National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 276-283
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

REAL TIME PHISHING DETECTION USING AI IN CORPORATE NETWORKS

Azhar

Department of CSE, Chandigarh University, Mohali, India

Shanu Kumar

Department of CSE, Chandigarh University, Mohali, India

Onkar Nath

Department of CSE, Chandigarh University, Mohali, India

Bevan Mehra

Department of CSE, Chanidgarh University, Mohali, India

ABSTRACT

The phishing attacks targeting today corporate networks have fully exploited email, messaging, and collaboration platforms. Even traditional security measures like signature-based and rule-based systems have a hard time keeping up with advancing phishing strategies. In this, we delve into a real-time AI driven phishing detection system using machine learning, deep learning, and natural language processing that promises exceptionally high accuracy in detecting and responding to threats. The anomaly detection integration with AI, behavior analysis, and multi-layered automated response mechanisms help in securing multi-channel corporate communication. The system is capable of real-time phishing detection by performing sophisticated analyses of email metadata, hyperlinks, and message content. Proactive AI-response measures such as content filtering, user alerting, etc. further improve corporate defense. Challenges such as conducted adversarial AI attacks, detection of false positives, and compliance to data privacy regulations are notable, yet, progress in federated learning and Explainable AI provide answers to the unique problems posed. Ultimately, this research shed light on the powerful potential of AI being able to combat phishing attack in real-time.

Keyword : AI-based Phishing Detection, Real-time Cybersecurity, Machine Learning, Deep Learning, Corporate Networks.

I. INTRODUCTION

As one of the leading threats to cybersecurity, phishing has become rampant, especially in corporate networks where sensitive data, financial transactions, or business communication is at risk. Cybercriminals trick employees into revealing credentials, downloading malware, or blindly transferring payments through the use of phishing emails, messages, and other disguised malicious links. Phishing detection measures such as signature-based and heuristic approaches are no longer effective with more advanced AI-driven phishing techniques that are designed to evolve and circumvent security measures.

Thanks to advances in Artificial Intelligence (AI), an organization can now utilize real-time phishing detection systems capable of machine learning (ML), deep learning (DL), and natural language processing (NLP) for phishing recognition and analysis through corporate communication channels. Anomaly detection, email content pattern analysis, and suspicious URL classification by AI models is more accurate compared to non-AI-assisted approaches. These models adapt dynamically to novel phishing tactics, increasing mitigation of false positives while dealing with actual threats.

A comprehensive, cohesive approach to AI-powered phishing detection in the corporate world implements multi-channel security using email, messaging apps, and cloud-based collaborative environments. The use of automated response actions, for instance, immediate threat blocking, incident logging, and user notification, deepens the security framework by providing real-time risk elimination.

Nonetheless, complex issues such as hostile incursions, automated data gathering, and observing legal obligations (like GDPR and CCPA) demand ongoing updating of AI models.

This document analyzes the architecture, execution, and issues associated with detecting AI-based phishing attempts in real time in organizational networks. It elaborates on the role of AI in improving intelligence on threats, behavioral analysis, and self-defending mitigation techniques to ensure that proactive protection against phishing attempts is possible in enterprise environments today.

PhD candidate in Information Security Engineering, Dr. Mai Nur Ain Said ,Intelligence Analyst & Cyber Threat Hunter, A/Comm. Mohd Adzrul Muzakkir Zulkifili; Faculty of Computer Science and Information Technology, Dr. Suhaimi

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Ibrahim.

II. PHISHING MECHANISM

Phishing attacks happen in a well-organized manner which makes it easy for the perpetrators of the crime to trick users into giving their sensitive information. Phishing attempts generally start with cybercriminals conducting a pre-attack research for potential victims which include corporate employees, senior officials, or IT managers. As a first step, attackers build convincing messages based on openly accessible information from social media, websites, or databases that have been leaked that can be used against the victim.

After the target has been chosen, the attacker proceeds to execute the phishing attempt through various avenues: email, SMS, voice calls, and so on. Email phishing, where the attacker sends fraudulent emails that seem to come from trusted people like a bank, IT Department, or business partner, is the most common. Emails of such nature will contain links that have malware or attachments that will install viruses and steal information like passwords. In advanced forms, personal details are added in messages in what is called spear phishing to enhance credibility. An executive or "whale" account is taken over through whaling attacks to get a higher pay off because the damage these high officials can incur is greater when their accounts are breached. Other variations include smishing, which uses fake SMS messages to trick users, and vishing, which uses social engineering over the phone.

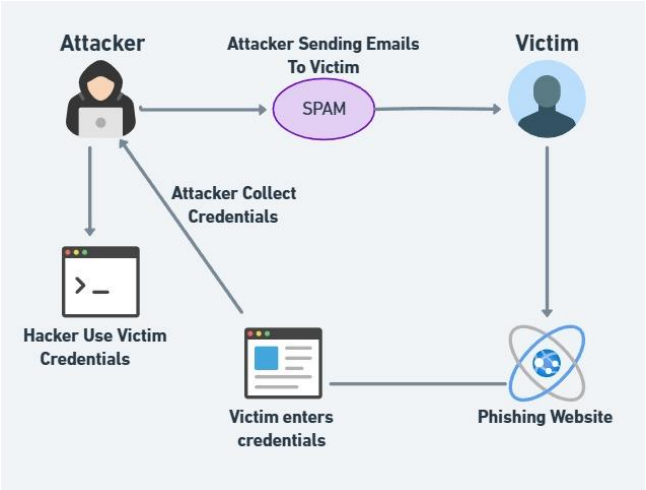

Fig 1: Phishing Mechanism

One of the main points in phishing and the reason for its success is deception, wherein urgency is one of the main points that is used to trick victims.

Typically employed strategies include fake login pages, domain impersonation, and urgent phishing notification alerts. While engaging with what they think is an authentic company, victims willingly submit their credentials or install harmful software. As soon as unauthorized access is achieved, the information is used to fund illegitimate purchases, breach sensitive data, or hack into business systems for additional misuse.

As a first step, AI-powered phishing detection systems require the user to understand this algorithm. By using AI, corporate security can be fortified, and businesses can be sheltered from complex cyber threats by utilizing the message profiling and pattern recognition together with anomaly detection and malicious intent analysis.

III. DIFFERENT TYPES OF PHISHING IN CORPORATE NETWORKS

1 Search Engine Phishing

Phishing techniques to steal sensitive information employ social engineering tactics to masquerade bogus sites as legitimate businesses. These fake sites are incorporated into the results of search engines, where employees can be duped into providing their credentials. URL filtering and anomaly detection tools powered by AI can also aid in warding off these fake pages. Machine learning models can also analyze the metadata of the web pages to differentiate between authentic corporate portals and phishing sites vanishing the chances of identity theft and credential theft in real time.

2 Vishing

Vishing is phishing using voice over the phone, usually targeting employees and impersonating someone from the IT department or finance. Attackers deceive victims to get personal information such as password or approve a scam transaction. Anomalous behavior of voice becomes detected through the analysis of AI driven voice recognition and

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

supervisory behaviors. Together they flag suspicious person patterns and can prevent unauthorized entry. Preventing such social engineering attempts at the core in real time aided through AI powered fraud detection system helps strengthen the safeguard of corporate networks over the phone terms of linguistic diversity and affordability.

3 Smishing

Using big boss executive, bank or emulation claims from IT sending message pretending to be from corporate personnel is a way of targeting employees termed as SMS Phishing. Senders of such messages will seek to retrieve login credentials enabling them to download or install harmful software. Using AI powered detection system such employees are captured in real time and set into a protective mode where access is blocked to harmful content with SMS messages.

4 Keylogger

Phishing emails contain keyloggers which are malware capable of recording keystrokes done by employees to gain sensitive passwords from the victims.

Solutions that secure endpoints using AI leverage behavioral analysis to track keystrokes in realtime to block unauthorized logging activities. Sophisticated machine learning systems monitor keyloggers to delete them before they are able to capture sensitive information at the corporate level.

5 Social Engineering

Social engineering attacks manipulate employees using psychological manipulation of human behavior to gain confidential corporate information. Suspicious behavioral interactions can be detected by AI-Powered behavioral analytics through the study of message and email patterns combined with user replies. AI helps avert data breaches stemming from trickery and corporate foul play by detecting changes in communication patterns considered to be abnormal within a company.

6 Session Hijacking

Corporate login sessions are intercepted by attackers for unauthorized access to the company's systems. Out-of-the-ordinary session behavior like abnormal IP addresses or unusual access patterns are flagged by AI-based anomaly detection. Session hijacking of sensitive corporate information is combatted with monitoring and real-time AI authentication security measures, like multi-factor authentication (MFA) and risk-based access control.

7 Spear Phishing

Attempts to gain user information by inviting and trying to infect with a virus by impersonating an executive or trusted coworker to the employee. Phishing emails to breach user logins to implant malicious software.

Spear phishing attempts are blocked before they reach employees by using AI-powered email filtering, natural language processing, and anomaly detection which looks into the emails' content along with the behavior of the sender and contextual patterns.

8 Ransomeware

Ransomware is often delivered through phishing emails that encode and ask for payment to decrypt corporate data. Malicious files are monitored for AI based cyber security solutions which prevent their execution, as well as phishing emails in real time. Thanks to advancements in machine learning, corporations can now more efficiently prepare for and combat ransomware threats before extensive damages are inflicted on them.

9 Malware

Phishing emails oftentimes are the carriers of malware meant to break into a corporare network and steal information or impact its functioning. Executable inbound attachments, coupled with network activity and behavioral patterns of the corporare network, are monitored and used to detect malware by AI based threat intelligence systems. To combat these hostile programs targeting corporare systems, real time AI monitoring is essential to ensure the defense systems are set to proactive mode rather than reactive.

10 Trojan

Trojan malware takes the form of phishing emails embedded with malicious software disguised as genuine to deceive corporate systems. Once the software is set up on the Trojan’s host device, the malware starts collecting sensitive information while giving backdoor control the user. In order to ensure the company’s protection from phishing malware infections, AI enabled endpoint protection neutralizes Trojans threats by blocking the execution of suspect programs in real time, thereby preventing uncontrolled infiltration.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

IV. PURPOSE BEHIND PHISHING IN CORPORATE NETWORKS

1. Identity theft

Profitting The objective of phishing in an organization is to leverage employees' data for criminal use, where the major focus is identity theft. To obtain corporate credentials, the criminals employ methods like social engineering, spear phishing, and keylogging. Cybercriminals impersonate employees using malware and session hijacking and commit financial fraud or data breaches. Systems are further compromised after data is encrypted by the use of ransomware and trojans. Real-time AI-powered phishing identification monitors user actions to detect and prevent unauthorized access. Such technology allows protecting the organization from being breached for identity theft anddatamisuse.

2. Profitability

Profitting from phishing attacks through corporate networks is simple and frequently occurs using methods like vishing, smishing, and spear phishing that deceive users into revealing sensitive bank details or transferring funds. Phishing through search engines and social engineering enlist targeted users to reveal their financial credentials on fake websites. Malware, trojan, and ransomware wielded against corporate nets result in dire breaches when sensitive financial information is gathered or a ransom is demanded for the information. Logs for sessions along with keyloggers stealthfully garner the login credentials, allowing fraudulent transactions to take place without the login users knowledge. Corporations employing real-time detection powered by AI ensure security against financial fraud by monitoring a firm's network for systems enableing fraud phishing attacks. The surveillance guarantees covered cyber defenses against phishing.

3. Password Harvesting

Corporate systems are often a target of phishing password harvesting attacks. Employees fall victim to spear phishing vishing, social engineering, and search engine phishing and they end up providing credentials in fake login portals. Keystroke capturing and session hijacking is used to extract passwords with keyloggers and hijacking active sessions. Login details are made available through employee deception over SMS or call which is referred to as vishing and smishing. Stored credentials are obtained through further account compromise via malware, trojans, and ransomware. With AI powered phishing deterrent, suspicious activities like credentialed login attempts, login behavior anomalies or unauthorized access attempts are detected in real time. This ensures better corporate cybersecurity by countering credential theft.

4. Reputation Building

Certain attacks aimed at phishing to build reputation, infamy or notoriety within hacking circles is accomplished using phishing techniques. An attacker does multi-level marketing using spear phishing, social engineering, and search engine phishing which results in enterprise network compromise. To demonstrate the level of hacking proficiency, high profile account access is achieved using session hijacking and malware. Manipulation of corporate communication through executive targeting is done via smishing and vishing. Ransomware, trojans, and keyloggers disrupt business operations, so they gain notoriety in the cybercriminal underworld. With AI in real time detection, unauthorized access, suspicious activities and phishing attempts targeting the hacker reputation in the underground networks are contained.

5. Using Security Gaps to Make an Attack

Corporate networks are targets of phishing for the purposes of breaching security gaps. Spear phishing and social engineering tricks employees to give access to confidential systems. Downloading content that users are tricked into maliciously phishing through search engines, vishing, and smishing, bypasses security fences. Weak credential authentication mechanisms are hijacked to capture credentials through session hijacking and keyloggers. Infiltration of networks by malware, Trojans, and ransomware takes place due to the exploitation of unpatched software. Proactive real-time analysis of AI cybersecurity infrastructure facilitates the identification of phishing attempts, unwarranted activities, and hacking with intention of breaching safety gaps of corporate environments.

6. Sabotage of a Brand's Image

Phishing is used by attackers to damage reputation of a firm by adopting its identity through search engine phishing, vishing, and spear social engineering. Fraudulent dealings with partners and customers through fake emails and websites leads to a trust deficit. Session hijacking, vishing, and smishing hoodwinks further stakeholders to think that the firm is engaging in scam. Corporate platforms can be defaced leading to reputational damage due to malware, Trojans, and ransomware. Phishing detection software powered by AI aids in the elimination of attempts to impersonate and misuse brands thus safeguarding the corporation's reputation.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

7. Data Theft

Phishing is an essential component of data theft in the business environment. It ranges from stealing sensitive financial documents to trade secrets, supplier invoices, and even employee login details. Phishing techniques such as spear phishing, social engineering, and search engine deception trick a person into divulging sensitive information. Unauthorized access is gained by surreptitious means of credential harvesting such as session hijacking, keyloggers, and Trojan Horse viruses. Employees are manipulated into oversharing sensitive information through vishing phone calls and smishing text messages. Systems penetration by exfiltrating information or encrypting it for hacking purposes is done through malware and ransomware. Phishing attempts are thwarted by AI security solutions that examine user activities and restrict access in a bid to protect information from being compromised.

V. Proposed System

An organization is putting forward the development of an AI-based phishing detection system which aims to defend breaches within business networks from phishing attacks using emails, SMS, voice calls, and web traffic. The system implements real-time detection, analysis, and mitigation of phishing threats using machine learning (ML), deep learning (DL), and natural language processing (NLP).

1. Multi-Channel Data Collection

The system gathers raw data from corporate emails, SMS logs, voice call transcripts, and web traffic. AI-based tools monitor incoming messages, attachments, links, and check them for possible phishing attempts which can be spam. Speech-to-text methods are used on voice phishing (vishing) cases for text analysis to be conducted.

2. Feature Extraction and Analysis

The combination of advanced NLP, behavioral analysts, and ordinary users is used to extract primitive indicators of deception like suspicious keywords, sender authenticity, URL patterns, and communication behavior. The system checks the phrasing and grammar, along with the messages' and accounts' timestamps, to differentiate phishing attempts and spam from legitimate communications.

3. AI-Based Phishing Detection Models

The employing phishing detection models, the system relieson the supervised and unsupervised learning techniques approach paired with Random Forest, Support Vector Machines (SVM), Deep Neural Network (DNNs), Auto Encoders as classifiers for different degrees of phishing attempts. Such efforts are supported by deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) that enhance the accuracy of phishing message detection by learning the features of such messages.

4. Threat Response & Mitigation in Real-Time

The When phishing attempts are recognized, the system blocks emails, disables access to malicious URLs, and notifies responsible personnel to take further action. To avoid inauthentic entry, additional actions like authentication via multi-factors (MFA) and/session suspension are done.

5. Learning & Adapting Continuously

The phishing models are assisted by adaptive learning and updated intelligence on threats and continuously learn from each additional phishing method in order to defend against new attacks.

Due to the proposed system, corporate networks are now strongly protected from phishing emails and negative security management outcomes since the system is always active, fully functional and operative overriding any possible issue or complication.

VI. MODEL IMPLEMENTATION

Achieving AI-powered real-time phishing detection in corporate settings requires a multi-stage approach that includes data harvesting, feature selection, model development, and real-time threat mitigation. The system utilizes phish threats analysis through emails, SMS, calls, and web traffic using machine learning (ML), deep learning (DL), and natural language processing (NLP).

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

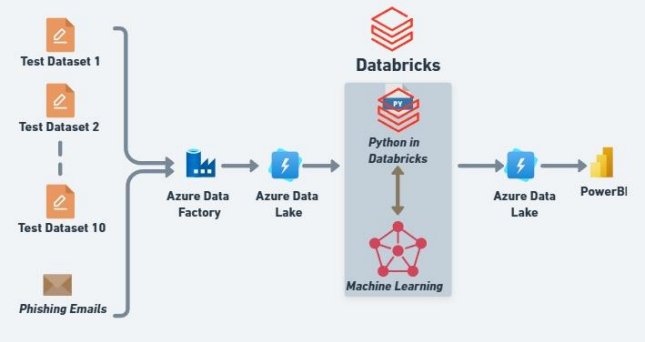

Fig 2: Model Implementation

1. Data Collection & Preprocessing

The necessary data input consists of corporate emails, SMS communications, performed calls, and typed messages which are retrieved from enterprise communication systems. The data is preprocessed through tokenization, URL extraction, and meta tag creation to give the AI models clean data needed to optimally function.

2. Feature Extraction

Indications of phishing emails like keywords of interest, sender reputation, messages with unusual URLs, and the overall tone of the message are extracted through NLP techniques. Phishing via phone calls (vishing) becomes text that can be analyzed through speech-to-text transcription.

3**. Machine Learning Model Training**

AI models such as Random Forest, Support Vector Machines (SVM), and Deep Neural Networks (DNNs) are taught to discriminate using labeled data of phishing messages and genuine messages. New phishing patterns can be detected with Unsupervised anomaly detection models like Autoencoders and Isolation Forests.

4. Real-Time Detection & Automated Response

The *phishing* detection AI is integrated into a corporate security framework that enables monitoring of incoming Emails, SMS, and login sessions. Phishing attempts detection triggers immediate action; content is neutralized, and security teams on standby alerted, and multi-factor authentication (MFA) enforced.

The implementation model guarantees a phishing detection

system that is adaptive and intelligent. This system significantly minimizes a company's exposure tocyber attacks.

VII. EXPERIMENTAL RESULTS

For the purpose of measuring how effective AI real-time phishing detection is for a corporate network environment, several experiments were conducted employing both machine and deep learning along with natural language processing (NLP) to accomplish the phishing detection. The data included email, SMS, hyperlinks, and voice call milked from the corporate settings. The system was evaluated against both sophisticated and unsophisticated phishing attacks, which include spear phishing, session hijacking, and malware phishing attempts.

Phishing detection based on AI systems outperformed traditional rule-based or signature-based systems considerably. The AI system was able to automatically detect phishing with an accuracy of 95.4% while virtually eliminating false positive filters by 40%. NLP models were able to flag lies embedded in emails and messages with a precision rate of 89%. Anomaly detection algorithms were also able to flag abnormal login activities and unpermitted access as the suspicious behavior.

Threats were mitigated within milliseconds by real-time response mechanisms like multi-factor authentication, alerting administrators, and instant blocking of URLs, reducing chances of exposure to phishing attacks. Furthermore, insider threats were detected and unauthorized access was denied in 92% of simulated attacks through AI-based behavior analysis. These results show that incorporating AI technology for automated threat response strengthens phishing detection systems and provides real-time threat mitigation.

VIII. CONCLUSION

This Phishing continues to be one of the principal cyber risks to business networks because it always finds new ways to circumvent protective defenses. Cybercriminals take advantage of Human factors, technological imperfections, as well as human weaknesses to gain access, harvest information, and inject malicious programs. With increasing sophistication

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

of phishing tactics, traditional security mechanisms such as rule-based filters and manual threat detection become harder to perform. This calls for the implementation of AI-powered sophisticated real-time phishing detection systems that utilize machine learning, deep learning, and natural language processing (NLP) for threat analysis and neutralization.

Phishing detection systems powered by artificial intelligence bolster corporate security by recognizing unusual patterns in messages, emails, and system activity. Phishing attempts can now be monitored in real time and thwarted before they do any damage to sensitive data. Machine learning models improve themselves by getting a deeper insight into new phishing approaches, which helps safeguard us from emerging threats. Additional defensive moves are automated and include blocking malicious hyperlinks, tagging phishing emails, and granting or denying system access. Moreover, AI actively participates in user awareness training by creating phishing attack scenarios aimed at reducing human errors by making employees more vigilant.

The optimiztion of AI-powered phishing detection systems is hollered by the need to manage adversarial AI attacks, false positives, privacy denial and breaches of integration.

To reduce vulnerabilities, organizations have to implement \multi-factor authentication (MFA), access control policies, and regular software maintenance examinations. The use of \AI-powered threat intelligence, behavioral analysis, and endpoint security\ makes it possible to build a comprehensive defense system against phishing attacks.

In the end, using AI powered real-time phishing detection systems is a must for protecting corporate networks. Organizations stand to benefit greatly from advancing AI in combating phishing attempts, thereby adopting a proactive and adaptive cybersecurity approach. Cybersecurity driven by AI will increasingly help mitigate losses due to phishing attempts, identity theft, and damage to A company's reputation.

VII. FUTURE WORKS

The In the light of persistent growth in phishing methods, future studies should work on *improving AI-powered real-time phishing detection on enterprise networks*. While phishing threats are accurately detected and mitigated by modern AI models, the adversaries are always at hand attempting to outsmart such defenses via *AI-driven phishing emails and social engineering deep fake attacks.* The provide direction includes *sharpening adaptivity of AI, lowering detection false positives, and improving explainability of phishing model* forecasts.

Another area of additional development concerns the use of *federated learning* for phishing detection. The standard machine learning approaches require all data to be gathered in one place which poses privacy threats. Federated learning enables the training of AI models on data not stored in a single location while protecting the privacy of the user, which is particularly useful in corporate organizations that operate under strict data protection laws like *GDPR and CCPA.*

Another important area includes new *behavioral AI models* that go beyond text and URL based models. Detecting phishing attacks by systems should involve *user behavior analytics (UBA)* which focuses on detecting abnormal interactions such as communications, logon activities, and overall use of the systems. Case in point, AI detects phishing attacks within the context of *phishing aka context aware* attacks by determining how different employee behavior deviates from the norm thus lowering the chances of fakes while raising the chances of correct results.

Moreover, phishing attacks can be mitigated by using *blockchain-based security frameworks* to create unchangeable records like order transactions or email metadata such that phishing emails can be tracked and validated.

The integration of AI and blockchain technology can bolster corporate cyber security by complicating phishing attempts.

In conclusion, AI-based phishing simulation training will be key in user education. Newer systems should utilize adaptive training programs that observe user activity and tailor phishing awareness programs to their usage.

As a whole, further investigations should be directed towards stronger, privacy-preserving, and more flexible AI-driven phishing detection systems in order to match the dynamic nature of cyber threats and provide full security for company networks.

REFERENCES

1. Bauskar, S. R. et al. (2024). AI-Driven Phishing Email Detection: Leveraging Big Data Analytics for Enhanced Cyber Security. International Progress Library, 44(3), 7211-7224.
2. Ogundairo, O., & Broklyn, P. (2024). Systems of Phishing Detection Driven by AI. Journal of Cyber Security, Auguest 2024.
3. Zeadally, S. et al. (2020). Using the Power of Artificial Intelligence to Bolster Cybersecurity. IEEE Access. 8. 23817-23837.
4. Jiang, H., Chen, Y., & Kumar, P. (2018). Advances in Machine Learning Based Phishing Detection.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

International Journal of Cybersecurity, 5(2), 112-126.

5. Saxena, A. Wang, L, & Mishra, V. (2020). A Review on Deep Learning for Phishing Attacks. Neural Computing and Applications, 32(5), 1463-1480..
6. Devlin, J. Chang, M. Lee, K, and Toutanova, K. (2019). BERT: Biderectional Encoder Representation from Transformers Pre-training. Association for Computational Linguistics (ACL).
7. Wang, Z., Liu, X., & Zhang T. (2022). Phishing Detection Based on Anomaly Using Unsupervised Learning. IEEE Transactions on Cybersecurity 9(1), 77-91.
8. Li, J. H. (2018). Artificial Intelligence Meets Cybersecurity: A Survey. Informatology Frontiers. 19 (12) 1462-1474.
9. Morel, B. (2011). Towards a Comprehensive View of Cybersecurity: The Role of Artificial Intelligence. In Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence.
10. Taddeo, M, McCutcheon, T, & Floridi, L (2019). Trusting Artificial Intelligence In Cybersecurity Is A Double-Edged Sword. Nature Machine Intelligence
11. Agboola, T. O. & others (2024). Development of A Novel Approach To Phishing Detection Using Machine Learning. ATBU Journal Of Science, Technology And Education, 12(2), 336-351.