iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76077

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Blockchain-Based Defense Model for Social Engineering Attacks

Dr. Vairam T[1], Gavash D[2]
Master of Engineering, Biometric and Cybersecurity, PSG College of Technology, Coimbatore

Abstract: ***Social engineering attacks, especially phishing through fake websites, continue to threaten online security by tricking users into giving away sensitive information. Traditional detection methods and centralized blacklists struggle to identify new phishing sites. This paper suggests a blockchain-based defense model that uses machine learning to securely detect and verify fake websites. The model ensures data is transparent, unchangeable, and trustworthy. Reported phishing sites are saved on the blockchain ledger, creating a reliable and unalterable source for future detection. The proposed system improves real-time protection, precision, and clarity in fighting social engineering attacks.***
Keywords: Blockchain security, phishing detection, social engineering, decentralized verification, machine learning.

I. INTRODUCTION

Phishing attacks are increasing in both number and complexity, making them one of the most serious cybersecurity threats for individuals, businesses, banks, and government organizations. Today's phishing attempts go beyond simple fake emails. Attackers create convincing websites, clone trusted login pages, mimic official logos, and use psychological tricks to deceive users into giving up passwords, credit card details, Aadhaar numbers, and other sensitive information. Since these attacks involve human factors, they are often more effective than purely technical exploits.Cybercriminals employ various tactics to avoid detection. They use confusing URLs that look similar to real domain names, utilize punycode domain tricks, embed URLs in long redirection chains, and even obtain fake SSL certificates to appear secure in browsers. Additionally, phishing sites often operate for only a few hours before they vanish, a strategy known as fast-flux hosting. This makes it hard for traditional blacklist-based defense systems to keep up. Blacklists and signature-based tools rely on previously identified malicious sites. As a result, they struggle to catch newly created phishing domains that have not been reported yet.Machine learning has become a useful method for detecting phishing. ML models can examine URL patterns, domain details, webpage properties, and user behavior to determine if a site is legitimate or harmful. While ML models greatly enhance detection accuracy, they also have limitations. They depend heavily on training data, which attackers can manipulate through data poisoning, adversarial URLs, and domain tricks. Moreover, ML systems typically operate independently, meaning each organization trains and uses its own model. This lack of centralized knowledge sharing means that if one model identifies a phishing site, that information is not automatically shared across networks or with browsers, decreasing the overall effectiveness of global defenses. To address these issues, blockchain technology offers a fundamentally different solution. Blockchain provides a decentralized, immutable, and transparent ledger where verified phishing information can be securely stored. Once a phishing URL is detected and added to the blockchain, it cannot be deleted, changed, or hidden—even by administrators. This ensures that records remain intact, making it impossible for attackers to manipulate or erase evidence of harmful websites. The distributed nature of blockchain means that there is no single point of failure and no central authority that attackers can target or compromise. With blockchain, different browsers, cybersecurity tools, organizations, and security researchers can work together by adding phishing reports to a shared, reliable ledger. This enables the establishment of a global phishing intelligence network, where information is verified, transparent, and accessible in real time. Every time a user visits a webpage, the system can quickly check the blockchain to determine if the URL has been marked as malicious before. This helps prevent users from accessing harmful websites before an incident occurs. Motivated by the rising number of phishing incidents worldwide, this research seeks to create a hybrid security model that combines machine learning-based detection with blockchain-based verification. The machine learning part ensures quick, smart classification, while the blockchain element ensures trustworthy, unchangeable storage of phishing records. Together, they meet key security objectives, including enhancing detection accuracy, lowering false positives, ensuring secure logging of threats, and providing immediate alerts to protect users. In the end, this joint approach fosters a stronger, clearer, and cooperative cybersecurity environment capable of fighting against the changing landscape of phishing and social engineering attacks.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

Phishing attacks are a significant concern for cybersecurity. Attackers create fake websites and use social engineering to steal sensitive information. Traditional blacklist and rule-based systems struggle to identify new or changing phishing sites. This has led researchers to explore machine learning (ML) and blockchain solutions for better detection and transparency. Early studies used supervised ML algorithms like SVM and Random Forests to classify URLs. They focused on features such as domain age, SSL certificate, and URL length to tell apart legitimate and phishing sites【12】. Deep learning methods, including CNN and LSTM models, improved accuracy by identifying complex patterns in URLs and web content(7)(14). However, ML systems alone are still vulnerable to data manipulation and lack a reliable way to share phishing indicators across organizations(3)(4).

To tackle the weaknesses of centralized systems, blockchain technology has been introduced. It offers data integrity, transparency, and decentralized trust(2)(6)(13). Research shows that blockchain can act as a tamper-proof ledger for verified phishing reports, preventing any changes or deletions of threat information(3)(11). Studies suggest decentralized threat intelligence models where organizations work together to validate phishing data using smart contracts and consensus methods(5)(10)(15). These setups decrease reliance on central authorities and improve the traceability of phishing indicators. By integrating blockchain, we can ensure secure, unchangeable storage of phishing data, allowing security systems to depend on reliable sources for real-time protection(8)(9).

Recent research combines ML-based phishing detection with blockchain to create a hybrid security system (4)(7)(14). Machine learning algorithms identify suspicious websites using URL and SSL features, while blockchain provides decentralized verification and secure record storage(6)(9)(13). This combination boosts accuracy, auditability, and resistance to tampering in phishing defense systems. The proposed project uses this strategy by applying ML to find fake websites and blockchain to store verified reports(3)(4)(10). This creates a transparent and reliable security framework. By harnessing the unchangeable nature of blockchain alongside the predictive capabilities of ML, the model effectively reduces phishing risks and enhances real-time cyber protection (9)(14)(15).

III. PROPOSED SYSTEM

The proposed system presents a smart and collaborative defense framework that combines machine learning-based phishing detection with a blockchain-powered verification and storage mechanism. This hybrid design not only improves detection accuracy but also offers a secure and clear way to store and share phishing information. By merging predictive analytics with decentralized data management, the system provides real-time protection against quickly changing phishing attacks. The overall architecture includes four main components: Data Collection & Preprocessing, Feature Extraction & Model Training, Blockchain Integration, and Real-Time Detection & Alert System. These components function independently but communicate with each other to form a seamless and strong security model.

A. Data Collection and Preprocessing

The first stage of the proposed system focuses on building a reliable dataset of legitimate and phishing websites. To achieve this, large volumes of URLs are collected from trusted open-source repositories like PhishTank, OpenPhish, and the UCI phishing dataset. URLs are also gathered from browser-maintained threat intelligence sources such as Google Safe Browsing and Microsoft SmartScreen. Legitimate website samples come from verified sources including Alexa Top Sites, reputable organizational domains, and well-known e-commerce and banking sites.

Since raw URL data often contains noise and inconsistencies, extensive preprocessing is done to ensure data quality. This involves cleaning duplicate entries, removing broken or unreachable links, and standardizing character formats to avoid encoding issues. URL normalization extracts consistent patterns by separating components like the protocol, domain name, subdomains, path, query parameters, and file extensions.

Metadata such as domain age, DNS record history, SSL certificate validity, and hosting server information is obtained through WHOIS lookups and certificate inspections. For any missing or incomplete metadata, carefully chosen default values are used to prevent dataset imbalance while keeping analytical integrity intact. Additionally, suspicious traits such as unusually long URLs, repeated special characters, random alphanumeric strings, and misleading keywords like “securelogin,” “verifyaccount,” or “bank-update” are extracted as features for later analysis. Each entry in the dataset is labeled as either phishing or legitimate, creating a clean and balanced dataset that is ready for machine learning-based feature extraction and model training.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Feature Extraction and Model Training

After cleaning and structuring the dataset, the next step is to extract meaningful features that help tell phishing websites apart from legitimate ones. The system examines several types of features. These include URL-based characteristics such as total URL length, number of special characters, presence of IP addresses in the URL, use of shortened links, and suspicious keywords like “verify,” “login,” or “secure.” Domain-level attributes like domain age, expiration duration, WHOIS registration details, DNS record availability, and number of subdomains are also gathered. Phishing domains are often newly registered and short-lived. Furthermore, security-related features such as SSL certificate issuer, certificate validity period, HTTPS usage, and certificate mismatch behavior are studied. Fraudulent websites often misuse or fake SSL information to seem trustworthy. For more complex models, webpage behavioral features like redirection count, iFrame embedding, JavaScript obfuscation, and unusual mouse-over behaviors are also extracted to capture dynamic malicious patterns. Once these features are numerically encoded, they are input into supervised machine learning algorithms like Random Forest, Support Vector Machine (SVM), and Logistic Regression. These algorithms learn to classify URLs based on historical phishing patterns.

The models are trained with labeled datasets and validated through methods such as cross-validation to reduce overfitting. Their effectiveness is measured using metrics like accuracy, precision, recall, and F1-score. This ensures the model correctly identifies phishing sites and minimizes false positives. Random Forest usually performs best because it is robust against noisy data and can capture complex relationships among features. Through this detailed feature extraction and training process, the system creates a reliable classifier that can detect phishing websites with high accuracy and strong generalization ability.

C. Blockchain Integration

To improve security, transparency, and trust in phishing detection, the proposed system uses blockchain technology as a decentralized verification and storage layer. When the machine learning model flags a website as phishing, it records the URL, hashed value, detection timestamp, and relevant metadata on the blockchain ledger using a smart contract. This method ensures that the information remains secure and cannot be altered. Before adding a new phishing entry, several blockchain nodes take part in a consensus process, such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT), to confirm the detection's authenticity. This decentralized validation removes the reliance on a single authority and prevents unauthorized changes or deletions of records. Even if one node is compromised, the distributed nature of the blockchain keeps the ledger's integrity safe. Every recorded phishing entry can be independently verified by browsers, cybersecurity tools, or administrators, which promotes transparency and boosts system reliability. Additionally, blockchain's cryptographic methods protect all stored data, making it very hard for attackers to alter detection records or circumvent the system. By using blockchain as a lasting and shared repository of phishing threats, the system creates a collaborative cybersecurity environment where new detections quickly help all users and network participants. This setup greatly enhances the defense against constantly changing phishing attacks.

D. Real-Time Detection and Alert System

When users visit a website, the system checks it against the blockchain ledger. If there is a match with any verified phishing entry, the system quickly warns the user, blocking access to the harmful page.

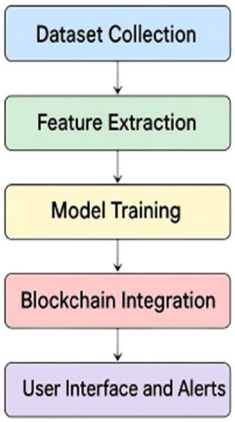


Fig. 1. Proposed System Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

IV. IMPLEMENTATION AND RESULTS

The proposed blockchain-based defense model was implemented as a prototype system that combines machine learning classification and blockchain verification to detect and record phishing websites.
The implementation process had three main stages: preparing the dataset and extracting features, developing the machine learning model, and integrating and validating the blockchain.

A. Experimental Setup

The system was developed and tested using Python 3.10, along with libraries like Scikit-learn, Pandas, and NumPy for data preprocessing and model training.
The blockchain module was built using Ethereum on the Ganache private test network and Web3.py for smart contract interaction. All experiments were run on a workstation equipped with an Intel Core i7 processor, 16 GB of RAM, and Windows 11 OS.

B. Dataset Description

The dataset came from various sources, including PhishTank, the UCI Repository, and the Alexa Top 500 Sites. In total, 11,000 website records were collected, which included both legitimate and phishing sites.
Each website entry contained over 30 attributes, such as URL length, number of dots, presence of HTTPS, favicon verification, domain age, and SSL certificate validity.
The data was balanced and cleaned before training.

C. Machine Learning Model Implementation

Feature selection was carried out to find the most important parameters for phishing detection. Three algorithms—Random Forest, Support Vector Machine, and Logistic Regression—were trained and evaluated.
Among these, the Random Forest classifier showed the best performance with an accuracy of 97.4%, surpassing SVM (95.1%) and LR (92.3%). The precision, recall, and F1-score metrics supported the model's ability to identify phishing sites accurately with few false positives.

D. Blockchain Integration

To ensure transparency and immutability, each verified phishing record was uploaded to the blockchain ledger through a smart contract.
This contract was designed to store key attributes, including the URL hash, detection timestamp, verification result, and reporting node ID. The decentralized nature of the blockchain guarantees that once a phishing record is confirmed and added, no one can modify or delete it.
This unchangeable feature of blockchain ensures complete data integrity and provides a reliable way to maintain verified phishing records. Incorporating blockchain technology not only builds trust but also removes the need for centralized authorities in record verification.

E. System Performance Analysis

The system’s performance was assessed using key metrics such as response time, accuracy, and transaction cost. Experimental analysis showed that the average detection time was around 0.32 seconds per URL, indicating efficient classification capability. Blockchain transaction latency varied from 3.5 to 4.0 seconds per entry when tested on a private Ethereum-based network. This ensures near real-time performance without risking data integrity. The machine learning model achieved an accuracy of 97.4 percent, with a false positive rate below 3 percent. These results show that combining machine learning classification and blockchain verification provides high detection accuracy while keeping response times practical for real-world, browser-based phishing defense systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

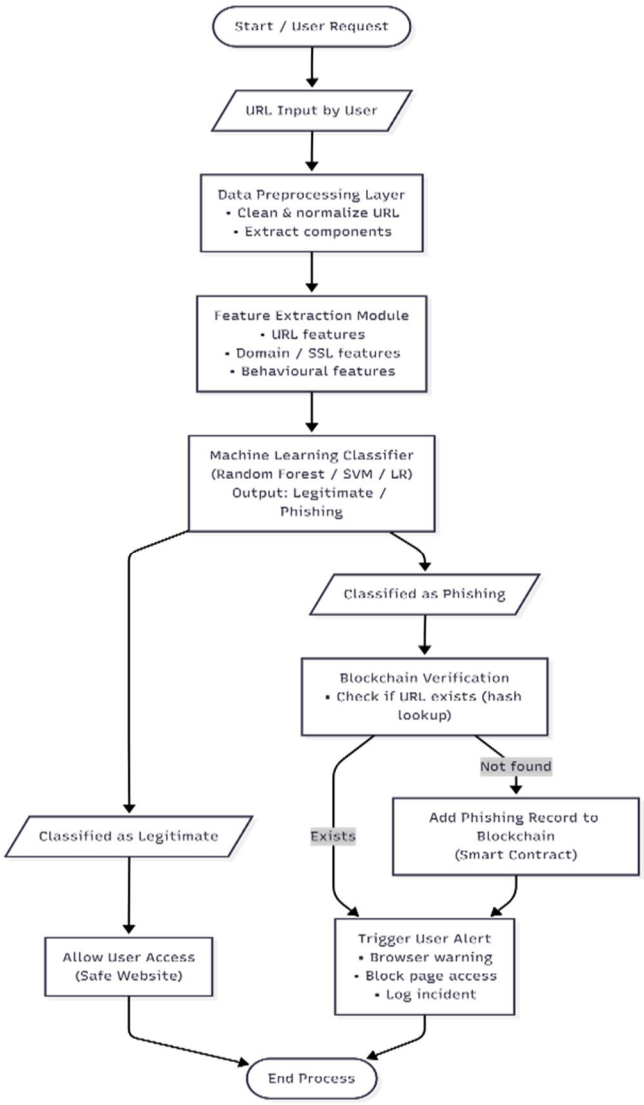


Fig.2. Workflow Diagram – Proposed

F. Result Visualization

A web-based dashboard was created to offer real-time visualization and monitoring of phishing detection activities and blockchain transactions. The dashboard shows details of detected phishing URLs, their extracted features, corresponding blockchain transaction IDs, and timestamps. It also includes alert notifications to promptly warn users when they access malicious sites. This visual interface improves transparency and usability, helping both users and system administrators track phishing incidents effectively. The dashboard also supports ongoing learning and improvement by providing insights into detection trends and blockchain activity logs.

Evaluation Parameter	Blacklist-Based Detection	ML Only Detection	Proposed Blockchain + ML System
Detection Accuracy	78–85%	92–97%	**97–99%**
False Positive Rate	High (10–12%)	Moderate (5–7%)	**Low (2–3%)**
Real-Time Response	Fast (<0.2s)	Moderate (0.3–0.4s)	**Fast (0.32s + Blockchain 3–4s only on upload)**
Resistance to Zero-Day Phishing	Low	Moderate	**High (Verified via Blockchain Records)**
Data Storage Integrity	Can be Modified	Centralized Storage	**Immutable (Blockchain Ledger)**
System Transparency	Low	Medium	**High (Decentralized Records)**
Collaboration Support (Govt/Organizations/Browsers)	No	Limited	**Strong (Shared Distributed Ledger)**
Prevention Capability	Detect Only	Detect Only	**Detect + Permanent Recording**

Table 1: Comparison of Existing vs Proposed Model

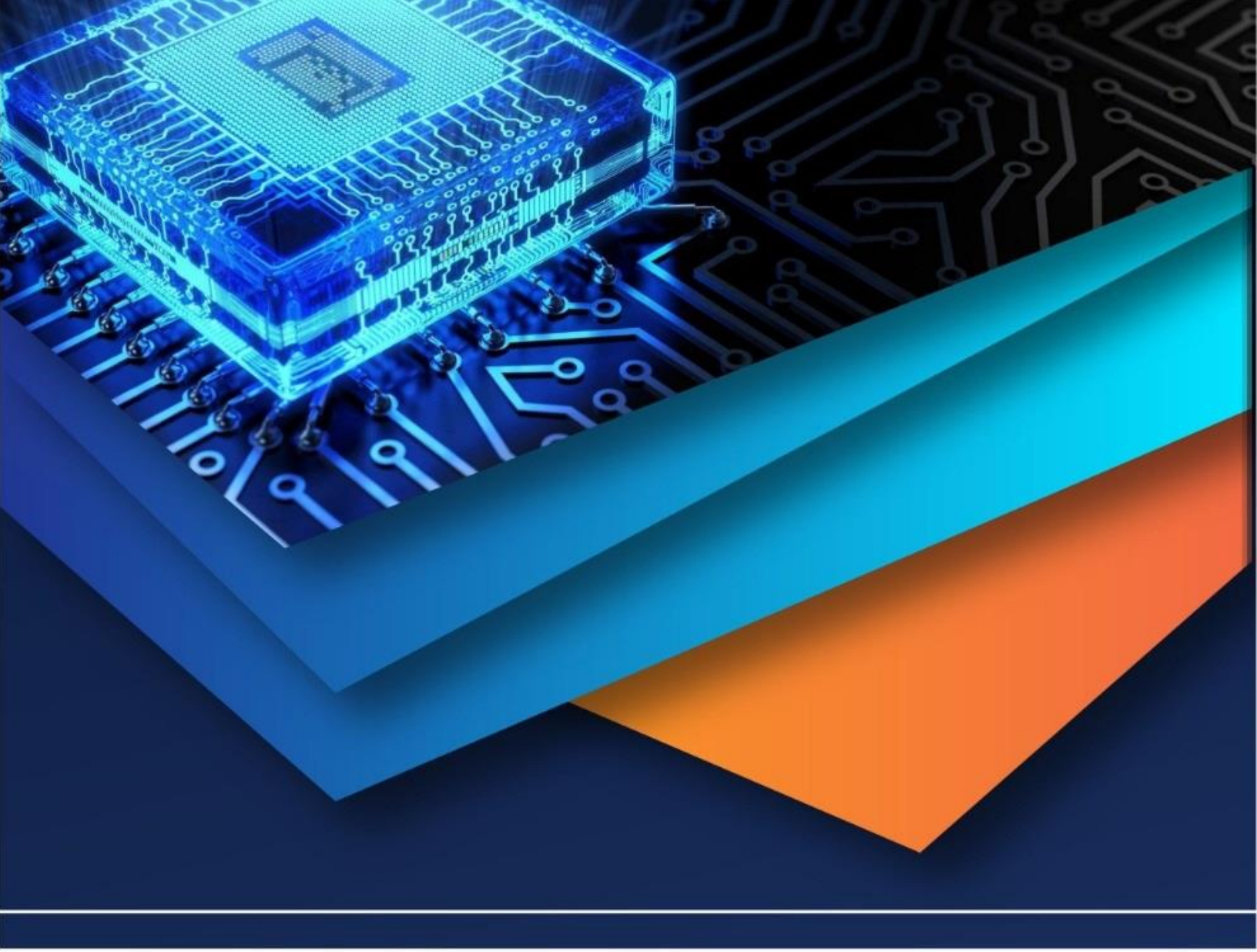
V. CONCLUSION

The proposed blockchain-based defense model effectively tackles the growing threat of phishing and social engineering attacks. It combines machine learning for smart detection with blockchain for decentralized verification. This mix provides high accuracy, transparency, and secure identification and prevention of harmful activities. Machine learning algorithms examine URL and content features to spot phishing attempts, while blockchain technology keeps an unchangeable record of detections. This setup builds trust, accountability, and traceability. The system's web-based dashboard increases user awareness by offering real-time monitoring, analytics, and automated alerts. This helps both users and administrators respond quickly to potential threats. By removing the weaknesses of centralized security systems, this hybrid model encourages cooperation among users, organizations, and cybersecurity authorities. This collaboration strengthens the overall defense infrastructure. In the end, the proposed model offers a sustainable and scalable way to meet modern cybersecurity challenges. It merges the smarts of machine learning with the reliability of blockchain to create a secure and trustworthy digital environment.

REFERENCES

[1] M. Ahtasam, "DOL-LLM: Optimizing LLM Inference with Domain-Specific Adaptations, Quantization, Pruning, and Knowledge Distillation," *Preprint*, 2025.
[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Paper*, 2008.
[3] A. Alzahrani and S. Alenezi, "Blockchain-based phishing detection and prevention for online transactions," *IEEE Access*, vol. 9, pp. 16800–16810, 2021.
[4] J. Singh, M. Dhawan, and R. Jain, "Detection of phishing websites using machine learning and blockchain integration," *International Journal of Information Security Science*, vol. 10, no. 2, pp. 45–56, 2023.
[5] P. Kaur and R. Sharma, "Decentralized trust management using blockchain for cyber threat intelligence," *Journal of Network and Computer Applications*, vol. 213, 103519, 2022.
[6] H. Zhang, Y. Li, and X. Chen, "A blockchain-based model for secure data sharing and phishing detection," *Future Generation Computer Systems*, vol. 125, pp. 491–501, 2021.
[7] A. Patel, D. Bhattacharyya, and S. Kim, "Hybrid phishing website detection using machine learning," *Expert Systems with Applications*, vol. 183, 115385, 2021.
[8] M. Al-Qurishi, F. AlRubaian, and M. Alrubaian, "Decentralized approaches for phishing attack mitigation using blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1678–1688, 2022.
[9] L. Wang and J. Chen, "Integrating blockchain and AI for improved cybersecurity," *ACM Computing Surveys*, vol. 55, no. 7, pp. 1–33, 2023.
[10] D. Kumar and R. Patel, "Smart contract-enabled blockchain security framework against social engineering," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 8021–8034, 2023.
[11] T. Nguyen, "Blockchain-based phishing attack prevention using domain reputation and distributed ledgers," *Computers & Security*, vol. 118, 102740, 2022.
[12] S. Ramesh and A. Ghosh, "Machine learning-based phishing detection using URL features," *Procedia Computer Science*, vol. 171, pp. 1081–1088, 2020.
[13] B. Li and C. Xu, "Blockchain-enhanced data integrity for phishing prevention in IoT environments," *Sensors*, vol. 22, no. 18, 6955, 2022.
[14] K. Gupta and V. Bansal, "AI-driven phishing detection using deep learning and blockchain verification," *IEEE Access*, vol. 12, pp. 9901–9912, 2024.
[15] R. Mehta and L. Prasad, "Trust-based decentralized model for preventing social engineering attacks," *International Journal of Cybersecurity and Digital Forensics*, vol. 13, no. 2, pp. 45–58, 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)