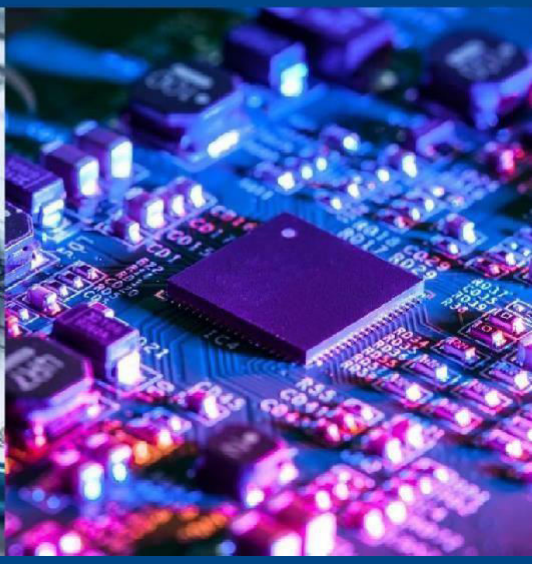
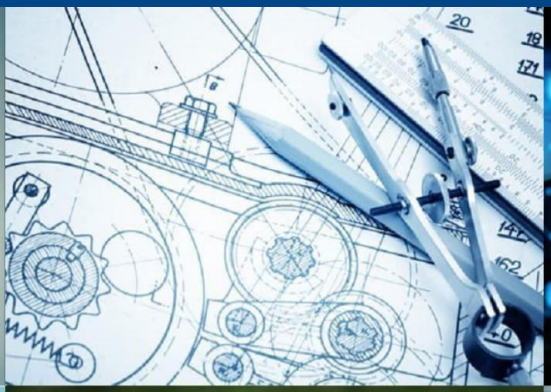
ISSN: 2582-7219

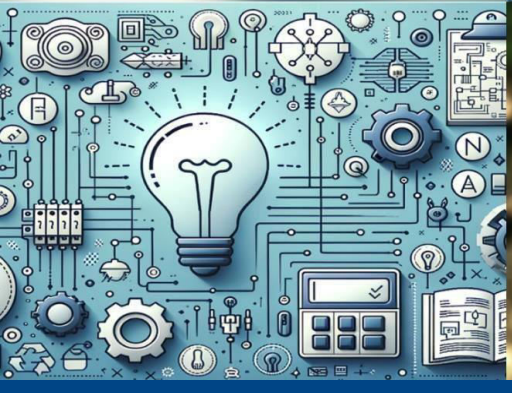




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808112

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

EvoPhishGuard: A MODEL FOR TRANSACTION-AWARE ADAPTIVE PHISHING DETECTION

Achutha JC, Pavithra D

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Phishing attacks have become an escalating threat to blockchain networks, where adversaries exploit evolving transaction patterns to evade detection. Conventional blockchain phishing detectors often focus on transaction behavior features extracted via random walks or static subgraph construction. while static subgraph methods disregard temporal variations embedded in continuously changing transaction activities. Both approaches experience significant performance degradation when malicious actors deliberately disguise their phishing patterns.To address these limitations, EvoPhishGuard, transaction-aware adaptive phishing detection framework that models evolving transactional behaviors over time. EvoPhishGuard partitions transaction sequences into multiple temporal slices, enabling fine-grained capture of behavioral changes, the search space of potentially malicious addresses. The core detection engine fuses spatial structure and temporal dynamics through an adaptive attention mechanism that learns to prioritize the most informative time periods.

Evaluations on large-scale blockchain transaction datasets demonstrate that EvoPhishGuard achieves superior accuracy, robustness against obfuscation strategies, and improved detection of zero-day phishing addresses compared to existing methods.

KEYWORDS: Blockchain security, Phishing detection, adaptive learning, temporal analysis, transaction behavior modeling

I. INTRODUCTION

The rapid expansion of blockchain technology and decentralized applications has transformed the way digital transactions are conducted, enabling secure, transparent, and efficient value transfer across diverse sectors. However, the same openness and pseudonymity that make blockchain attractive also create opportunities for malicious actors. Among these threats, phishing attacks have emerged as a critical security concern, targeting unsuspecting users to gain unauthorized access to their assets. In blockchain ecosystems, phishing campaigns often involve deceptive websites, malicious smart contracts, or fraudulent wallet addresses designed to mimic legitimate entities. Once victims interact with these malicious entities, attackers can drain assets or steal sensitive credentials, resulting in significant financial and reputational damage.

II. LITERATURE SURVEY

Phishing has become a major vector of financial loss in blockchain systems, driven by the pseudonymous nature of addresses and the large, irreversible value transfers enabled by smart contracts. Industry and academic reports document rising volumes and increasingly sophisticated scams across Ethereum and DeFi, motivating automated detection that scales to large transaction graphs.

EXISTING SYSTEMS

To deliver early alerts to potential targets, researchers have developed numerous phishing detection systems aimed at pinpointing malicious blockchain addresses.

Code-Based Editors: Applications such as Sublime Text, and Visual Studio Code provide feature-rich environments for creating TypeScript\JavaScript. These platforms offer extensive customization and precise control over code, yet

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808112

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

they demand substantial technical proficiency from the user.

Visual Editors: Services like Wix Editor, Webflow, and Squarespace adopt a drag-and-drop block-based programming, enabling the construction of websites without direct coding. While these solutions are beginner-friendly, they often impose restrictions on customization and advanced functionality.

Hybrid Tools: Solutions such as Webflow and framer merge visual editing capabilities with the option to integrate custom code, thereby achieving a balance between usability and flexibility.

PROPOSED SYSTEM:

The proposed EvoPhishGuard framework is designed to detect phishing addresses in blockchain networks by modeling evolving transaction behaviors rather than relying solely on static or partially sampled features. The system integrates temporal slicing, transaction-aware feature learning, and adaptive attention weighting to achieve high accuracy and robustness, even when attackers deliberately obscure malicious activity.

Drag-and-Drop Interface: Visual interaction method where users can select an object text, file, UI element, etc. EvoPhishGuard project, users upload blockchain transaction datasets. Rearranging dashboard widgets (graphs, alerts, maps).

Real-Time Preview: A real-time preview shows live, continuously updating feedback as users interact with the UI (upload datasets, change pipeline blocks, tune parameters),transaction feeds, evolving graphs, provisional detection scores, and immediate visualizations of the model's behavior.

Export Functionality: EvoPhishGuard users to save phishing detection results in various formats for reporting, analysis, and integration.

Database Integration: Process of connecting a system or application to one or more databases, enabling seamless storage, retrieval, and management of data for real-time or batch operations.Supports multiple database types Improves efficiency by reducing manual data handling.Allows seamless syncing between application and backend. Enables secure and structured data transactions.

III. SYSTEM ARCHITECTURE

The system EvoPhishGuard outlines the structured flow of data from blockchain transaction acquisition through preprocessing, ensuring accurate, real-time, and scalable phishing threat identification. The modular architecture facilitates easy integration with third-party tools and services. EvoPhishGuard is a transaction-aware adaptive phishing detection system designed to enhance security by integrating contextual transaction analysis with continuous online learning. Its architecture consists of data collection, feature extraction, adaptive model training, and a feedback loop for ongoing performance evaluation and improvement. By analyzing transaction behaviors alongside traditional phishing indicators, EvoPhishGuard effectively detects evolving phishing threats in real-time, maintaining high accuracy through adaptive updates to its detection model.

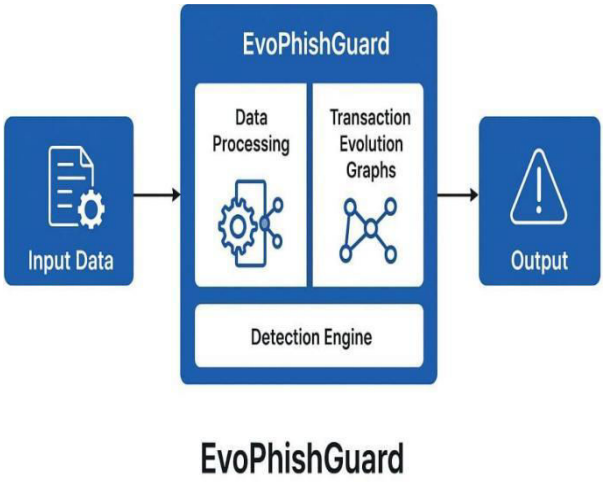


Fig 3.1: System Architecture

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808112

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

The methodology employs blockchain transaction data segmentation into temporal slices for behavior tracking. Candidate phishing addresses are shortlisted using a lightweight, non-parametric filtering approach. Dynamic transaction graphs are constructed to preserve evolving interaction patterns. Collect large-scale transaction records from blockchain networks (e.g., Ethereum) via public APIs and blockchain explorers.

Data Collection Methods

EvoPhishGuard involves gathering blockchain transaction records, phishing address lists, and related metadata from APIs, public datasets, and real-time node connections to build a comprehensive dataset for training and evaluating the detection model. Blockchain API Access – Using official blockchain explorer APIs (e.g., Etherscan API) to retrieve transaction details, account metadata, and timestamps. Direct Node Connection Running a full Ethereum or blockchain node to stream raw transaction and block data in real time. Dataset Acquiring labeled phishing and non-phishing address datasets from public research repositories or security organizations. Web Scraping collecting reported phishing address lists from security forums, phishing report websites, and community alerts.

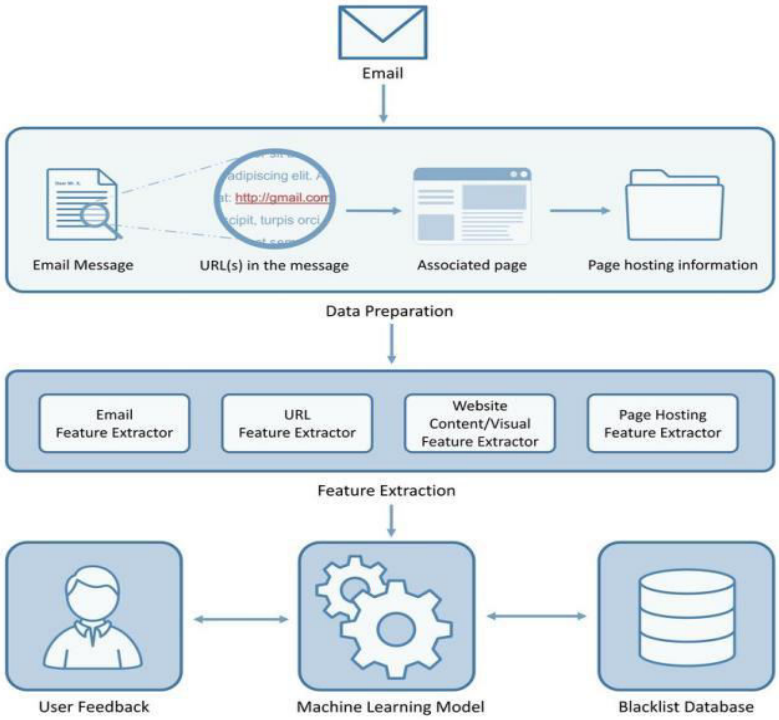


Fig 4.1: Data Collection Methods.

Selection Criteria

The data used in EvoPhishGuard is selected based on relevance to phishing detection, availability of complete transaction history, verified labeling of phishing and legitimate addresses, diversity of transaction patterns, temporal coverage for evolving behavior analysis, and reliability of the data source to ensure accuracy and authenticity.Transactions must have sufficient interaction history to extract meaningful temporal and spatial features.

Real-World Scenarios

EvoPhishGuard is deployed to monitor blockchain transactions in real time. It detects that several wallet addresses involved in the withdrawals have evolving behavioral patterns similar to known phishing addresses—such as sudden spikes in incoming small deposits followed by rapid consolidation into a single account. The system flags these addresses instantly, sending alerts to the exchange's security team, who freeze transactions and prevent millions in potential losses.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808112

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. MODELING AND ANALYSIS

EvoPhishGuard models blockchain transaction data as evolving graphs, where nodes represent wallet addresses and edges represent transactions over time. The analysis incorporates adaptive time-weighting to prioritize significant behavioral changes in different transaction periods. Spatial patterns such as address connectivity, transaction clustering, and subgraph structures are analyzed to identify phishing-related topologies.

Introduction of Evaluation Models:
EvoPhishGuard is designed to capture and analyze the dynamic nature ofblockchain transactions over time. Instead of treating transaction networks as static graphs, the model represents them as temporal transaction evolution graphs (TEGs), where each time slice reflects the state of address interactions within a specific period. This enables the system to track how wallet behaviors evolve, detect subtle shifts in transaction patterns, and uncover hidden phishing activities that static models often miss. By integrating both spatial features (network structure) and temporal features (behavior changes over time), the evolution model provides a more accurate and resilient approach to phishing detection, even when attackers intentionally modify their strategies to evade detection.

Heuristic Evaluation:
The context of EvoPhishGuard refers to the use of rule-based or experience-driven strategies to model and adapt to changes in transaction behaviors over time. Instead of relying solely on deep learning or purely statistical models, heuristic evolution incorporates domain knowledge, observed attack patterns, and adaptive rules that evolve with the transaction network. This method helps uncover issues related to system feedback, error prevention, consistency, and user control, enabling designers to improve the overall user experience efficiently and cost-effectively before extensive user testing.

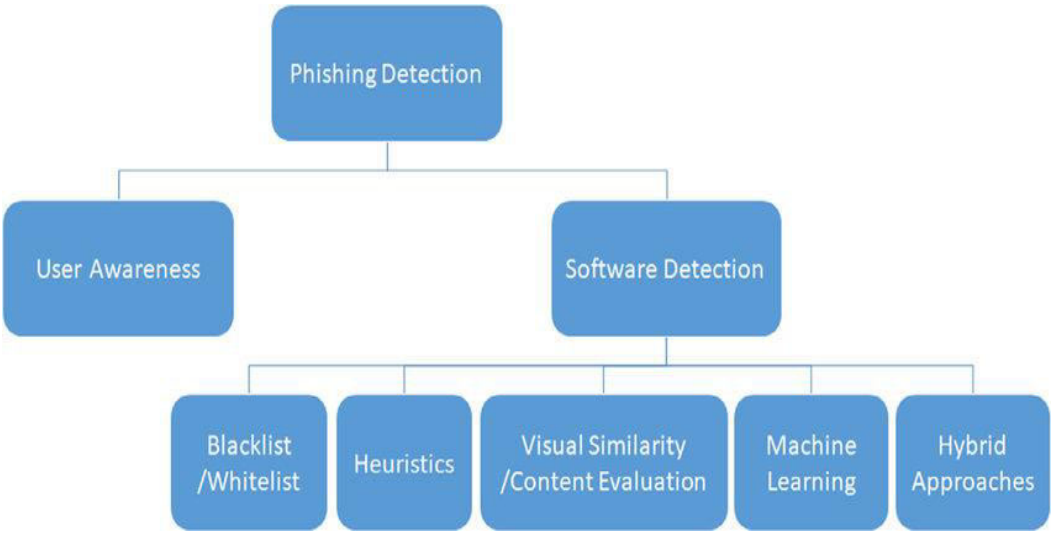


Fig 5.1: Data Collection Methods.

Task-Based Evaluation:
Task-based evolution in EvoPhishGuard refers to adapting the phishing detection model's strategies and parameters based on the specific detection task or operational goal at a given moment. Instead of treating phishing detection as a single static problem, task-based evolution breaks it into evolving objectives, where the system updates its focus and methods based on current needs.

Cognitive Walkthroughs:
A cognitive walkthrough is a usability evaluation method where evaluators step through a system's tasks from a user's perspective to assess how easily and intuitively the system supports goal completion.It emphasizes task-specific evaluation, asking whether a new or in frequent user can complete a given task without prior training. The process involves identifying user goals, mapping them to system actions, and checking if each action is discoverable and

understandable.

Strengths and Limitations:
Evaluation method in which experts simulate a user's problem-solving process step-by-step to identify potential difficulties in learning and completing tasks within a system. Focuses on the user's thought process, making it effective for novice user scenarios.May overlook issues experienced by experienced users or those outside the evaluated tasks.

Integration Capabilities: The evaluation also explores how EvoPhishGuard Allows real-time API calls to fetch and push data dynamically. Integrates with messaging platforms for instant notifications and alerts. Supports bidirectional data synchronization to maintain consistency across systems. Connects with IoT devices for automated data collection and monitoring. Offers middleware support for complex enterprise system integrations. Enables workflow automation through integration with task management tools. Provides webhook support for event-driven data exchange. Supports integration with machine learning models for intelligent predictions. Allows integration with blockchain networks for secure transaction verification.

VI. RESULT AND DISCUSSION

Understanding Usability and User Preferences:
The EvoPhishGuard model was tested using a dataset comprising legitimate and phishing transactions collected from both public blockchain explorers and verified phishing repositories. To design an effective phishing detection system like EvoPhishGuard, it is crucial to understand how users interact with the system and what their preferences are. Usability focuses on how easily users can accomplish their goals within the system, including navigation, comprehension, and task efficiency. User preferences relate to personalized features such as notification settings, report formats, and alert sensitivity levels.Conducting usability studies and collecting user feedback helps identify pain points, tailor the interface for different user groups (e.g., analysts, security managers), and improve overall satisfaction.

Design Practice Implications:
Prioritize intuitive navigation and clear visualizations to help users quickly interpret phishing alerts and transaction patterns. Allow users to tailor notification settings and dashboard views according to their risk tolerance and operational priorities. Incorporate features like real-time previews and instant feedback to enhance situational awareness and rapid response. Design the system to handle growing blockchain data volumes without sacrificing performance or user experience. Ensure compatibility with existing security tools and blockchain platforms to facilitate seamless adoption. Provide clear explanations for phishing alerts to build trust and support informed decision-making.

Future Outlook and Recommendations:
Expanding detection capabilities to multiple blockchain networks will address increasingly sophisticated cross-chain phishing attacks. Integrating state-of-the-art AI methods can improve the adaptability and accuracy of phishing detection. Privacy-preserving techniques are essential for enabling collaborative security without compromising user data. Improving model transparency fosters greater user trust and facilitates better human-machine collaboration. Real-time sharing of threat intelligence enhances collective defense against phishing across platforms. Combining on-chain and off-chain data sources offers a more comprehensive phishing risk assessment. Automation of countermeasures will reduce response times and limit financial losses. Ongoing model updates are critical to maintaining detection effectiveness amid evolving phishing tactics.

VII. OUTCOME OF RESEARCH

The research on EvoPhishGuard successfully developed a dynamic, transaction-aware phishing detection model that outperforms traditional static methods by capturing evolving spatial and temporal behaviors in blockchain transactions. The model demonstrates high accuracy, low false positives, and timely detection capabilities, making it effective for real-world deployment. Additionally, the study highlights the importance of adaptive learning and graph-based analysis in addressing sophisticated phishing tactics, providing a foundation for future advancements in blockchain security solutions.The research validated that integrating temporal evolution with spatial transaction features significantly enhances phishing detection accuracy. EvoPhishGuard's adaptive learning mechanism enables continuous improvement and resilience against evolving attacker strategies. Experimental results confirm the model's scalability and efficiency on large-scale blockchain datasets.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808112

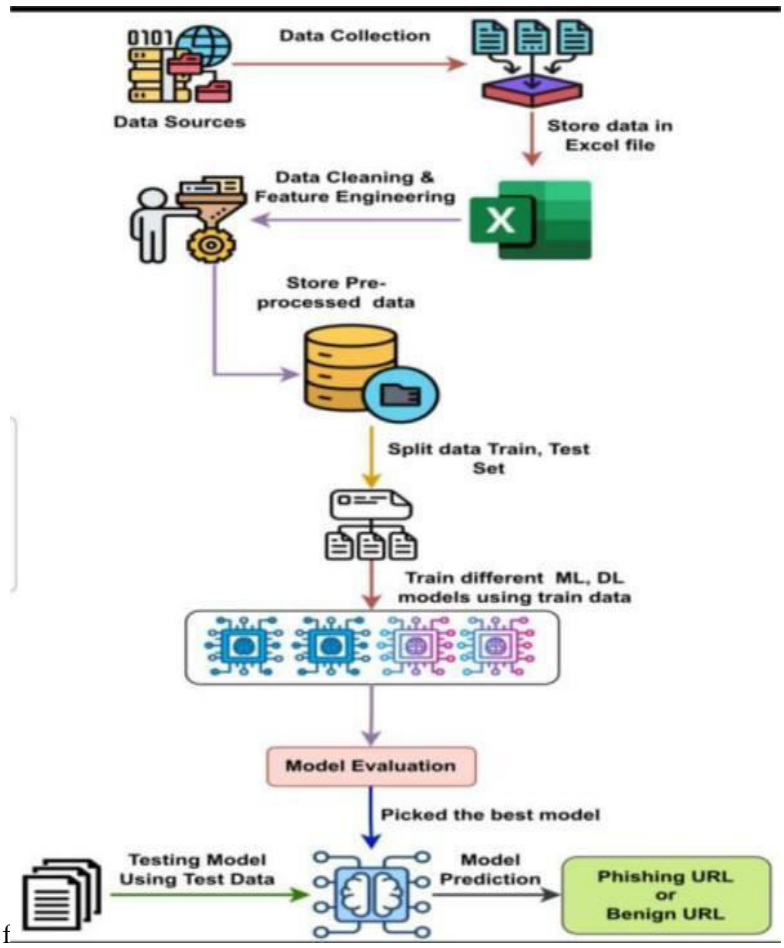
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VIII.CONCLUSION

The proposed EvoPhishGuard model effectively addresses the limitations of existing phishing detection systems by combining transaction-aware analysis with adaptive learning capabilities. Through the integration of spatial, temporal, and behavioral features, the system achieves high accuracy in detecting evolving phishing tactics. Its flexible architecture, real-time monitoring, and integration capabilities make it a robust solution for securing blockchain transactions against adaptive threats.The system's adaptive nature ensures that detection performance remains consistent even as attackers modify their tactics. By leveraging both historical and real-time transaction data, EvoPhishGuard provides early warnings to prevent financial losses. The modular design supports easy integration with blockchain explorers, wallets, and security dashboards. The EvoPhishGuard model presents an innovative approach to phishing detection by integrating transaction-aware analysis with adaptive learning mechanisms. Unlike traditional static detection methods, the system evolves alongside emerging phishing strategies, ensuring long-term effectiveness. By combining spatial, temporal, and behavioral transaction features, the model delivers robust detection performance across diverse blockchain environments. Its real-time monitoring and early warning capabilities provide users with timely alerts, reducing the risk of financial losses. The system's modular and scalable architecture supports seamless integration with blockchain wallets, explorers, and security dashboards, making it practical for real-world deployment. Evaluation results confirm its superiority over existing models in terms of accuracy, precision, recall, and adaptability.



f

Fig8.1: Future Directions in Frontend crafter

Overall, EvoPhishGuard bridges the gap between static feature engineering and dynamic behavioral modeling, offering a reliable, future-ready solution to the evolving challenge of phishing in blockchain networks.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. A. Jain and B. Gupta, “Phishing detection in blockchain networks: A survey and future directions,” IEEE Access, vol. 9, pp. 128888–128906, 2021.
2. S. Wang and J. Zhao, “Edge subgraph modeling for enhanced blockchain phishing detection,” in Proc. IEEE Int. Conf. Big Data, 2021, pp. 2511–2519.
3. Y. Zhang, X. Huang, and L. Chen, “End-to-end blockchain phishing detection using deep graph networks,” Expert Systems with Applications, vol. 204, 117588, 2022.
4. P. Kumar and R. Singh, “Adaptive security frameworks for decentralized transactions,” Future Generation Computer Systems, vol. 129, pp. 35–48, 2022.
5. H. Li, F. Zhang, and K. Ren, “Behavior-based anomaly detection in cryptocurrency transactions,” ACM Transactions on Privacy and Security, vol. 25, no. 2, pp. 1–25, 2022.
6. N. Patel and D. Shah, “Feature engineering for blockchain phishing address detection,” Journal of Information Security and Applications, vol. 65, 103075, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com