

Reducing phishing attacks in online/mobile wallets and net banking

A PROJECT REPORT

Submitted by,

Mr. Aditya Pratap Singh - 20201CSE0863

Mr. Aditya Mishra -20201CSE0866

Mr. Rajat Saha -20201CSE0906

Under the guidance of,

Ms. Alina Raheen

in partial fulfillment for the award of the

degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At



PRESIDENCY UNIVERSITY

BENGALURU

JANUARY 2024

PRESIDENCY UNIVERSITY
SCHOOL OF COMPUTER SCIENCE^{AND} ENGINEERING

CERTIFICATE

This is to certify that the Project report “Reducing phishing attacks in online/mobile wallets and net banking” being submitted by “Aditya Pratap Singh, Aditya Mishra, Rajat Saha” bearing roll number(s) “20201CSE0863, 20201CSE0866, 20201CSE0906” in partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering is a Bonafede work carried out under my supervision.



Ms. ALINA RAHEEN
Asst.Prof
School of CSE&IS
Presidency University



Dr. Pallavi R
Asso.Prof & HoD
School of CSE&IS
Presidency University



Dr. C. KALAIARASAN
Associate Dean
School of CSE&IS
Presidency University



Dr. SHAKKEERA L
Associate Dean
School of CSE&IS
Presidency University




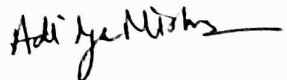

Dr. SAMEERUDDIN KHAN
Dean
School of CSE&IS
Presidency University

PRESIDENCY UNIVERSITY
SCHOOL OF COMPUTER SCIENCE^{AND} ENGINEERING &
INFORMATION SCIENCE

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled Reducing phishing attacks in online/mobile wallets and net banking in partial fulfilment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering** is a record of our own investigations carried under the guidance of Ms. Alina Raheen, Asst. Prof. School of CSE, School of Computer Science^{AND} Engineering, Presidency University, Bengaluru.

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	Roll. No.	Signature
Aditya Pratap Singh	20201CSE0863	
Aditya Mishra	20201CSE0866	
Rajat Saha	20201CSE0906	

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 defense 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.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Dean, School of Computer Science ^{AND} Engineering, Presidency University for getting us permission to undergo the project.

We record our heartfelt gratitude to our beloved Associate Deans **Dr. C. Kalaiarasan** and **Dr. Shakkeera L**, School of Computer Science and Engineering, Presidency University and **Dr. Pallavi R**, Head of the Department, School of Computer Science ^{AND} Engineering, Presidency University for rendering timely help for the successful completion of this project.

We are greatly indebted to our guide **Ms. Alina Raheen**, Asst-Prof, School of Computer Science ^{AND} Engineering, Presidency University for her inspirational guidance, valuable suggestions and providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the University Project-II Coordinators **Dr. Sanjeev P Kaulgud**, **Dr. Mrutyunjaya MS** and also the department Project Coordinators. **Mr Zia Ur Rahman**, **Mr Peniel**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project

Aditya Pratap Singh

Aditya Mishra

Rajat Saha

LIST OF FIGURES

Sl. No.	Figure Name	Caption	Page No.
1	Figure 1	Gantt Chart	22
2	Figure 2	Home Page.	31
3	Figure 3	Login Page	31
4	Figure 4	Sign Up Page	32
5	Figure 5	Transaction Page	32
6	Figure 6	Fraud Reporting Page	33
7	Figure 7	User Data	33
8	Figure 8	Payment Data	34
9	Figure 9	Reporting Database	34

TABLE OF CONTENTS

Contents

PROJECT REPORT.....	i
CHAPTER-1.....	10
INTRODUCTION	10
CHAPTER-2.....	12
LITERATURE SURVEY.....	12
CHAPTER-3.....	20
RESEARCH GAPS OF EXISTING METHODS	20
3.0.1 Email Filtering:.....	20
3.0.2 Two-Factor Authentication (2FA):.....	20
3.0.3 Web Browser Security Features:	20
3.0.4 Educational Training Programs:.....	20
3.0.5 Blacklists and URL Filtering:.....	20
3.0.6 Behavioral Analysis:	21
3.0.7 DKIM, SPF, and DMARC Email Authentication Protocols:	21
3.0.8 AI and Machine Learning:	21
CHAPTER-4.....	22
PROPOSED METHODOLOGY	22
4.1 Introduction:	22
4.2 Understanding the Menace:	22
4.3 The Anatomy of a Phishing Attack:	22
4.4 Credential Entry:	22
4.5 Exploiting Trust:.....	22
4.6 Financial Transactions:.....	23
4.7 Proposed Methods	23
4.7.1. Entering Account Details:	23
4.7.2. Checking Against Fraudulent Accounts Database:	23
4.7.3. Real-Time Check:	23
4.7.4. Proactive Alert:	23
4.7.5. Alerting You Promptly:.....	23
4.7.6. Defense Against Past Troubles:	24
4.8 Leveraging Machine Learning for Fraud Detection:	24
4.8.1. Super Smart Detective:.....	24
4.8.2 Learning from the Past:	24
4.8.3 Checking Transactions:	24

4.8.4 Spotting Odd Stuff:	
4.8.5 Adapting to New Tricks:	
4.8.6. Always Guarding:	
4.9 Verifying Website Authenticity:	24
4.9.1. Entering a Website:	24
4.9.2. Authenticity Check:	24
4.9.3. Looking at Certificates:	24
4.9.4. Checking Reputation:	24
4.9.5. Other Important Details:	24
4.9.6. Alerting You to Risks:	24
4.9.7. Avoiding Phishing Traps:	25
CHAPTER-5.....	26
OBJECTIVES.....	26
CHAPTER-6.....	27
SYSTEM DESIGN & IMPLEMENTATION	27
The Need for a Smart Defense System Against Phishing:	28
6.3 The Algorithm Comparison Module	29
6.3.1. Data Storage with MongoDB:	29
6.3.2. Backend Development with Node.js and Express.js:	29
6.3.3. Integration of Machine Learning Models:	
6.3.4. Real-time Interaction with React:	29
6.3.5. User Interface with HTML and CSS:	29
6.3.6. Dynamic User Experience with JavaScript:	29
6.3.7. MERN Stack Collaboration:	30
CHAPTER-7.....	31
TIMELINE FOR EXECUTION OF PROJECT.....	31
(GANTT CHART)	31
Figure 1: Gantt Chart	31
CHAPTER-8.....	32
OUTCOMES.....	32
CHAPTER-9.....	34
RESULTS AND DISCUSSIONS	34
CHAPTER-10.....	36
CONCLUSION	36
10.1 Summary of Achievements:	36
10.1.1 Objective Recap:	36
10.1.2 Accomplishments:	36
10.2 Key Findings and Insights:	36

10.2.1 Data Analysis Recap:	36
Summarize the insights gained from analyzing reported fraud accounts, including patterns, common characteristics, and any trends observed.	36
10.2.2 Effectiveness Assessment:	36
10.3 Lessons Learned and Recommendations:	36
10.3.1 Lessons Learned:.....	36
10.3.2 Recommendations for Improvement:.....	37
10.4 Impact and Future Prospects:	37
10.4.1 Impact Assessment:.....	37
10.4.2 Future Directions:.....	37
4.5 Conclusion Statement:.....	37
Closing Remarks:	37
Final Thoughts:	37
REFERENCES	38
APPENDIX-A.....	
SCREENSHOTS.....	39

CHAPTER-1

INTRODUCTION

1.1.1 Aim of the Project

The primary aim of this project is to fortify the security infrastructure of net banking and mobile wallet platforms by developing a comprehensive defense 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 defense against phishing attacks within online financial ecosystems.

1.2 Scope of the Project

The project's scope is expansive, encompassing a holistic approach to counter the pervasive threat of phishing attacks within the realms of net banking and mobile wallet platforms. It involves several key focal points, starting with the development and deployment of a sophisticated system dedicated to swiftly identifying and thwarting real-time phishing attempts. Additionally, the scope entails refining algorithms to minimize false positives, ensuring the accurate detection of threats while avoiding the misidentification of legitimate communications.

User education is another pivotal aspect, necessitating the creation of an extensive educational program. This program aims to enlighten users about the risks posed by phishing attacks and empower them with the knowledge and skills to discern and appropriately respond to potential threats. The project also emphasizes seamless integration with existing security frameworks, fostering compatibility without compromising user experience.

To validate the efficacy of the proposed system, comprehensive real-world testing against diverse phishing scenarios is included within the project's purview. This validation process encompasses various metrics, including reaction times, false positive rates, and overall

detection accuracy, ensuring the system's reliability in practical settings.

Furthermore, the project endeavors to craft a system adaptable to evolving phishing tactics, maintaining its effectiveness over time. Scalability and compliance with data protection legislation are integral components, ensuring the system's ability to handle increased email traffic while adhering to legal standards.

Extensive documentation will facilitate knowledge transfer, system upkeep, and future enhancements, complemented by collaborative efforts with industry experts to stay abreast of emerging threats and industry best practices. In essence, the project's scope is far-reaching, aiming to fortify the security infrastructure of net banking and mobile wallet platforms through a comprehensive blend of cutting-edge technology and user-focused education, thereby establishing a robust defense against phishing attacks.

1.3 Sub topic-3

- False Positive Reduction Module:
- User Education and Awareness Module:
- Integration with Security Frameworks Module:
- Real-world Testing and Validation Module:
- Dynamic Adaptability Module:
- User Feedback and Enhancement Module:
- Compliance and Scalability Module:
- Documentation and Knowledge Transfer Module:

CHAPTER-2

LITERATURE SURVEY

1.) As a part of survey on the genre of phishing attacks, Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz khan submitted a research paper entitled "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy". The study investigates that With the substantial expansion of internet operations, individuals are increasingly refraining from sharing their personal information online. Consequently, a vast amount of private data and financial transactions are becoming susceptible to cybercriminals. Phishing stands out as a highly effective form of cybercrime, enabling perpetrators to deceive users and pilfer crucial information. Since the inaugural reported phishing attack in 1990, it has evolved into a more sophisticated attack vector, now being recognized as one of the most prevalent manifestations of fraudulent activity on the Internet. The ramifications of phishing attacks can result in significant losses for victims, encompassing sensitive information compromise, identity theft, and the exposure of corporate and government secrets. This composition endeavors to assess these attacks by examining the current state of phishing and scrutinizing prevalent phishing methodologies. Previous studies have categorized phishing attacks based on rudimentary mechanisms, often overlooking the comprehensive end-to-end lifecycle of phishing. To address this gap, this composition proposes a meticulous deconstruction of phishing, encompassing attack phases, perpetrator types, vulnerabilities, pitfalls, targets, attack mediums, and techniques. This detailed deconstruction aims to provide a comprehensive understanding of the entire lifecycle of a phishing attack, enhancing awareness of the evolving methods employed. Furthermore, it aids in the development of a holistic anti-phishing system. The composition also explores preventative countermeasures while introducing novel strategies to mitigate the risks associated with phishing attacks.

2.) Muhammad Adil and Rahim Khan presented a study titled "Preventive Techniques of Phishing Attacks in Networks," emphasizing the pervasive use of the internet in the current era of information technology, deeply ingrained in daily life activities. The internet serves various purposes, including social media platforms like Facebook, WhatsApp, and Messenger, as well as online applications such as e-counseling, e-banking, online businesses, website advertisements, e-hunting platforms, and e-doctor services for appointments and opinions. Despite its convenience and accessibility, the widespread utilization of internet technology

exposes it to numerous security threats.

A particularly significant threat associated with this technology, or specific applications, is the "Phishing attack," employed by attackers to compromise network security. Phishing attacks involve deceptive emails, fraudulent websites, and fake applications designed to steal user credentials or compromise security. This paper provides a comprehensive overview of various phishing attacks, delving into their background knowledge and exploring solutions proposed in the literature. Various techniques such as anti-phishing measures, honeypots, firewalls, and the implementation of intrusion detection systems (IDS) and intrusion detection and prevention systems (IPS) in networks are discussed to facilitate authentic traffic in operational networks. Additionally, the study incorporates an end-user awareness campaign aimed at educating and training employees to minimize the likelihood of phishing attacks. The analysis of the results obtained from this survey indicates the effectiveness of the implemented strategies in addressing the a forementioned security issues, showcasing positive outcomes in combating phishing attacks.

3.) Kesniia Perova, Jari Porras, Sola Oyedeji, Bilal Naqvi, Imran Makhdoom, and Ali Farooq authored an article titled "Mitigation Strategies against Phishing Attacks," highlighting the prevalence of phishing attacks as one of the most widely employed mechanisms by attackers. Successful phishing attacks can lead to various adverse outcomes, including but not limited to financial losses, damage to reputation, and identity theft. The article undertakes a systematic literature review, examining 248 articles from the inception of 2018 to March 2023 from major digital libraries. The primary objectives of the review are as follows: (1) to identify existing mitigation strategies against phishing attacks and explore the underlying technologies integral to these strategies; (2) to assess the most commonly considered phishing vectors in the formulation of mitigation strategies; (3) to outline anti-phishing guidelines and recommendations tailored for both organizations and end-users; and (4) to pinpoint gaps and unresolved issues within the current state of the art. The paper emphasizes the necessity of incorporating the capabilities of human users into the design and development of mitigation strategies, asserting that solely relying on technology-centric solutions is insufficient to effectively address the challenges posed by phishing attacks. 4.) The paper titled "Human Factors in Phishing Attacks" was authored by Giuseppe Desolda, Lauren S. Ferro, Andrea MArrella, Tiziana Catarci, this study provides the information that Phishing attacks are among the most prevalent attack mechanisms employed by attackers. The consequences of successful phishing include (and are not limited to) financial losses, impact on reputation, and identity

theft. The paper presents a systematic literature review featuring 248 articles (from the beginning of 2018 until March 2023) across the main digital libraries to identify, (1) the existing mitigation strategies against phishing attacks, and the underlying technologies considered in the development of these strategies; (2) the most considered phishing vectors in the development of the mitigation strategies; (3) anti-phishing guidelines and recommendations for organizations and end-users respectively; and (4) gaps and open issues that exist in the state of the art. The paper advocates for the need to consider the abilities of human users during the design and development of the mitigation strategies as only technology-centric solutions will not suffice to cater to the challenges posed by phishing attacks.

5.) The article titled "An Effective and Secure Mechanism for Phishing Attacks Using a Machine Learning Approach," authored by Gori Mohamed, J. Visumathi, Miroslav Mahdal, Jose Anand, and Muniyandy Elangovan, delves into the significant issue of phishing, a widespread criminal activity involving the illicit theft of sensitive user data. Typically, phishing websites target individuals, organizations, cloud storage sites, and government websites. Many internet users remain unaware of the lurking threat of phishing attacks while navigating online. Previous phishing approaches have often fallen short in addressing the challenges posed by email attacks, leading to the adoption of hardware-based phishing methods to counter software attacks. Acknowledging the escalating nature of these problems, the proposed work concentrates on a three-stage phishing series attack aimed at precisely identifying issues in a content-based manner, serving as an effective phishing attack mechanism. The approach incorporates three input values—uniform resource locators, traffic, and web content—based on features distinctive to phishing attacks and non-phishing website techniques. To validate the proposed phishing attack mechanism, a dataset is compiled from recent phishing cases. The study reveals that real phishing cases contribute to higher accuracy in both zero-day phishing attacks and phishing attack detection. Employing three different classifiers, namely NN, SVM, and RF, the study attains classification accuracies of 95.18%, 85.45%, and 78.89%, respectively, in detecting phishing. The findings underscore the efficacy of a machine learning approach in effectively identifying and mitigating phishing attacks. The study titled "STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS" highlights the internet as a significant platform for communication among the general public. Individuals with malicious intent have devised methods to illicitly obtain personal information without direct contact and with minimal risk of detection, known as Phishing. This practice

poses a substantial threat to the e-commerce industry, not only eroding customer trust but also inflicting significant economic losses on electronic service providers. Therefore, understanding phishing becomes crucial. This paper aims to raise awareness regarding phishing attacks and the available anti-phishing tools.

7.) In an article authored by Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage, and Md. Ali Babar, titled "Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors," the authors address the persistent challenge of individuals being deceived by phishing emails, despite the presence of advanced detection systems and awareness programs. To gain deeper insights into why phishing email attacks remain effective and how to enhance mitigation strategies, the authors conducted an empirical study focusing on understanding people's cognitive processes while interacting with their emails. The study utilized a scenario-based role-play method, employing a "think aloud" approach along with follow-up interviews to gather data from 19 participants. The experiment unfolded within a simulated web email client, incorporating both genuine and phishing emails tailored to specific scenarios. The analysis of the collected data led to the identification of eleven factors influencing individuals' decision-making processes in response to both phishing and legitimate emails. Building on the findings from the user study, the authors present novel insights into inherent flaws in general email decision-making behaviors that render individuals susceptible to phishing attacks.

8.) The article titled "How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society," authored by Flona Carroll, John Ayooluwa Adejobi, and Rexa Montasari, addresses the escalating threat of phishing attacks. The significant shift in our lifestyles, education, and work dynamics due to the COVID-19 pandemic, leading to a surge in online activities, has given rise to new cybersecurity challenges. The transition to remote work has particularly amplified the volume of phishing emails targeting employees, as evidenced by the 2020 Phishing Attack Landscape Report, which reported a marked increase in attempted phishing attacks. This paper delves into the evolution of phishing email attacks, exploring their current characteristics and the growing challenges exacerbated by the pandemic. The study conducted for this paper involved presenting test participants with five distinct categories of emails, encompassing both phishing and non-phishing scenarios. The study findings reveal a notable difficulty among participants in detecting modern phishing email attacks. While participants demonstrated vigilance towards older phishing tactics like spelling mistakes and requests for sensitive

information, they struggled to identify contemporary phishing attempts. Furthermore, the research highlights that individuals lack confidence and express concerns and dissatisfaction with the existing technologies designed to protect against phishing emails. The prevailing sentiment of distrust underscores the severity of the phishing attack situation and underscores the vulnerability of society in the face of evolving cyber threats.

9.) The authors Asif Ejaz, Adnan Noor Mian, and Sanaullah Manzoor delve into the subject of "Life-long Phishing Attack Detection using Continual Learning," elucidating phishing as a form of identity theft employing social engineering techniques to extract confidential data from unsuspecting users. Phishers commonly employ tactics to lure victims into clicking malicious URLs, leading them to deceptive websites. Numerous individuals fall victim to phishing attacks daily, resulting in the compromise of credentials and digital assets. This study focuses on showcasing how the effectiveness of traditional machine learning (ML)-based phishing detection models diminishes over time. The deterioration is attributed to significant shifts in feature distributions brought about by the emergence of new phishing techniques and technological advancements. The paper introduces continual learning (CL) techniques as a solution to sustain optimal phishing detection performance over time. To illustrate this phenomenon, the authors collect phishing and benign samples spanning three consecutive years from 2018 to 2020, segregating them into six datasets for evaluating both traditional ML and proposed CL algorithms. A vanilla neural network (VNN) model is trained in a continual learning fashion, utilizing deep feature embedding of HTML contents. The study compares the performance of the proposed CL algorithms with the VNN model trained from scratch and through transfer learning (TL). The results demonstrate that CL algorithms effectively maintain accuracy over time, experiencing only a tolerable deterioration of 2.45%. In contrast, models based on VNN and TL exhibit more substantial performance declines, surpassing 20.65% and 8%, respectively.

10.) As part of a survey on phishing attack genres, Ritika Arora, Sharad, Sanjeet Singh, Narendra Kumar, and A.K. Saini submitted a research paper titled "Phishing Attacks Prevention and Detection Techniques." The research delves into the realm of online security attacks, specifically phishing attacks, which involve the illicit acquisition of sensitive information. Perpetrators craft precise replicas of existing web content to deceive users and gain access to their personal financial data, online banking passwords, and ATM card numbers. The escalating sophistication of phishing attacks necessitates effective detection methods. Phishers strategically target websites that closely resemble authentic ones, impacting

various sectors such as e-commerce and digital marketing through the dissemination of spam emails and the creation of imitation websites. The study advocates for preventive measures involving the examination of properties like dataset characteristics, feature extraction, and detection algorithms, employing performance evaluation metrics in conjunction with detection techniques. The primary objective is to propose a robust framework for detecting phishing websites with high accuracy in minimal time. The paper focuses on a comparative analysis of various phishing detection mechanisms and explores diverse countermeasures to enhance cybersecurity defenses against these threats.

Title of Paper	Author(s)	Year	Method Used	Result Obtained	Drawbacks of the Method
Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz khan	2021	Survey and Analysis	Identification and analysis of common phishing techniques, such as email spoofing, deceptive websites, or social engineering tactics used by attackers.	Limited Real-World Simulation
Preventive Techniques of Phishing Attacks in Networks	Muhammad Adil and Rahim Khan	2020	URL Analysis	Effectiveness of Training and Awareness Programs	Lack of comprehensive data analysis or case studies from real-world phishing incidents could limit the

					paper's practical relevance and applicability.
Mitigation strategies against the phishing attacks	Kesniia Perova, Jari porras, Sola Oyedeji, Bilal Naqvi, Imran Makhdoom and Ali Farooq	2022	Email Content Analysis	Identification of Phishing Trend	Limited Consideration of Human Factors
Human Factors in Phishing Attacks	Giuseppe Desolda, Lauren S. Ferro, Andrea MArrella	2021	Interviews and Focus Groups	Behavioural Patterns of The Users	Dynamic Nature of Phishing Attacks
An Effective and Secure Mechanism for Phishing Attacks Using a Machine Learning Approach	Gori mohamed, J. Visumathi, Miroslav Mahdal, Jose Anand and Muniyandy Elangovan	2022	Dataset Collection and Preprocessing	Accuracy of Phishing Detection	Lack of Explainability
Study on Phishing Attacks and Antiphishing Tools	Zwalowski Mukherjee And Zaid Mohammad Kasba	2016	Data Collection and Analysis	Ethical Implications and Privacy Concerns	Data Bias and Imbalance

Falling for Phishing: An Empirical Investigation into People's Email Response. Behaviours	Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage and Md. Ali Babar	2019	Experimental Studies	Factors Influencing Susceptibility	Ethical Concerns
How Good Are We at Detecting a Phishing Attack?	Flona Carroll, John Ayooluwa Adejobi and Rexa Montasari	2022	Experimental Simulations	Identification of Phishing Trend	Dynamic Nature of Phishing Attacks
Life-long phishing attack detection using continual learning	Asif Ejaz, Adnan Noor Mian and Sanaullah Manzoor	2023	Machine Learning	Detection of Suspicious websites	Not Accurate
Phishing Attacks Prevention and Detection Techniques	Ritika Arora, Sharad, Sanjeet Singh, Narendra Kumar and A.K. Saini	2020	Data Collection and Analysis	Effectiveness of Anti-Phishing Tools	Imbalanced or Biased Data

CHAPTER-3

RESEARCH GAPS OF EXISTING METHODS

Several existing methods aim to mitigate phishing attacks, each with its strengths and drawbacks. Here are some common methods:

3.0.1 Email Filtering:

Method: Use of email filtering systems to identify and block phishing emails based on known patterns and characteristics.

Drawbacks:

Limited effectiveness against sophisticated phishing attacks that mimic legitimate communication. False positives can lead to blocking legitimate emails, causing inconvenience.

3.0.2 Two-Factor Authentication (2FA):

Method: Requires users to provide a secondary form of identification in addition to their password.

Drawbacks:

The OTP do not contain the Proper Warning, some users find 2FA processes inconvenient or confusing.

3.0.3 Web Browser Security Features:

Method: Browsers often have built-in security features that identify and warn users about potentially malicious websites.

Drawbacks:

May not detect newly created phishing sites immediately, Users may ignore or not understand warning messages.

3.0.4 Educational Training Programs:

Method: Conducting educational programs to increase user awareness about phishing techniques and how to identify them.

Drawbacks:

Effectiveness depends on user engagement and retention of the information. Some users may still fall victim to phishing attacks due to evolving tactics.

3.0.5 Blacklists and URL Filtering:

Method: Maintaining databases of known phishing URLs and blocking access to these sites.

Drawbacks:

Phishers can quickly create new URLs to bypass blacklists. Legitimate sites may be mistakenly added to blacklists.

3.0.6 Behavioral Analysis:

Method: Analyzing user behavior to detect anomalies that may indicate a phishing attempt.

Drawbacks:

False positives can occur if users' behavior changes for legitimate reasons, Initial setup may require significant resources for accurate profiling.

3.0.7 DKIM, SPF, and DMARC Email Authentication Protocols:

Method: Email authentication protocols that verify the authenticity of the sender's domain.

Drawbacks:

Not foolproof; some phishing emails may still pass these checks, Implementation challenges for small businesses and organizations.

3.0.8 AI and Machine Learning:

Method: Using machine learning algorithms to detect patterns indicative of phishing attacks.

Drawbacks:

Requires continuous training to keep up with evolving phishing techniques, May produce false positives or false negatives based on the training data.

CHAPTER-4

PROPOSED METHODOLOGY

4.1 Introduction:

In the rapidly evolving landscape of online financial transactions, the threat of phishing attacks looms large, casting a shadow over the security of card-based and digital wallet transactions. Phishing, a form of cybercrime where attackers masquerade as trustworthy entities to trick individuals into divulging sensitive information, has become a pervasive menace. This introduction delves into the intricacies of phishing attacks, shedding light on their insidious nature and the proposed method aimed at fortifying users against these threats through real-time information and cutting-edge machine learning algorithms.

4.2 Understanding the Menace:

Phishing attacks typically unfold in a series of carefully orchestrated steps, each designed to exploit the trust and vulnerabilities of unsuspecting individuals. The journey begins with deceptive communication, often in the form of seemingly legitimate emails, messages, or websites. These communications, known as phishing lures, lure users into providing confidential information, such as login credentials or financial details. The attackers skillfully mimic trusted entities, ranging from banks to e-commerce platforms, exploiting the familiarity users have with these institutions.

4.3 The Anatomy of a Phishing Attack:

Deceptive Communication:

Phishing attacks initiate with the delivery of deceptive messages, often disguised as urgent alerts or enticing offers. These messages employ social engineering tactics, manipulating emotions like fear or curiosity to prompt users to take immediate action.

4.4 Credential Entry:

Once the user is enticed, the attackers redirect them to fraudulent websites that closely resemble legitimate ones. Unsuspecting users then enter their login credentials, handing over sensitive information directly to the attackers.

4.5 Exploiting Trust:

Phishers capitalize on trust, creating replicas of familiar interfaces to deceive users into believing they are interacting with a legitimate platform. This exploitation of trust makes it challenging for users to discern between authentic and fraudulent sites.

4.6 Financial Transactions:

With login credentials in hand, the attackers gain unauthorized access to financial accounts. This stage often involves fraudulent transactions, unauthorized fund transfers, or the pilfering of sensitive financial information stored in digital wallets.

4.7 Proposed Methods

Empowering Users with Real-Time Information:

Empowering users with real-time information involves creating a smart system that checks entered account details against a big list of known fraudulent accounts. Let's break down how this works:

4.7.1. Entering Account Details:

When you type in your account number during a transaction, our system gets to work.

4.7.2. Checking Against Fraudulent Accounts Database:

We have a big list, like a digital blacklist, that contains account numbers reported for being involved in fraud before.

4.7.3. Real-Time Check:

Our system instantly compares the entered account number with this list in real-time, like a quick background check.

4.7.4. Proactive Alert:

If there's a match, meaning the account number you entered has been linked to fraud in the past, the system doesn't just stay silent.

4.7.5. Alerting You Promptly:

It actively tells you right away, sending you a notification or a message. This is like your digital guard saying, "Hey, be careful! This account has had some trouble in the past."

4.7.6. Defence Against Past Troubles:

Essentially, this is a way to defend you before anything goes wrong. It's like having a friend warn you about a potentially risky situation before you step into it.

By having this real-time account check, we're putting a shield around your transactions, making sure you have the latest information about the safety of the account you're dealing with. It's all about being proactive and keeping you informed to prevent any unwanted surprises.

4.8 Verifying Website Authenticity:

Making sure a website is the real deal is like double-checking before entering a new place. Here's how we do it, step by step:

4.8.1. Entering a Website:

When you go to a website, especially during login, our system gets to work.

4.8.2. Authenticity Check:

We have this nifty system that checks if the website is genuine or not. It's like having a digital bouncer making sure you're entering a safe place.

4.8.3. Looking at Certificates:

One of the things our system does is check for SSL certificates. It's a bit like looking at the ID of the website to confirm it's the real deal.

4.8.4. Checking Reputation:

Our system also looks at the website's reputation. It's like asking around to see if people know and trust this place. If the website has a good reputation, great! If not, our system gives a heads up.

4.8.5. Other Important Details:

There are a few other things our system looks at, like how the website behaves and if it's following the usual rules. It's like making sure everything adds up and feels right.

4.8.6. Alerting You to Risks:

If our system spots anything fishy – maybe a fake certificate or a bad reputation – it doesn't keep quiet. It sends you a warning, like a friend saying, "Hold on, this place might not be safe."

4.8.7. Avoiding Phishing Traps:

By doing all this, our goal is to keep you from falling into any phishing traps. It's like having a guide that ensures you only enter secure websites, protecting you from potential risks.

In a nutshell, by checking a website's authenticity, we're making sure you're entering a safe digital space. It's all about having your back and making sure you're not walking into any online tricks or traps.

CHAPTER-5

OBJECTIVES

1.) Enhance User Security:

The principal objective of this project is to enhance user security in the online/mobile wallet and net banking domains substantially. This will be achieved through the development of a system that proficiently addresses and mitigates the threats posed by phishing attacks.

2.) Empower Vulnerable User Groups:

Focus on designing user-friendly solutions that cater to the unique needs of vulnerable groups, including the elderly, individuals from rural areas, non-technical users, and children, ensuring they can safely engage in digital financial transactions.

3.) Educate and Raise Awareness:

Develop educational materials and resources that teach users to recognize and respond to phishing attempts. By raising awareness and providing accessible educational content, the project aims to reduce the success rate of phishing attacks.

4.) Technology-Enhanced Security:

Implement cutting-edge technology, including user-centric authentication methods, phishing detection algorithms, and user-friendly alerts, to create a multi-layered security system that combats phishing effectively without overwhelming users with technical details.

5.) Multilingual and Inclusive Approach:

The project will support multiple local languages and ensure accessibility for users from diverse backgrounds, fostering a safer online financial environment for everyone.

In summary, the project seeks to create a secure, user-centric, and inclusive ecosystem for online/mobile wallets and net banking, mitigating the threat of phishing attacks and promoting a safer digital financial experience.

CHAPTER-6

SYSTEM DESIGN & IMPLEMENTATION

6.1 Introduction:

In today's digital age, where everything from buying groceries to transferring money happens with just a few clicks, the convenience of online transactions has become a part of our daily lives. However, this convenience also brings along challenges, and one major challenge is the threat of scams, especially through a sneaky technique called phishing. Picture this: you receive an email or a message that looks like it's from your bank, asking you to urgently confirm your account details by clicking on a link. It seems normal, but in reality, it's a trap set by cyber tricksters to steal your personal information. This kind of trickery is just one example of the many phishing scams happening today, and it's important to understand how these scams work and, more importantly, how we can protect ourselves from falling into their digital traps.

6.2 Phishing in Today's World:

Phishing scams have become like modern-day traps set by online tricksters, and they come in many forms. Imagine getting an email saying you've won a prize, and all you need to do is provide your bank details to claim it. Or a message appearing on your phone, pretending to be your favourite shopping app, asking for your login credentials. These scams are like digital wolves in sheep's clothing, pretending to be something they're not to get what they want – your personal information. As technology advances, so do these scams, becoming more sophisticated and harder to spot. They prey on our trust and often catch us off guard, leading to financial losses and identity theft.

So, in the midst of this digital jungle, how do we protect ourselves? This is where a smart and user-friendly approach to online transactions comes into play. By creating systems that actively watch out for potential scams, verify information in real-time, and keep users in the loop about every transaction, we build a shield against these cunning phishing attempts. The goal is to make our online experiences not only convenient but also secure, ensuring that we can navigate the digital world without constantly looking over our shoulders for lurking cyber threats.

The Need for a Smart Defense System Against Phishing:

In the bustling world of online transactions, where the click of a button can swiftly move money or purchase goods, the convenience we enjoy comes hand in hand with the lurking threat of phishing scams. These scams, cleverly disguised as trustworthy entities, aim to trick individuals into revealing sensitive information, leading to financial losses and identity theft. Today's phishing tactics have evolved to become more sophisticated, often catching even tech-savvy individuals off guard. This escalating challenge prompts the critical question: Why do we need a smart defence system, and how can it effectively tackle the current phishing issue?

Consider the common scenario of receiving an urgent email or message purportedly from a bank, requesting immediate confirmation of account details. Unbeknownst to the recipient, this seemingly innocuous communication is a phishing attempt, aiming to harvest sensitive information for malicious purposes. Similarly, deceptive messages claiming prize winnings or mimicking trusted apps coerce users into sharing their credentials, falling victim to these digital wolves in sheep's clothing. The prevalence of such scams underscores the urgent need for a proactive defence mechanism.

Enter the proposed smart defence system, designed to revolutionize our approach to online transactions. This system recognizes the intricate nature of phishing scams and introduces a multi-layered strategy to counteract them. By incorporating real-time checks during the payment process, users are empowered with instant feedback on the accuracy of entered details. Imagine receiving a prompt warning if the recipient's account has been reported for fraudulent activities – a crucial shield against potential scams. Furthermore, the transparent OTP confirmation process, explicitly stating the deduction amount and remaining balance, acts as a powerful deterrent, making it harder for scammers to manipulate users into authorizing fraudulent transactions.

The need for such a system goes beyond mere convenience; it is a response to the evolving tactics of cyber tricksters. It's about creating a secure digital environment where users can navigate the online landscape with confidence. By actively addressing the vulnerabilities that phishing exploits, this system not only safeguards individuals from financial harm but also disrupts the very foundation upon which these scams thrive. In a world where every click matters, the smart defence system emerges as a beacon of protection, ensuring that the convenience of online transactions is not overshadowed by the ever-present threat of phishing.

scams. It's a step towards a future where users can enjoy the benefits of digital transactions without constantly worrying about falling prey to the cunning traps set by cyber adversaries.

6.3 The Algorithm Comparison Module

Is the core of our security enhancement project, employing a combination of machine learning models and the MENN stack (MongoDB, Express.js, NextJs, Node.js) along with HTML, CSS, and JavaScript to create a robust and user-friendly solution.

6.3.1. Data Storage with MongoDB:

We kick off our project by utilizing MongoDB, a NoSQL database, to efficiently store and manage data related to phishing indicators, historical scam patterns, and the performance metrics of various machine learning models.

6.3.2. Backend Development with Node.js and Express.js:

Node.js and Express.js form the backbone of our server-side development. They enable us to build a fast and scalable backend, handling data processing, algorithmic computations, and communication with the database.

6.3.3. Real-time Interaction with NextJs:

NextJs, a JavaScript library for building user interfaces, is employed for the frontend development. The Algorithm Comparison Module is visually presented through a NextJs-based user interface, providing an intuitive and responsive experience for users interacting with the security features in real-time.

6.3.4. User Interface with HTML and CSS:

HTML and CSS contribute to the creation of a user-friendly interface. HTML structures the content, while CSS styles it, ensuring a clean and visually appealing presentation. The interface allows users to compare the performance of different algorithms and make informed decisions based on the presented data.

6.3.5. Dynamic User Experience with JavaScript:

JavaScript, both on the frontend and backend, enhances the dynamic aspects of our project. On the frontend, it enables real-time updates and interactions, while on the backend, it facilitates algorithmic computations, ensuring that users receive up-to-date and accurate information regarding the effectiveness of each algorithm.

6.3.6. MENN Stack Collaboration:

The MENN stack collaborates seamlessly, with the frontend (NextJs) communicating with the backend (Node.js and Express.js), which in turn interacts with the MongoDB database. This full-stack architecture ensures smooth data flow and real-time responsiveness, essential for an effective Algorithm Comparison Module.

In essence, our project takes advantage of the MENN stack, HTML, CSS, and JavaScript to create a comprehensive Algorithm Comparison Module. This module serves as a pivotal component in our cybersecurity endeavour, allowing users to assess, compare, and select the most effective machine learning algorithms in the ongoing battle against phishing threats. The combination of a powerful backend, an interactive frontend, and machine learning prowess makes our solution both sophisticated and user-centric, contributing to a safer online environment.

CHAPTER-7

TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)

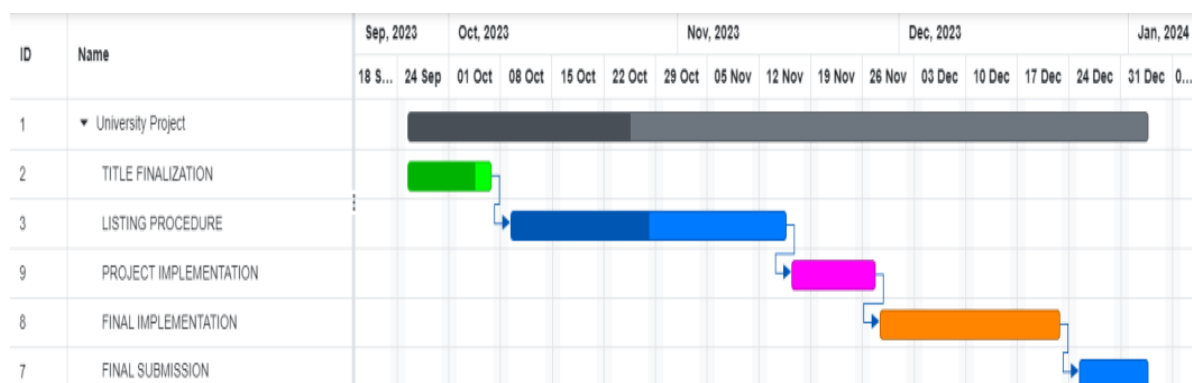


Figure 1: Gantt Chart

CHAPTER-8

OUTCOMES

1. Functional Website:

The primary outcome is the successful creation of a fully functional website that serves its intended purpose. This includes user authentication, reporting fraud accounts, and other features you implement.

2. Enhanced Security Measures:

Implementing a reporting system for fraud accounts indicates a commitment to user safety and security. This can lead to increased trust among users and a more secure environment for your platform.

3. Improved User Experience:

Providing users with a platform where they can report fraudulent accounts can enhance their experience by empowering them to contribute to the safety and integrity of the community.

4. Data Collection and Analysis:

As users report fraudulent accounts, you'll accumulate valuable data. Analyzing this data can help identify patterns of fraudulent behavior, enabling you to take proactive measures to prevent future occurrences.

5. Learning and Development:

Building this project will provide you and your team with valuable experience in using technologies like Next.js, Node.js, Express, MongoDB, and integrating them to create a functional web application. This can contribute to the skill development of your team members.

6. Community Engagement:

Encouraging users to report fraud accounts fosters a sense of community engagement and responsibility, contributing to a healthier and safer online environment.

7. Potential Business Impact:

If this project is part of a larger business strategy, the successful implementation of such security features can attract more users, improve the reputation of your platform, and potentially contribute to business growth and success.

8. Scalability and Future Improvements:

Building this initial version of your platform provides a foundation for future enhancements. You can further develop and scale the platform based on user feedback, technological advancements, and changing requirements.

9. Compliance and Trust:

If your platform handles sensitive data or operates in regulated industries, implementing secure reporting systems can help meet compliance standards, enhancing trust among users and stakeholders.

CHAPTER-9

RESULTS AND DISCUSSIONS

Results:

1. Functionality Evaluation:

Describe the functionality and usability of the reporting system implemented. Present details about the user interface, how users interact with the system, and how reports are submitted.

2. Data Collection and Analysis:

Discuss the data collected through reported fraud accounts.

Highlight patterns, trends, or common characteristics observed in reported fraudulent activities.

3. System Performance:

Present any performance metrics related to the system, such as response times for reporting, system uptime, or any bottlenecks encountered.

4. User Engagement and Participation:

Discuss the level of user engagement and participation in reporting fraudulent accounts.

Analyze the frequency and consistency of user submissions.

5. Case Studies or Examples:

Provide case studies or specific examples of how reported fraudulent activities were handled or resolved by the system.

Discussions:

1. Impact Assessment:

Evaluate the impact of the implemented reporting system on reducing fraud or enhancing security within the platform.

Discuss whether the system met its initial goals and objectives.

2. Effectiveness and Challenges:

Analyze the effectiveness of the reporting system in identifying and addressing fraudulent accounts.

Discuss any challenges faced during implementation, including technical, user adoption, or other obstacles.

3. Data Insights and Future Improvements:

Interpret the insights gained from the data collected through reported cases.

Suggest potential improvements or modifications based on the data analysis to enhance the system's effectiveness.

4. User Feedback and Satisfaction:

Include any user feedback or satisfaction surveys related to the reporting system.

Discuss how user feedback might influence future iterations or improvements.

5. Lessons Learned and Recommendations:

Summarize key lessons learned during the project implementation.

Provide recommendations for enhancements, changes, or additional features that could further improve the system's ability to mitigate fraud.

6. Future Prospects and Expansion:

Discuss potential future developments or expansions of the reporting system, considering scalability, additional functionalities, or integration with other security measures.

CHAPTER-10

CONCLUSION

The conclusion of a project summarizes the key findings, outcomes, and insights gained from the implementation of the fraud reporting system in a Next.js and Node.js website using MongoDB. Here's an outline of points that could be included in the conclusion:

10.1 Summary of Achievements:

10.1.1 Objective Recap:

Restate the main objectives and goals of the project, emphasizing the focus on reducing fraud through the implementation of a reporting system.

10.1.2 Accomplishments:

Highlight the achievements and successful implementation of the reporting system, emphasizing its functionalities, user engagement, and the data collected.

10.2 Key Findings and Insights:

10.2.1 Data Analysis Recap:

Summarize the insights gained from analyzing reported fraud accounts, including patterns, common characteristics, and any trends observed.

10.2.2 Effectiveness Assessment:

Evaluate the effectiveness of the reporting system in addressing fraudulent activities based on the collected data and user engagement.

10.3 Learned Lessons and Recommendations:

10.3.1 Lessons Learned:

Discuss lessons learned during the project implementation, including challenges faced, technical insights, and user behavior observations.

10.3.2 Recommendations for Improvement:

Provide actionable recommendations for further enhancements or modifications to the reporting system based on the identified weaknesses or opportunities for improvement.

10.4 Impact and Future Prospects:

10.4.1 Impact Assessment:

Assess the impact of the reporting system on reducing fraud within the platform and improving overall security measures.

10.4.2 Future Directions:

Outline potential future developments or expansions of the reporting system, considering scalability, additional functionalities, or integration with other security measures.

4.5 Conclusion Statement:

Closing Remarks:

Sum up the significance of the project in addressing the issue of fraud, highlighting its contributions to the platform's security and user trust.

Final Thoughts:

Conclude with final thoughts or reflections on the project, expressing the project team's satisfaction with the achieved outcomes and a commitment to continuous improvement.

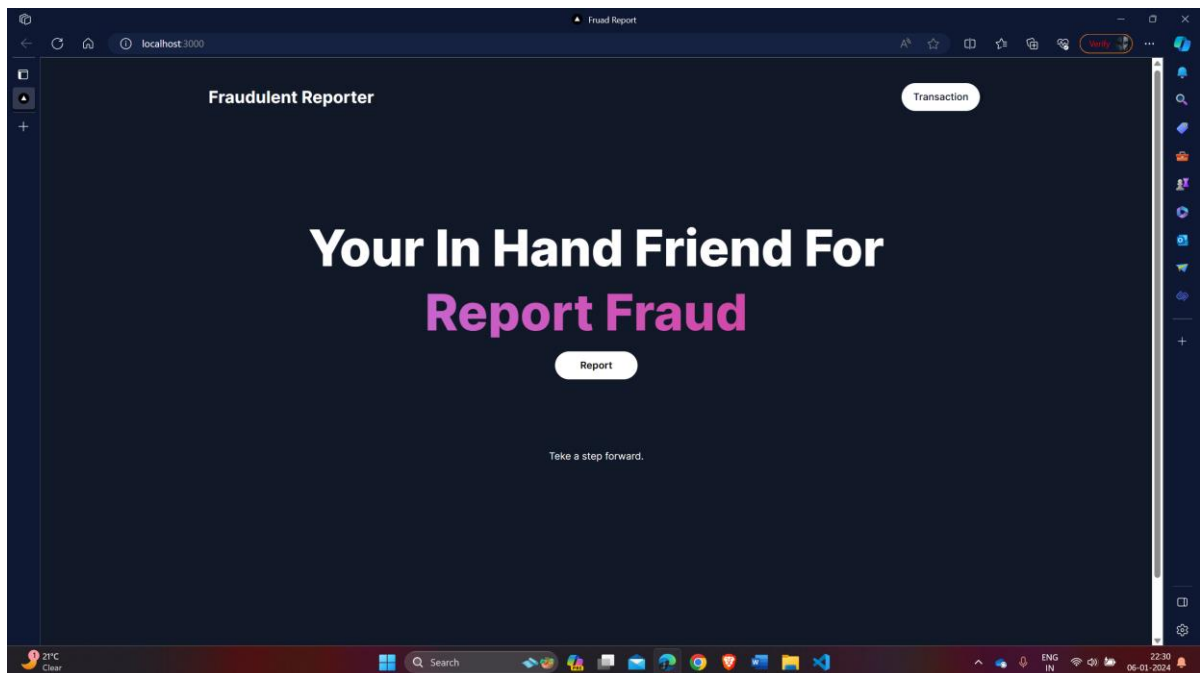
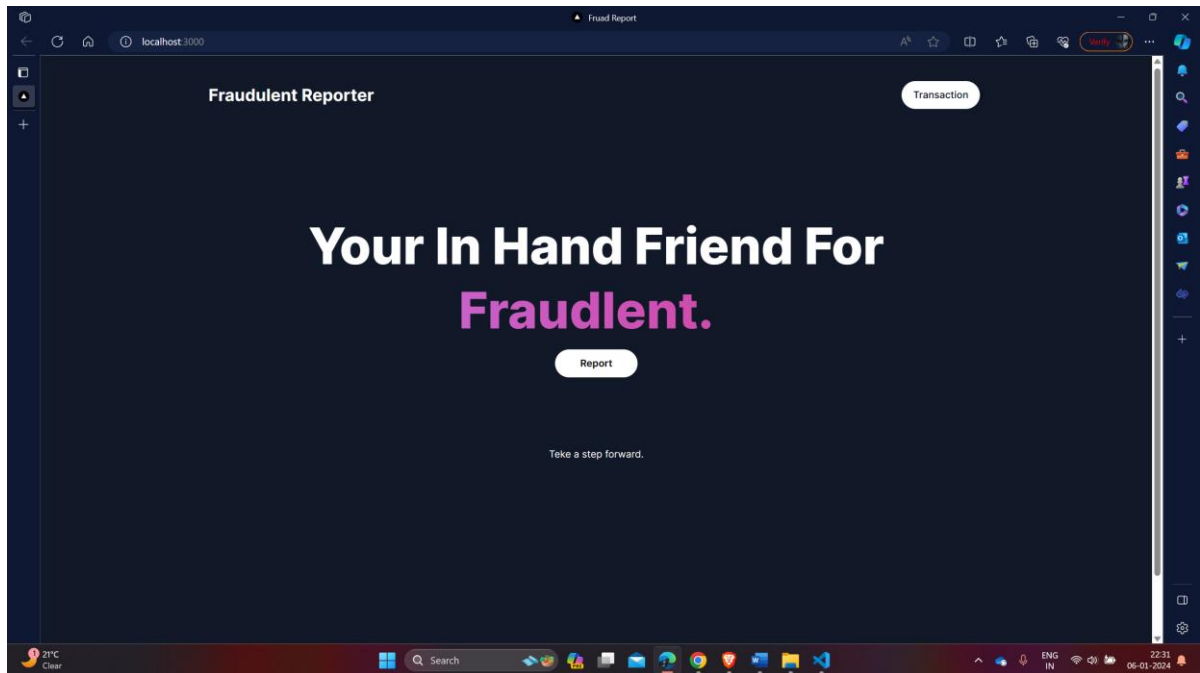
REFERENCES

- <https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>
- https://www.researchgate.net/publication/340507635_Preventive_Techniques_of_Phishing_Attacks_in_Networks
- <https://www.sciencedirect.com/science/article/pii/S0167404823002973>
- <https://dl.acm.org/doi/10.1145/3469886>
- <https://www.mdpi.com/2227-9717/10/7/1356>
- <https://www.irjet.net/archives/V3/i1/IRJET-V3I1121.pdf>
- <https://link.springer.com/article/10.1007/s10586-022-03604-4>
- <https://arxiv.org/ftp/arxiv/papers/2108/2108.04766.pdf>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8864450/>
- <https://www.nature.com/articles/s41598-023-37552-9>
- <https://www.onlinegantt.com/#/gantt>

CODES

- <https://github.com/Aditya-Mishra19/GigPay/tree/main/gigskybackend-main>
- <https://github.com/Aditya-Mishra19/GigPay/tree/main/gigskyfrontend-main>

SCREENSHOTS



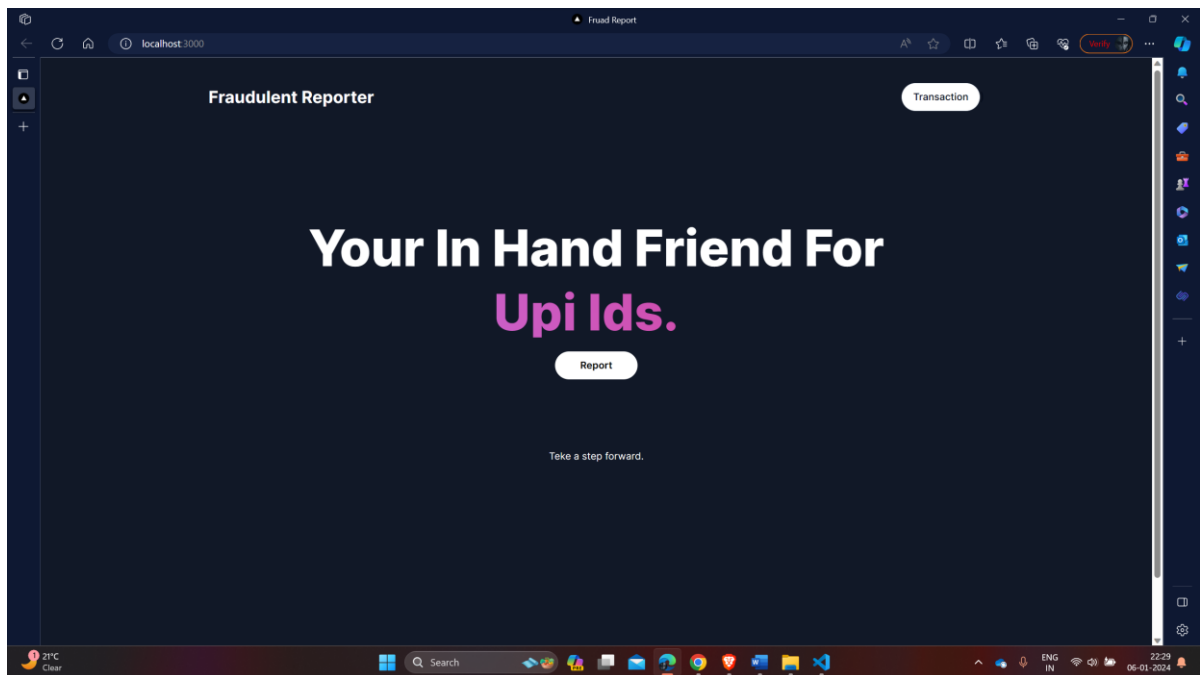


Figure 2: Home Page.

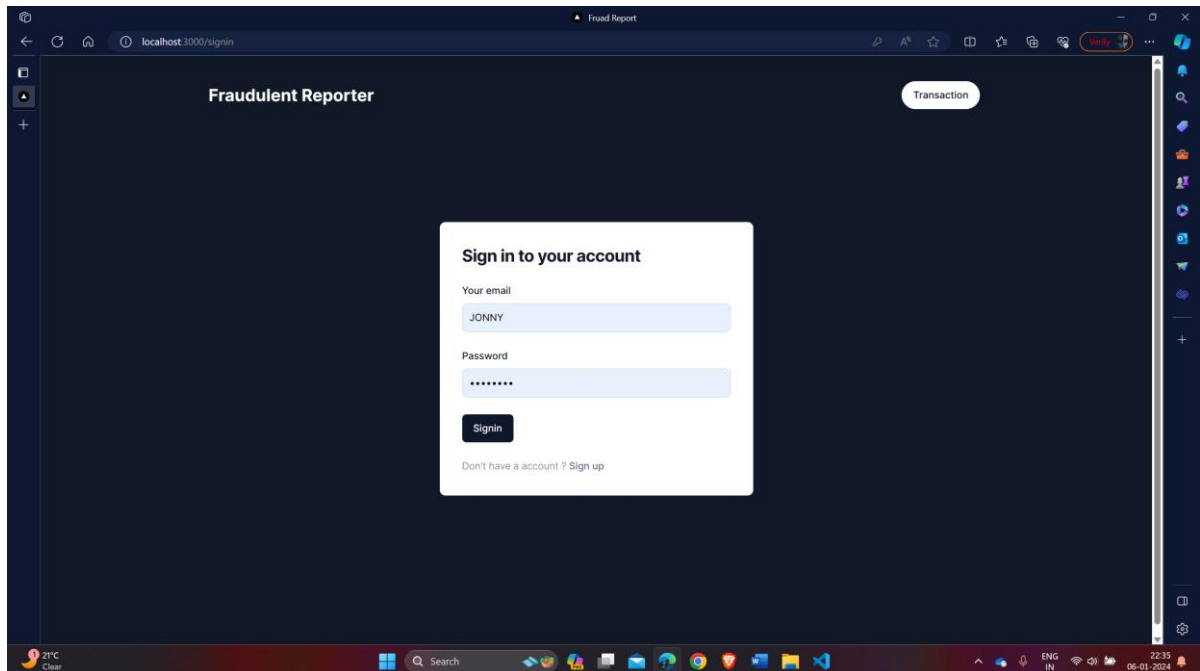


Figure 3: Login Page.

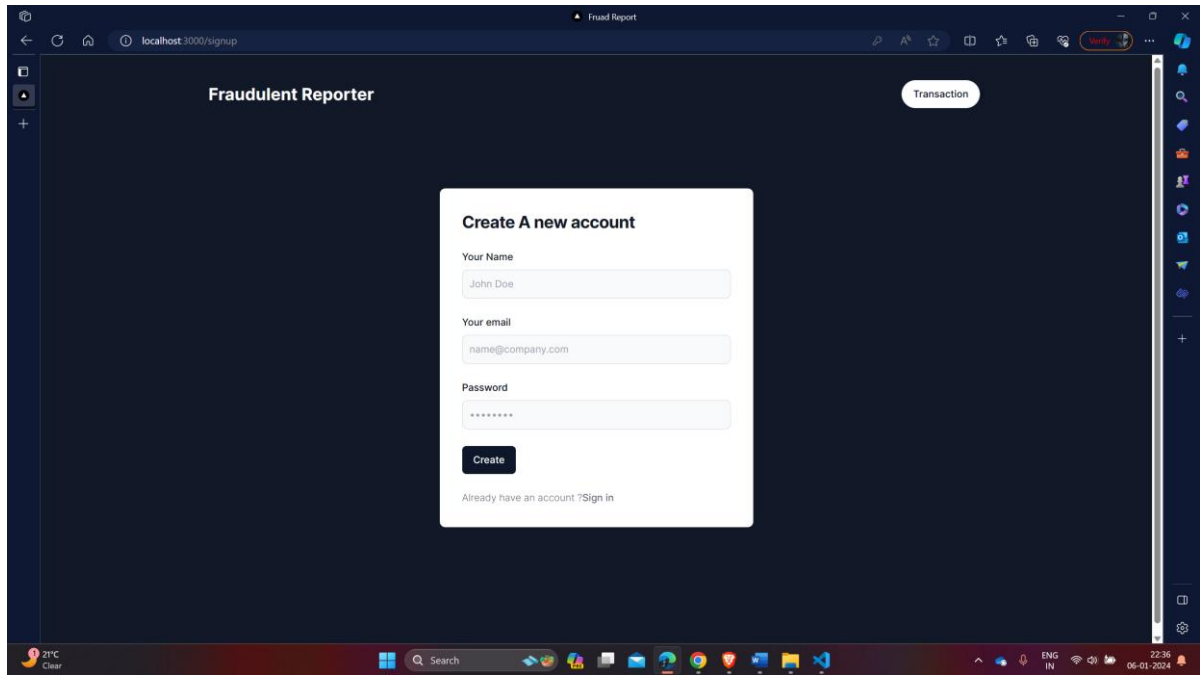


Figure 4: Sign Up Page.

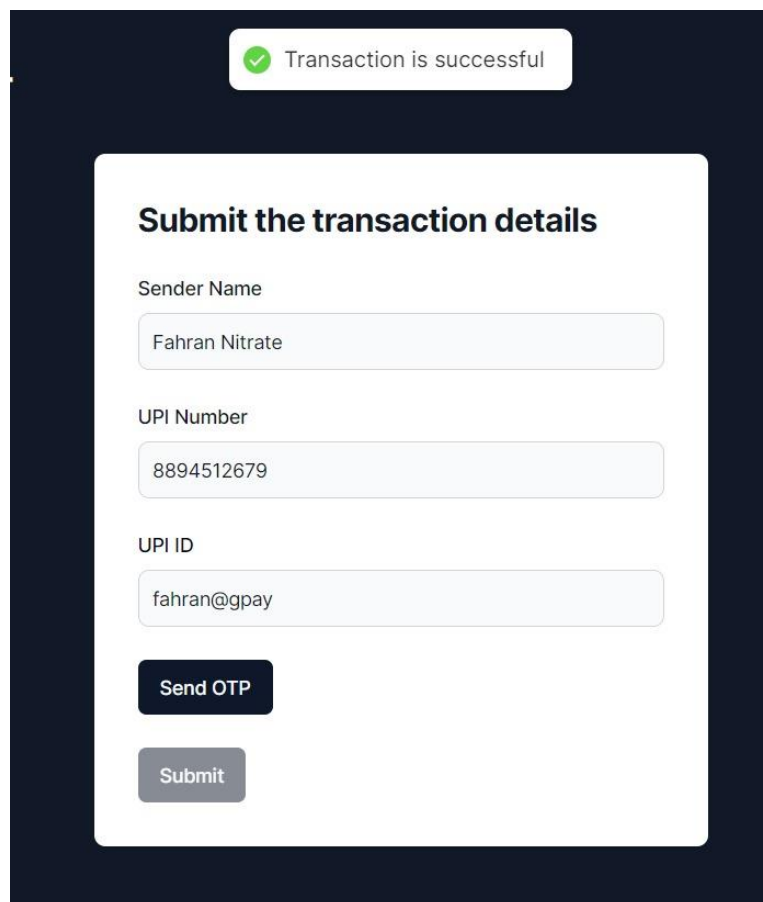



Figure 5: Transaction Page.

 This UPIID is Reported an Fraud

Submit the transaction details

Sender Name

Mishra

UPI Number

884512398

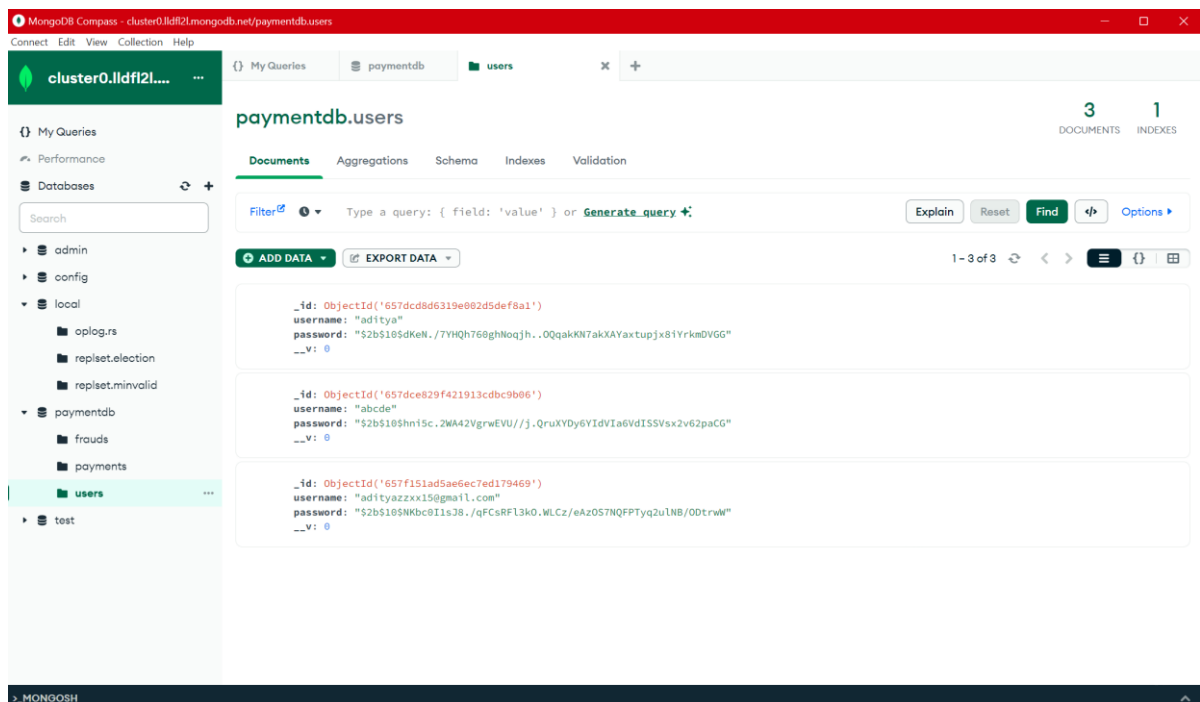
UPI ID

mishra@okicic

Send OTP

Submit

Figure 6: Fraud Reporting Page.



The screenshot shows the MongoDB Compass interface. The left sidebar displays the database structure with 'paymentdb' expanded and 'users' selected. The main panel shows the 'paymentdb.users' collection with 3 documents and 1 index. The 'Documents' tab is active, displaying a list of three user records. Each record contains fields for '_id', 'username', 'password', and 'v'.

_id	username	password	v
ObjectId('657dcd8d6319e002d5def8a1')	aditya	\$2b\$10\$dKcN./7YHQh76ghNoqjh...OqakKN7akXAYaxtupjx81YrkmDVGG	0
ObjectId('657dce829f421913cdbc9b06')	abcde	\$2b\$10\$hn1Sc.2WA42VgrwEVU//j..QruXYDy6YdV1a6VdISSvx2v62paCG	0
ObjectId('657f151ad5ae6ec7ed179469')	adityazxx150gmail.com	\$2b\$10\$Nkbc0I1s38./qFcSRf13k0.WLcz/eAz057NQFPTyq2u1NB/ODtrwW	0

Figure 7: User Data.

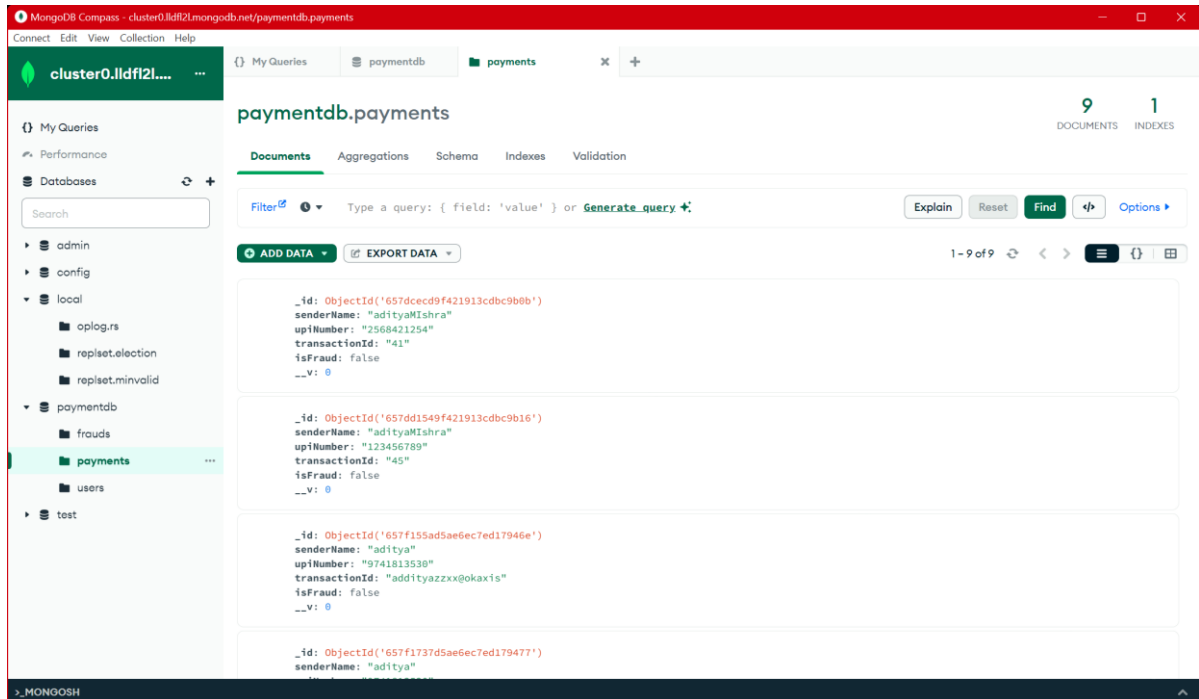


Figure 8: Payment Data.

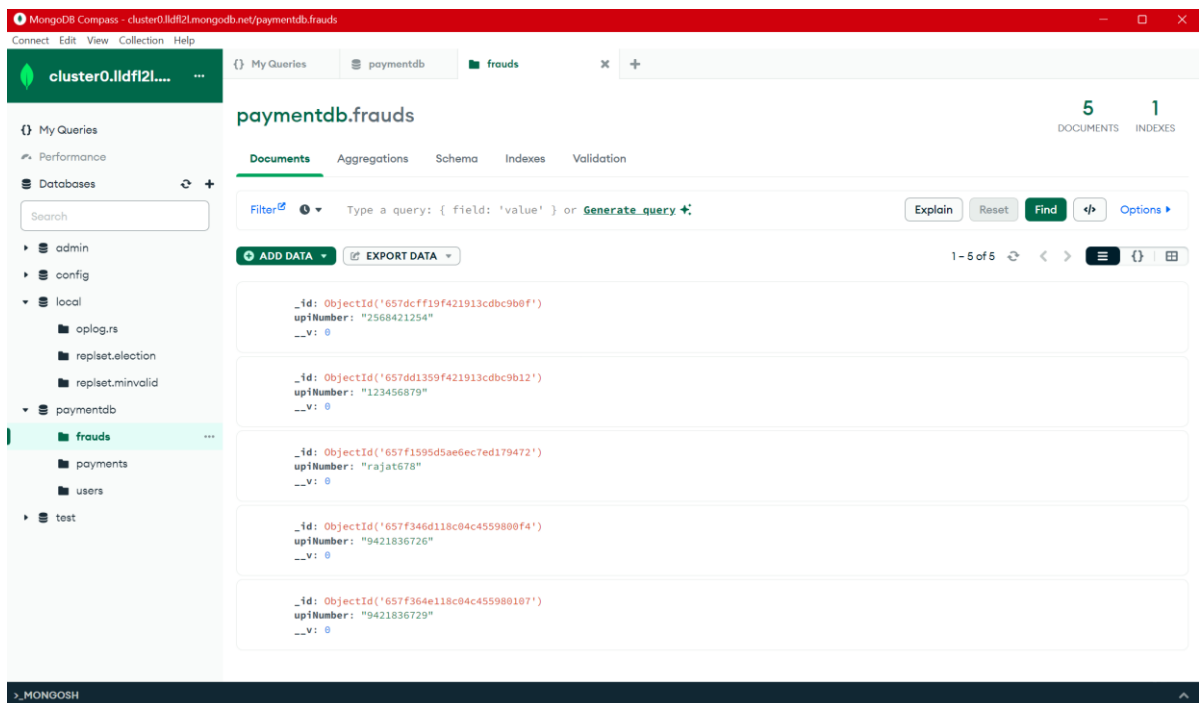


Figure 9: Reporting Database.







G173

ORIGINALITY REPORT

22%

SIMILARITY INDEX

18%

INTERNET SOURCES

14%

PUBLICATIONS

15%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Presidency University Student Paper	3%
2	www.researchgate.net Internet Source	3%
3	research.lut.fi Internet Source	2%
4	www.nature.com Internet Source	2%
5	ukcatalogue.oup.com Internet Source	1%
6	Submitted to M S Ramaiah University of Applied Sciences Student Paper	1%
7	archives.palarch.nl Internet Source	1%
8	cs.paperswithcode.com Internet Source	1%
9	cronfa.swan.ac.uk Internet Source	1%



Introduction to Industry Innovation and Infrastructure:

The project to address phishing attacks aligns closely with the Sustainable Development Goal (SDG) of Industry, Innovation, and Infrastructure. The pervasive threat of phishing attacks, exploiting human weaknesses to compromise digital systems, necessitates innovative solutions within the cybersecurity realm. By developing a sophisticated system with a multifaceted approach, this initiative not only addresses immediate security concerns but also contributes to ongoing innovation in the industry. The seamless integration of the system with existing email security frameworks underscores a commitment to strengthening digital infrastructure.

In the context of sustainable development, resilient and secure digital infrastructure is crucial for the continuous growth of industries. This project supports SDG 9 by fostering innovation in the cybersecurity sector and ensuring the development of robust systems that can adapt to ever-evolving threats. As industries increasingly rely on digital platforms, the project's emphasis on creating an additional layer of defense against phishing tactics promotes the sustainable advancement of industry practices. Overall, by enhancing cybersecurity measures and promoting innovation in digital defense, the project aligns with the broader goals of building resilient industry infrastructure for a sustainable and secure future.