Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
March 2024 5(3), 1198–1203

MULTIPLE CLOUD DATA DIVISION ON BANKING SECURITY ON DATA HACKER HIDING WITH CRYPTOGRAPHIC

Dr. Prasanna D[1], Sujith Kumar M K[2], Tamilvel C[3], Ranjith T[4]

[1]Associate Professor, Computer Science and Engineering, Mahendra Engineering College Autonomous, India.
[2]UG Scholar, Computer Science and Engineering, Mahendra Engineering College Autonomous, India.
[3]UG Scholar, Computer Science and Engineering, Mahendra Engineering College Autonomous, India.
[4]UG Scholar, Computer Science and Engineering, Mahendra Engineering College Autonomous, India.

DOI
10.29121/shodhkosh.v5.i3.2024.4127

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In the present digital era, securing banking transactions remains of utmost importance. With the rise of cloud computing, the banking sector has increasingly adopted cloud servers for efficient data management. However, sharing sensitive information via a centralized server poses notable challenges in terms of security and privacy.This paper proposes an innovative solution to address these challenges by integrating Attribute-Based Key Policy Encryption (ABKPE) standards into the banking transaction system. ABKPE offers a robust cryptographic mechanism that enables secure sharing of confidential messages across cloud servers while maintaining stringent access control policies based on user attributes. By leveraging ABKPE, our system ensures heightened security and privacy for banking transactions in a cloud environment. Multiple servers are employed for data shall This research contributes to advancing secure banking systems by presenting a practical approach to managing sensitive information in the cloud. The integration of ABKPE enhances data security and privacy, guarding against unauthorized access and potential threats.

Keywords: Banking transaction System, Cloud Computing, Attribute-Based Key Policy

1. INTRODUCTION

The banking sector has undergone a significant transformation with the advent of cloud computing, leading to increased efficiency and accessibility in managing financial transactions and data. However, this transition has also brought to light critical challenges, particularly in ensuring the security and confidentiality of sensitive information within cloud-based environments. Traditionally, banking systems have relied on centralized servers for storing and processing data, which, while convenient, have exposed institutions to potential security risks. The concentration of data in one location makes it vulnerable to breaches and unauthorized access, jeopardizing the integrity of customer transactions and data privacy. In response to these challenges, this paper proposes an innovative solution: the integration of Attribute-Based Key Policy Encryption (ABKPE) standards into cloud-based banking systems. ABKPE offers a sophisticated cryptographic mechanism that enables secure sharing of confidential information while enforcing access control policies based on user attributes. By leveraging ABKPE, banks can enhance the security posture of their cloud-based transactions, reducing the risks associated with centralized server architectures. This study aims to explore the implementation of ABKPE within

the context of cloud-based banking systems, providing insights into its potential benefits and challenges. Through an in-depth analysis of underlying principles and practical considerations, this research seeks to offer guidance on how banks can effectively leverage ABKPE to strengthen the security and privacy of their transactions. The subsequent sections of this paper delve into the existing challenges in securing banking transactions in the cloud, introduce the concept of Attribute-Based Key Policy Encryption and its relevance to banking systems, discuss implementation considerations, and conclude with a summary of key findings and recommendations for future research. In summary, this paper contributes to the ongoing discourse on enhancing security in cloud-based banking transactions, offering a novel approach to address the pressing cyber security concerns facing the industry amidst the digital transformation.

2. LITERATURE SURVEY

In[1] Maria Rona L. Perez; Bobby Gerardo; Ruji Medina While the concept of blockchain is not new in today's technology landscape, its significance has been further underscored by its association with Bitcoin, described by some researchers as the "most disruptive technology," as outlined in [1]. Blockchain, often linked with Bitcoin [2], operates as a computational paradigm characterized by a distributed ledger system that records all network transactions, introducing novel trust models over the Internet. In 2008, an anonymous entity, identified as Satoshi Nakamoto, introduced the concept of blockchain through a seminal white paper, heralding the emergence of Bitcoin as a digital cryptocurrency. Initially underestimated, Bitcoin's decentralized nature facilitated parallel currency transactions verified through a consensus mechanism, devoid of central authority, gradually gaining momentum.

In[2] Eric Y. Chen; Shuo Chen; Shaz Qadeer; The increasing popularity of online banking has sparked concerns about security, prompting the need for robust measures to safeguard transactions and personal data. As online banking becomes indispensable across all age groups, the reliance on traditional security methods like passwords and tokens proves inadequate. To address these shortcomings, banks are turning to biometric authentication, with some institutions now employing multiple biometric modalities such as face and fingerprint recognition. This approach enhances security by requiring both biometrics for login authentication and only one for transaction authorization. Additionally, ongoing research explores feature-level matching, a promising avenue for improving authentication accuracy. Overall, these advancements aim to fortify online banking security and protect users from potential threats.

In[3] Greg Olmschenk, Zhigang Zhu, Hao Tang The rise of security vulnerabilities in multiparty online services like Single-sign-on and third-party payment systems highlights the crucial need for robust engineering practices backed by formal program verification. However, implementing program verification faces challenges, including complex logic property specification due to informal protocol specifications and modeling difficulties for attackers and runtime platforms. To overcome these obstacles, we introduce Certification of Symbolic Transaction (CST), which simplifies program verification by jointly defining a protocol-independent safety property across all involved parties. CST utilizes static verification at runtime, symbolically verifying transactions on-the-fly, reducing proof obligations and enabling minimal code changes per party. Applied to five commercially deployed applications, CST effectively prevents the majority of logic flaws, demonstrating its practicality and effectiveness for real-world deployment.

[4] Eric Y. Chen; Shuo Chen; Shaz Qadeer; Rui Wang The rise of security vulnerabilities in multiparty online services like Single-sign-on and third-party payment systems highlights the crucial need for robust engineering practices backed by formal program verification. However, implementing program verification faces challenges, including complex logic property specification due to informal protocol specifications and modeling difficulties for attackers and runtime platforms. To overcome these obstacles, we introduce Certification of Symbolic Transaction (CST), which simplifies program verification by jointly defining a protocol-independent safety property across all involved parties. CST utilizes static verification at runtime, symbolically verifying transactions on-the-fly, reducing proof obligations and enabling minimal code changes per party. Applied to five commercially deployed applications, CST effectively prevents the majority of logic flaws, demonstrating its practicality and effectiveness for real-world deployment.

In[5] V. Oliyil. Kunnil; A. Pillai; S. Milshtein Biometric authentication methods, such as fingerprints and iris scans, offer enhanced security and uniqueness compared to traditional knowledge-based methods like passwords. However, online transactions predominantly rely on vulnerable key-based authentication. Our proposed system aims to revolutionize authentication by integrating a user's biometric identifier, such as contactless fingerprint images, into authentication keys, rendering traditional methods obsolete. By leveraging randomly selected segments of fingerprints to generate keys and incorporating blood vessel maps for live finger verification, our protocol enhances security significantly. This approach ensures robust protection for network transactions by utilizing the rich and unique information present in fingerprint data.

In[6] Chin-Ming Hsu; Hui-Mei Chao This study A novel technology is introduced to enhance the security of credit card e-transactions, focusing on online fraud prevention. The system features cardholder-driven identification, merchant-driven verification, and issuer-driven authorization, aiming to bolster resistance against fraud. The paper evaluates the system's resilience to fraud attempts, its security features, and computational costs. The method demonstrates increased fraud resistance with minimal computational overhead, while remaining compatible with existing security mechanisms like SSL and SET. This compatibility ensures seamless integration and effectiveness in real-world ecommerce scenarios.
In[7] Sona Kaushik; Shalini Puri Authentication and reliability are paramount in online transaction systems, which face greater vulnerability to attacks compared to offline counterparts. With the exponential growth of e-commerce, robust security measures are essential to safeguard transactions. While the Secure Electronic Transaction (SET) System has been pivotal, the rising incidence of malicious activities calls for more intricate approaches. This study introduces an algorithm aimed at enhancing the security of critical information exchanged during online transaction processing (OLTP). By addressing vulnerabilities inherent in online transactions, the algorithm aims to ensure a safer and more reliable e-commerce environment for users and businesses alike.
In[8] Jian Xu; Andi Wang; Jun Wu; Chen Wang; Ruijin Wang; With the surge in online social networks' usage by criminal suspects, there's a pressing need for research focused on analyzing their social data for potential criminal evidence. However, existing studies often overlook privacy concerns, risking the exposure of sensitive information during analysis. In response, our innovative approach integrates social and crime data from social networks and police information systems. We ensure privacy by securely exchanging social information and public data while preserving privacy using techniques like oblivious transfer. Additionally, components such as encrypted data comparison and a secure CART model enhance analysis without compromising privacy. This privacy-preserving scheme for sensing criminal suspects proves effective in performance evaluation, ensuring minimal overhead and privacy risks.
In[9] Pascal Urien The paper examines the Bitcoin system with the aim of dissecting the production costs and market valuation. This analysis relies on publicly available data and technical research papers. Furthermore, the paper proposes the design of secure elements specifically tailored for Bitcoin transactions. These devices are envisioned to facilitate trusted and efficient transactions, while also mitigating the risk of Bitcoin address hijacking.
In[10] Sri Wahjuni; Rizky Pristian Online transactions face constant threats from malicious activities like spoofing and phishing. Implementing a token-based authentication system is an effective solution, and this paper introduces an Android-based system utilizing the One-time Pad (OTP) algorithm. Leveraging mobile phones eliminates the need for dedicated token machines, enhancing user convenience. Experimentation confirms the system's ability to generate unique token keys for each user within designated timeframes. Rigorous testing against diverse attack scenarios affirms the system's resilience in safeguarding online transactions.

3. EXISTING SYSTEM

The current online banking system necessitates users to input their card details directly into the payment gateway of a website. These details undergo encryption using advanced algorithms and keys before being transmitted to the bank server via the internet. Despite the assurances of high-security levels provided by encryption methods and algorithms, professional hackers still manage to compromise the system. The vulnerability lies in the fact that the data is solely encrypted using a key, making it susceptible to hacking by skilled attackers. Beyond encryption, there lacks additional mechanisms to conceal such crucial data from potential hackers.

4. PROPOSED SYSTEM

Our the proposed system focuses on preventing and detecting fraud through a combination of cryptography, steganography, and data mining techniques. User card details are encrypted using cryptography, ensuring secure transmission. These encrypted details are then embedded within an image using steganography, providing an additional layer of concealment during transactions. Finally, data mining algorithms analyze the user's transaction patterns to identify significant deviations, enabling the system to take appropriate actions such as blocking or completing the transaction. The system comprises three main modules: data encryption, image steganography, and data mining, each playing a vital role in enhancing fraud prevention and detection capabilities.

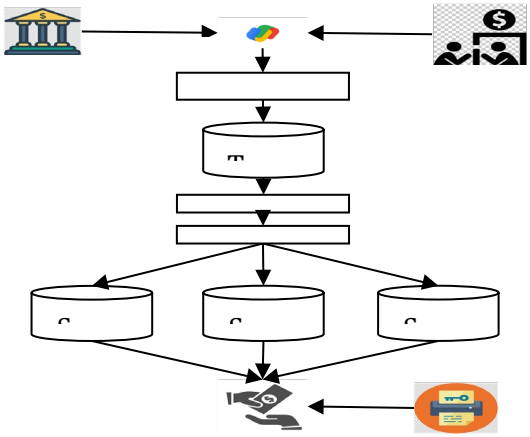

Fig 1 System Architecture of Proposed System

5. METHODOLOGY AND IMPLEMENTATION

BANKING TRANSACTION

Entities or administrators typically register with the system to establish accounts, ensuring secure access across multiple users. The account creation process is designed to provide varying levels of access security. Users can engage in banking processes facilitated by the module, including depositing, withdrawing, and conducting transactions. The development servers verify authentication levels comprehensively, ensuring the integrity of the system.

ATTRIBUTE DIVISION

Attribute division involves fragmenting and storing uploaded server details securely. This process categorizes data based on attributes such as account number, name, IFSC code, and branch name. Bank details undergo comprehensive storage fragmentation, ensuring data integrity and security at various authorization levels.

ATTRIBUTE BASED KEY POLICY ENCRYPTION

In this system, ABKPE encryption is employed as the primary method for attribute division and encryption. Attribute-Based Encryption (ABE) enables flexible one-to-many encryption based on attributes. Decryption of a cipher text is contingent upon the user key's attributes aligning with those of the cipher text, ensuring secure and precise access control.

PRIVATE KEY GENERATOR

A private key, alternatively termed as a secret key, serves as a critical variable in cryptography, employed alongside an algorithm to facilitate code encryption and decryption processes. These secret keys are strictly shared solely with the key's generator, ensuring robust security measures. Typically, private keys are generated from a secure random number generator or derived from a seed value, itself produced by a secure random number generator. This meticulous process ensures the integrity and confidentiality of the private key, enhancing overall cryptographic security.

SECURE TRANSACTION

Transactions conducted within the entities are meticulously stored, employing a three-tiered access system.
At Level 1, transactional details undergo fragmentation through attribute division, enhancing data organization and security. Subsequently,
at Level 2, the fragmented data is encrypted using ABKPE, ensuring robust protection against unauthorized access.
Finally, at Level 3, the encrypted data is stored across multiple cloud servers, further fortifying the security measures by dispersing data storage and minimizing the risk of data loss or breach.

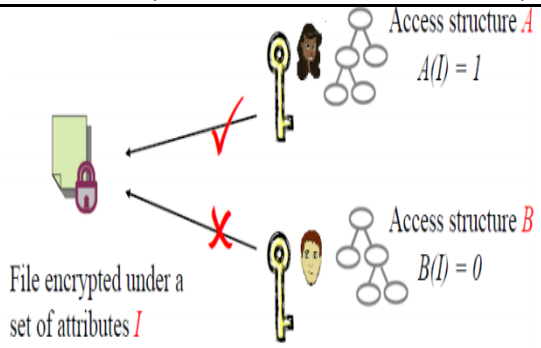

Fig 2 Algorithm Explanation

HACKER INTIMATION

The authority side possesses knowledge of hacker details, facilitating easy identification when necessary. Through server-side extraction, the hacker's IP, MAC address, latitude, and longitude values are obtained, aiding in their identification process. These extracted details play a crucial role in accurately pinpointing the hacker's identity and location, enabling swift and effective countermeasures against cyber threats.

6. RESULT AND DISCUSSION

The proposed system represents a comprehensive approach to combating fraud in online transactions by integrating cryptography, steganography, and data mining techniques. Through cryptography, user card details are encrypted to ensure secure transmission, while steganography embeds these encrypted details within innocuous images, adding an extra layer of concealment. Additionally, data mining algorithms analyze user transaction patterns to detect deviations, enabling prompt action to block or complete transactions. Each module - data encryption, image steganography, and data mining - plays a vital role in enhancing fraud prevention and detection capabilities, collectively forming a robust defense mechanism against various forms of online fraud. By leveraging these advanced techniques, the system offers enhanced security, safeguarding both users and financial institutions from potential threats and minimizing financial losses resulting from fraudulent activities. Overall, the proposed system represents a significant advancement in online transaction security, providing users and stakeholders with increased protection and peace of mind.

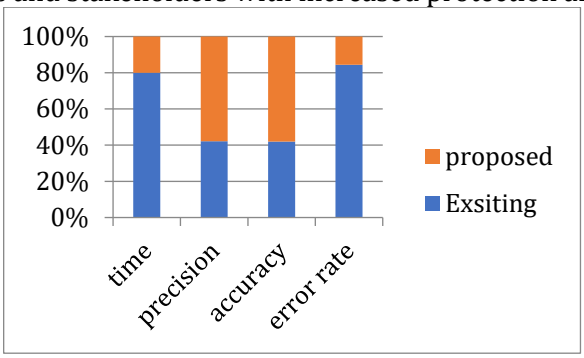

Fig 3 Evaluating the Existing and Proposed Systems Using Table 1

	time	precision	accuracy	error rate
Exsiting	8	70	68	54
proposed	2	96	94	10

Fig 4 Real time data analysis of comparison system

7. CONCLUSION

In conclusion, the proposed system presents a comprehensive and effective approach to combatting fraud in online transactions. By integrating cryptography, steganography, and data mining techniques, the system offers multi-layered protection against various forms of fraudulent activities. Through encryption of user card details, secure transmission is ensured, while steganography conceals this information within innocuous images, bolstering security measures. Furthermore, data mining algorithms analyze transaction patterns to detect deviations, enabling timely actions to mitigate risks. Each module - data encryption, image steganography, and data mining - contributes significantly to enhancing fraud prevention and detection capabilities. Overall, the proposed system represents a significant

advancement in online transaction security, providing users and financial institutions with enhanced protection and peace of mind in the digital landscape.

8. FUTURE WORK

In future works, we aim to enhance the scalability and efficiency of the proposed system to accommodate larger transaction volumes. Additionally, we plan to explore advanced machine learning techniques to further improve fraud detection accuracy. Furthermore, integrating biometric authentication methods could provide an additional layer of security and user convenience. Exploring blockchain technology for immutable transaction records is also a potential avenue for future research. Lastly, investigating real-time monitoring and alerting systems to respond swiftly to emerging fraud patterns is essential for continued system improvement.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Maria Rona L. Perez; Bobby Gerardo Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM) 2018

Hridya Venugopal; N Viswanath A robust and secure authentication mechanism in online banking 2016 Online International Conference on Green Engineering and Technologies (IC-GET) 2016

Eric Y. Chen; Shuo Chen; Shaz Qadeer; Rui Wang Securing Multiparty Online Services Via Certification of Symbolic Transactions 2015 IEEE Symposium on Security and Privacy 2015

Eric Y. Chen; Shuo Chen; Shaz Qadeer; Rui Wang Securing Multiparty Online Services Via Certification of Symbolic Transactions 2015 IEEE Symposium on Security and Privacy 2015

V. Oliyil. Kunnil; A. Pillai; S. Milshtein Biometrics assisted secure network transactions 2011 IEEE International Conference on Technologies for Homeland Security (HST) 2011

Chin-Ming Hsu; Hui-Mei Chao An online fraud-resistant technology for credit card E-transactions TENCON 2007 - 2007 IEEE Region 10 Conference 2007

Sona Kaushik; Shalini Puri Online transaction processing using enhanced sensitive data transfer security model 2012 Students Conference on Engineering and Systems 2012

Jian Xu; Andi Wang; Jun Wu; Chen Wang SPCSS: Social Network Based Privacy-Preserving Criminal Suspects Sensing IEEE Transactions on Computational Social Systems (Volume: 7, Issue: 1, February 2020) 2020

Pascal Urien Towards secure Bitcoin fast trading: Designing secure elements for digital currency 2017 Third International Conference on Mobile and Secure Services (MobiSecServ) 2017

Sri Wahjuni; Rizky Pristian Android-based token authentication for securing the online transaction system 2016 International Conference on Information and Communication Technology Convergence (ICTC) 2016