International Journal of Environmental Sciences
ISSN:2229-7359
Vol.11 No.17s, 2025
https://www.theaspd.com/ijes.php

Security-Aware Malicious Hyperlinks Phishing Detection Using Combined Machine Learning Models

Shivani Yadao
Department of Computer Science and Engineering, Stanley College of Engineering and Technology for Women, Hyderabad, India, shivaniyadao@stanley.edu.in

Abstract: *Phishers utilise email phishing through URLs that are obfuscated, malicious, or phished, and they continually adapt or reinvent their techniques in order to entice victims. The problem of phishing attacks in enterprise is the next issue that is rising in wide scale and complexity. The use of visceral variables and familiarity signals has become more common in phishing attempts in order to earn the trust and confidence of victims. It would be naive to think that phishing is always focused on financial gain, even if it is usually the phisher's obvious goal when they commit identity theft. The goodwill and character of an internet user can also be taken by a phisher. In this kind of situation, a phisher has no boundaries. Making a fool of oneself in the academic or professional world might be more fatal than revealing oneself on a social media site. It is not an easy process to resolve this matter. An analysis of the available literature reveals that traditional methods of phishing detection filters are inadequate for spotting the many types of phishing attempts that can occur in a corporate setting. As a result, we provide an innovative anti-phishing solution for businesses based on an artificial neural network. This approach also successfully determines if an email is known or unknown phishing, which helps to lessen the impact of trust and familiarity-based email phishing in business environments. To improve the URL categorisation process, we use the Feed-Forward Backpropagation and Levenberg-Marquart methods of Artificial Neural Networks (ANNs). To acquire results with imprecise data of social aspects, we use the Fuzzy Inference System. When it comes to URL-based email phishing, the suggested model can correctly categorise both common and uncommon examples.*
Keywords: *Phishing Detection, Machine Learning, Cybersecurity, Web Link Analysis, Hyperlink Classification.*

1. INTRODUCTION

Email phishing is a major problem in the modern digital world that leads to financial losses when people buy things online [1]. In order to identify email phishing attempts, many anti-phishing methods are now being considered. There are a lot of anti-phishing methods out there, but they are not up to the task of dealing with problems as they happen in real time. While URL blacklisting is commonly used in business and organisations, it is not very effective when it comes to accurately detecting email phishing assaults, according to a group of researchers who reviewed the relevant literature. Phishing attacks are still common since most people using the internet don't know how computers work or aren't aware of the dangers that lurk on the internet. Even today, a large percentage of internet users do not know how to spot phishing emails [2]. When it comes to distinguishing between fake and real websites, for example, neither users nor workers have a firm grasp of the syntax nor semantics of URLs. Phishers take advantage of the fact that internet users aren't very vigilant by creating phishing emails with harmful links or faked websites, which they then send to specific users or distribute in bulk [3]. Despite this, phishing attacks can be launched in a variety of ways, including via URLs, emails, instant messages, forum posts and comments, social media, and so on. Addressing the growing issue of email phishing in enterprises is no easy feat [4].

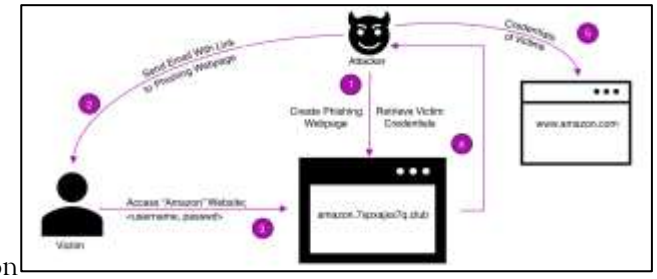

Figure 1. Represents phishing detection

The purpose of this study is to examine methods for identifying business email phishing attempts. In order to overcome these obstacles, researchers have come up with a variety of potential solutions, such as email phishing detection systems or models that use advanced machine learning techniques. There are now two main types of security mechanisms [5]. There is a heuristic-based method and a list-based technique. According to [6], a list-based technique determines whether a website is valid and adds it to a preset list, which could be a whitelist, a blacklist, or both. The heuristic-based technique, in contrast, relies on known characteristics of phishing websites or malicious URLs to aid in their detection and identification [7]. Using Naïve Bayes and Support Vector Machine classifiers, a heuristic-based model can identify email phishing attempts through URLs, whether they are obfuscated, malicious, or phished. According to Social Network Analysis [8], this model incorporates a URL detection algorithm that effectively distinguishes between real and phishing URLs. The rule-based phishing detection strategy has been found to be useful in analysing website information and detecting phishing attacks, according to research. There is currently a plethora of ML-based phishing filtering methods available, including decision trees, random forests, logistic regression, Support Vector Machines, Markov Models, and many more [9]. This chapter presents an innovative method that uses artificial neural networks (ANN) to identify email phishing in an organisational setting.

2. LITERATURE SURVEY

A tremendous level of user attention has been drawn to social networking since its rise to prominence in the last decade. What we call "social networking" these days are online platforms that facilitate user-to-user interactions inside a certain niche. In order to connect with others socially, either through acquaintances or at random, users can create profiles that are either public or protected. An increasingly popular way for people to meet virtually and share ideas, information, opinions, and experiences is through social networking sites. Phishers have taken notice of the growing number of people who rely on and prefer to use e-communication and social networking sites as a source of information, news, opinions, and other different subjects [10].

2.1 Phishing Attack through Social Engineering

The ease, effectiveness, and efficiency of social engineering have been understood by current antagonists. The use of email as a conduit for phishing attacks—which include data collecting, foot-printing, and persuasion—has been very effective. Email and social media have also become targets of widespread phishing assaults. In order to create and carry out these assaults, phishers must engage in extensive social engineering to ensure that their traps are both effective and difficult to detect [11]. Social engineering attacks in enterprise environments are on the rise. Examples of social engineering attacks include deceiving, psychological manipulation, and impersonation. Intended to trick unsuspecting users or staff into divulging sensitive information [12]. A common tool for hammering the theory into a framework is electronic communication, such as email. The emails or other forms of communication are designed to make the victim feel a sense of urgency, panic, or similar emotions, which can encourage them to quickly trust or disclose important information. For example, [13] going to an unsafe website after clicking on a malicious link or file. Nowadays, it's extremely difficult for corporate employees to escape these attacks, especially with the prevalence of social engineering [14]. The vast majority of people who fall for phishing schemes are familiar with the fact that people would rather avoid confrontation with authoritative figures or awkward social situations. This is why phishers engage in social engineering, take advantage of users' actions, and start collecting information about them, such as their job history, interests, family history, and any other personal details. Then, based on these observations, the attacker creates an email or profile that might make the victim feel like they're dealing with a real person. According to [15], the next step for the attackers is to attempt to establish a remote relationship with the user by concealing his preferences or sending online invitations to specific seminars, tenders, projects, assignments, or unsolicited promotions, job offers, or a call for job interviews. In general, the attackers are attempting to attract the user to their area of interest [16].

The term "familiarity exploitation" is a type of phishing assault in which the perpetrator tries to pass themselves off as friendly in order to trick a user, who may or may not be familiar with the attack. An important part of social engineering and a common tactic in phishing attempts is preying on people's

familiarity with them [17]. To sum up, it's all about giving the impression that joining the relevant webpage or website is completely natural and authentic. While everyone has their own unique reactions to new experiences and individuals, those with whom they are already familiar will never make an impression. When someone one knows is around, one's natural cynicism is calmed. Therefore, a business insider is often a double-edged sword [18]. The purpose of creating an imposter account is to trick users, customers, or employees of a business into divulging sensitive information, such as login credentials, personal details, or data related to the business. This is typically accomplished by sending a fake link to the target. There is a risk that visiting a website through an email link can lead to the theft of personal information or login credentials [19]. Anyone with unapproved access to a company's confidential information, systems, data, or personnel—whether they are employed there or not—is considered an insider threat [20]. More than three-quarters of all cyber security breaches in organisational environments that involve trusted individuals or insiders are caused by this. With more and more people using their phones and other electronic devices to access email and social media, insider threats and phishing attacks have become more common [21]. Within an organisation setting, the biggest and most pervasive pool of potential phishers consists of careless and unaware individuals who fall prey to insider fraudsters [22]. In order to trick users or employees into falling for their traps, phishers use psychological tricks like manipulation of thoughts to make them feel bad about themselves, trusting the scammer, anxious about losing money, or even elated [23]. Enterprise users and employees have been the targets of phishing attacks thus far, leaving them susceptible to falling for the scams [24]. In the end, the biggest problem is that people aren't paying attention [25].

3. METHODOLOGY

An Anti-Phishing in Enterprise Environment (Anti-PhiEE) is a comprehensive method for detecting email phishing attempts that use malicious URLs in an enterprise setting. Figure 1 depicts Anti-PhiEE, a model for detecting email phishing attempts. With 25 heuristics that function as multi-layer filters, Anti-Phishing Multi-Filter (APMF) was developed. Figure 2 shows that APMF uses a Social Facet filter, also known as a social human factor scanner, and five other layers to distinguish between real and malicious URLs, as well as to detect both known and undiscovered forms of phishing.

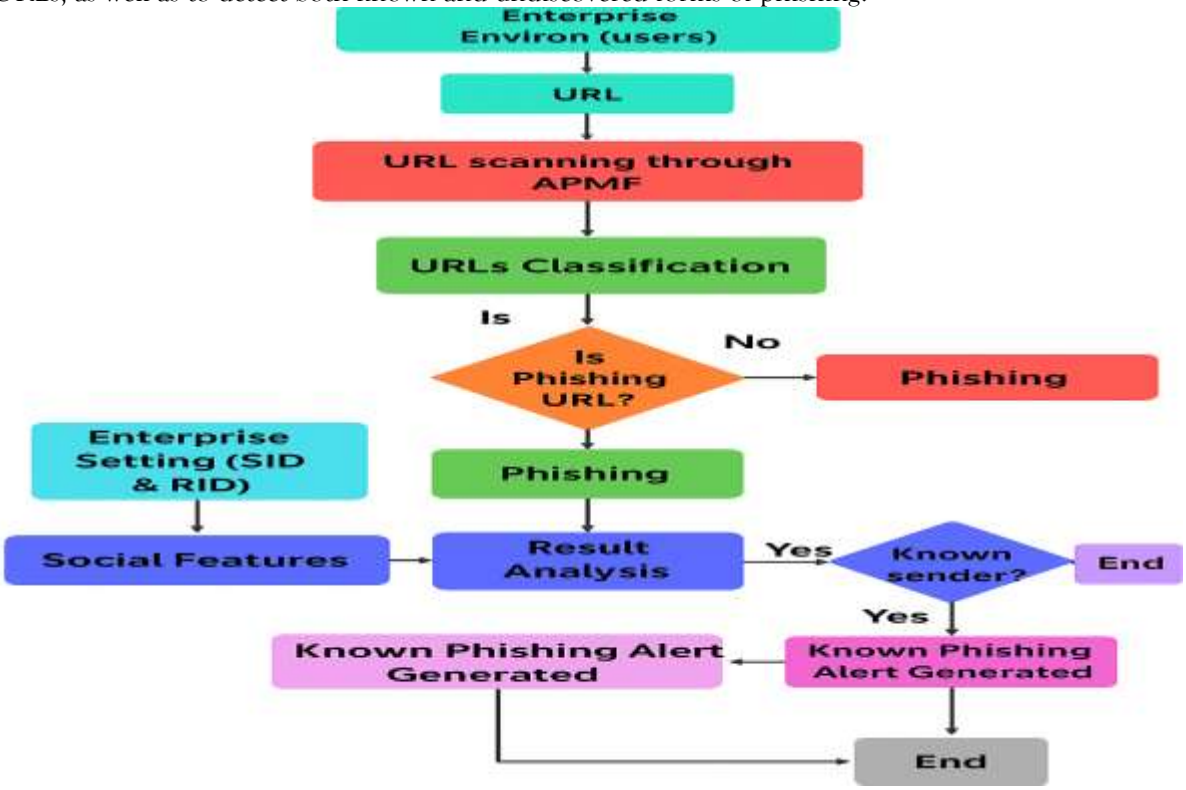

Figure 2. Flow chart of Anti-Phishing Model

The examination of phished and legal URLs/websites, along with statistical investigations, led to the identification of 25 relevant heuristics. This research makes use of the Python neural network toolbox, namely the backpropagation learning technique. This method also makes use of the TRAINLIM algorithm, which stands for Levenberg-Marquardt back-propagation. To classify URLs, we utilise the Feed-Forward Backpropagation and Levenberg-Marquardt Neural Network algorithms. To identify known and unknown phishing attempts, we employ the Social Facet Filter with Mamdani FIS.

3.1 Architecture of Proposed Approach

The Anti-PhiEE (Anti-Phishing in Enterprise Environment) model is a comprehensive framework designed to detect phishing attempts in enterprise email systems. Its dual objective is to first identify whether a given URL is phishing-related using the APMF technique, and then determine whether the phishing attempt originates from a known or unknown source. This is illustrated in Figure 1 and unfolds in three distinct phases:

Phase I: URL Analysis and Classification

Step 1: The process begins with extracting URLs embedded in received emails within the enterprise environment.

Step 2: These URLs are then passed through the Anti-Phishing Multi-Filter (APMF), which screens them to evaluate their legitimacy.

Step 3: For classification, a combination of Artificial Neural Network (ANN) models is employed — specifically, the Feed-Forward Backpropagation Neural Network and the Levenberg-Marquardt Neural Network — to analyze the filtered URLs.

Step 4: The classifier then determines whether each URL is legitimate or indicative of phishing activity.

Step 5: The classification results are systematically stored to serve as input for subsequent analysis in later phases.

Phase II: Sender Identity and Social Feature Analysis

Step 1: This phase focuses on distinguishing between known and unknown phishing sources. It incorporates social facets as inputs — typically imprecise or fuzzy data — which are categorized into four specific social features: X1, X2, X3, and X4 (detailed in Section 4.4.3).

Step 2: These social features are processed through a Social Feature Algorithm, designed to assess the identity of the sender (i.e., whether the sender is familiar to the enterprise environment).

Step 3: The Mamdani Fuzzy Inference System (FIS) is then applied to analyze the input values derived from the social features.

Step 4: The outputs from Phase I (URL classification) and Phase II (sender identity analysis) are combined to produce the final result — a determination of whether the phishing attempt is from a known or unknown source. The system subsequently generates an alert message. Notably, for known phishing cases, the alert's content is customized based on the degree of familiarity between the sender and receiver, using fuzzy linguistic rules to reflect this relationship.

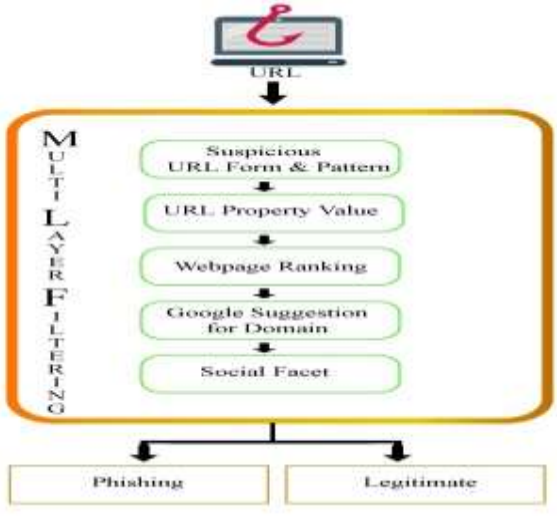

Figure 3. Design of Anti-Phishing Multi-Filter (APMF)

3.2 URL Feature Set

Phishing URLs and websites are distinguished from authentic URLs, webpages, and connections using heuristics. By means of a thorough literature research, statistical investigations, and examination of both valid and phishing websites or URLs, the phishing heuristics are identified based on advanced pertinent risks [26, 27]. As stated below, a total of 25 heuristics are defined here to efficiently distinguish between a legitimate and a phished URL.

Table 1. Suspicious URL Forms or Patterns

Heuristics	Description
IP Address, Hexadecimal or ASCII code in URL	If URL in the form of IP Address, If URL in the form hexadecimal or Unicode.
Abnormal URL	URL- phishing Page Redirection
No. of Sub Domain	Length of sub domain
No of Dot '.' In URL	More than 5 Dots in URL
URL of length	Length of URL
Special Characters	Whether URL has '- ', '@' symbol or '//'
Phishing Keyword	Phishing words as a hyperlink like- verify, click here, submit, login, sign-in etc.
Age of Domain (in Days)	Domain is less than 43 days
Port number matching	Whether explicit port number and protocol port no. are equal.
Number of TLDs	More than one TLD in a URL
Primary Domain Spelling Mistakes	Whether primary domain is
Number of Slash '/'	Number of '/' slash
Login Form	Login Form in Fake webpage

3.3 Suspicious URL Forms or Patterns

The suspicious URL forms, patterns, and symbols are linked to these heuristics. Seldom do characters like "@" and repeatedly occurring "//" show up in a URL. Since trustworthy websites only have one TLD, URLs with multiple TLDs are regarded as phishing sites. Phishing websites are blocked and have a very short lifespan. According to Table.1 [28], a phishing page's fake login form is a warning flag that money or sensitive information may be lost. These heuristics for identifying phishing URLs and websites are based on URL Property Values. The phoney or transient phishing website lacks the necessary characteristics indicated in Table 2.

Table 2. URL Property Values

Heuristics	Description
Country matching	TLD country and domain country-code are equal.
HTTPS protocol	Whether URL use HTTPS or not.
DNS record	Whether URL has DNS record or not.
Reverse DNS look-up	Query of DNS to determine the domain associated with an IP Address.
WHOIS Record	WHOIS record (Domain name, Registration, Expiry details etc.)
Value of TTL	TTL value of domain.
PTR record	Whether domain has PTR record or not.

3.4 Page Ranking

These heuristics are based on page ranking; it is a numerical value calculated by the number of visitors and degree of popularity.

Table 3. Page Ranking

Heuristics	Description
Google page rank (Indexing)	Domain's PageRank value
Alexa rank	Alexa Rank value of domain
Alexa reputation	Alexa reputation value of domain

It is seen that the phishing site has very low page rank value as rarely visited by bulk users and these sites are exist for less time. Therefore, domain page rank value is very low as mentioned in Table 3.

4. RESULTS AND DISCUSSION

The APMF uses legal and phishing URL data collected from 2000 as input to evaluate its performance using machine learning. We employ the ANN techniques of Levenberg-Marquardt Neural Network and Feedforward-BackPropagation. The same dataset is divided into 50% for training and 50% for testing in both ANN approaches. Statistical analysis is performed for validation and ANN applications are implemented using the neural network toolbox of MATLAB version R2016a. Table 5, together with Figure 6 and Figure 7, graphically display the results of this strategy.

Experiments were conducted on two fronts to prove the study's overall efficacy: Both approaches were evaluated based on their R2 and Root Mean Square Error (RMSE) values. Table 5 displays the results of both strategies. It is adapted to use k-fold cross-validation to get the classifier's accuracy with a minimal dataset. The suggested phishing detection approaches are validated using k-fold cross-validation. Ten equal-sized subsets were created from the original 2000 dataset. Training, testing, and validation are all done on this dataset. For both Feed-Forward Back propagation and Levenberg–Meyer, 10-fold cross-validation is used. -Laplacian Neural Network

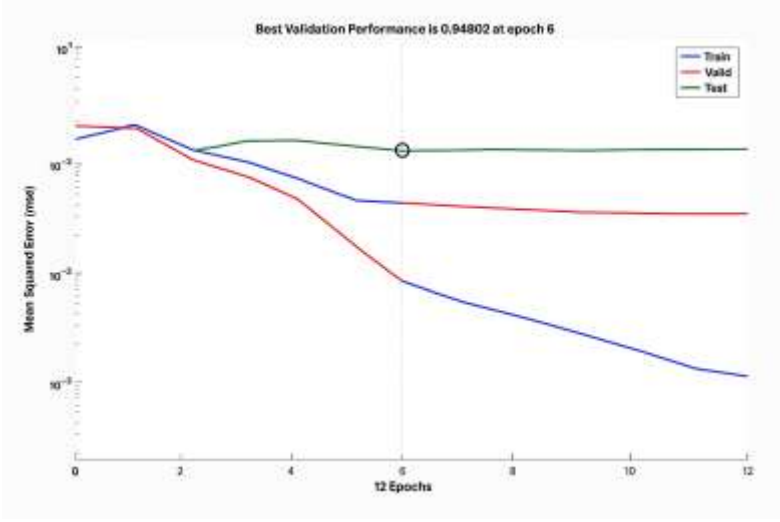

Figure 4. Performance of Feed-Forward Back propagation Neural Network

Table 5. Comparison between FFNN and LM Neural Network

Different NN Architecture	Process	Sample size	RMSE	R2
Feed-Forward Backpropagation	Training Set	1000	0.28	0.92
	Testing Sets (10 set each size 100)	1000	0.42	0.82
	10-Fold Cross Validation	100	0.24	0.94
Levenberg-Marquardt Neural Network	Training Set	1000	0.30	0.91
	Testing Sets (10 set each size 100)	1000	0.55	0.69
	10-Fold Cross Validation	100	0.46	0.78

A set of 256 rules was manually developed to analyse the results of the traditional fuzzy reasoning tools. These tools used four inputs: social media contacts, common contacts, common social media activity, and times of email communication. Each input had four possible responses: low, medium, high, and very high. Figure 5 shows that the known and unknown person output variables are most affected by Social Media Contacts (X1) and social media Common Contacts (X2), according to this method. Figure 6 shows that the output variables are most affected by Common Activity in social media (X3) and social media Common Contacts (X2). Phishing URL detection and Enterprise Environment are the outcome factors that rely on them. This demonstrates that the two most popular social media features, common contact and common activity, are Phishing attacks that leverage social aspects.

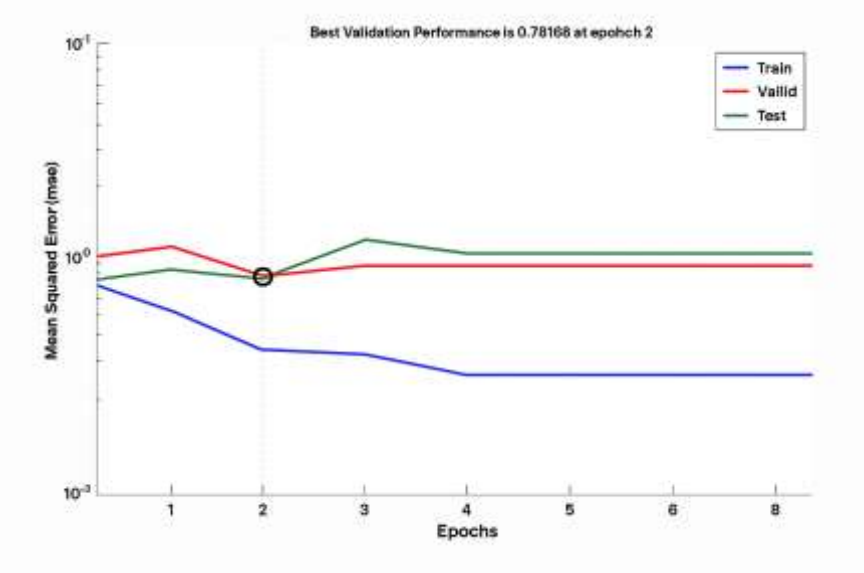

Figure 5. Performance of Levenberg-Marquardt Neural Network

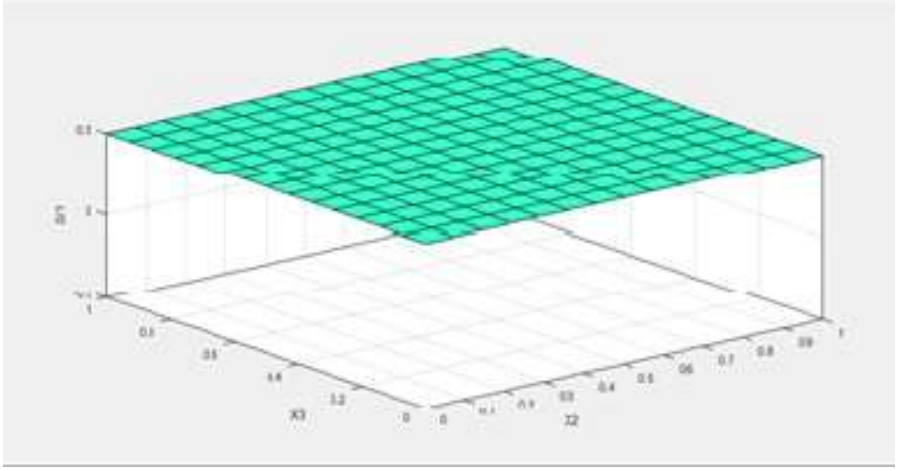

Figure 6. Social media Common Contacts (X2) vs Common Activity in social media (X3)

An FLC consists of a set of rules presented in the form of IF (a set of conditions are satisfied) THEN (a set of consequences can be prepared). Here, antecedent is a condition in its application domain and the consequent is a control action for the system under control. Both the antecedents and consequents of the IF-THEN rules are represented using some linguistic terms. The inputs of fuzzy rule-based systems should be given by fuzzy sets, and therefore, we have to fuzzify the crisp inputs. Moreover, the output of an FLC is always a fuzzy set, and therefore, to get the corresponding crisp value, a method of defuzzification is to be used.

5. CONCLUSION

A devastating enterprise risk, phishing depends on the dispersed decision-making of enterprise employees. The amount to which an organisation responds to and recovers from phishing attempts is one example of how enterprise environment security risk is affected. Enterprise personnel and employees are the most attractive targets for phishers in this area. Employees' actions online reveal their level of expertise, which is why phishers often succeed in luring their victims away from a systematic assessment of rationality. Phishers avoid using logical reasoning and instead plan successful deceptions regarding employees' consent to use peripheral routes. Also, the con artists' use of familiar contextual signals, such as fear, lust, greed, pity, anxiety, and urgency, as well as splanchnic emotions, is crucial in convincing or dissuading the worker to fall for their traps. Using two distinct ANN methods—FBNN and LM neural networks—and training and evaluating the dataset, this research proposes a unique anti-phish model and implements it in two stages. The first part involves measuring the model's performance. When comparing FBNN with LM neural networks, the results reveal that FBNN has better RMSE and R2 values. When compared to the alternative method, the Feed-Forward Backpropagation strategy produced superior outcomes. This could occur because the neural network's training weights were optimal for each processing element. In the second stage, business environments use Mamdani FIS with four social traits to identify known and unknown e-mail senders: social media contacts, common contacts, common activity in social media, and email communication frequency. Lastly, the approach to determine if the sender of a phishing email is known or unknown takes into account both phases' outputs. Using this method, we find that phishing attacks are most affected by social media contacts (X1) and common contacts (X2), while common activity in social media (X3) and common contacts (X2) have the greatest impact on other input variables. Phishing URL detection and Enterprise Environment are the outcome factors that rely on them. This demonstrates that the two most popular social media features, common contact and common activity, are social aspects that initiate email phishing attacks.

REFERENCES

1. Alluqmani, K., Karrar, A. E., Alhaidari, M., Alharbi, R., & Alharbi, S. (2025). Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review. *International Journal*, *14*(3).
2. Blancaflor, E., Deldacan, L. F., Hunat, S., Rivera, B. M., & Liberato, E. K. (2024, September). AI-Driven Phishing Detection: Combating Cyber Threats Through Homoglyph Recognition and User Awareness. In Proceedings of the 2024 The 6th World Symposium on Software Engineering (WSSE) (pp. 226-231).
3. Thayyaba Khatoon Mohammad, Puranam Revanth Kumar, Gifta Jerith, and E. Krishnaveni Reddy, "Multimodal Language Models for End-to-End Automated Speech Recognition Using Bidirectional Recurrent Neural Network", 14th International Advanced Computing Conference, pp. 33 – 47, 2025.
4. Sakthipriya, N., Govindasamy, V., & Akila, V. (2024). Security-aware IoT botnet attack detection framework using dilated and cascaded deep learning mechanism with conditional adversarial autoencoder-based features. Peer-to-Peer Networking and Applications, 17(3), 1467-1485.
5. Mudgerikar, A., & Bertino, E. (2023, July). Intelligent security aware routing: Using model-free reinforcement learning. In 2023 32nd International Conference on Computer Communications and Networks (ICCCN) (pp. 1-10). IEEE.
6. Kishor, K., Agrawal, K. K., Yadav, S. P., Thakur, H. K., & Naruka, M. S. (2024). SPAM: An Enhanced Performance of Security and Privacy-Aware Model over Split Learning in Consumer Electronics. Programming and Computer Software, 50(8), 875-899.
7. Soveizi, N., & Turkmen, F. (2023, October). SecFlow: Adaptive Security-Aware Workflow Management System in Multi-cloud Environments. In International Conference on Enterprise Design, Operations, and Computing (pp. 281-297). Cham: Springer Nature Switzerland.
8. Thayyaba Khatoon Mohammed, D N Vasundhara, Syeda Husna Mehanoor, E. Sreedevi, Puranam Revanth Kumar, CH Manihass, Shaik Fareed Baba "A Novel Fusion Approach for Advancement in Crime Prediction and Forecasting using Hybridization of ARIMA and Recurrent Neural Networks", Journal of Information Systems Engineering and Management, Vol. 10, Issue 38, pp. 404-420, 2025.
9. B Shilpa, Puranam Revanth Kumar, and Rajesh Kumar Jha, "LoRa DL: a deep learning model for enhancing the data transmission over LoRa using autoencoder", The Journal of Supercomputing, vol. 79, pp. 17079 –17097, 2023.
10. Damerau, F. J. (1964). A technique for computer detection and correction of spelling errors. Communications of the ACM, 7(3), 171–176.
11. Roop Ranjan, Dilkeshwar Pandey, Ashok Kumar Rai, Deepak Gupta, Pawan Singh, Puranam Revanth Kumar, and Sachi Nandan Mohanty, "A Manifold-Level Hybrid Deep Learning Approach for Sentiment Classification Using an Autoregressive Model", Applied Sciences, vol. 13, no. 5, p.3091, 2023.
12. Firake, S. M., Soni, P., & Meshram, B. (2011). Tool for Prevention and Detection of Phishing E-Mail Attacks. International Conference on Network Security and Applications, 78–88.

13. Gansterer, W. N., & Pölz, D. (2009). E-mail classification for phishing defense. European Conference on Information Retrieval, 449–460.
14. N. Arivazhagan, K. Somasundaram, Gouse Baig Mohammad, Puranam Revanth Kumar et al., "Cloud-Internet of Health Things (IOHT) Task Scheduling Using Hybrid Moth Flame Optimization with Deep Neural Network Algorithm for E Healthcare Systems", Scientific Programming, Volume 2022, Article ID 4100352, pp. 1-12, 2022
15. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. Neural Computing and Applications, 28(12), 3629–3654.
16. Herzberg, A. (2009). DNS-based email sender authentication mechanisms: A critical review. Computers & Security, 28(8), 731–742.
17. Gouse Baig Mohammad, Shitharth, and Puranam Revanth Kumar, "Integrated Machine Learning Model for an URL Phishing Detection", International Journal of Grid and Distributed Computing, vol. 14, Issue 1, pp: 513-529, 2021.
18. Puranam Revanth Kumar, and T Ananthan "Machine Vision using LabVIEW for Label Inspection", Journal of Innovation in Computer Science and Engineering (JICSE), Vol.9, Issue 1, pp: 58 - 62, 2019.
19. Kaivanto, K. (2014). The effect of decentralized behavioral decision making on system-level risk. Risk Analysis, 34(12), 2121–2142.
20. Puranam Revanth Kumar "Wireless Mobile Charger using Inductive coupling", Journal of Emerging Technologies and Innovative Research (JETIR), Vol.5, Issue 10, pp: 40-44, 2018.
21. Puranam Revanth Kumar, Thayyaba Khatoon Mohammad, Aylapogu Pramod Kumar, Ruslan Kassym, Tolegenova A. S, and Tlenshieva Akmaral, "Synthesizing Multi-Modal Imaging for Enhanced Brain Mapping in Neurology: A State-of-the-art Review", 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), pp. 1-6, 2025.
22. A. Pramod Kumar, D. M. Sudan, P. V. Sai Charisma, N. Agarwal and Puranam Revanth Kumar, "A Novel Antenna Design and Analysis for 5G mm Wave Broadband Systems," 21st India Council International Conference (INDICON), Kharagpur, India, 2025, pp. 1-4.
23. A. Pramod Kumar, Puranam Revanth Kumar and N. Agarwal, "Design and Implementation of Partially Static High Frequency DFF for Low Power Applications", 3rd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC), pp. 1-4, 2024.
24. B Shilpa, Puranam Revanth Kumar, Rajesh Kumar Jha, "Spreading Factor Optimization for Interference Mitigation in Dense Indoor LoRa Networks", IEEE IAS Global Conference on Emerging Technologies (GlobConET), pp. 1-5, 2023.
25. H. Siriwardana, Kamakhya Narain Singh, Puranam Revanth Kumar, Chinmay Misra, "Automated Road Crossing System Using Real-Time Object Tracking", 10th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), pp. 1-5, 2022.
26. Puranam Revanth Kumar "Position Control of a Stepper Motor using LabVIEW" 3rd International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), pp. 1551 - 1554, 2018.
27. Mamdani, E., & Assilian, S. (1999). An experiment in linguistic synthesis with a fuzzy logic controller. International Journal of Human-Computer Studies, 51(2), 135–147.
28. Puranam Revanth Kumar and B. Shilpa, "An IoT-Based Smart Healthcare System with Edge Intelligence Computing", Reconnoitering the Landscape of Edge Intelligence in Healthcare, CRC Press, pp. 31-46, 2024.