Detect and Prevent Check Scams in Online Banking Services

Suresh.P[1], Sangeetha Varadhan[2]
Department of Computer Applications
[1]PG Student, Dr. M.G.R. Educational and Research Institute, Chennai - 95
[2]Associate professor, Dr. M.G.R. Educational and Research Institute, Chennai - 95

Abstract- *In the realtime of online banking, the detection and prevention of check scams have become paramount to safeguarding customers' assets and ensuring the integrity of financial transactions. This paper outlines a multifaceted approach to combat check fraud in digital banking environments. By leveraging advanced technologies such as check verification services, image analysis, and machine learning-based fraud detection systems, online banking platforms can effectively identify and mitigate various forms of check scams, including counterfeit checks and altered check schemes. Additionally, proactive prevention measures, such as customer education, secure authentication, and transaction monitoring, are crucial to fortifying the security posture of online banking services. Collaboration with law enforcement agencies, regular updates, and continuous training further augment the resilience against evolving fraud tactics. Implementing these comprehensive strategies can significantly reduce the risk of check scams and foster trust among online banking customers.*

Keywords: *Online Banking, Check Scams, Fraud Detection, Check Verification Services, Image Analysis, Machine Learning, Customer Education, Secure Authentication, Transaction Monitoring.*

I. INTRODUCTION

In our current society, checks are one of the most common payment methods. A check is an order written by a depositor, an order given to the bank to pay a certain amount from the depositor's bank account to the recipient. Unfortunately, many malicious fraudsters take advantage of flaws in the banking system to commit fraud. In fact, fake check fraud is growing rapidly and costs billions of dollars. Federal Trade Commission (FTC)Consumer Watchdog Database number of complaints [1].

A continuation of our previous work where we presented a method to detect fake checks. However, our previous work did not consider another case where a fraudster uses real information to create a fake check. Thus, the detection method fails to detect fraud, rendering it effective. To fix this shortcoming of the previous approach, extends it so that the extended approach can detect all possible authentication frauds [2].

Our approach is mainly based on blockchain and Lagrange interpolation polynomial. This section briefly describes these concepts. Blockchain is not a new concept for banks. Indeed, many studies have described the challenges and opportunities of implementing blockchain technology in the banking sector (e.g. Central Bank Digital Currency (CBDC),Central Bank Managed PCS Systems, Fund Transfer and Holding, Audit Trail, Regulatory Compliance (Regulation)[3].

Blockchain technology was created to solve the problem of double spending in cryptocurrencies. However, many works currently explore blockchain applications for various use cases and use them as a secure way to create and manage a distributed database and keep records of all kinds of digital events. A blockchain ledger consists of several blocks, and each block consists of two parts [4].

We use the blockchain to implement our approach. The denomination uses the Nakamoto Consensus. Nakamoto proposed a permission less consensus protocol, based on a crypto-block mining competition game also known as proof-of-work (POW). From the perspective of a single node, Nakamoto's consensus protocol defines three main procedures [5].

II. LITERATURE SURVEY

According to **Lydia M Rose**.et al., 2018 Fake checks from overseas are the scourge of online dating sites, classifieds forums and mailboxes across the country. Checks are also exploited by other types of fraud such as embezzlement, theft, and bounced checks. Check fraud is estimated to cost both financial institutions and consumers hundreds of millions each year, and the problem is getting worse. Fraud investigators and financial institutions must be better trained and armed to successfully combat it[6].

According to **Tenuche Bashir**.et al., 2020 Phishing is not just about sending fake messages to users, as most people assume, but is a multifaceted techno-social problem that has no concrete solution to end its dominance. This has spawned a number of studies in the field as researchers try to create more effective anti-phishing solutions by identifying risks and user

vulnerability. Most anti-phishing tools are not able to make dynamic decisions to determine the risk level of a site, allowing a large number of false positive [7].

According to **Jay Nanduri**.et al., 2020 In "online scams," fraudulent websites offer fraudulent companies or fake services to steal money and sensitive information from unsuspecting victims. Despite the efforts of researchers to develop anti-counterfeiting techniques, fraud schemes continue to evolve and pose online threats. State-of-the-art anti-counterfeiting research still faces some challenges, such as automatically obtaining a set of detected counterfeit data and providing mechanisms for early detection and prevention of attacks using cryptocurrency as a means of payment [8].

According to **Hussein Badawi**.et al., 2021 Many businessmen do their business through e-commerce. One of the main challenges in combating e-commerce fraud stems from dynamic fraud patterns, which can weaken the detection capabilities of risk models and cause them to fail to detect fraud with new, unknown patterns. Traditional decision-making frameworks make the problem worse [9].

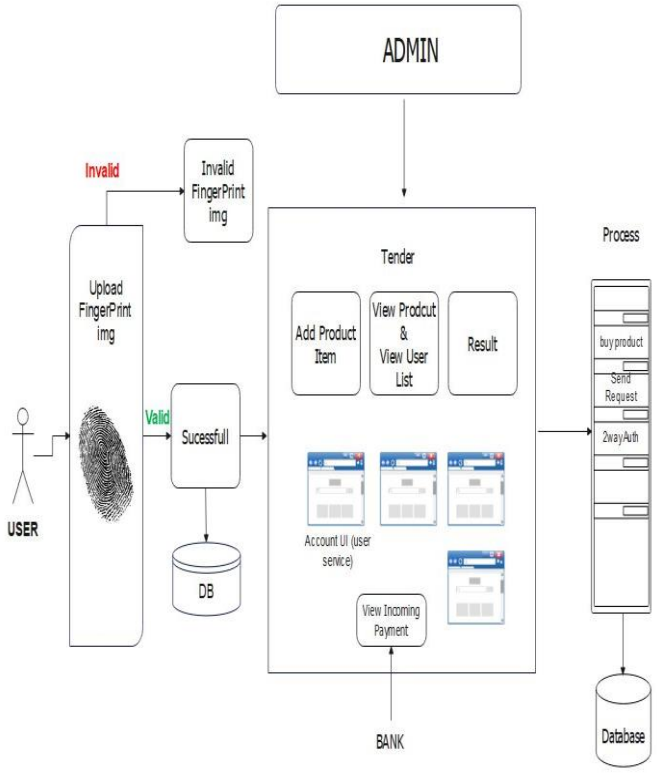
According to **Xin Tong Tan**.et al., 2023 The survey assessed participants' perceptions of online banking fraud related to the relationship between personal financial difficulties, empathy, fraud attitudes and online banking knowledge. In this study, several analytical tests such as descriptive analysis, scale measurement, initial data screening and inferential analysis were used to analyze the hypothesis. The results of this study are important for financial institutions and policy makers working to combat online banking fraud [10].

III.PROPOSED SYSTEM

With a user-friendly interface, it offers a comprehensive collection of essential retail banking modules through a centralized, customer-centric design. OBS was created to automate daily operations at any bank and offers all the capabilities required to run a banking procedure. When making a deposit, the user can access this page if they have the encryption key. just when they are signed onto the website. The most crucial element of a website is a web server. All data on the server will become publicly available in the event of an unauthorized attack.

The administrator can view or remove any user's general data, but they are still unable to examine any user's transaction history. Recovering the user password is really challenging.

ARCHITECTURE DIAGRAM



IV.RESULTS AND DISCUSSION

Fig 1. HOME PAGE

a).The home page provides users with a visually appealing and user-friendly interface that showcases featured products, promotional offers, and important announcements. It effectively communicates the brand's identity, values, and offerings, encouraging visitors to explore the website further and engage with the content.

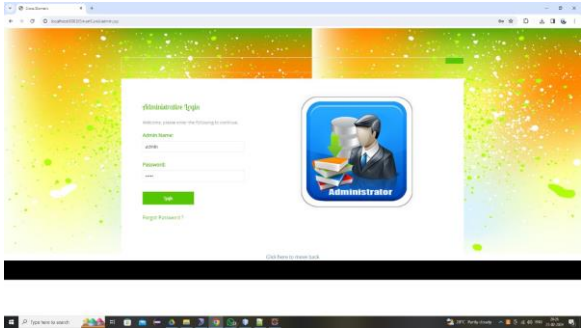


Fig 2. ADMIN LOGIN PAGE

The admin login page offers a secure and efficient authentication process for administrators to access the backend system.

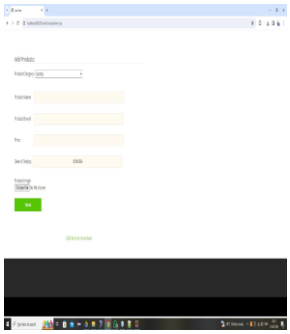


Fig 3.ADD PRODUCT PAGE

Fig 4. VIEW PRODUCT

a).The add product page enables administrators to easily add new products to the database by entering relevant details such as product name, description, price, and images. It validates the input data to ensure accuracy and consistency, and provides feedback to the user upon successful addition of the product.

b).The view product page displays a comprehensive list of products available on the platform, organized in a user-friendly manner with filters and sorting options.

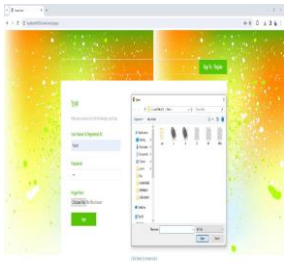


Fig 5.USER LOGIN PAGE

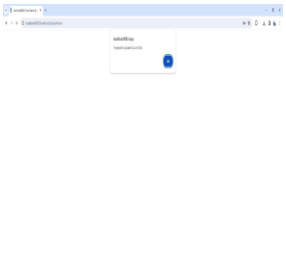


Fig 6. LOGIN VALIDATION

a).The user login functionality offers a secure and seamless authentication process for registered users to access their accounts. It includes features like password hashing, CAPTCHA verification, and account lockout policies to enhance security and protect user data from unauthorized access and brute-force attacks.

b).The login validation process verifies the authenticity of user credentials by comparing them against the stored data in the database. It checks for correct username/email and password combinations, and handles errors and exceptions gracefully, providing clear and informative error messages to users to facilitate troubleshooting and resolution.

Fig 7. USER HOME PAGE

Fig 8 .USER VIEW PRODUCT

a).The user home page serves as a personalized dashboard for authenticated users, displaying relevant information such as order history, account details, saved items, and personalized recommendations.

b). The user view product page presents detailed information about a specific product selected by the user, including images, descriptions, prices, and reviews.

Fig 9 .CONFORM ORDER PAGE

The confirm order page allows users to review and finalize their purchase before proceeding to payment. It displays a summary of selected items, quantities, prices, and total order value, along with shipping and billing information. It includes validation checks to ensure accuracy and completeness of order details, and provides clear instructions for payment processing.

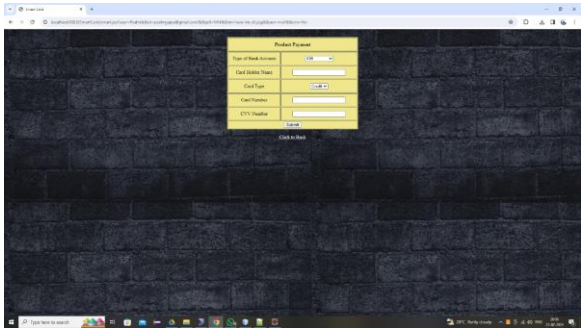


Fig 10 .SMART CARD

The smart card functionality offers a secure and convenient payment method for users to complete transactions on the platform. It utilizes encrypted technology, tokenization, and

secure authentication processes to safeguard sensitive financial information and prevent fraud. It supports multiple payment options, including credit/debit cards, digital wallets, and bank transfers, providing flexibility and ease of use for customers.

V.CONCLUSION

In conclusion, detecting and preventing check scams in online banking services is a shared responsibility between financial institutions and customers. Banks should invest in advanced fraud detection systems, implement Positive Pay services, use check image verification, and employ multi-factor authentication to safeguard against fraudulent activities. Regular monitoring, customer education, and internal audits are also essential for identifying vulnerabilities and strengthening security measures. On the other hand, customers play a crucial role in protecting their accounts by using secure online banking practices, verifying check authenticity, protecting personal information, and regularly monitoring their account activities. Being skeptical of overpayments and promptly reporting suspicious activities to the bank can help prevent potential losses from check scams.

REFERENCES

[1] Ke Li Chin, Xin Tong Tan, Jia Hooi Tang, Khai Li Toh 2023, The influencing factors of online banking fraud awareness in UTAR Kampar,UTAR.

[2] Jay Nanduri, Yuting Jia, Anand Oka, John Beaver, Yung-Wen Liu 2020,Emad Mohammad Hussein Badawi 2021, Towards Algorithmic Identification of Online Scams,Université d'Ottawa University of Ottawa.

[3] Natalia Dashkevich, Steve Counsell, and Giuseppe Destefanis. Blockchain application for central banks: A systematic mapping study. IEEE Access, 8:139918–139952, 2020.

[4] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7:22328–22370, 2019.

[5] Hammi Badis and Elloh Adja Yves Christian. Fake check scams: A blockchain based detection solution. In 9th International Conference on Computer Science and Information Technology (CCSIT 2019), pages 81–97, 2019.

[6] Lydia M Rose 2018,Modernizing check fraud detection with machine learningLydia M Rose Utica College.,2018

[7] Steven Baker. Don't Cash That Check: BBB Study Shows How Fake Check Scams Bait Consumers. Technical report, Better Business Bureau (BBB), September, 2018.

[8] Mohamed Tahar Hammi, Patrick Bellot, and Ahmed Serhrouchni. BCTrust: A decentralized authentication blockchain-based mechanism. In Wireless Communications and Networking Conference (WCNC), 2018 IEEE, pages 1–6. IEEE, 2018.

[9] Microsoft uses machine learning and optimization to reduce e-commerce fraud, INFORMS Journal on Applied Analytics 50 (1), 64-79.

[10] Tenuche Bashir, BC Agbata, William Obeng-Denteh Emmanuel Ogala 2020,The Fuzzy Experiment Approach for Detection and Prevention of Phishing attacks in online Domain,East African Scholars Journal of Engineering and Computer Sciences, 205-215.