IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

A Hybrid Approach for Secured Banking Transaction using Ras and Two Fish Blockcypher Algorithms

D. Naveen[1] and Dr. C. Meenakshi[2]

MCA Student, Department of Computer Applications[1]

Associate Professor, Department of Computer Applications[2]

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

mohanraj672000@gmail.com and cmeenakshi.scs@velsuniv.ac.in

Abstract: *We designed a secure and efficient E-Payment protocol. The new protocol offers an extra layer of protection for cardholders and merchants. Customers are asked to enter an additional password after checkout completion to verify they are truly the cardholder, the authentication is done directly between the cardholder and card issuer using the issuer security certificate and without involving the third- party electronic commerce or e-commerce provides participants, including consumers and merchants, with a number of benefits, such as convenience and time savings. E-commerce transactions can be categorized into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government we focus on B2C transactions in this paper.*

Keywords: E-Payment

I. INTRODUCTION

The rise of electronic banking, or online banking, has transformed banking operations, cutting transaction costs and offering diverse integrated services. Security and privacy are paramount in this realm, crucial for combating potential fraudulent activities. Encryption methods like passwords, PIN codes, biometrics, and digital signatures serve as defences against unauthorized access and data breaches. As online and mobile banking expand, financial institutions face heightened demands for robust data security. Cryptography emerges as pivotal, ensuring the confidentiality and integrity of transactions while authenticating message sources and thwarting counterfeiting attempts. Banks prioritize encryption algorithms and software-based security to fortify communication channels, safeguarding data transactions and fortifying networks against malicious intrusions. This paper delves into cryptography's essential role in securing online banking and explores the evolving landscape of technology-driven banking services worldwide.

II. LITERATURE REVIEW

1. Title: Secure Banking Transactions: RSA and Two Fish Algorithms Year: 2020

Authors: Gaurav Ramtri, Chir Patel

Abstract: Internet banking simplifies global money transfers, but persistent security vulnerabilities pose risks. To fortify security, this paper proposes cryptographic techniques. Utilizing RSA and Two Fish algorithms, transactions are encrypted, ensuring decryption only by authenticated users, bolstering online banking security.

2. Title: Visual Cryptography for Secure Bank Transactions Year: 2019

Authors: Avinash Nagul, Pooja More, Sharayu Sawant, Jyoti Sawant

Abstract: Security is vital in modern banking systems, ensuring secure core services. User authenticity is pivotal, restricting transactions to authorized users. Despite biometric authentication, banking databases are vulnerable to malicious exploitation. Hackers can access biometric data for fraud. To address this, the paper suggests using visual cryptography with AES for improved security.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

3. Title: Database Encryption SchemesYear: 2017

Authors: P.R.Hariharan, K.P. Thooyamani

Abstract: Database security is paramount in the IT world, safeguarding confidential organizational information. Encryption plays a crucial role in securing databases by transforming data into cipher text, rendering it inaccessible to unauthorized users. This paper provides a concise overview of various encryption techniques. Transparent database encryption encrypts the entire database, ensuring security for inactive data on physical storage using symmetric keys. Column-level encryption encrypts each database column uniquely, enhancing data security at a granular level.

III. PROPOSED METHODOLOGY

The proposed methodology harnesses the synergies of cryptography, block chain technology, and data mining to fortify transaction security comprehensively. Firstly, data encryption is employed to shield user details, ensuring that sensitive information remains protected from unauthorized access. Secondly, block chain technology is utilized to establish a tamper-proof storage system, where encrypted user data is securely stored within a decentralized ledger, enhancing transparency and integrity in transactions. Thirdly, data mining techniques are leveraged to detect fraudulent activities by analyzing transaction patterns, enabling the timely identification of anomalies and facilitating proactive intervention to prevent unauthorized transactions. This holistic approach not only guarantees robust security but also fosters transparency in transactions, while empowering stakeholders with the tools to detect and mitigate potential fraud effectively.

IV. MODULE DESCRIPTION

ADMIN MODULE:

LOGIN: This module facilitates user authentication through a set of credentials, typically comprising a username and password. It serves as a security measure to prevent unauthorized access to sensitive data.

VIEW TRANSACTION: Admins can access and review user details and transaction histories. This functionality provides insights into user activities and transactional patterns.

BANK MODULE:

REGISTER & LOGIN: Bank users can register by submitting their details and obtain unique login credentials upon completion. This ensures secure access to bank-specific features.

VIEW TRANSACTION: Bank users can monitor user details and transaction records, enabling them to track user interactions with the platform.

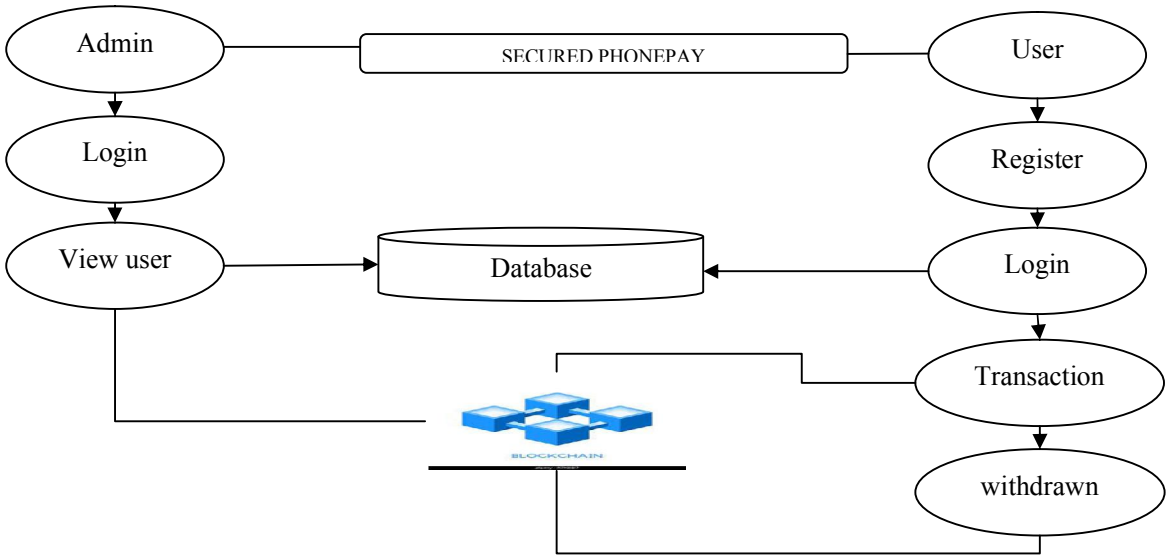
USER MODULE:

REGISTER & LOGIN: Users can register on the website to utilize the money transaction application. Upon registration completion, users receive login credentials for accessing the platform securely.

TRANSACTION: This module enables users to perform various banking transactions, including deposits and withdrawals, ensuring convenient and secure money management.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

SYSTEM ARCHITECTURE:

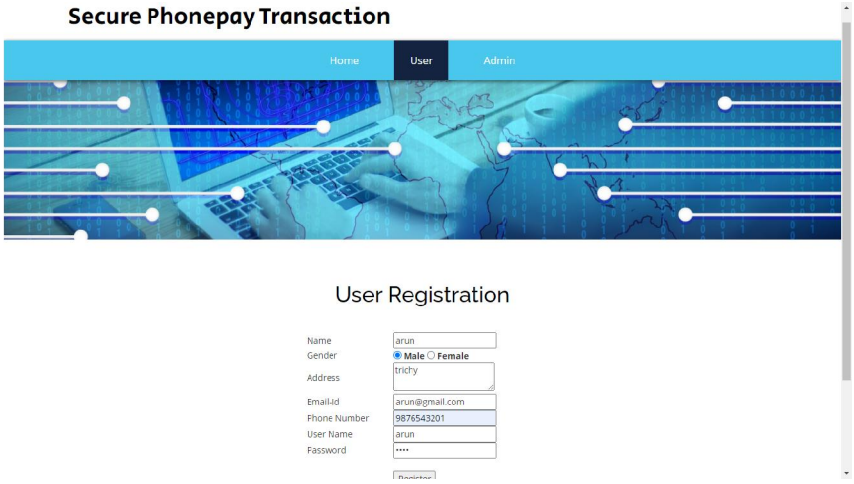


V. RESULT & DISSCUSSION

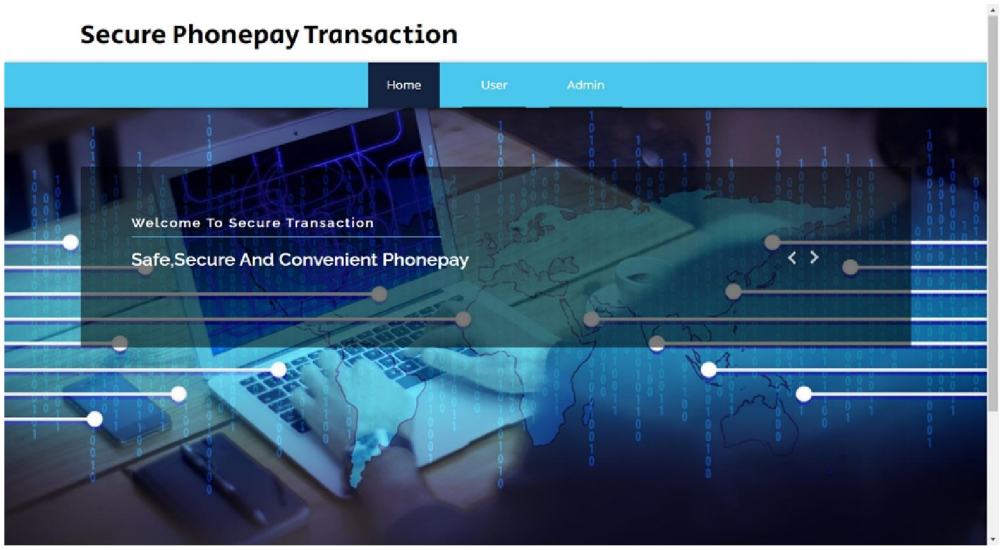
The proposed system employs a multifaceted approach to transaction security by integrating cryptography, block chain, and data mining. Through data encryption, sensitive user card details are rendered inaccessible to unauthorized parties, bolstering security with robust encryption mechanisms. Block chain integration ensures the secure storage of encrypted user card details in a decentralized and tamper-resistant ledger, enhancing transparency and immutability while reducing the risk of data manipulation. Data mining techniques enable the system to detect anomalies in transaction behavior in real-time, allowing for proactive intervention to prevent unauthorized transactions. This comprehensive security framework instills confidence in users by providing a reliable platform with enhanced security measures. Additionally, the system's modular design allows for scalability and adaptability to evolving security threats, ensuring continued effectiveness in safeguarding online banking transactions.

VI. SAMPLE OUTPUT

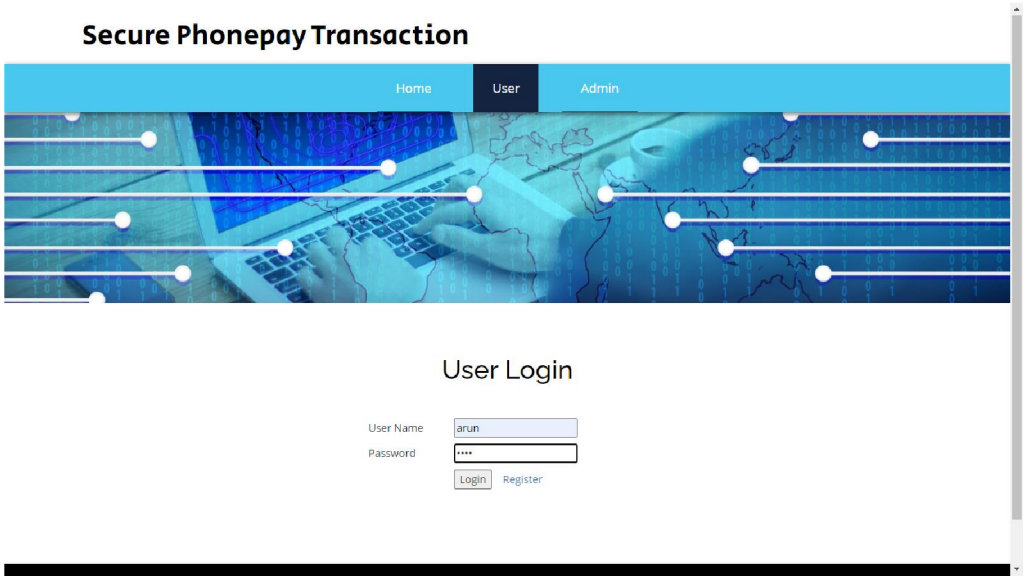
USER REGISTER:



IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

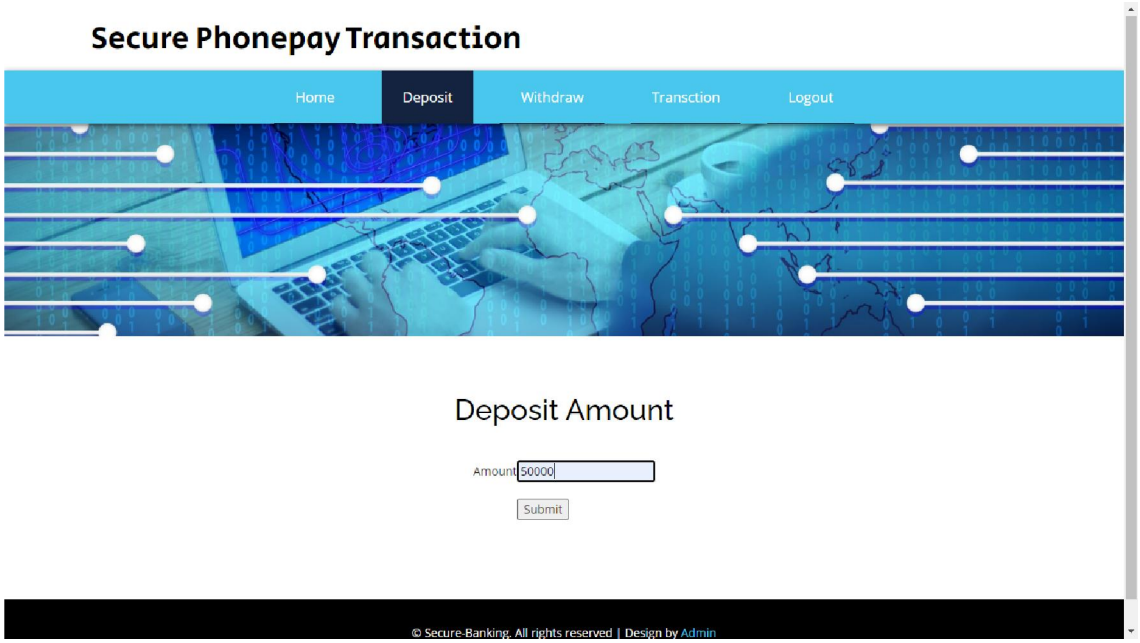


USER LOGIN:

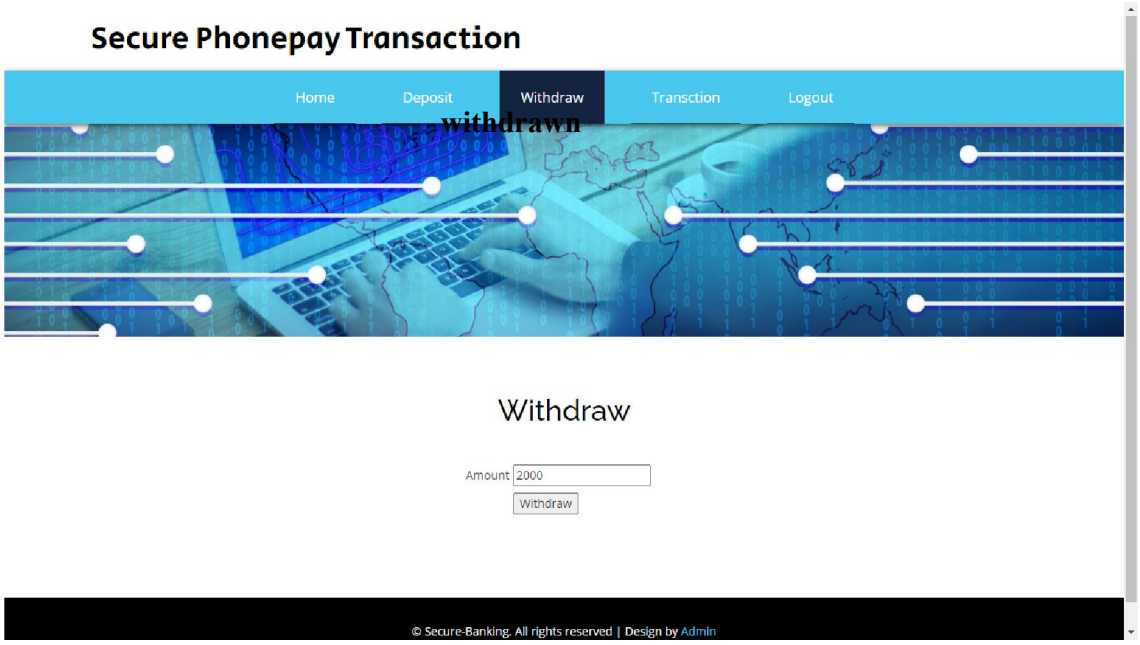


IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

DEPOSIT:

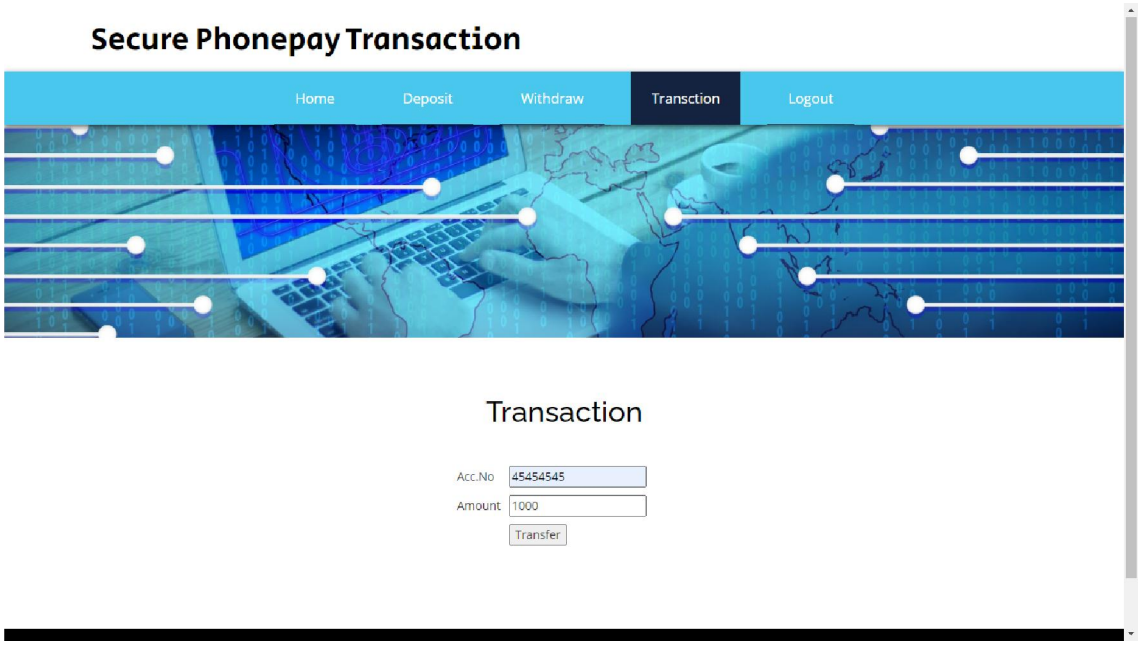


WITHDRAWN



IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

TRANSACTION:



VII. CONCLUSION

In conclusion, the implemented system has successfully delivered a secure E-Banking experience for users. Through the utilization of cryptography and block chain on the client side, the system effectively prevents online frauds, while data mining on the server side ensures fraud detection. Extensive testing, including analysis of steganography-generated images and data mining modules with various datasets, confirms the system's ability to handle normal and extreme cases efficiently. Overall, the system fulfils its primary objective of providing a safe and protected online banking experience.

FUTURE ENHANCEMENT

Future enhancements could involve further analysis of the system's security and performance. Additionally, the development of an Android application and the integration of new algorithms for user data security represent potential avenues for future research and development. Further technical elaboration and refinement are necessary for the continued evolution and effectiveness of the system.

REFERENCES

[1]. Paul Benjamin Lowry, Taylor Michael wells, Georgy Daniel moody, online payment gateway used to facilitate E-commerce transaction and improve risk management,february-2006.

[2]. AKM Bahaullah Hague, block chain technology: methodology, application and security issues. December-2020.

[3]. Mausumi Das, Tapeline bhattasali, impact of block chain to secured E-banking transaction.

[4]. Bruce W Perry, Java Servlet and JSP Cookbook, O′Reilly; 1 edition (6 February 2004)

[5]. Phillip Hanna, JSP 2.0: The Complete Reference, Second Edition , McGraw Hill Education; 1 edition (1 July 2017)

[6]. Santosh Kumar K. , JDBC 4.2, Servlet 3.1, and JSP 2.3 Includes JSF 2.2 and Design Patterns, Black Book, 2ed, Dreamtech Press; Second edition (2016)