IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 12, December 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212032 |

Reducing Phishing Attacks in Online/Mobile Wallets and Net Banking

Aditya Pratap Singh, Aditya Mishra, Rajat Saha, Ms. Alina Raheen

U.G. Students, Department of Computer Engineering, Presidency University, Bangalore, India

Assistant Professor, Department of Computer Engineering, Presidency University, Bangalore, India

ABSTRACT: Phishing attacks, which take advantage of human weaknesses to obtain unauthorized access to sensitive information, continue to be a serious danger to the security of digital systems. The goal of this project is to create and put into use a sophisticated system that uses a multifaceted approach to identify and mitigate phishing assaults. In order to guarantee practical implementation, the system will be crafted to effortlessly mesh with current email security frameworks, offering an extra defence against ever-evolving phishing tactics. The project's effectiveness will be assessed by measuring user awareness and reaction to simulated attacks, conducting comprehensive testing and validation against well-known phishing scenarios, and more.

KEYWORDS: Phishing attacks, unauthorized access, human weaknesses, digital systems security, sophisticated system, multifaceted approach, identify, mitigate, practical implementation, email security frameworks, defence, evolving phishing tactics, effectiveness assessment, user awareness, simulated attacks, comprehensive testing, validation, well-known phishing scenarios.

I. INTRODUCTION

The primary aim of this project is to fortify the security infrastructure of net banking and mobile wallet platforms by developing a comprehensive defence mechanism against the pervasive threat of phishing attacks. Moreover, the project aims to minimize false positives within the detection algorithm while concurrently fostering user education and awareness programs. These educational modules will empower users to recognize and appropriately respond to potential phishing threats. Seamless integration with existing security frameworks, real-world testing, and continuous adaptation to evolving phishing tactics are integral facets of the project's objectives. By adhering to compliance standards, ensuring scalability, fostering user engagement, and collaborating with industry experts, the ultimate goal is to amalgamate cutting-edge technological solutions with user-centric education, culminating in a robust defence against phishing attacks within online financial ecosystems.

Paper is organized as follows. Section II System Implementation with Flow Charts (visual representations of the system's implementation process) and technologies used (overview of the key technologies employed in the project). Section III An in-depth evaluation of the proposed methodology and the ensuing outcomes and achievements of the implemented system. Section IV presents the website Screenshots (visual walkthrough of the developed website) and payment process results (screenshots highlighting the successful execution of the payment process). Finally, Section V presents conclusion.

II. SYSTEM IMPLEMENTATION & WORK FLOW

In the rapidly evolving landscape of online transactions, the prevalence of phishing scams poses a significant threat to the security of personal information and financial assets. These scams, often disguised as legitimate entities, exploit unsuspecting individuals by tricking them into revealing sensitive details. Recognizing the urgent need for a robust defence mechanism against phishing, our project introduces a smart and user-friendly approach to enhance online transaction security. By actively addressing the vulnerabilities exploited by phishing attempts, the proposed system aims to create a secure digital environment, allowing users to navigate the online landscape with confidence.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212032 |

The core of our security enhancement project is the Algorithm Comparison Module, a sophisticated solution that leverages Next.js for frontend development, Node.js with Express.js for the backend, and MongoDB for efficient data storage. This module serves as a pivotal component in our cybersecurity endeavor, offering users a platform to assess, compare, and select the most effective strategies in the ongoing battle against phishing threats.

To initiate the project, MongoDB, a NoSQL database, is employed for efficient data storage related to phishing indicators, historical scam patterns, and performance metrics. Node.js and Express.js form the backbone of our server-side development, enabling the construction of a fast and scalable backend that handles data processing, algorithmic computations, and communication with the database.

The integration of Next.js ensures a responsive and intuitive user interface, allowing real-time interaction with the Algorithm Comparison Module. JavaScript, employed on both the frontend and backend, enhances the dynamic aspects of the project, facilitating real-time updates and interactions.

In essence, our project leverages Next.js, Node.js with Express.js, and MongoDB to create a comprehensive Algorithm Comparison Module. This module represents a significant step towards a safer online environment, empowering users to make informed decisions and fortifying the digital landscape against the ever-evolving threat of phishing scams.

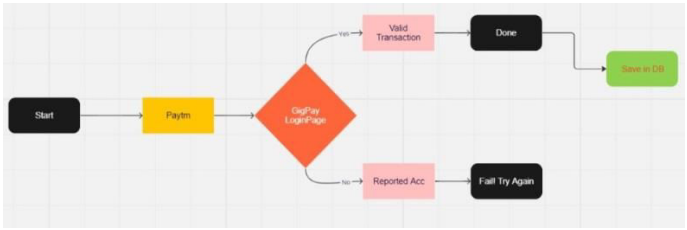


Fig: Flow Chart of the System.

The workflow begins with the user interacting with the frontend, where they can create an account, sign in, and proceed to fill in the transaction details. Upon entering the transaction information, the system checks the validity of the provided UPI ID. If the UPI ID is reported as fraudulent, the transaction is halted, and the user is notified that the payment cannot proceed due to the fraudulent nature of the UPI account. On the other hand, if the UPI ID is not flagged as fraudulent, the transaction proceeds successfully. Users are given the option to explicitly report UPI IDs that they suspect to be fraudulent, contributing to the collective security of the system. All transaction details, including transaction ID, timestamp, and details of reported fraud accounts, are securely stored in the database, providing a comprehensive record for monitoring and analysis to ensure the integrity and security of the online transaction environment.

III. OUTCOMES

The outcomes of the implemented system showcase a series of significant achievements and contributions to the digital landscape.[1] Functional Website: The foremost accomplishment is the successful development of a fully operational website, encompassing crucial functionalities such as user authentication and the capability to report fraudulent accounts.[2] Enhanced Security Measures: The introduction of a reporting system for fraudulent accounts demonstrates a commitment to bolstering user safety. This not only establishes a foundation of trust among users but also contributes to creating a more secure online environment.[3] Improved User Experience: By providing users with a platform to report fraudulent accounts, the project enhances user experience. Empowering users to actively contribute to the safety and integrity of the community adds value to their overall interaction with the platform.[4] Data Collection and Analysis: The system's reporting functionality enables the accumulation of valuable data. Analyzing this data allows for the identification of patterns in fraudulent behaviour, facilitating proactive measures to prevent future occurrences.[5] Learning and Development: The project serves as a learning opportunity, allowing the team to gain valuable experience in utilizing technologies like Next.js, Node.js, Express, and MongoDB. This contributes to the ongoing skill development of the team members.[6] Community Engagement: Encouraging users to report fraud accounts fosters a sense of community engagement and shared responsibility. This engagement contributes to cultivating a healthier and safer online environment.[7] Potential Business Impact: Successful implementation of robust security features can attract more users, enhance the platform's reputation, and potentially drive business growth and success.[8] Scalability and Future Improvements: The developed platform provides a

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

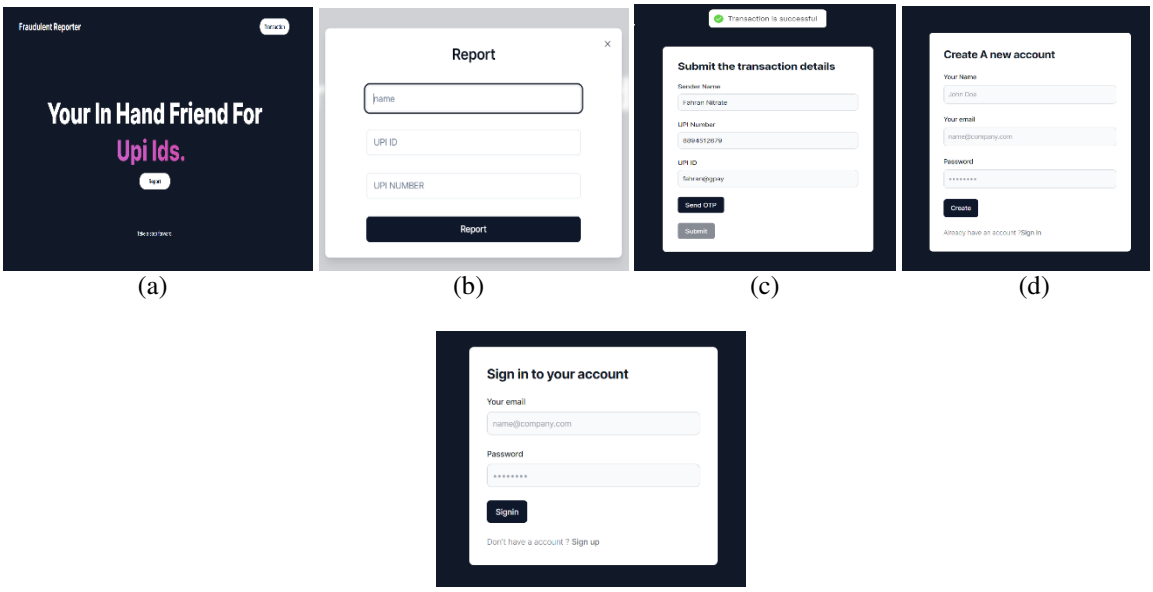
|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212032 |

foundational structure for future enhancements. This scalability enables ongoing development based on user feedback, technological advancements, and evolving requirements.[9] Compliance and Trust: For platforms dealing with sensitive data or operating in regulated industries, the implementation of secure reporting systems aligns with compliance standards. This enhances trust among users and stakeholders, ensuring a responsible and trustworthy digital presence.

IV. EXPERIMENTAL RESULTS

Figures shows the results of text detection from an image and inpainting by using exemplar based Inpainting algorithm. Figs. 2, 3, 4 (a) shows the original image. (b) is the image obtained by applying first set of criteria. All objects whose area greater than 10000 and filled area greater than 8000 are eliminated and major axis lengths are in between 20 to 3000 are considered to be text. Still, some small non-text objects are detected.



(a) (b) (c) (d)

(e)

Fig 1. The frontend interaction seamlessly guides users through the online transaction process: [d]Sign Up: New users initiate their journey by signing up, providing necessary details for account creation.[e]Login: After successful registration, users can log in using their credentials, ensuring a secure and personalized experience.[c]Transaction Submission: Once logged in, users access the transaction submission interface, where they input relevant details and authenticate with an OTP before hitting the submit button.[c,b]Fraud Check: The system performs a real-time check on the provided UPI ID against a database of reported fraud accounts. If the UPI ID is not flagged as fraudulent, the user receives a success message, confirming the transaction. Alternatively, if the UPI ID is reported as fraudulent, the system notifies the user that the transaction cannot proceed to safeguard against potential fraud. This user-friendly approach ensures that users are informed promptly about the legitimacy of their transactions, enhancing the overall security and trustworthiness of the platform.

(f) (g) (h)

Fig 2.The backend of the system operates seamlessly with three distinct databases:[f]Details Database: This database, aptly named "Details," serves as the repository for transaction-related information. It stores crucial details

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212032 |

such as transaction ID, timestamps, and other relevant data, providing a comprehensive record of all user transactions.[g]Fraud Database: The "Fraud" database is dedicated to tracking reported fraudulent activities. It functions as a digital blacklist, storing UPI IDs that have been reported as fraudulent. This proactive approach enables the system to perform real-time checks and prevent transactions involving reported fraudulent accounts.[h]Users Database: The "Users" database is designed to store essential user details. This includes user information collected during the sign-up process, ensuring a secure and personalized experience for users as they interact with the platform. This database plays a crucial role in user authentication and authorization processes.

The synergy of these three databases allows the backend to efficiently manage user transactions, monitor and mitigate fraud risks, and maintain a secure and user-friendly environment. This architecture ensures that the system operates with integrity, providing a robust foundation for the overall functionality of the platform.

V. CONCLUSION

[1] Summary of Achievements: [1.1] Objective Recap: The primary objective of implementing a fraud reporting system within the Next.js and Node.js website has been accomplished successfully, underscoring a commitment to bolstering platform security. [1.2] Accomplishments: The seamless integration of the reporting system highlights significant achievements, including enhanced functionalities, heightened user engagement, and the acquisition of valuable fraud-related data.

[2] Key Findings and Insights: [2.1] Data Analysis Recap: The analysis of reported fraud accounts uncovered noteworthy patterns, characteristics, and trends, offering critical insights into the dynamics of fraudulent activities on the platform. [2.2] Effectiveness Assessment: The reporting system's effectiveness in addressing and mitigating fraudulent activities is evident through increased user engagement in reporting and tangible data outcomes. [3] Lessons Learned and Recommendations: [3.1] Lessons Learned: Overcoming challenges provided valuable lessons, fostering continuous learning within the team in terms of technical insights and user behaviour nuances. [3.2] Recommendations for Improvement: To refine the reporting system, actionable recommendations include addressing identified weaknesses, refining functionalities, and exploring opportunities for enhancement.

[4] Impact and Future Prospects: [4.1] Impact Assessment: The reporting system has significantly reduced fraud on the platform, instilling a heightened sense of security and trust among users.

[4.2] Future Directions: Future prospects involve scalability considerations, additional functionalities, and potential integration with complementary security measures, ensuring the platform remains resilient against evolving threats.

[5] Conclusion Statement: [5.1] Closing Remarks: The successful implementation of the fraud reporting system marks a pivotal advancement in fortifying platform security. Seamless integration, coupled with valuable insights, positions the platform to proactively combat fraud, and the team is gratified with the achieved outcomes. A dedication to ongoing improvements underscores the commitment to providing users with a secure and trustworthy digital environment.

REFERENCES

[1] https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full
[2] https://www.researchgate.net/publication/340507635_Preventive_Techniques_of_Phishing_Attacks_in_Networks
[3] https://www.sciencedirect.com/science/article/pii/S0167404823002973
[4] https://dl.acm.org/doi/10.1145/3469886
[5] https://www.mdpi.com/2227-9717/10/7/1356
[6] https://www.irjet.net/archives/V3/i1/IRJET-V3I1121.pdf
[7] https://link.springer.com/article/10.1007/s10586-022-03604-4
[8] https://arxiv.org/ftp/arxiv/papers/2108/2108.04766.pdf
[9] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8864450/
[10] https://www.nature.com/articles/s41598-023-37552-9
[11] https://www.onlinegantt.com/#/gantt
[12] CODES
[13] https://github.com/Aditya-Mishra19/GigPay/tree/main/gigskybackend-main
https://github.com/Aditya-Mishra19/GigPay/tree/main/gigskyfrontend-main

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details