can be produced in the following equation (11).

$$\begin{cases} w^i = \frac{wq^i}{max(|wq|)}; wq^i = q^i.sin(\theta(j)) \\ z^i = \frac{zq^i}{max(|zq|)}; zq^i = q^i.cos\left(\theta(j)\right) \\ \theta = D_1.\pi.rand; q = \theta.Q \end{cases} \tag{11}$$

This can be derived as follows as equation (12): where D_1 is a control gain and Q is a constant [*0.5, 2*].

$$D_1 = \alpha_1\left(1 + \frac{S_{max} - s}{S_{max} + s}\right) \tag{12}$$

The constant α_1 is found in [*5, 10*]. A continuous defense against the developing art of phishing attacks is offered by the integration of BE into financial cloud infrastructure, which enhances current security measures. Businesses can improve their defenses and guarantee the confidentiality and integrity of financial data stored on cloud storage by incorporating BE into email security procedures.

4 Result and Discussion

This study used python 3.11.4 to increase the essential protocol. Using a Windows 11 laptop with an Intel i5 11th Gen CPU and 32 GB of RAM, the recommended approach is performed. Our proposed method, BE-VRF is used to identify email phishing threats in financial cloud infrastructure which has several concert indicators utilized to assess the recall, f1-score, precision, accuracy and means absolute percentage error (MAPE). We compare the suggested technique to other existing methods like support vector machine (SVM) (Balim & Gunal, 2019), random forest (RF) (Balim & Gunal), linear regression (LR) (Balim & Gunal 2019), K-nearest neighbor (KNN) (Mridha et al., 2021), decision tree (DT) (Mridha et al., 2021) and RF (Mridha et al., 2021). Table 1 shows the comparison of precision, recall and f1-score.

Table 1: Comparison of Precision, Recall, F1 Score

Method	Precision	Recall	F1-Score
SVM (Balim and Gunal 2019)	0.880	0.980	0.927
RF (Balim and Gunal 2019)	0.880	0.980	0.927
LR (Balim and Gunal 2019)	0.890	0.960	0.924
BE-VRF (Proposed)	0.924	0.99	0.95

Precision

Accurately separating fraudulent emails from valid ones is crucial for detecting email phishing risks in financial cloud infrastructure with precision and few false positives. It verifies that the emails which have been reported as threats are real, increasing the effectiveness of security by concentrating efforts on real threats, strengthening defenses and protecting financial information and operations from cyber-

attacks. Figure 2 demonstrates the graphical representation of precision. The existing methods such as SVM (Balim & Gunal, 2019) attained 0.880, RF (Balim & Gunal, 2019) attained 0.880 and LR (Balim & Gunal, 2019) attained 0.890. When compared to other current approaches, our suggested BE-VRF method achieved a 0.924 with improved efficiency.

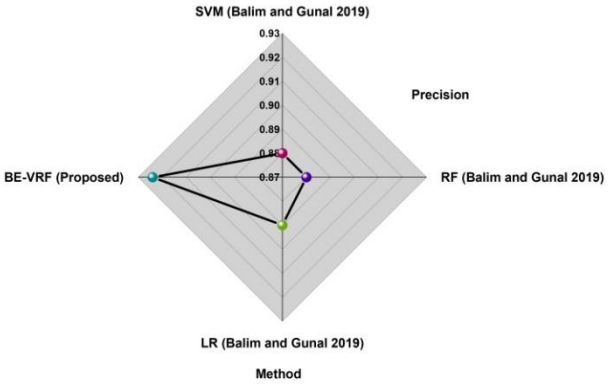

Figure 2: Graphical Representation of Precision

Recall

The economic cloud infrastructure prioritizes memory when identifying email phishing threats; ensure inclusive detection of phishing attempts with recall. By successfully detect fake emails, this technique attempts to reduce false negative and advance security, defensive cloud-hosted economic systems from potential intrusion. Figure 3 demonstrates the graphical demonstration of recall. The existing methods such as SVM (Balim & Gunal, 2019) with 0.980, RF (Balim & Gunal, 2019) with 0.980, and LR (Balim & Gunal, 2019) with 0.960. In comparison with other existing approaches, our suggested BE-VRF method provides a 0.99 with a higher success of recall.

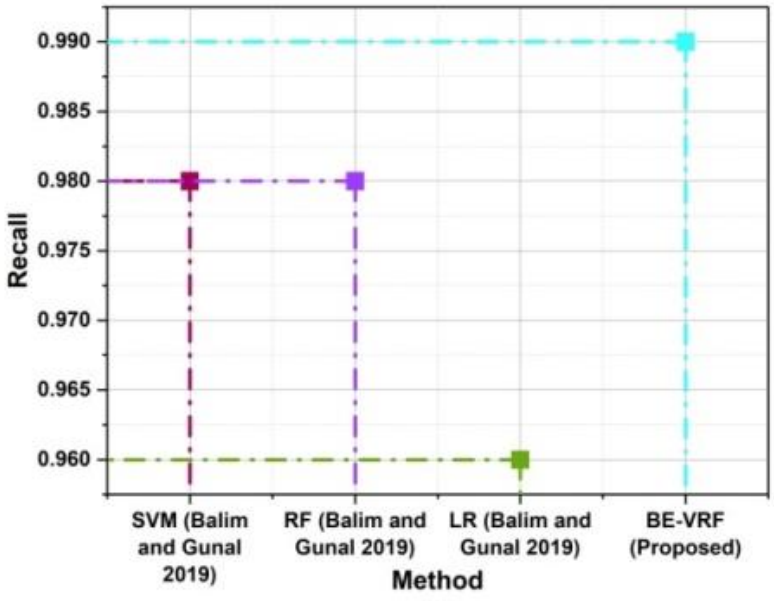

Figure 3: Graphical Representation of Recall

F1-Score

The F1-score assess the difference between recall and accuracy, which is significant for specific hazard detection and is used in the identification of email phishing attacks in financial cloud infrastructure. This technique improves the competence of phishing detection technique by using an F1-score assessment that provides strong security procedures in financial cloud settings. Figure 4 demonstrates the graphical representation of f1-score. The existing method such as SVM (Balim & Gunal, 2019) attained 0.927, RF (Balim & Gunal, 2019) attained 0.927, and LR (Balim & Gunal, 2019) attained 0.924. When compare to other current approaches, our suggested BE-VRF method gives a 0.95 with better efficiency of the f1 score. Table 2 shows the comparison of accuracy and MAPE.

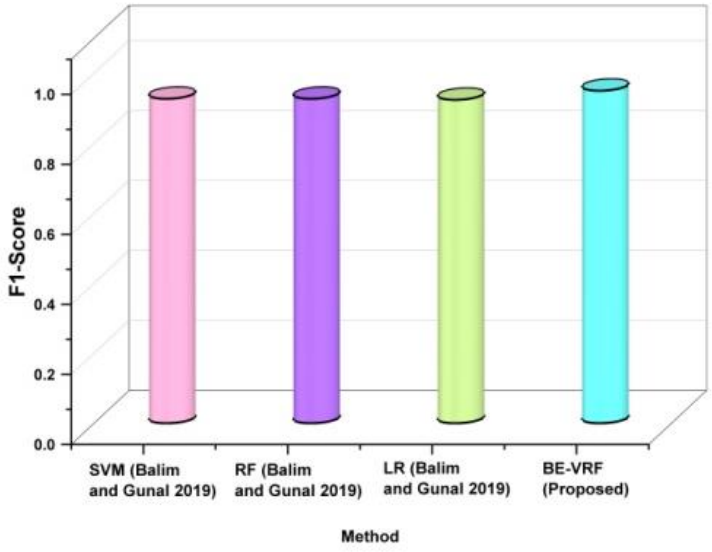

Figure 4: Graphical Representation of f1-score

Table 2: Comparison of Accuracy and MAPE

Method	Accuracy (%)	MAPE
RF (Mridha et al., 2021)	97.65	0.565
DT (Mridha et al., 2021)	96.61	0.562
KNN (Mridha et al., 2021)	95.73	0.567
BE-VRF (proposed)	99.2	0.431

Accuracy

Financial cloud communications is able of detecting email phishing threats via the use of exactness metrics. The expertise detects suspicious action with high accuracy, intensification security protocols and protecting sensitive financial data from fraudulent schemes by evaluate email content, sender repute and user presentation model. Figure 5 demonstrates the graphical representation of the accuracy. The existing methods such as KNN (Mridha et al., 2021) (95.73%), DT (Mridha et al., 2021) (96.61%) and RF (Mridha et al., 2021) (97.65%). In comparison with other current approaches, our suggested BE-VRF method provides a (99.2%) with higher efficiency of accuracy.

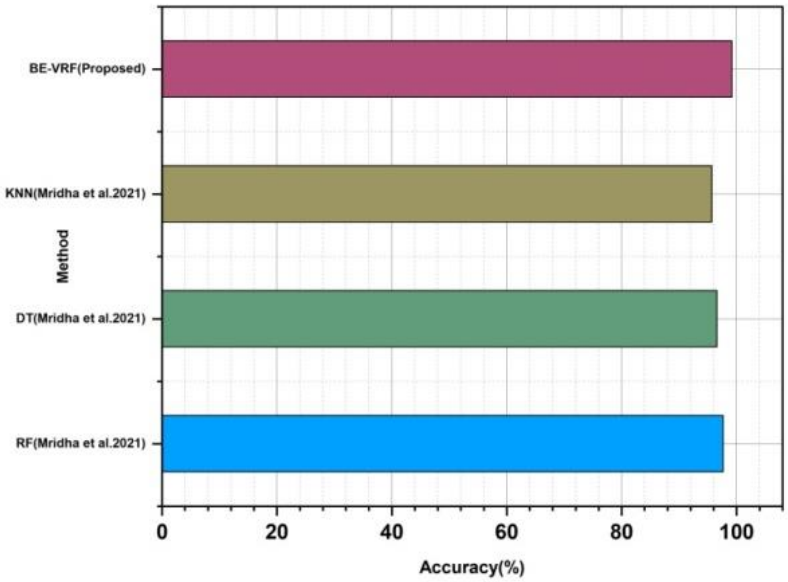

Figure 5: Graphical Representation of Accuracy

MAPE

MAPE is a functional tool for assess the accuracy of phishing threat forecasts when identify email phishing threats in financial cloud infrastructure. Through the assessment of predictable and observed values, MAPE measures the extent of forecasting mistakes, enabling the efficient detection and counteraction of potential fake hazards. Figure 6 demonstrates the graphical representation of the MAPE. The existing methods obtained like KNN (Mridha et al., 2021) (0.567), DT (Mridha et al., 2021) (0.562) and RF (Mridha et al., 2021) (0.565). Our proposed BE-VRF method offers a MAPE (0.431) with lesser error rate efficiency when compared to other existing methods.

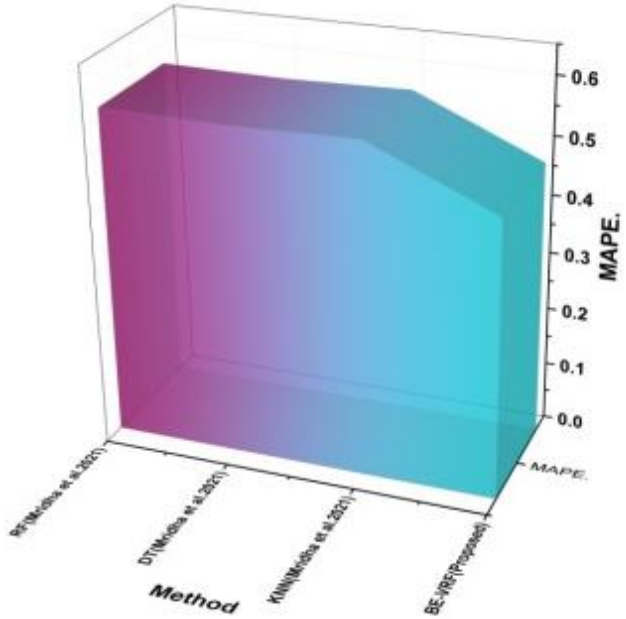

Figure 6: Graphical representation of MAPE

5 Conclusion

This research presents an approach that uses ML to classify emails as phishing attack. The novel ML advance has been recommended as a dependable way to identify email phishing risks in financial cloud architecture. It improves protection measures, reducing risks and defensive sensitive economic information by using modern algorithms and data study methods, enhancing the reliability of cloud-based operations. The BE-VRF technique is employed for email phishing threats in financial cloud infrastructure. Our proposed BE-VRF method provided accuracy (99.2), precision (0.924), recall (0.99), MAPE (0.431), and f1-score (0.95). By analyzing the general conclusion, our proposed method provided better efficiency in identifying email phishing threats in financial cloud infrastructure. A limitation is the potential for false positives and negative since machine learning algorithms can struggle to distinguish between legitimate emails and phishing ones. The efficiency of the method can be further risk by the need for continuous updates to the training data and the dynamic nature of phishing attempt. Future research could focus on developing a user-friendly dashboard for real-time threat monitoring, leveraging reinforcement learning for dynamic threat adaptation, integrating advanced anomaly detection techniques to enhance the accuracy of the ML model and investigating the integration of natural language processing for a deeper semantic analysis of phishing emails in financial cloud infrastructure.

Reference

[1] Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., ... & Cambiaso, E. (2021). Identifying and mitigating phishing attack threats in IoT use cases using a threat modeling approach. *Sensors*, 21(14), 4816. https://doi.org/10.3390/s21144816

[2] Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2020). Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management, 36(3), 747-766. https://doi.org/10.1149/10701.1387ecst

[3] Alani, M. M., &Tawfik, H. (2022). Phishnot: A cloud-based machine-learning approach to phishing URL detection. *Computer Networks, 218,* 109407. https://doi.org/10.1016/j.comnet.2022.109407

[4] Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., &Alzahrani, A. I. (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

[5] Alnumay, W. S. (2024). Use of machine learning for the detection, identification, and mitigation of cyber-attacks. *International Journal of Communication and Computer Technologies, 12*(1), 38-44. https://doi.org/10.31838/IJCCTS/12.01.05

[6] Alshehri, M., Abugabah, A., Algarni, A., & Almotairi, S. (2022). Character-level word encoding deep learning model for combating cyber threats in phishing URL detection. *Computers and Electrical Engineering, 100,* 107868. https://doi.org/10.1016/j.compeleceng.2022.107868

[7] Anthony Sahaya Michael, M., Sathya Narayanan, P., Veera Mani, S., & Rathika, S. K. B. (2018). Education Data Mining Using Fuzzy Clustering and Classification. *International Journal of Advances in Engineering and Emerging Technology, 9*(2), 28–31.

[8] Balim, C., & Gunal, E. S. (2019, November). Automatic detection of smishing attacks by machine learning methods. In *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (pp. 1-3). IEEE. https://doi.org/10.1109/UBMYK48245.2019.8965429

[9] Bansal, C., & Sidhu, B. (2021, September). Machine learning based hybrid approach for email spam detection. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICRITO51393.2021.9596149

[10] Barlow, L., Bendiab, G., Shiaeles, S., & Savage, N. (2020, October). A novel approach to detect phishing attacks using binary visualisation and machine learning. In *2020 IEEE World Congress on Services (SERVICES)* (pp. 177-182). IEEE. https://doi.org/10.1109/SERVICES48979.2020.00046

[11] Bindu, N. V. M., Nassa, V. K., Vasuki, P., Manikandan, G., Jeena, R., & Mahaveerakannan, R. (2025). IoT botnet detection from software defined network using American zebra optimization algorithm with SSRNN-ELM. *International Journal of Information Technology*, 1-9.

[12] Bountakas, P., Koutroumpouchos, K., & Xenakis, C. (2021, August). A comparison of natural language processing and machine learning methods for phishing email detection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-12). https://doi.org/10.1145/3465481.3469205

[13] Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep learning for phishing detection: Taxonomy, current challenges, and future directions. *Ieee Access*, *10*, 36429-36463. https://doi.org/10.1109/ACCESS.2022.3151903

[14] Fang, Y., Zhang, C., Huang, C., Liu, L., & Yang, Y. (2019). Phishing email detection using an improved RCNN model with multilevel vectors and attention mechanism. *IEEE Access*, *7*, 56329-56340. https://doi.org/10.1109/ACCESS.2019.2913705

[15] Li, Q., Cheng, M., Wang, J., & Sun, B. (2020). LSTM-based phishing detection for big email data. *IEEE transactions on big data*, *8*(1), 278-288. https://doi.org/10.1109/TBDATA.2020.2978915

[16] Mridha, K., Hasan, J., & Ghosh, A. (2021, September). Phishing URL classification analysis using ANN algorithm. In *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 1-7). IEEE. https://doi.org/10.1109/GUCON50781.2021.9573797

[17] Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819-3828.https://doi.org/10.1007/s10586-022-03604-4

[18] 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. https://doi.org/10.1016/j.future.2019.02.013

[19] Prasad, V. K., Dansana, D., Mishra, B. K., & Bhavsar, M. (2022). Intensify cloud security and privacy against phishing attacks. *ECS Transactions*, *107*(1), 1387. https://doi.org/10.1149/10701.1387ecst

[20] Raman, A., Balakrishnan, R., Arokiasamy, A. R., Pant, M., Batumalai, C., & Kuppusamy, M. (2024). Design and Developing a Security and Threat Model for Sustainable Manufacturing. *Journal of Internet Services and Information Security*, *14*(3), 245-255. https://doi.org/10.58346/JISIS.2024.I3.014

[21] Singh, S., Singh, M. P., & Pandey, R. (2020, October). Phishing detection from URLs using deep learning approach. In *2020 5th International Conference on Computing, communication and Security (ICCCS)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCS49678.2020.9277459

[22] Sriwardany, S., Fadhilah, D. D., & Sunny, R. (2025). Risk Management In Rice Farming Using Hybrid Fmea-Ahp: A Case Study From Hamparan Perak, Indonesia. *Acta Innovations*, 24–37. https://doi.org/10.62441/actainnovations.vi.402

[23] Sundararaj, A., & Kul, G. (2021). Impact Analysis of Training Data Characteristics for Phishing Email Classification. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *12*(2), 85-98.

[24] Vinayakumar, R., Soman, K. P., Poornachandran, P., Akarsh, S., & Elhoseny, M. (2019). Deep learning framework for cyber threat situational awareness based on email and url data analysis. *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*, 87-124. https://doi.org/10.1007/978-3-030-16837-7_6

[25] Zendehboudi, M., Azimpour, J., & Gorginpour, H. (2014). Offering a Method for Ensuring Data Storage Security in the Cloud Network by Using Kerberos Algorithm. *International Academic Journal of Science and Engineering, 1*(2), 75–81.

Authors Biography

Dr. V. Selvakumar is an Assistant Professor in the Department of Mathematics and Statistics at Bhavan's Vivekananda College of Science, Humanities, and Commerce, Hyderabad, Telangana, India. With a strong foundation in mathematical sciences, his research interests include mathematical modeling, optimization, statistical methods, computational mathematics, probability theory, and applied statistics. He has actively contributed to academia through teaching, mentoring, and publishing research articles in reputed journals, along with presenting at national and international conferences. As a dedicated researcher, he is also a reviewer for scientific journals and a member of various mathematical and statistical societies. His expertise extends to problem-solving approaches, statistical techniques, and interdisciplinary methodologies, making significant contributions to the field. He remains committed to advancing research and education, inspiring students and scholars in mathematics and statistics.

Dr. John Yesudas Valluri is an Associate Professor at CMS Business School, Faculty of Management Studies, Jain (Deemed-to-Be University), Bengaluru, India. With extensive expertise in management studies, he specializes in areas such as business strategy, organizational behavior, financial management, and leadership development. Dr. Valluri is actively engaged in teaching, research, and mentoring, contributing to the academic growth of students and professionals. He has published research papers in reputed journals, presented at national and international conferences, and collaborated on industry-oriented projects. His academic excellence and commitment to innovation in management education make him a distinguished scholar in his field.

Dr. Takveer Singh is a researcher at the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His research interests focus on research impact assessment, innovation management, outcome evaluation, and technological advancements. Actively engaged in research and collaboration, Dr. Singh has contributed to reputed journals, conferences, and projects aimed at enhancing research quality and societal impact. Dedicated to fostering innovation and academic excellence, he continues to make significant contributions to his field.

Dr.V. Haripriya is an Assistant Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-Be University), Bangalore, Karnataka, India. Her research interests span across cutting-edge areas in computer science, including artificial intelligence, machine learning, data science, and cybersecurity. She is actively involved in teaching, mentoring, and conducting innovative research, with several publications in reputed journals and presentations at national and international conferences. With a strong commitment to academic excellence and technological advancements, she continues to contribute significantly to the field of computer science.

Dr. Shibani Borah is an Assistant Professor in the Department of Faculty of Commerce & Management at Assam Down Town University, Guwahati, Assam, India. Her research interests include business management, finance, marketing, entrepreneurship, and organizational behavior. Actively involved in teaching, mentoring, and research, Dr. Borah has published papers in reputed journals, presented at national and international conferences, and contributed to various academic projects. Committed to promoting

excellence in commerce and management education, she continues to make valuable contributions to her field.

Dr. Sachin S. Pund is an Assistant Professor in the Department of Mechanical Engineering at Ramdeobaba University (RBU), Nagpur, Maharashtra, India. His research interests include thermal engineering, fluid mechanics, advanced manufacturing processes, and automation in mechanical systems. With a strong academic and research background, he has contributed significantly to the field through publications in reputed journals, conference presentations, and collaborative projects. Dr. Pund is dedicated to mentoring students and fostering innovation in mechanical engineering education.