VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CHENNAI

Information Security Analysis and Audit (BCSE353E)

Research Paper on

Secure Online Transaction Using Cryptography

Submitted to-

Brindha S

Submitted by-

Ishita Agarwal (21BCE5060)

S. Caitlin (21BCE5737)

Shivansh Bansal (21BCE5742)

PROBLEM STATEMENT-

With the increasing popularity of e-commerce and online transactions, ensuring the security and privacy of sensitive user information has become a critical concern. The objective of this project is to investigate the role of cryptography in securing online transactions and identify the challenges and opportunities associated with its implementation. By conducting a detailed literature survey of recent research journals, this project aims to provide a comprehensive overview of the current state-of-the-art cryptographic techniques employed in secure online transactions.

ABSTRACT-

The rapid growth of e-commerce and online transactions has necessitated the development of robust security measures to protect sensitive user information. Cryptography has emerged as a fundamental technology for ensuring secure online transactions. This research paper aims to explore the role of cryptography in securing online transactions. It provides an overview of cryptographic techniques and protocols commonly used in online transactions, analyzes their strengths and weaknesses, and discusses potential areas for further research and improvement. The paper concludes by emphasizing the importance of cryptography in maintaining the confidentiality, integrity, and authenticity of online transactions.

OBJECTIVES-

- To investigate the fundamentals of cryptography and its applications in securing online transactions.
- To analyze and evaluate various cryptographic algorithms and protocols commonly used in online transactions.
- To identify the strengths and weaknesses of existing cryptographic techniques in terms of security, efficiency, and usability.
- To explore emerging trends and challenges in secure online transactions, including quantum computing, post-quantum cryptography, and biometric-based cryptographic systems.
- To propose recommendations for enhancing the security of online transactions using cryptography and suggest areas for future research and development.

INTRODUCTION

In the digital era, the widespread adoption of e-commerce and online transactions has revolutionized the way we conduct business and interact with services. The convenience and accessibility offered by online platforms have made them an integral part of our daily lives. However, the increasing reliance on these platforms has also raised concerns regarding the security and privacy of sensitive user information during online transactions.

The transmission of data over the internet inherently carries risks, including interception, unauthorized access, and tampering. To address these challenges and ensure the confidentiality, integrity, and authenticity of online transactions, cryptography has emerged as a fundamental technology. Cryptography involves the use of mathematical algorithms and protocols to secure data communication, making it unintelligible to unauthorized parties.

The primary objective of this project is to explore the role of cryptography in securing online transactions. By employing cryptographic techniques, such as encryption, authentication, digital signatures, and public key infrastructure (PKI), the project aims to enhance the security of online transactions and protect user information from unauthorized access and manipulation.

This project seeks to conduct a detailed literature survey to gain insights into the current state-of-the-art cryptographic techniques used in secure online transactions. The survey will examine recent research journals, focusing on the advancements, challenges, and emerging trends in the field of cryptography. By analyzing a minimum of 10 recent research journals, the project aims to provide a comprehensive overview of the existing cryptographic algorithms and protocols employed in secure online transactions.

The literature survey will encompass various aspects, including encryption techniques to safeguard the confidentiality of data, authentication mechanisms to verify the identities of transaction participants, integrity verification methods to ensure data integrity throughout the transaction process, and non-repudiation mechanisms to prevent parties from denying their involvement in transactions.

Furthermore, this project will explore the strengths and weaknesses of the identified cryptographic techniques, assessing their security, efficiency, and usability. It will also address emerging challenges and trends in the field, such as the impact of quantum computing on cryptography, the development of post-quantum cryptographic algorithms, the integration of blockchain technology, and the utilization of biometric-based cryptographic systems.

The findings of this project will contribute to a deeper understanding of the current state of secure online transactions using cryptography. It will provide valuable insights for researchers, practitioners, and policymakers seeking to enhance the security of online transactions and protect user data from evolving threats.

DETAILED LITERATURE SURVEY

1. The Impact of Global Economic Recession on Crypto Asset Trading and Transaction Security in Indonesia

Bthari Octaviani Putri, Zulkarnain Sitompul (2023)

The abstract discusses the impact of the COVID-19 pandemic on the growth of the crypto asset trading sector and highlights the need for regulations and supporting platforms to ensure business certainty and security in investing in crypto assets, particularly in Indonesia. A literature review in this context would provide an overview of existing research and discussions on the subject.

The COVID-19 pandemic has indeed had a significant impact on the global economy, leading to reduced economic growth in many countries. However, it has also resulted in some benefits for the digital investment sector, particularly in crypto asset trading. This is due to the nature of crypto asset transactions, which can be conducted online without the need for face-to-face interactions, making it attractive for investors during times of social distancing and movement restrictions.

Throughout 2021, the crypto asset trading sector witnessed substantial growth worldwide, including in Indonesia. The increasing number of investors participating in crypto asset trading reflects the growing interest and demand for these digital commodities. However, concerns regarding the security system in crypto asset investments remain. The vulnerability to fraud cases and the potential for weak security measures pose risks to investors and the overall stability of the crypto asset trading ecosystem.

Furthermore, geopolitical conflicts such as the Russia-Ukraine conflict and subsequent commodity price increases have led to inflation and the threat of a global economic recession. These economic uncertainties and the weakening global economy could potentially hinder the future growth of crypto asset trading.

In response to these challenges, the abstract emphasizes the importance of government actions in establishing regulations and supporting platforms specific to crypto asset trading. Effective regulation can provide a sense of business certainty and enhance security for investors in the crypto asset market. By creating a regulatory framework that aligns with the evolving needs of the sector, governments can stimulate the growth and development of crypto assets, both nationally and internationally.

In the literature review, relevant studies and scholarly articles would be explored to examine the impact of the COVID-19 pandemic on the crypto asset trading sector, the potential risks and vulnerabilities associated with investing in crypto assets, the role of regulations in providing security and business certainty, and the importance of supporting platforms for fostering growth in the crypto asset market. The review would also highlight any existing research gaps and areas that require further exploration to enhance understanding and inform policy decisions in this rapidly evolving field.

2. Privacy Security System for Video Data Transmission in Edge-Fog-cloud Environment

Ekhlas K. Gbashi, Abeer Tariq Maolood, Yaseen Naser Jurn (2023)

The abstract discusses a proposed light-weight cryptographic scheme for ensuring the secrecy and privacy of video data transferred within an edge-fog-cloud platform, specifically targeting video surveillance systems. Fog computing is introduced as an efficient paradigm that leverages edge devices to reduce network latency and congestion by bringing applications and data closer to end users. The paper highlights the need for secure video data transfer between fog and cloud servers and presents a three-phase framework for achieving this.

The first phase involves the generation and distribution of a secret key (SK) algorithm, implemented in a central fog node (CFN) to ensure higher security. The second phase focuses on pre-processing video frames using a frame region of interest extraction (FROI) approach. The final phase encompasses the encryption and decryption of video data using a 2D chaotic map. The key parameters affecting video encryption performance within the edge-fog-cloud infrastructure are identified as latency, accuracy, and practicability.

The performance evaluation of the proposed cryptographic scheme is conducted using common evaluation benchmarks and the urban surveillance video dataset (USVD). Several metrics are considered, including memory consumption rate, encryption and decryption time, key sensitivity analysis, and computation complexity.

The results demonstrate the effectiveness of the proposed scheme in securing transmitted video data against intruders within the edge-fog-cloud structure. Scientific comparisons are also conducted against state-of-the-art methods to highlight the performance evaluation of the proposed scheme. The findings from these comparisons support the suitability of the proposed scheme for encrypting video frames during transfer from the fog layer to the cloud computing layer.

Overall, the abstract provides an overview of the challenges in securing video data in a fog computing environment and introduces a light-weight cryptographic scheme as a potential solution. The proposed framework and evaluation metrics provide insights into the performance and effectiveness of the scheme, highlighting its suitability for securing video data in the edge-fog-cloud structure. Further exploration and comparisons with existing methods are conducted to validate the proposed scheme's performance and demonstrate its advantages over alternative approaches.

3. Robust Password Encryption Technique with an Extra Security Layer

Qusay Zuhair Abdulla, Mustafa Dhiaa Al-Hassani (2023)

The abstract highlights the vulnerability of e-banking services to fraudulent acts such as password hacking and personal information theft. With the increasing reliance on passwords for online activities, including online transactions and email communication, the need for secure passwords has become paramount. The paper introduces a novel approach to password encryption using fingerprints and random numbers to enhance password security, making each password unique and robust against attacks.

The proposed method aims to protect the password accounts of bank clients within the bank's database. It achieves this by encrypting passwords with fingerprints and random numbers, ensuring a high level of security. The encryption process is designed to be efficient, with a time elapsed of under 40 milliseconds, ensuring minimal impact on user experience.

To validate the effectiveness of the proposed method, global password datasets with varying levels of password complexity are utilized. These datasets serve as a benchmark for evaluating the strength and reliability of the encryption scheme. By testing the proposed approach against real-world password data, the paper aims to demonstrate its ability to protect user accounts effectively.

The literature review within the paper is expected to provide an overview of existing password encryption methods, highlighting their strengths and limitations. It may explore techniques such as hashing algorithms, salted passwords, and multi-factor authentication as common approaches to password security. The review will likely emphasize the shortcomings of traditional password-based authentication and the increasing need for more robust solutions.

Furthermore, the literature review may discuss the significance of fingerprint-based authentication and its advantages in terms of uniqueness and reliability. It may also explore the use of random numbers as an additional layer of security to further strengthen password encryption.

Overall, the literature review is expected to provide a comprehensive understanding of the existing research landscape in password encryption and authentication methods. By introducing a novel approach that incorporates fingerprints and random numbers, the paper aims to contribute to the field of password security and protect users' online identities and transactions.

4. Secure Payments in the Quantum Era: A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector

Onkenhout, Bharosa, N., Zhauniarovich, Y. (2023)

The abstract presents a literature review addressing the impact of quantum computing on the security of digital infrastructures in the Dutch banking sector. It emphasizes the need for guidance and governance to mitigate risks associated with quantum threats and ensure the safety and security of digital infrastructures through the adoption of post-quantum cryptography (PQC). The literature review encompasses three main methods: exploratory research, semi-structured interviews, and the development of a Technology Roadmap (TRM) framework.

The exploratory research phase involves identifying vulnerabilities in banking processes and operations in relation to quantum threats. Key concepts in cryptography, PQC developments, and banking services are described, and stakeholder and dependency mapping of the Dutch banking environment is conducted.

Semi-structured interviews are conducted with security architects, payment security specialists, and cryptography specialists from Dutch banks to gather perceptions on the impact, challenges, resources, capabilities, preparedness, and governance related to quantum threats. The interviews provide valuable insights into the perceptions and requirements of the banking sector in transitioning to PQC.

The TRM framework is developed based on thematic analysis of the qualitative data obtained from the interviews. The TRM presents a 3-phase transition plan to ensure the safety and security of digital infrastructures. Phase 1 involves developing a response plan for potential privacy breaches and a central cryptographic inventory. Phase 2 focuses on the adoption of PQC algorithms in online payment networks, including the development of requirement lists for vendors and service providers. Phase 3 includes hardware replacement, software and network infrastructure updates, and addressing technical challenges related to PQC algorithms' larger key sizes.

The literature review concludes with recommendations for the Dutch banking sector, including the need for management priority and organizational awareness regarding the quantum threat. It suggests executing initial risk-free actions, such as developing a privacy breach response plan and a hardware replacement strategy. Additionally, it emphasizes the importance of continuous collaborative research and knowledge sharing to address the quantum threat effectively.

Overall, the literature review provides a comprehensive analysis of the quantum threat to the Dutch banking sector's digital infrastructures and highlights the significance of adopting PQC and implementing a well-defined transition plan guided by the TRM framework

5. High-performance distributed system of record with cryptographic service support

(David C. Carver, Andrew F. Champagne, Ramanath Mallikarjuna, Thomas Houman,2023)

The described system is a highly efficient and scalable distributed ledger and transaction computing network fabric. It enables the simultaneous processing of a large number of transactions involving the transformation, conversion, or transfer of information or value in a reliable, secure, and efficient manner. The fabric consists of a distributed blockchain network that organizes data to allow concurrent communication, processing, and storage of blockchain blocks. This organization minimizes the need for synchronization, resulting in exceptional performance and low latency, even when transactions originate from distant sources.

The data organization within the blockchain network relies on segmenting a transaction space among autonomous but cooperating computing nodes, forming a processing mesh. Each computing node is functionally equivalent to others in the core, independently operating on blocks while maintaining a consistent and comprehensive view of the blockchain. Another key aspect of the system involves secure transaction processing, achieved by storing cryptographic key materials within secure and trusted computing environments associated with the computing nodes. This facilitates the construction of trust chains for transaction requests and their corresponding responses, ensuring a robust level of security throughout the process.

This disclosure presents a distributed ledger and transaction computing network fabric designed for high performance. It facilitates the concurrent processing of a large volume of transactions involving the transformation, conversion, or transfer of information or value in a manner that is scalable, reliable, secure, and efficient. The fabric's "core" is configured to support a distributed blockchain network that organizes the blockchain data to enable concurrent communication, processing, and storage of blockchain blocks. This concurrent operation occurs with minimal synchronization, resulting in exceptional performance and low latency, even when transactions originate from remote sources.

The data organization within the blockchain network is achieved by segmenting a transaction space among autonomous computing nodes that collaborate as a processing mesh. Each computing node within the core is typically functionally equivalent to others, capable of independently processing the entire workload of the system. A computing node consists of computing, communications, and storage elements clustered together. Importantly, all computing nodes within the core network are considered equal, without any single node being inherently trusted or having control over another. The nodes operate independently on blocks while maintaining a consistent and comprehensive view of the blockchain as a whole, ensuring data integrity and completeness.

6. Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming

(J Kh-Madhloom - Wasit Journal of Computer and Mathematics Sciences, 2022)

Blocks and chains are essential components of a blockchain, which is a decentralized network. These terms refer to collections of data that are interconnected through cryptography. Cryptography ensures the security of the blockchain by adding entries to each block as the list expands.

Two important cryptographic techniques used in blockchains are asymmetric-key cryptography and hash functions. Hash functions provide participants with a comprehensive representation of the network. The SHA-256 hashing algorithm is commonly employed in blockchains. In blockchain systems like Bitcoin, where addresses are linked to public-private key pairs, blockchains play a crucial role.

In blockchain cryptography, a public key represents a person's address, which is accessible to all participants. The private key is utilized to access the address database and authorize activities associated with the address. Encryption is vital for maintaining the integrity of the blockchain ledger. Each transaction on the blockchain is recorded using encrypted data. As long as users possess their cryptographic keys, they can buy or trade cryptocurrencies securely. Cryptographic hashing is employed to store the root hashes of all transactions in blockchains. If anyone tries to tamper with any data within the blockchain, the root hash will be completely altered. By comparing root hashes with other systems, data integrity can be verified.

Presently, both governments and corporations are actively incorporating blockchain technology to safeguard their applications. They aim to ensure privacy and integrity through the implementation of secure Proof of Work (PoW) algorithms. In the field of criminal forensic and law enforcement, researchers and forensic scientists can leverage blockchain technology to accurately predict the identities of certain individuals. To store transaction data, as well as private and public keys (such as a private/public key pair), software tools like Electrum and Bitcoin Core, along with hardware devices like Ledger, can be utilized. It is crucial to understand that these wallets do not contain any actual money like Bitcoin or Ethereum. They simply serve as storage for private keys and transaction balances. A blockchain wallet is required for conducting transactions with other users. Essentially, the blockchain holds all the factual information and currency within blocks, not within the wallet itself. It functions similarly to a digital signature, providing identification for both the recipient and the entire blockchain network. To create a unique digital signature each time a transaction is initiated with another node, a specific method combines your data and cryptographic signature. This ensures the authenticity of your node and the data it transmits.

7. A Three-Level Gateway protocol for secure M-Commerce Transactions using Encrypted OTP

S. Ramana; S China Ramu; N. Bhaskar; M. V. Ramana Murthy; C. R. K. Reddy, 2022

Mobile commerce, which began in ancient times as the trade system, has grown in the ultramodern age due to improvements in technology, the Internet, the use of Financial Coffers, and the lives of mortal humans. There was a significant extemporization in the tackle industry and concurrent software development that led to a wide range of uses for computers and mobile phones. Ninety percent of people who take prescription drugs do so on handhelds, laptops, or cellphones, and the lives of mortals have been profoundly altered as a result of the smart operations available on mobile systems, which may be utilized at any time and from any location (Everything through one device). With mobile dispatching, so-called trade has been transformed into mobile commerce. Mobile commerce, or m-commerce, is a term used to describe all aspects of a possible marketable commercial agreement that are carried out over wireless or mobile networks, such as text messaging and email. Mobile Commerce tackles the mobile bias of electronic commerce, where the customer does not view any product that is being purchased physically. Mobile Commerce He has just a virtual representation of the thing being purchased. As a consumer and as a producer, the advantages of mobile commerce are vast, but there are also many challenges and security considerations that are keeping many mobile druggies from making the leap. Despite the adoption of several cryptographic security techniques and communication protocols, there are still a few ifs and buts. Three-Level Gateway Protocol for Secure M-Commerce Deals is presented in this paper, which uses any conventional or public-crucial algorithm and the Advanced Message Queuing Protocol (AMQP), an open standard for passing messages between operations or associations, and an Encrypted OTP in the payment process to ensure confidentiality of da and to prevent Replay Attacks, Man in the Middle Attacks, and Masking attacks of Cryptography systems.

8. **Secure online payment through facial recognition and proxy detection with the help of TripleDES encryption**

R. Venkatesan,B. Anni Princy,V. D. Ambeth Kumar,Manish Raghuraman,Mukesh Kumar Gupta,Ankit Kumar,Abhishek Kumar &Ajoy Kumar Khan, 2021

The rapid adoption of online secure payment systems has transformed the way transactions are conducted, enabling even roadside shops in countries like India to accept cashless payments. However, amidst this digital revolution, ensuring the security of online transactions remains a critical concern. As a result, researchers have been actively developing new techniques to enhance security, each with its own advantages and disadvantages.

To address this issue, a two-way authentication system has been introduced in this paper, aiming to bolster the security of online transactions. This system incorporates facial recognition and proxy detection as additional layers of security before the user enters their UPI (Unified Payments Interface) pin. The algorithm utilized in this research focuses on embedding 128 feature points of the user's face, thereby improving the accuracy of facial recognition. By employing this approach, the system can verify the identity of the user with a higher level of certainty.

Furthermore, to ensure the secure transmission of data during verification, tripleDES (Triple Data Encryption Standard) encryption has been implemented. This encryption technique adds an extra layer of protection to the sensitive data being transmitted, enhancing the overall security of the system.

Once the verification process is successfully completed by the system, the user's bank balance is verified, and the transaction is carried out. The proposed system boasts improved efficiency compared to existing approaches, offering a more streamlined and secure experience for users. Additionally, the system's simple user interface (UI) contributes to its usability and accessibility, making it easy for individuals to adopt and navigate.

This literature review highlights the significance of addressing security concerns in online transactions, particularly in the context of secure payment systems. The proposed two-way authentication system, incorporating facial recognition, proxy detection, and tripleDES encryption, demonstrates advancements in security measures while also prioritizing efficiency and user-friendliness. As the digital landscape continues to evolve, it is crucial to develop robust security mechanisms that can adapt to emerging threats and safeguard sensitive financial information during online transactions.

9. Resilient Concurrent Consensus for High-Throughput Secure Transaction Processing

(S Gupta, J Hellings, M Sadoghi - 2021 IEEE 37th International …, 2021)

In recent times, the emergence of consensus-based database systems that offer various advantages such as resilience against failures, robust data provenance, and federated data management is witnessed. Typically, these systems rely on a primary-backup consensus protocol, where fully-replicated systems operate with a primary replica, resulting in throughput limitations determined by the capabilities of a single replica.

To overcome this limitation and increase throughput, we propose the concept of concurrent consensus. In concurrent consensus, replicas independently propose transactions, reducing the impact of any individual replica on performance. To implement this idea, we introduce our RCC (Replica Concurrent Consensus) paradigm, which can transform any primary-backup consensus protocol into a concurrent consensus protocol by concurrently running multiple consensus instances. RCC is specifically designed to optimize performance and requires minimal coordination between instances. Additionally, RCC offers improved resilience against failures.

To validate the effectiveness of RCC, we implemented it in RESILIENTDB, our high-performance resilient blockchain fabric, and compared it against state-of-the-art primary-backup consensus protocols. Through experiments, we demonstrated that RCC achieves up to 2.75 times higher throughput compared to other consensus protocols and can be scaled up to 91 replicas.

Concurrent consensus has been proposed as a significant advancement towards e.nabling high-throughput and more scalable consensus-based database systems. The concept suggests that concurrent consensus can achieve higher throughputs than primary-backup consensus systems. To put this idea into practice, the RCC paradigm was introduced, which allows normal primary-backup consensus protocols to be made concurrent. RCC not only increases throughput but also enhances the resilience of consensus-based systems by minimizing the impact of faulty replicas. To validate the effectiveness of the RCC paradigm, it was implemented in RESILIENTDB, a high-performance resilient blockchain fabric, and compared against state-of-the-art primary-backup consensus protocols. The experiments demonstrated that RCC surpasses other consensus protocols, delivering superior performance and scalability. These results indicate that RCC has the potential to pave the way for the development of new high-throughput resilient database and federated transaction processing systems.

10. An Efficient Secure Electronic Payment System for E-Commerce

Md Arif Hassan, Zarina Shukur, Mohammad Kamrul Hasan, 2020

E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. As e-commerce is quickly developing on the planet, particularly in recent years, many areas of life are affected, particularly the improvement in how individuals regulate themselves non-financially and financially in different transactions. In electronic payment or e-commerce payment, the gateway is a major component of the structure to assure that such exchanges occur without disputes, while maintaining the common security over such systems. Most Internet payment gateways in e-commerce provide monetary information to customers using trusted third parties directly to a payment gateway. Nonetheless, it is recognized that the cloud Web server is not considered a protected entity. This article aims to develop an efficient and secure electronic payment protocol for e-commerce where consumers can immediately connect with the merchant properly. Interestingly, the proposed system does not require the customer to input his/her identity in the merchant's website even though the customer can hide his/her identity and make a temporary identity to perform the service. It has been found that our protocol has much improved security effectiveness in terms of confidentiality, integrity, non-repudiation, anonymity availability, authentication, and authorization.

In the electronic payment system, the payment gateway is an essential component of the infrastructure to confirm that such exchanges happen with no concerns and to ensure that the common security over electronic systems is maintained. Such a system will help secure a purchase along with a person's transaction information. A payment gateway defends transaction information by encrypting personal information, such as credit/debit card details, to guarantee that information is transferred securely between a consumer and the transaction processor. Each online exchange should go through a managed transaction gateway. The secure electronic payment structure includes four system segments. The interaction between the segments operate through protected communication tunnels. Secure communication tunnels offer a protected method for interaction between two or more people, or between segments, such as the buyer to the merchant, on the transaction gateway. The e-payment system must be harmless for online transaction applicants, for instance, fee gateway server, bank account server, and merchant server.

11. Cross Blockchain secure transactions

(Peter Joseph Vessenes, Philip Hofer,2019)

The paper titled "Cross blockchain secure transactions" by PJ Vessenes and P Hofer, published in a US Patent Application in 2019, explores the concept of securely conducting transactions between different blockchains. The authors propose a method that involves utilizing cryptographic properties to establish a secure connection between a Bitcoin (BTC) address and an Ethereum address and leveraging the smart contract functionality of Ethereum to verify corresponding Bitcoin transactions.

The disclosed invention introduces computing devices, systems, and methods that facilitate the operation of a cross-blockchain secure token transaction engine. This engine aims to enable seamless token transfers between different blockchains. The process involves identifying a specific set of one or more tokens from a first blockchain, securely locking these identified tokens, and generating a corresponding set of one or more tokens from a second blockchain. These tokens from the second blockchain are intended to be converted back to tokens of the first blockchain at a later stage, utilizing the locked set of tokens from the first blockchain. By employing this mechanism, the invention enables efficient and secure token transactions across multiple blockchains, enhancing interoperability and expanding the possibilities of token-based ecosystems.

The computing devices, systems, and methods described in the invention play a crucial role in ensuring the smooth operation of the cross-blockchain secure token transaction engine. By implementing this technology, users can seamlessly bridge tokens between different blockchains, overcoming the limitations of operating within a single blockchain. The engine accomplishes this by first identifying and securely locking a specific set of tokens from the first blockchain. Subsequently, it generates a corresponding set of tokens from the second blockchain, which can be later converted back to tokens of the first blockchain using the locked set of tokens. This innovative approach enhances the flexibility, efficiency, and utility of token transactions, opening up new opportunities for decentralized applications and token-based systems.

12. Securing Online Transaction Using Visual Cryptography

(Rajguru P, Dhomse J, Pawar PY,2018)

Information security plays a very important role in the current era of technologies. Multimedia data like images, video etc. are widely used and they are widely transmitted using the network. So security is an important aspect. Visual cryptography is a type of secret sharing for encrypting written material like text, images in a perfectly secure way. For this project we are using anti-phishing for detecting the attack, there many types of anti-phishing mechanisms are used. In phishing process, suppose attacker sends out thousands of phishing emails with a link to the fake website.

Hash-Based password schemes are easy and fast because those are based on text and famed cryptography. So, cyber-attacks get the password by cracking tool or hash-cracking online sites. Attackers can get easily original password from the hash value when that is relatively simple and plain. As a result, many hacking accidents have been happened in systems adopting those hash-based schemes In this work, password processing scheme based on an image using visual cryptography (VC). Different from the traditional scheme based on hash and text, this scheme transforms a user ID of text type to two images encrypted by VC. The user should make two images consisted of sub pixels by random function with SEED which includes personal information. The server only has user’s ID and one of the images instead of the password. When the user logs and sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate the user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hash cracking and supports authentication not to expose personal information such as ID to attackers .In these paper new scheme for providing security during an online transaction for online frauds detection using Extended Visual Cryptography (EVC) and QR code. By using this technique, we provide better security to people. In proposed system user first registered on the website. The client sends ID and password to bank server for verification. If it is valid then generate One Time Password (OTP) and apply EVC for shares generation. Bank server sends one share to the client and one share to the server. At the time of reconstruction, two shares are combined to reveal the original OTP. Then the client sends this OTP to bank server for verification.