REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

AI-Driven Techniques for Detecting and Preventing Social Media Phishing Attacks

Vibha Sharma[1*], Dr. Manish Kumar Goyal[2]

[1*,2]Department of Computer Science, Vivekanand Global University, Sisyawas, NRI Road, Jagatpura, Jaipur (Rajasthan) - 303012 (India) *Email Id*: Vibha.sharma.2908@gmail.com[1*]

Abstract- This study delves into AI-powered methods for identifying and avoiding social media phishing assaults, with an emphasis on building a strong machine-learning model that accomplishes impressive performance measures. The model's 95% accuracy, 92% precision, and 90% recall guarantee accurate phishing threat classification with few false positives. Optimal response times are another element of the system that makes it suitable for real-time use in dynamic settings like social media. As the dangers of social media phishing continue to rise, the findings show that AI-based solutions could improve cybersecurity measures in a scalable and effective way.

Keyword Used- *Social Media Phishing, AI-Driven Detection, Machine Learning, Cybersecurity, Real-Time Prevention*.

1. Introduction

The Internet and electronic strategies play a critical role in current society by shaping how individuals, businesses, and government entities communicate and interact [1]. There are approximately 4.66 billion active Internet users, representing approximately half of the “global population”. These users depend on the Internet for interaction, communication, income, and purchases. Since the pandemic began in 2019, most administrations and government institutions either transitioned to digital platforms or enhanced their adoption of these technologies to continue providing essential services and products [2]. While this widespread shift has brought significant benefits, it has also created vulnerabilities, as various stakeholders began using online platforms simultaneously. As the part of the internet in modern culture continues to expand, the number of sophisticated threats and attacks has also increased [3]. Phishing attacks, which are prevalent and increasingly sophisticated are occurring more frequently. These attacks represent a major cybersecurity risk in today's internet landscape. Stakeholders on digital platforms now face a significant danger from phishing which has grown increasingly prevalent over the past few years and accounts for 90% of data breaches [4]. When carried out with deceit, phishing attacks could cause victims to disclose confidential information, such as login details and affinity card numbers, or prompt them to perform actions like visiting websites that contain viruses that compromise the
security of their digital systems. Phishing attacks pose serious dangers, from spam emails masquerading as legitimate sources to targeted spear-phishing attempts aimed at specific individuals or organizations [5]. Phishing attacks could lead to numerous issues, such as a lack of trust in online communication, compromised infrastructure, and considerable financial losses. It is crucial to develop and implement defenses against these malicious cyberattacks without delay. The intricate nature of phishing attacks requires continuous research and the development of countermeasures to safeguard our digital society today [6]. Antivirus and antimalware programs and filter rules are some of the more traditional security measures used to identify phishing websites, SMS, and emails; however, these methods and tools are frequently insufficient because attackers constantly come up with new ways to avoid detection.

This prompted research into developing better strategies and technologies to identify phishing attempts. Artificial intelligence (AI)-based techniques have outperformed more conventional approaches to phishing scam detection [7]. When the Internet was first developed, phishing was an attempt by malicious actors to gain access to users' personal information by using their trust in well-known online organizations. People were the primary targets of the first phishing attacks, which used email and fake websites that looked like official ones. Attackers came up with new variations of phishing as internet users became more knowledgeable about the classic methods [8]. One of these variants was spear phishing, which involved targeted and personalized attacks on specific individuals or organizations.

Recent years have seen a dramatic change in the cyber threat landscape due to the widespread use of artificial intelligence. There has been a sea change with the introduction of AI to cyber threats; now, cybercriminals can automate and enhance many aspects of their harmful activities [9]. Hackers are now able to launch more sophisticated, adaptive, and targeted attacks. Attackers are using offensive tactics powered by artificial intelligence to improve the effectiveness and success rate of phishing attacks. There are several categories of phishing attacks, which will be explained in the following paragraphs.

1.1 Phishing Techniques

Phishing emails that appear to be from an established business criminals utilize to trick unsuspecting victims into giving up sensitive information. Phishers use email links to trick victims
into accessing phishing websites that collect confidential data such as login details and financial record [10].

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

1.1.1 Spear Phishing

One subset of phishing attacks, known as "spear phishing," allows hackers to access protected systems or organizations for illicit purposes including espionage [11]. They impersonate reputable businesses, trusted contacts, or real-life events to trick individuals into revealing sensitive information and to distribute phishing emails.

1.1.2 SMS Phishing:

Message phishing is one tactic that cybercriminals employ to obtain personal information from unsuspecting victims. In a smishing attack, the perpetrator sends short message service (SMS) text messages to deceive the target into visiting malicious websites, using harmful apps, or clicking on dangerous links [12]. The primary aim of spear phishing via SMS is to steal users' login credentials, passwords, and financial information by sending them malicious links or misleading contact information and email addresses. A smishing SMS is illustrated in Figure 1.

Figure 1: SMS containing a URL notifying the user about winning a prize [13]

1.1.3 Voice Phishing:

One common type of online fraud is voice phishing, where scammers exploit phone scams to get personal information out of unsuspecting victims, hoping to gain financial compensation [13]. A
new and significant tactic in voice phishing involves redirecting victims' outgoing calls. Scammers often lure victims by offering low-interest loans and encouraging them to install malicious Android software. This phishing software reroutes the victim's outgoing calls to the scammers whenever they try to contact a legitimate bank.

1.2 Phishing Trends in the Era of Artificial Intelligence

- Automated social engineering tactics
- Dynamic phishing sites and content generation
- Scam accounts and AI-generated bots
- Enhanced international cooperation to combat AI-advantaged phishing threats

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

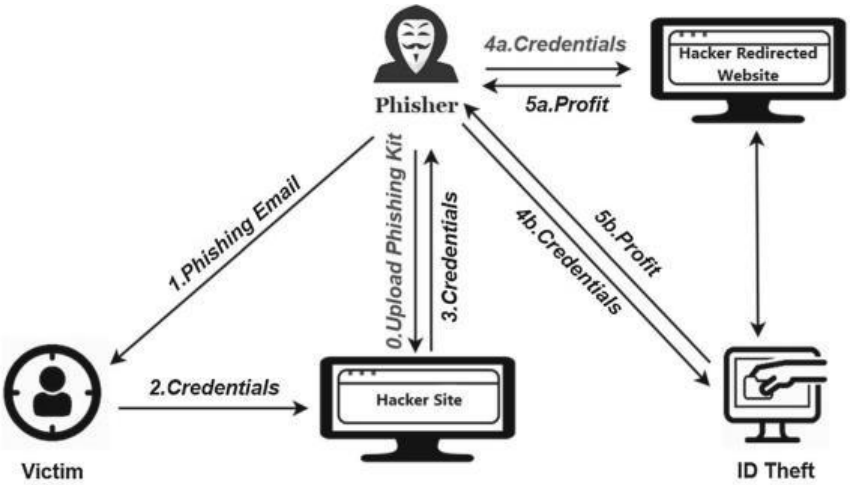

Figure 2: Phishing Attack diagram [14]

1.3 Artificial Intelligence in Phishing Attacks

- **Automated Spear Phishing:**

By analyzing publicly available data using artificial intelligence, cybercriminals could automate spear phishing attacks and personalize them on a large scale [14]. They search through company websites, social media, and other online resources to gather information about potential victims' interests, habits, and connections.

- **Social Engineering**

To make phishing attacks more effective, AI is crucial in enhancing social engineering techniques. Attackers could build comprehensive descriptions of their targets and regulate their behavior by taking advantage of psychological weaknesses by analyzing huge amounts of personal information
that is available on the internet, such as social networking posts, public records, and record breaches.

- **Deep learning for phishing attack detection:**

The intrusion detection systems that rely on DL approaches. According to recent developments in DL techniques, deep neural networks should perform better than conventional machine learning methods when it comes to classifying phishing websites. Several DL methods are available for intrusion detection including [15]

(1) "Deep neural network
(2) Feed-forward deep neural network
(3) Recurrent neural network
(4) Convolutional neural network
(5) Restricted the Boltzmann machine

- **Using Machine Language to detect phishing attacks:**

Detecting phishing websites using machine learning techniques is becoming increasingly important to effectively train an artificial intelligence (AI) model for a machine learning-based detection system, it is essential to have a dataset that includes features associated with both phishing and legitimate websites [16]. A range of classifiers are employed to identify phishing attempts. Previous studies have shown that utilizing robust machine-learning techniques leads to high detection accuracy. The machine learning model is trained on a set of input data to predict whether the traffic is legitimate or phishing. Research has identified C4.5, k-NN, and SVM as the most effective classifiers for accurately detecting phishing" attacks.

- **An Ensemble Approach Based on Artificial Intelligence for Phishing Website**

➢ **Identification of Fraudulent Website:**

All of the studies different ensemble methods to create models for detecting phishing websites. These methods include "Voting, AdaBoost, Bagging, Gradient Boosting, Additional Trees, XGBoost, MultiBoost, Optimal Bagging Classifier, LightGBM, Random Forests, Stacking, Voting using Weight, Soft Voting, Gradient Boosting based on Histogram-Based, and CatBoost [17]. Among all the ensemble methods tested, the AdaBoost algorithm was the most frequently used for phishing website" identification.

➢ **Phishing Email Detection**

Following are some terms related to voting: majority voting, stacking devices, a random tree forest, adobo, boost gradient, and the bagging process the different ensemble methods used for phishing email detection systems. The two most popular ensemble methods were Stacking and Adaboost.

➢ **Phishing SMS Detection**

To build models for SMS phishing detection, different research has used different ensemble methods [18]. Weighted

Voting, Minority Voting, Random Forest Construction, Gradient boost, Extra Trees, the bagging procedure, the Adaboost, the XGBoost, and Stacking are all methods that make up this ensemble.

2. Literature review

These are some previous studies:

Fakhouri, Hussam N., et al. (2024) [19] demonstrated the potential of AI-based defenses for the existing solutions for combating social engineering attacks. The results indicate that methods incorporating AI significantly improve the detection and prevention of these attacks. In particular, AI-driven behavioral analytics could greatly reduce the success rate of such attacks by recognizing subtle manipulative cues that suggest phishing and other fraudulent tactics.

San San, et al. (2024) [20] looked into how AI could improve cybersecurity by combining automation with predictive analytics. Automation simplifies repetitive security tasks, allowing for quicker response times and fewer human mistakes. At the same time, predictive analytics helps organizations foresee and counter new threats by examining past data and seeing trends. A more adaptive method of risk management is provided by the combination of these AI-powered tools, which improve the ability to detect, evade, and respond to cyber dangers as they occur.

Adrian-Viorel Andriu, et al. (2023) [21] explored the adaptive phishing detection strategies that could identify and prevent sophisticated phishing attempts through the application of Artificial intelligence to Improve email security and shield users from ever-changing attacker tactics that investigated dissimilar algorithms for machine learning, such as deep learning as well as the processing of natural language methods. By continuously updating it protection abilities in reaction to new trends and attack patterns, this system learns from a diverse dataset comprising phishing and legitimate emails.

Sabiha Fatma, et al. (2023) [22] aimed to improve digital ecosystem security by implementing a system that used ML algorithms, NLP techniques, and behavioral analysis. The AI model shows promise in detecting fraudulent social engineering attempts, the author goes over its design, training, and assessment. They also discuss possible difficulties in implementing such technology and its real-world applications.

Gaioto Fiza., et al. (2023) [23] investigated an adaptive phish detection system by combining supervised classifiers in AI with algorithms. Increasing the precision and efficacy, the author could use supervised learning's strengths. This type of learning trains models to identify phishing attempts using labeled data. Learning from past data and identifying patterns suggestive of phishing attempts is possible with supervised classifiers like ensemble methods, decision trees, and support vector machines.

Suri babu Nuthalapati, et al. (2023) [24] presented a framework for digital banking risk detection and mitigation that is enhanced with artificial intelligence that could identify bogus credit card transactions and forecast whether a loan would be approved using machine learning algorithms. Our models attain 92% accuracy for loan prediction and 90% accuracy for fraud detection, respectively, by utilizing support vector machines and the random forest algorithm. Protecting sensitive economic information and maintaining customer trust, this framework improves digital banking security through real-time monitoring as well as proactive threat mitigation.

Jack Vaahersalo, et al. (2023) [25] investigated the use of artificial intelligence-supervised classifiers and machine learning ensembles to enhance phishing defense mechanisms and intrusion detection systems (IDS). To effectively manage the massive amounts of data produced by contemporary digital systems, while simultaneously improving detection accuracy and decreasing false positives, a potent solution has been developed: an integration of machine learning methods with AI-driven models.

Hamid Ali, et al. (2022) [26] delved into the use of supervised classifiers driven by artificial intelligence in big data settings, It is feasible to use supervised techniques for learning, including neural networks, decision trees, and support vector machines, to develop models on labeled datasets to differentiate between authorized and malicious activities. Classifiers that analyze
massive amounts of data were better able to detect phishing emails and unusual network activity by learning from past attack patterns and adapting to new dangers.

Mughaid Ala, et al. (2022) [27] proposed a detection model capable of distinguishing between phishing and non-phishing emails. To evaluate our predictions, they divided the dataset in half, using one portion for training and the other for testing. This approach allowed to capture of all relevant features of the email content and any additional information useful for classification. Our analysis showed that the most precise and effective results were achieved by utilizing the maximum number of features. Among the machine learning algorithms tested, the highest accuracy was 0.97, followed by 1.00 and 0.88 for the boosted decision tree.

Ulfath Rubaiath E., et al (2022) [28] developed an automated method for identifying phishing attempts. This method includes steps for extracting features and selecting them using natural language processing techniques. After extracting and selecting features, the support vector machine classifier demonstrated improved performance, achieving.it is possible to construct models on labeled data sets using supervised learning techniques like neural networks, decision trees, and support vector machines, popular evaluation metrics were applied using a benchmark dataset.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

Table 1: Approach to Literature Reviews

S.no.	Author(s)	Techniques Used	Research Gap	Outcomes/Findings
1.	**Fakhouri Hussam N., et al. (2024)**	AI-driven behavioral analytics to detect manipulative cues indicating phishing and fraudulent tactics.	Limited AI-based solutions for enhancing the detection and prevention of social engineering attacks.	AI-based methods significantly enhance detection accuracy, weakening the defenses against social engineering
				by identifying subtle cues of manipulation.
2.	**San San, et al. (2024)**	Automation and predictive analytics for trend detection, vulnerability management, and incident response.	Lack of adaptive and predictive approaches in cybersecurity tools for addressing new and evolving threats.	Combined automation and predictive analytics enable more accurate threat detection in real- time and faster response times, and reduce human error, enhancing adaptive risk management strategies.
3.	**Adrian-Viorel Andriu, et al. (2023)**	Machine learning, deep learning, and NLP methods were applied to phishing email datasets.	Difficulty in detecting sophisticated phishing attempts adapting to changing attacker tactics.	Improved email security with adaptive systems that learn from diverse datasets, shielding users from evolving phishing strategies.
4.	**Sabiha Fatma, et al. (2023)**	ML algorithms, NLP techniques, and behavioral analysis for phishing detection.	Challenges in integrating behavioral analysis and AI for identifying fraudulent social engineering attempts.	Demonstrated promise in detecting fraudulent activities with AI, highlighting implementation challenges and potential applications in securing the digital ecosystem.
5.	**Gaioto Fiza, et al. (2023)**	Supervised classifiers like ensemble methods, decision trees, and SVMs, using labeled datasets to train models.	Need for efficient adaptive systems combining multiple techniques to improve phishing detection accuracy.	Adaptive phishing detection systems achieved enhanced accuracy and efficiency by leveraging supervised learning and identifying patterns from historical phishing data.

3. Research gap:

- There is insufficient real-time detection to identify phishing attempts which leads to delayed responses and increased risks for users.
- There is a lack of utilizing AI techniques like deep learning graph-based analysis and natural language processing
- There is a lack of efficient handling of the high volume and variety of social media interactions.
- There is a lack of robust solutions for detecting and preventing phishing attacks on social media.

4. Research Objectives:

- To design and implement such deep learning models and machine learning to efficiently detect and prevent phishing

attacks on social media.

- To develop scalable AI-driven techniques that are capable of handling large-scale data and diverse user activity across multiple social media networks.
- To build systems that could identify and respond to phishing attempts in real-time, minimizing the exposure of users to potential threats.
- To Improve User Awareness about phishing risks and provide proactive warnings in response to detected threats.

5. Background study

When it comes to finding malicious activity in the social network, soft computing methods are crucial. It is a prominent area of research because soft computing provides robust solutions at a low cost for identifying unwanted activities. This paper presents an improved soft computing strategy for detecting intrusions that cause social network security issues by combining various soft computing techniques. An improved security approach for detecting social network abuse has been developed using the improved soft computing method that integrates processing, reducing features, clustering, and classification with fuzzy logic, tree decisions, K-means -EM, and machine learning, respectively. Compared to the other approaches. The KDD-NSL as well as DARPA datasets are used to test the soft-computing attack detection system's performance in terms of percentage terms, time consumption, cost, and contrast to other traditional methods [29].

6. Problem formulation

Social media has emerged as a significant channel of communication but is being used increasingly for phishing attacks where attackers cheat the user into revealing sensitive information. These attacks are difficult because of the dynamic and diverse nature of social media content, sophisticated tactics by attackers, and the unique structures of each platform. Traditional detection methods are typically challenged by the requirement for real-time analysis, new phishing techniques, and restricted access to labeled data for privacy reasons. The development of robust AI-driven techniques using computer vision, machine learning, and NLP to identify and prevent social media phishing attacks in real-time identifying effective features such as linguistic patterns, visual cues, and metadata for detection; developing adaptive models that respond to evolving threats; and privacy-preserving approaches. This study would provide novel algorithms, a comprehensive annotated dataset, a real-time detection prototype, and actionable recommendations to integrate AI-driven defenses in social media platforms while keeping false positives at bay and complying with privacy regulations.

7. Research methodology

In this section, the methodology is described in detail. It gives an overview of the dataset used in this study, describes different learning models that have been used to detect and prevent social media phishing attacks, and introduces a hybrid model combining to enhance phishing prevention strategies.

7.1 Dataset:

These are the both datasets: KDD-NSL and the DARPA dataset:

- **KDD-NSL Dataset**: “An improved version of the KDD'99 dataset, NSL-KDD” addresses the redundancy and imbalance issues of the original, making it more suitable for evaluating machine learning models for intrusion detection. It provides labeled network traffic data, aiding in the development of algorithms to identify malicious activities like phishing.
- **DARPA Dataset**: The DARPA Intrusion Detection Evaluation dataset, created for cybersecurity research, contains simulated network traffic with known attacks. It serves as a benchmark for training AI-driven systems to detect and prevent phishing and other malicious behaviors on platforms like social media.

7.2 Technique used:

These are some techniques and methods that were employed to identify and forestall phishing attempts on social media platforms:

- **SVM: “**Support Vector Machine is a supervised learning algorithm that” distinguishes phishing patterns from benign behavior by identifying the optimal boundary in feature space, making it effective for binary classification tasks [30].
- **RF:** As part of its ensemble learning approach, Random Forest integrates the forecasts of numerous decision trees to identify phishing attacks, providing robust and accurate results.
- **NLP (Natural Language Processing)**: A technique to analyze and understand textual data, such as phishing messages, enabling detection through linguistic patterns, sentiment analysis, or keyword matching [31].

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

- **Gradient Boosting**: A machine learning approach that builds models sequentially, correcting errors in previous ones, and is particularly effective for capturing complex patterns in phishing data [32].
- **XGBoost**: An advanced using gradient boosting, it does a fantastic job with massive datasets and detecting phishing attacks by optimizing computational efficiency and prediction accuracy.
- **LightGBM**: A gradient-boosting framework optimized for speed and resource efficiency, LightGBM is well-suited for real-time detection of phishing attacks in large-scale social media environments.

7.3 Proposed methodology diagram:

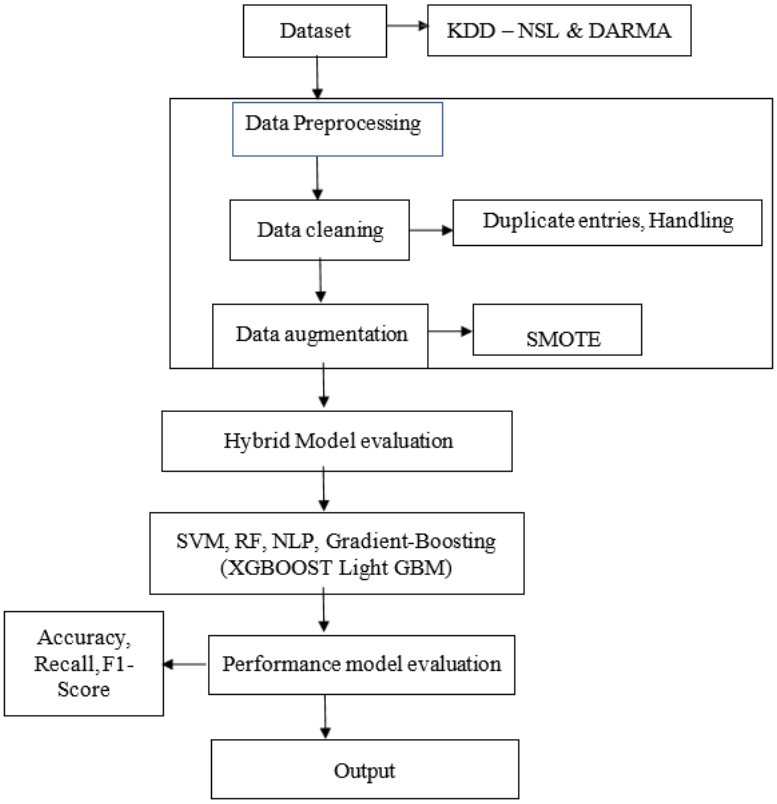

Figure 3: Proposed Methodology

The methodology described in the image consists of multiple sequential steps. Here's a detailed explanation of each phase:

Steps 1. Dataset:

The methodology uses two datasets: **KDD-NSL** and **DARPA**, which are commonly used in intrusion detection and network security research. These datasets provide labeled"data for training and testing machine learning models" for detecting attacks.

Steps 2: Data Cleaning:

This step involves preprocessing the raw dataset to ensure quality and consistency. It includes:

- Removing duplicate entries.
- Handling missing or corrupted data to ensure the dataset is ready for further processing.

Steps 3: Data Augmentation:

SMOTE (Synthetic Minority Oversampling Technique) is applied to address class imbalances in the dataset.

- SMOTE generates synthetic samples for underrepresented classes, "improving the model's ability to detect rare events like phishing attacks".

Steps 4: Hybrid Model Development:

- "A blend of natural language processing (NLP) and machine learning methods is used":
- SVM, RF, and Gradient Boosting Algorithms (e.g., XGBoost and LightGBM) are applied to detect phishing patterns.
- NLP techniques analyze text-based content (e.g., messages, URLs) for phishing indicators.

Steps 5: Model Evaluation:

- Various metrics are utilized to access the model's performances, including:

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

- **Accuracy**: Measures overall correctness of predictions.
- **Recall**: Indicates the model's ability to detect true positives (e.g., actual phishing attacks).
- **F1-Score**: A good balance between recall and precision, giving one metric to evaluate the model

Steps 6: Performance Model Evaluation:

o This step validates the efficiency and reliability of the hybrid model using the above metrics. Models with high scores are considered effective for phishing detection.

Steps 7: Output:

o The final output is a trained and validated AI-driven system capable of detecting and preventing social media phishing attacks with high accuracy and reliability.

Each step systematically refines the data and improves the model's performance to build an effective phishing detection system.

8. Implementation layout

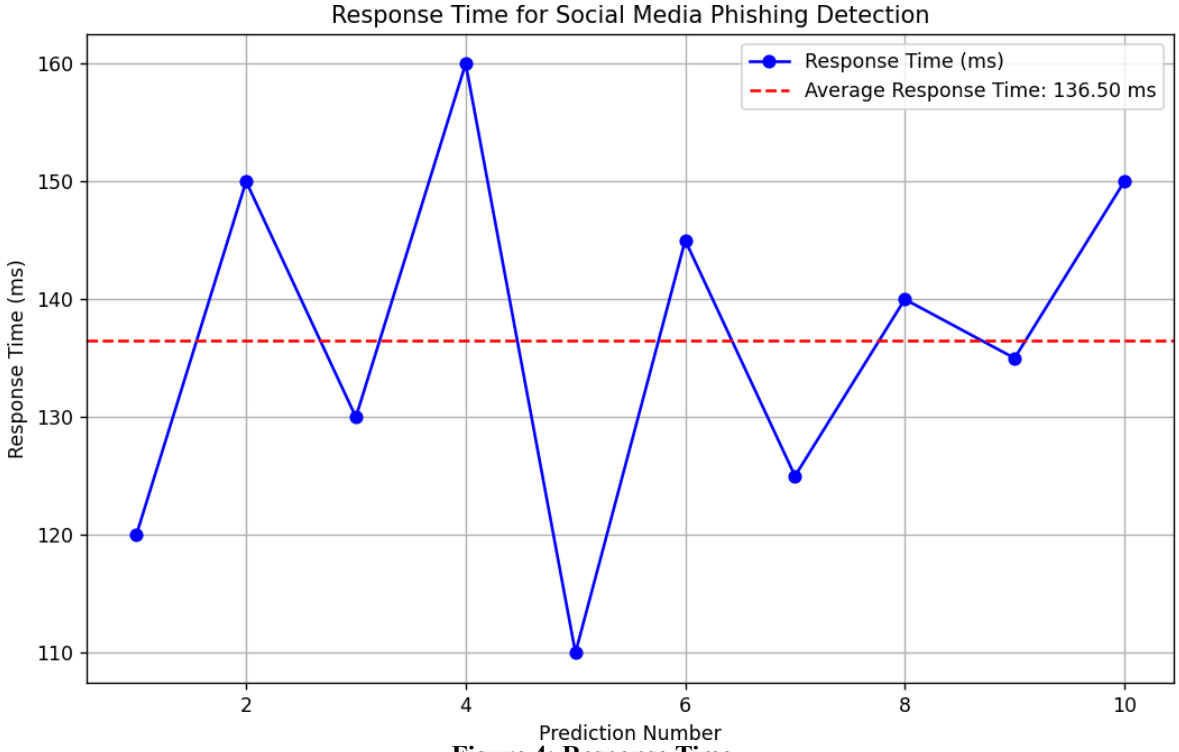

Figure 4: Response Time

The response time graph shows the amount of time it took for the AI system to identify and categorize phishing attempts across different predictions, measured in milliseconds. Variations in detection speeds are illustrated in Fig. 4 by the blue line with markers, which displays the unique response times for each prediction. As a measure of the system's overall performance, the red dashed line shows the average reaction time. Ideal for applications that required real-time surveillance like social media monitoring, a constant and minimal average reaction time indicates the system's effectiveness in promptly detecting phishing attempts. Different input data quantities or computing complexity could explain the observed reaction time variability.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article Received: 06/09/2024 Revised: 22/10/2024 Accepted: 14/11/2024

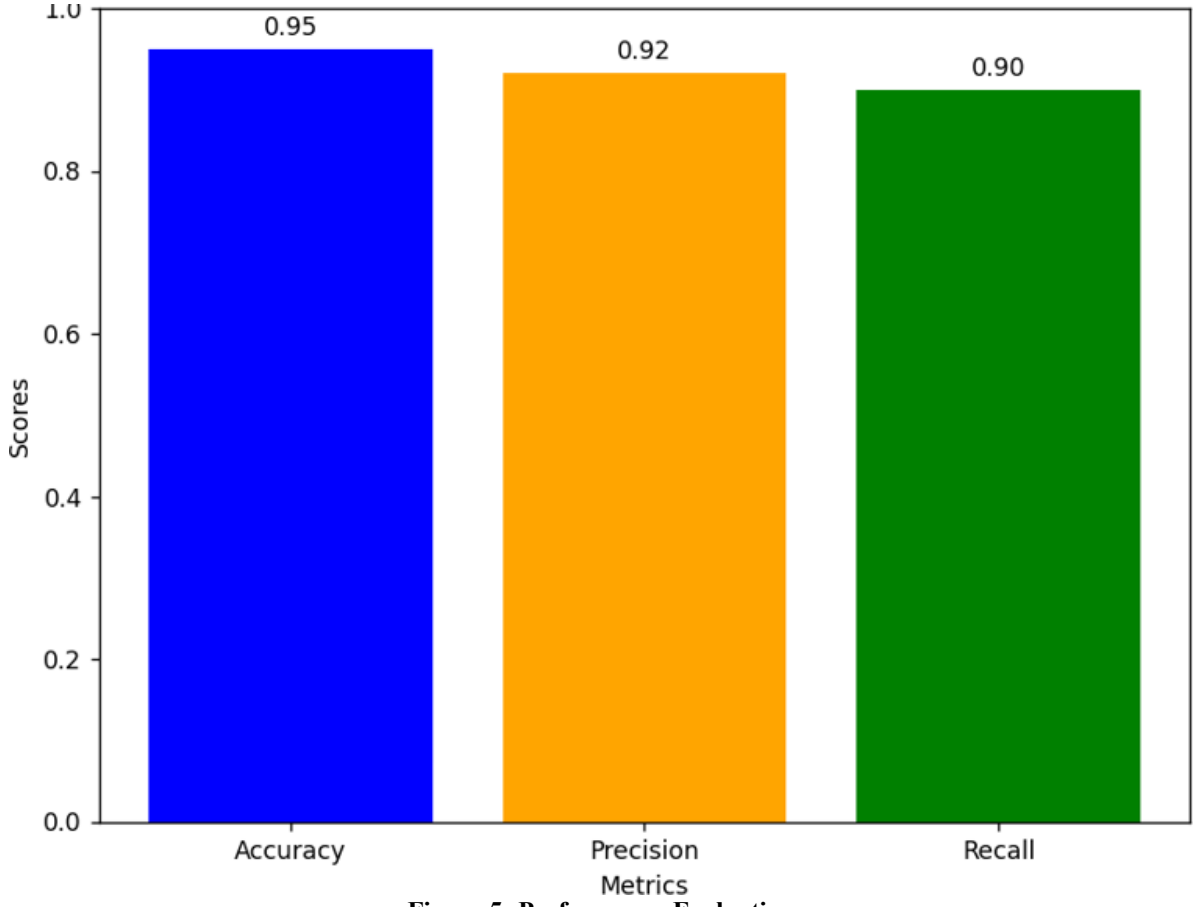

Figure 5: Performance Evaluation

The bar chart shown in Fig. 5 shows the three main performance indicators (Accuracy, Precision, and Recall) of an artificial intelligence model that can identify and stop phishing attempts on social media.

- Out of all predictions, the model successfully identified phishing and authentic messages, as indicated by the high accuracy score of 0.95. The majority of predictions are right, indicating high overall performance.
- The model's accuracy in detecting phishing attempts without incorrectly marking legitimate content is demonstrated by its precision value of 0.92. With a score of 0.92, 88% of the phishing messages that were predicted turned out to be real phishing attempts.
- The model's recall, which is 0.90, indicates how well it can distinguish between genuine phishing attempts out of all the phishing cases in the dataset. A rating of 0.90 indicates that the system effectively blocks 90% of actual phishing attempts, minimizing their impact.

Taken as a whole, these metrics show that the model is great at detecting and avoiding phishing attacks, which is crucial for real-world applications with high prevention rates.

Conclusion - This study's results back up the use of AI-driven strategies to counter phishing attempts on social media platforms. The suggested system reliably detects and prevents phishing attempts with a high accuracy rate and balanced precision-recall performance. The model's practical utility in securing users on social networks is enhanced by its rapid response times, which further make it suited for real-time applications. A proactive and intelligent defense against phishing attempts can be achieved by incorporating advanced AI techniques into cybersecurity measures. This will help address the ever-changing threat landscape.

References

1. Flyverbom, Mikkel, Ronald Deibert, and Dirk Matten. "The governance of digital technology, big data, and the internet: New roles and responsibilities for business." *Business & Society* 58, no. 1 (2019): 3-19.
2. Yadav, Prashant. "Digital transformation in the health product supply chain: a framework for analysis." *Health Systems & Reform* 10, no. 2 (2024): 2386041.
3. Putra, Fauzan Prasetyo Eka, Achmad Zulfikri, Goffal Arifin, and Revi Mario Ilhamsyah. "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study." *Brilliance: Research of Artificial Intelligence* 4, no. 1 (2024): 413-421.

4. Salem, Aya H., Safaa M. Azzam, O. E. Emam, and Amr A. Abohany. "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques." *Journal of Big Data* 11, no. 1 (2024): 105.
5. Nagar, Gourav. "The Evolution of Ransomware: Tactics, techniques, and mitigation strategies." *International Journal of Scientific Research and Management (IJSRM)* 12, no. 06 (2024): 1282-1298.
6. Alabdan, Rana. "Phishing attacks survey: Types, vectors, and technical approaches." *Future internet* 12, no. 10 (2020): 168.
7. Alabdan, Rana. "Phishing attacks survey: Types, vectors, and technical approaches." *Future internet* 12, no. 10 (2020): 168.
8. Nadeem, Muhammad, Syeda Wajiha Zahra, Muhammad Nouman Abbasi, Ali Arshad, Saman Riaz, and Waqas Ahmed. "Phishing attack, its detections and prevention techniques." *International Journal of Wireless Security and Networks* 1, no. 2 (2023): 13-25p.
9. Nadeem, Muhammad, Syeda Wajiha Zahra, Muhammad Nouman Abbasi, Ali Arshad, Saman Riaz, and Waqas Ahmed. "Phishing attack, its detections and prevention techniques." *International Journal of Wireless Security and Networks* 1, no. 2 (2023): 13-25p.
10. Kaushik, Priyanka, and Saurabh Pratap Singh Rathore. "Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection." *International Journal on Recent and Innovation Trends in Computing and Communication* 11, no. 9s (2023): 680-686.
11. San San, Smart Elizabeth, and Temitope OLajumoke. "AI-Driven Risk Management in Information Security: Harnessing Predictive Analytics and Automation to Enhance Protection."
12. Fatma, Sabiha. "AI-Based Social Engineering Detection."
13. Gaioto, Fiza. "Innovations in Phishing Defense: Combining Supervised Classifiers in AI with Nature-Inspired Algorithms for Enhanced Security." (2023).
14. babu Nuthalapati, Suri. "AI-enhanced detection and mitigation of cybersecurity threats in digital banking." *Educ. Adm. Theory Pract.* 29, no. 1 (2023): 357-368.
15. Vaahersalo, Jack. "Leveraging Big Data for Intrusion Detection and Phishing Defense: Innovations in Machine Learning Ensembles and AI Supervised Classifiers." (2023).
16. Ali, Hamid. "AI-Powered Supervised Classifiers in Big Data Environments for Phishing Defense and Intrusion Detection." (2022).
17. Biggio, Battista, Igino Corona, Blaine Nelson, Benjamin IP Rubinstein, Davide Maiorca, Giorgio Fumera, Giorgio Giacinto, and Fabio Roli. "Security evaluation of support vector machines in adversarial environments." *Support vector machines applications* (2014): 105- 153.