A logo for a university

Description automatically generated

**School of Computer Science Engineering and Information Systems**

**Fall Semester 2023-24 MTech (Software Engineering)**

**SWE3002 – Information and System Security – C1+TC1**

**J Component**

**FINAL REVIEW**

SECURE ELECTRONIC FUND TRANSFER OVER INTERNET USING AES & SHA-512

Team Members:

**MOGITH P - 21MIS0204**

**MOTHISWAR T B G - 21MIS0258**

**SHOMESH M – 21MIS0384**

Faculty:

**Prof. SUDHA M**

**Date: 24.11.23**

**Table of Contents:**

* Executive Summary and Keywords
* Problem statement
* Literature Review
* Scope of Application in real time scenarios
* Proposed Model Framework Design
* Protocol Steps and Pseudo code
* Module Description
* Implementation Platform
* Performance Metrics and Run results
* Demo Screenshot.
* Conclusion
* References

**Executive Summary:**

This electronic fund transfer platform, designed to offer a seamless and secure financial management experience. Our commitment to user-friendly design ensures that navigating our website is intuitive, allowing you to effortlessly access key features. Stay in control of your financial landscape by easily checking account balances, reviewing transaction histories, and setting up personalized alerts to stay informed about your financial activities. Our emphasis on security is paramount; we employ state-of-the-art encryption and robust security measures to safeguard your transactions and personal information. Managing your money is made convenient through features such as easy fund transfers between accounts and the ability to pay bills online with just a few clicks. Whether you're at home or on the go, our mobile app mirrors the functionality of our website, providing flexibility and accessibility. Our dedicated customer support team is ready to assist you with any queries or concerns, ensuring a responsive and personalized experience. Stay up-to-date with the latest news and updates in the financial world through our platform, as we strive to keep you informed about enhancements to security measures and the introduction of new features. Embrace the convenience and peace of mind that come with secure online banking, where your financial well-being is our top priority.

**Keywords:**

E-Fund TransferElectronic Money MovementVirtual Fund TransferDigital Currency TransferOnline Funds TransmissionDigital Transaction of FundsE-Wallet TransferInternet Fund TransferElectronic Payment SystemDigital RemittanceCyber Money MovementOnline Financial Transaction

**Problem Statement:**

The existing electronic fund transfer systems are confronted with a series of challenges that compromise their efficiency and reliability, posing potential risks to users. One notable issue is the frequent occurrence of delays in transaction processing, which not only hampers the speed of financial transactions but also introduces uncertainties into the user experience. These delays can be attributed to various factors, including network congestion, technical glitches, and interbank communication bottlenecks. Consequently, these inefficiencies undermine the core promise of electronic fund transfers to provide a quick and seamless financial transaction experience.

Moreover, system downtimes have been a recurring problem, causing disruptions in service availability. Unplanned outages can result from technical issues, maintenance activities, or cyber threats, leaving users unable to access their funds or complete crucial transactions during such periods. These interruptions not only inconvenience users but can also lead to financial losses and erode trust in electronic fund transfer systems.

In addition to operational challenges, the electronic fund transfer landscape grapples with complexities, particularly in the context of cross-border transactions. The intricacies involved in navigating different regulatory frameworks, currency exchanges, and varied banking protocols can create obstacles for users seeking to transfer funds seamlessly across international borders. These complexities not only hinder the user experience but also raise concerns about the transparency and predictability of cross-border electronic fund transfers.

As the demand for efficient and secure electronic transactions continues to grow, addressing these multifaceted challenges becomes imperative to ensure that electronic fund transfer systems fulfill their promise of providing users with a reliable, swift, and secure financial transaction experience.

**Literature Review:**

1. **Citation: Akash, Aryan, Astha, Diksha. “Secure Electronic Fund Transfer Over Internet Using AES Algorithm.” *International Advanced Research Journal in Science, Engineering and Technology* - Vol. 8, Issue 7, July 2021**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Electronic Fund Transfer Over Internet | This paper proposes a method to secure Electronic Fund Transfer using AES algorithm. The AES algorithm is very secure and is used in a variety of applications, including electronic fund transfer. The one-time password (OTP) is a security mechanism that is used to authenticate the user's identity | Uses combination of AES and One Time Password which is randomly generated number that is sent to user’s mobile phone. | AES is a very secure algorithm. It has been subjected to extensive cryptanalysis. It is efficient. It is easy to implement. There are many freely available implementations of AES available, making it easy to integrate into existing systems. | Side-channel attacks: Side-channel attacks are a type of attack that exploits information that is leaked during the encryption process.  Hardware attacks: Hardware attacks are a type of attack that targets the physical implementation of the encryption algorithm.  Quantum attacks: Quantum attacks are a type of attack that uses quantum mechanics to break encryption algorithms. |

1. **Citation: Aysan, Mohammed Abdullah Mohammed. "Implementation of electronic fund transfer using new symmetric key algorithm based on simple logarithm." *International Journal of Advanced Research in IT and Engineering* 3.4 (2014): 10-16.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Electronic fund transfer Over Internet | This paper proposes a symmetric key algo to implement electronic fund transfer. Here,the sender generates a random key pair (public key, private key). The sender encrypts the message using the receiver's public key. The receiver decrypts the message using their private key. | Uses Symmetric Key algorithm based on simple logarithm | **Efficiency:** The proposed algorithm is efficient because it only requires basic mathematical operations.  **Security:** The proposed algorithm is secure because it is based on a well-known cryptographic primitive, simple logarithm.  **Simplicity:** The proposed algorithm is simple to implement and use. | One weakness of the proposed algorithm is that it is vulnerable to a chosen-plaintext attack. In a chosen-plaintext attack, the attacker can choose the plaintext that is encrypted. This allows the attacker to learn more about the encryption algorithm and potentially break the encryption. Another weakness of the proposed algorithm is that it is not as secure as more modern cryptographic algorithms. |

1. **Citation: Islam, Md Syeful. "An algorithm for electronic money transaction security (Three Layer Security): A new approach." *International Journal of Security and Its Applications* 9.2 (2015): 203-214.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Secure Electronic money transaction | This paper proposes a technique to perform electronic money transaction in a secure way using algorithm (Three Layer Security:  **Physical Layer** – encryption, authentication, access control.  **Data Link Layer** – encryption, authentication, message integrity.  **Application Layer** – encryption, authentication, authorization) | Uses Three Layer Security (Physical, Data Link and Application Layer) | It is a comprehensive security algorithm that addresses the security needs of electronic money transactions at all layers. It uses a variety of techniques to achieve security, which makes it more difficult for attackers to circumvent. It is flexible and can be adapted to meet the specific needs of different applications. | It is complex and may be difficult to implement and maintain. It may not be as efficient as some other security algorithms. It may not be able to withstand attacks that exploit vulnerabilities in the underlying technologies |

1. **Citation: Dixit, Uma. “Cryptography – Security in E-Banking.” (2017).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Security in E-banking | This paper proposes cryptographic technique to provide security in E-banking. This type of security is carried out by Symmetric encryption (AES), Asymmetric Encryption (RSA) and Hash Functions. | Uses Symmetric Encryption, Asymmetric Encryption and Hash Functions. | It is a comprehensive methodology that addresses the security needs of e-banking at all levels. It uses a variety of techniques to achieve security, which makes it more difficult for attackers to circumvent. It is flexible and can be adapted to meet the specific needs of different e-banking applications. It is based on well-established cryptographic principles, which makes it reliable and secure. | It can be complex and difficult to implement. It can be expensive to deploy and maintain. It can be vulnerable to new attacks. It can rely on human factors, such as user education and behaviour, which can be unpredictable. |

1. **Citation: A. Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar. " Securing Online Transactions with Cryptography and Secured Authentication Methods." *International Journal of Recent Technology and Engineering (IJRTE)*: 2277-3878 (Online), Volume-8, Issue-1, May 2019**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Online Transactions carried out during payments | This paper proposes a method to secure Online Transactions with Cryptography and Secured Authentication Methods which covers Authentication (two-factor authentication), Securing connection (transport layer security or secure sockets layer) and Encrypting message (Symmetric key and Unsymmetric key) | Uses authentication, Securing the connection, Encryption (Symmetric Key and Unsymmetric Key). | It is a layered approach that uses multiple security mechanisms to protect against a variety of attacks. It is based on well-established and proven technologies, such as TLS and AES. It is flexible and can be adapted to different needs and requirements. It is scalable and can be used to protect large volumes of transactions. It is cost-effective and can be implemented with relatively low investment. | It is complex and can be difficult to implement and maintain. It relies on the security of the underlying technologies, which could be compromised in the future. It may not be suitable for all types of online transactions. |

1. **Citation: Manvandra Tomar, Sourabh Pal, Shefali Raina. “Card Payment Security Using RSA.” *JETIR*: July 2021, Volume 8, Issue 7**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Card Payment Security | This paper proposes a technique to secure card payment using RSA **(**public-key cryptography algorithm that is considered to be secure, It uses a combination of two large prime numbers to generate a public and private key pair. The public key can be used to encrypt data, while the private key can be used to decrypt it.) | Uses RSA | It is a secure approach to securing card payments. The use of RSA cryptography helps to protect cardholder data from unauthorized access. It is a scalable approach. The methodology can be used to protect card payments at any scale, from small businesses to large enterprises. It is a reliable approach. The RSA algorithm has been used for many years to protect sensitive data | It is complex and can be difficult to implement and maintain. The methodology involves several different steps that need to be implemented correctly. It relies on the security of the RSA algorithm. If the RSA algorithm is compromised, then the methodology could be rendered ineffective. |

1. **Citation: Saad M. Darwish, Ahmed M. Hassan. “A model to authenticate requests for online banking transactions.” *Alexandria Engineering Journal*, Volume 51, Issue 3, 2012, Pages 185-191, ISSN 1110-0168.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Authentication Requests for Online Banking Transactions | This paper proposes a model for authenticating requests for online banking transaction way by usingIdentity-Based Mediated RSA (IB-mRSA) technique with a one-time ID concept to increase security, avoid swallow sorties, and prevent counterattacks. The model is more secure than traditional methods and resistant to common attacks but requires the use of a trusted third party and can be more complex to implement. | Uses Identity-Based Mediated RSA | It is more secure than traditional authentication methods, such as usernames and passwords, because it does not require the customer to share his private key with the bank server. It is immune to swallowing and counterattacks. It is practical from both computational and storage point of view. | It requires the use of a trusted third party, SEM server. It can be more complicated to implement than traditional authentication methods |

1. **Citation: Khudhur, D. Yaseen, S. Saad Hameed, and Shokhan M. Al-Barzinji. "Enhancing e-banking security: using whirlpool hash function for card number encryption." *International Journal of Engineering and Technology* 7.2 (2018): 281-286**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Enhancing E-banking Security | This paper proposes a technique to secure E-banking using the Whirlpool Hash Function for Card Number Encryption. The proposed technique is secure and collision-resistant, and it reduces the risk of data breach. The hash value is stored only on the customer's device and the bank's server which reduces the risk of data breach. | Uses Whirlpool Hash Function | The Whirlpool hash function is a secure and collision-resistant hash function. Using a salt value makes it more difficult to crack the hash value. The hash value is stored only on the customer's device and the bank's server, which reduces the risk of a data breach. | The hash value is not reversible, so the original card number cannot be recovered. If a salt value is compromised, all hash values ​​generated with that salt value will be compromised. |

1. **Citation: S. M. T. Toapanta, A. A. S. Balladares, D. F. H. Subia and L. E. M. Gallegos, "Prototype of a Security Model to Mitigate Risks in the Management of Electronic Money in Ecuador." 2019 Third World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, UK, 2019**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Mitigate Risks in the Management of Electronic Money in Ecuador. | This paper proposes a Prototype of a Security Model to Mitigate Risks in the Management of Electronic Money in Ecuador. This method is well established encryption algo and is relatively easy to implement. It uses AES algo to encrypt electronic money transactions. This algo is robust and efficient. | Uses AES to encrypt electronic money transactions. | It is a strong and effective method to secure electronic money transactions. It is relatively easy to implement and use. It is compatible with existing electronic money systems. | It requires the use of strong session keys, which can be compromised if not generated or stored properly. It can add some overhead to electronic money transactions. |

1. **Citation: Jadhao, Abhilesh S., and Shital B. Kumbhalkar. "Technical review on secure banking using RSA and AES encryptor methodologies." *IOSR Journal of Electronics and Communication Engineering* 11.1 (2016): 1-4.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Secure Banking | This paper proposes technical review on secure banking using RSA and AES Encryptor Methodologies**.** RSA ensures strong encryption for data transmission and authentication, while AES efficiently secures bulk data. The robustness of RSA and efficiency of AES collectively enhance security. This methodology highlights the significance of proper key management and encryption for bolstering online banking security. | Uses RSA encryption and AES encryption | **RSA's Strong Encryption:** RSA provides robust asymmetric encryption, ensuring secure data transmission and user authentication in online banking transactions.  **AES Efficiency:** AES offers efficient symmetric encryption for bulk data, ensuring confidentiality and integrity of sensitive information.  **Key Management**: RSA's public-private key pair and AES's session keys enable effective key management, enhancing security. | **RSA Processing Overhead:** RSA encryption is computationally intensive, which can slow down systems during encryption and decryption processes.  **Key Distribution:** Secure distribution of RSA public keys and management of AES session keys  **Key Storage:** Safeguarding RSA private keys and AES keys from unauthorized access is crucial; any breach could compromise security. |

1. **Citation: Maheshwari, Anita. "Two-way authentication protocol for mobile payment system." *International Journal of Engineering Research and Applications* 2.4 (2012): 2003-2007.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Mobile Payment System | This paper proposes a technique for mobile payment system using two-way authentication protocol. The protocol is designed to be secure because it uses symmetric encryption, hashing, and digital signatures. These techniques ensure that the communication is private, secure, and authentic. The protocol is also designed to be efficient because it does not require the use of a third party. | Uses symmetric encryption, hashing (generate message authentication codes) and digital signatures. | **Security:** MACs can help to protect mobile payments from tampering and replay attacks.  **Efficiency**: MACs are relatively easy to implement, and they do not add a significant amount of overhead to the communication process.  **Scalability:** MACs can be used to secure mobile payments at scale. | **Tamper resistance:** MACs are not as tamper resistant as digital signatures.  **Key management:** The secret key used to generate and verify MACs must be kept secure.  **Performance:** MACs can add some overhead to the communication process. |

1. **Citation: Qulmurodovich, Shonazarov Soatmurot, Bozorov Asqar Khaitmurotovich, and Xolliyev Faxriddin Boxodirovich. "APPLICATION OF SECURE ELECTRONIC TRANSACTION PROTOCOL IN ELECTRONIC PAYMENT SYSTEM." *Galaxy International Interdisciplinary Research Journal* 9.6 (2021): 222-225.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Electronic Payment System | This paper proposes a method to use Electronic Payment System by Application of Secure Electronic Transaction Protocol (Initialization, Authorization, Purchase and Settlement). The SET protocol is a complex protocol, but it provides a high level of security for electronic payments. The protocol is used by many e-commerce websites and other organizations that accept electronic payments. | Uses SET protocol | The SET protocol provides a high level of security for electronic payments.  It uses a variety of security techniques, including authentication, encryption, integrity, and non-repudiation.  It is widely used by e-commerce websites and other organizations that accept electronic payments. | The SET protocol is complex and can be difficult to implement.  It requires all parties involved in a transaction to use SET-compliant software.  It can be expensive to deploy and maintain. |

1. **Citation: Venkatesh, Gotimukul, et al. "Application of session login and one time password in fund transfer system using RSA algorithm." *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*. Vol. 2. IEEE, 2017.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Fund Transfer System | This paper proposes a technique for session login and one time password in fund transfer system using RSA algorithm.The proposed methodology and algorithm provide a high level of security for fund transfer transactions. The session ID ensures that the user is authenticated for the duration of the session. The OTP provides an additional layer of security by ensuring that the user is in possession of the mobile phone that received the OTP. | Uses RSA | **High level of security:** The use of session login and OTP authentication provides a high level of security for fund transfer transactions.  **Easy to use:** The methodology and algorithm are easy to use for both users and system administrators.  **Scalable:** The methodology and algorithm can be scaled to support a large number of users and transactions.  **Cost-effective:** The methodology and algorithm are cost-effective to implement and maintain. | **Dependency on mobile phones:** The methodology and algorithm are dependent on mobile phones to deliver the OTP...  **Susceptible to phishing attacks:** The methodology and algorithm is susceptible to phishing attacks as attacker can send a fake email or text message that appears from banks. |

1. **Citation: Manakshe, Amit R., et al. "Analysis of secure electronic transmission (SET) system for electronic transactions." *International Journal of Research in Advent Technology* 2.3 (2014): 12-15.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Electronic Transmission Systems | This paper proposes a method of analysing Secure Electronic Transmission (SET) System for Electronic Transactions. The algorithm used in the SET protocol is a combination of public-key cryptography and symmetric cryptography. Public-key cryptography is used to authenticate the parties involved in a transaction and to encrypt the payment information during transmission. Symmetric cryptography is used to encrypt the payment information after it has been authenticated and transmitted | Uses Secure Electronic Transmission System | **High level of security:**The SET protocol provides a high level of security for electronic payments.  **Widespread adoption:** The SET protocol is widely adopted by e-commerce websites and other organizations that accept electronic payments.  **Scalability:** The SET protocol is scalable, meaning that it can be used to support a large volume of transactions. | **Complexity:** The SET protocol is complex and can be difficult to implement.  **Cost:** The SET protocol can be expensive to deploy and maintain  **Interoperability:** The SET protocol is not always interoperable with other security protocols. |

1. **Citation: Akinyede, R. Olufemi, and O. Aidohelen Esese. "Development of a secure mobile e-banking system." *International Journal of Computer (IJC)* 26.1 (2017): 23-42.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Secure Mobile E-banking System | This paper proposes a technique for development of a secure mobile E-banking System using Salted SHA-512 hash function (more difficult to crack hashed password), AES and One-time password (generated by bank’s server and sent to user’s mobile device. | Uses Salted SHA-512, AES and OTP. | It uses a variety of security measures to protect users' data and transactions, including salted SHA-512 hash function, AES encryption, and OTP authentication. It is implemented using PHP, JavaScript, CSS, and MySQL database, which are all widely used and well-tested technologies. The system has been evaluated and found to be secure against a number of common hacking attacks. | It is still a relatively new system, and it is possible that there are still security vulnerabilities that have not been identified. The system depends on the user's mobile device to be secure. If the user's device is compromised, then the system could also be compromised. The system is not immune to social engineering attacks. For example, a user could be tricked into clicking on a malicious link that steals their login credentials. |

1. **Citation: Moe, Sandar, and Zin May Aye. *Online Money Transfer System Using ElGamal Digital Signature Scheme*. Diss. MERAL Portal, 2010.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Summary** | **Method** | **Strength** | **Weakness** |
| Online Money Transfer System | This paper proposes a technique to transfer money online using ElGamal Digital Signature Scheme. This digital signature is a public key cryptography scheme that allows users to sign digital messages in such a way that the signature can be verified by anyone with the user's public key. This makes it possible to verify the authenticity of a message and to ensure that the message has not been tampered with. | Uses ElGamal Digital Signature Scheme | It uses a secure digital signature scheme to authenticate money transfer messages. It is relatively easy to implement. It is efficient in terms of computational resources. | It is still a relatively new system, and it is possible that there are still security vulnerabilities that have not been identified. The system depends on the user's devices to be secure. If the user's device is compromised, then the system could also be compromised. The system is not immune to social engineering attacks. For example, a user could be tricked into clicking on a malicious link that steals their login credentials. |

**Scope of Application in real time scenarios:**

An electronic fund transfer has a wide range of applications and can provide creative answers for a variety of real-time problems. Below are major areas of application:

**1. Swift Transactions:** Real-time electronic fund transfer systems facilitate instant money transfers, allowing individuals and businesses to execute financial transactions swiftly. This is particularly crucial in scenarios where time-sensitive payments, such as bill payments and urgent fund transfers, are required.**2. Seamless Cross-Border Transactions:** Real-time electronic fund transfer solutions can bridge the gap in cross-border transactions. With the capability to process transactions rapidly and efficiently, users can engage in international money transfers with reduced processing times and enhanced convenience, fostering global economic interactions.**3. Enhanced Financial Inclusion:** Real-time fund transfer can contribute to financial inclusion by providing individuals in remote or underserved areas with quick and accessible banking services. Mobile banking and digital wallets powered by real-time transfer capabilities enable people in diverse locations to participate in the formal financial sector.**4. Business Efficiency:** For businesses, real-time electronic fund transfer is instrumental in improving operational efficiency. Quick disbursement of salaries, instant supplier payments, and prompt settlement of invoices contribute to smoother business operations and better cash flow management.**5. Emergency Situations:** Real-time electronic fund transfer is invaluable in emergency situations where immediate access to funds is crucial. Whether it's for medical emergencies, unexpected expenses, or urgent financial needs, real-time transactions offer a lifeline in critical situations.**6. Fintech Innovation:** Real-time fund transfer systems provide a fertile ground for fintech innovation. Startups and established financial technology companies can leverage real-time capabilities to create innovative solutions, such as peer-to-peer payment platforms, budgeting apps, and other financial tools that enhance user experiences.

**Proposed Model Framework Design:**

A screenshot of a computer screen

Description automatically generated

**Protocol Steps and Pseudocode:**

**AES:**

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used for securing sensitive data. Here are the basic protocol steps for AES encryption and decryption:**AES Encryption:Key Expansion:** Derive round keys from the original encryption key using the key expansion algorithm. The number of rounds is determined by the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

**Initial Round:**  Add the initial round key (derived from the encryption key) to the plaintext.

**Rounds:** Perform a series of substitution (SubBytes), permutation (ShiftRows), mixing (MixColumns), and key addition (AddRoundKey) operations for the specified number of rounds based on the key size.

**Final Round:** Perform a final round without the Mix Columns operation.

**Cipher Text:** The result after the final round is the ciphertext.

**AES Decryption:Key Expansion:** Use the same key expansion algorithm to derive round keys for decryption.

**Initial Round:**

Add the initial round key to the ciphertext.

**Rounds (in reverse order):** Perform the inverse operations of the encryption rounds: inverse SubBytes, inverse ShiftRows, inverse MixColumns, and key addition with the derived round key.

**Final Round:**

Perform a final round without the inverse MixColumns operation.

**Decrypted Text:**

The result after the final round is the decrypted plaintext.**Note:** The key expansion process is crucial for generating the round keys used in each round of encryption and decryption. SubBytes involves replacing each byte of the state with a corresponding byte from the S-box (a predefined substitution table). ShiftRows involves cyclically shifting the rows of the state. MixColumns is a mixing operation performed on the columns of the state. AddRoundKey involves bitwise XOR of the state with a round key.

<?php

function aes\_encrypt($plaintext, $key) {

    // Add necessary error checking for inputs

    $blockSize = 16; // 128-bit block size for AES

    $cipher = "AES-128-ECB"; // AES with a 128-bit key in ECB mode

    // Check and pad the plaintext

    $plaintext = pad($plaintext, $blockSize);

    // Encrypt using AES

    $ciphertext = openssl\_encrypt($plaintext, $cipher, $key, OPENSSL\_RAW\_DATA);

    return base64\_encode($ciphertext);

}

function aes\_decrypt($ciphertext, $key) {

    // Add necessary error checking for inputs

    $blockSize = 16; // 128-bit block size for AES

    $cipher = "AES-128-ECB"; // AES with a 128-bit key in ECB mode

    // Decrypt using AES

    $decrypted = openssl\_decrypt(base64\_decode($ciphertext), $cipher, $key, OPENSSL\_RAW\_DATA);

    // Remove padding

    $decrypted = unpad($decrypted);

    return $decrypted;

}

function pad($data, $blockSize) {

    $padding = $blockSize - (strlen($data) % $blockSize);

    return $data . str\_repeat(chr($padding), $padding);

}

function unpad($data) {

    $padding = ord($data[strlen($data) - 1]);

    return substr($data, 0, -$padding);

}

>?

**SHA-512:**

SHA-512 (Secure Hash Algorithm 512-bit) is a cryptographic hash function that produces a fixed-size output (512 bits). Below are the basic protocol steps for generating a SHA-512 hash:**Initialization:** Initialize the hash values (H) for SHA-512. These values are derived from the fractional parts of the square roots of the first eight prime numbers.**Pre-processing:** Pad the input message to ensure its length is congruent to 896 (mod 1024). Append the bit length of the original message to the padded message.**Message Block Processing:** Divide the padded message into 1024-bit blocks. Break each 1024-bit block into sixteen 64-bit words. Extend the sixteen 64-bit words into eighty 64-bit words using logical and bitwise operations.**Initialize Working Variables:** Initialize eight working variables (a through h) with the hash values from the initialization step.**Main Loop:** Perform 80 rounds of processing for each message block. Update working variables using bitwise and logical operations, message schedule, and constant values.**Finalization:** Add the initial hash values to the working variables. The resulting values are the final hash digest.The SHA-512 algorithm processes data in 1024-bit blocks and performs a series of logical and bitwise operations to produce the final hash. It is important to note that SHA-512 is a one-way function, meaning it should be computationally infeasible to reverse the process and obtain the original input from the hash value.

<?php

function calculateSHA512($message) {

    // Use the hash function with the SHA-512 algorithm

    $hashValue = hash('sha512', $message);

    return $hashValue;

}

?>

* The hash function is used with the 'sha512' algorithm to calculate the SHA-512 hash of the input message.
* The result is a hexadecimal representation of the SHA-512 hash.
* It's important to note that PHP provides native functions for hashing and using them is recommended for security reasons. The hash function is a part of the PHP core and is a convenient and secure way to calculate hash values.

**Module Description:**

* Sign in / Signup
* Fund Transfer
* OTP generation and verification
* Hashing the passwords and storing it in Database

**Sign in/Signup:**

Within this system, the user is prompted to provide essential information such as user data, wallet address, private key, username, and password. The password, following best security practices, undergoes a hashing process. Subsequently, the hashed data is systematically stored in the database, ensuring a secure and structured storage mechanism for sensitive user information.

**Fund Transfer:**

The Fund Transfer module in a banking website serves as a pivotal feature, enabling users to seamlessly manage their finances. Users, after authenticating securely, can perform a range of transactions, including internal transfers between their own accounts, external transfers to accounts in other banks, and scheduled transfers for recurring payments. The module integrates bill payment functionality, allowing users to settle utilities, credit cards, loans, and subscriptions directly through the platform.

**OTP generation and verification:** The OTP (One-Time Password) Generation and Verification module in a banking website plays a crucial role in enhancing security during sensitive transactions. When initiating actions like fund transfers or changes to account settings, users receive a unique OTP via SMS, email, or a mobile app. This dynamic code serves as a time-sensitive and one-time authentication method. The OTP Generation module generates these codes securely, ensuring unpredictability. On the user end, the Verification module prompts for the entered OTP to validate the transaction.

**Hashing the password and Storing into Databases:**

In the process of securing password, the system employs hashing for password handling. Upon user input of passwords incorporating the SHA-512 algorithm, is utilized to perform a secure one-way hash transformation. This hashed password is then systematically stored within the database. During subsequent login attempts, the entered password undergoes the same hashing procedure, and the resultant hash value is compared with the stored hash value corresponding to the original password provided during the initial sign-in phase. This method ensures a heightened level of security by safeguarding sensitive user credentials through the consistent application of cryptographic hashing techniques.

**External modules used:**

**PHP mailer:**

The PHPMailer module in PHP is a robust library that streamlines the process of sending emails through PHP scripts. With support for various email transfer methods, including SMTP and PHP's built-in mail function, PHPMailer allows developers to configure and send emails with ease. It simplifies tasks such as setting up SMTP server details, handling attachments, and composing HTML-formatted emails. By encapsulating these complexities, PHPMailer enhances the security and reliability of email functionality in PHP applications. Exception handling capabilities further assist developers in identifying and addressing issues, contributing to a seamless and secure email-sending experience. Whether sending simple text emails or more complex messages with attachments and HTML content, PHPMailer provides a versatile and widely adopted solution for integrating email capabilities into PHP applications.

use PHPMailer\PHPMailer\PHPMailer;use PHPMailer\PHPMailer\SMTP;use PHPMailer\PHPMailer\Exception;require 'vendor/autoload.php';$mail = new PHPMailer(true);try { // Server settings $mail->isSMTP(); $mail->Host = 'smtp.example.com'; $mail->SMTPAuth = true; $mail->Username = 'your-email@example.com'; $mail->Password = 'your-email-password'; $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; $mail->Port = 587; // Recipient and sender details $mail->setFrom('your-email@example.com', 'Your Name'); $mail->addAddress('recipient@example.com', 'Recipient Name'); // Content $mail->isHTML(true); $mail->Subject = 'Subject of the Email'; $mail->Body = 'HTML content of the email'; $mail->send(); echo 'Email has been sent';} catch (Exception $e) { echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";}

**8. Implementation Platform (Include Core Function calls):**

**Programming Language:** HTML, CSS, JS, JSON, PHP, MYSQL

**Operating System:** Windows 11

**Browser:** Google Chrome, Mozilla Firefox, Microsoft Edge.

|  |  |
| --- | --- |
| **Function call** | **Function Description** |
| openssl\_encrypt($plaintext, 'aes-128-cbc', $key, 0, $iv) | Encrypts data using the OpenSSL library with a specified encryption algorithm (e.g., AES) and key. |
| openssl\_decrypt($cipherText, 'aes-128-cbc', $key, 0, $iv); | Decrypts data that was encrypted using OpenSSL, using a specified decryption algorithm and key. |
| hash('sha512', $originalMessage) | Calculates the hash value of a given string using a specified hashing algorithm (e.g., SHA-512). |
| hash\_hmac('sha512', $message, $key) | Computes the HMAC (Hash-based Message Authentication Code) using a secret key. |
| hash\_file('sha512', $filePath) | Calculates the hash value of a file using a specified hashing algorithm. |

**Signin:**

<?php

include "database.php";

function login($username,$password){

$conn = database::pdo\_getconnection();

$stmt=$conn->prepare("select \* from userlogin where userid='$username'");

$stmt->execute();

$result = $stmt->fetchAll();

$password1=hash('sha512',$password);

if (count($result) == 1) {

if (password\_verify($password1,$result[0]['password'])) {

return true;

}

}

else {

return false;

}

}

        ?>

**Signup:**

<?php

include "database.php";

function signup($ac,$username1,$password)

{

try {

$conn=database::pdo\_getconnection();

$option=['cost'=>8];

$password1=hash('sha512',$password);

$password\_hashed = password\_hash($password1, PASSWORD\_DEFAULT, $option);

$sql="INSERT INTO userlogin(userid,password,accountnumber) VALUES

('$username1','$password\_hashed','$ac')";

return $conn->exec($sql);

}

catch (exception $e){

echo $e->getMessage();

}

}

?>

**OTP Generation and Verification:**

function encryptOTP($otp, $key) {

$iv = random\_bytes(16); // Initialization Vector

$cipherText = openssl\_encrypt($otp, 'aes-256-cbc', $key, 0, $iv);

return base64\_encode($iv . $cipherText);

}

function decryptOTP($encryptedOTP, $key) {

$data = base64\_decode($encryptedOTP);

$iv = substr($data, 0, 16);

$cipherText = substr($data, 16);

return openssl\_decrypt($cipherText, 'aes-256-cbc', $key, 0, $iv);

}

$encryptionKey = "YourSecretKey";

**PHP Mailer:**

<html>

<head>

<title> mail</title>

</title>

<?php

$name ='ADMIN';

$email =$\_POST["mailid"];

$subject = 'Don not share your otp to anyone';

class ExampleClass {

public static $t=0;

public static function generateRandomNumber() {

self::$t = rand(1000, 9999);

return ExampleClass::$t;

}

}

$r=ExampleClass::generateRandomNumber() ;

$myObj = new stdClass();

$myObj->name = $r;

$myJSON = json\_encode($myObj);

file\_put\_contents('C:\myfolder\iss project\sample.json',$myJSON);

use PHPMailer\PHPMailer\PHPMailer;

use PHPMailer\PHPMailer\SMTP;

use PHPMailer\PHPMailer\Exception;

require './PHPMailer/src/Exception.php';

require './PHPMailer/src/PHPMailer.php';

require './PHPMailer/src/SMTP.php';

$mail = new PHPMailer(true);

try {

$mail->SMTPOptions = array(

'ssl' => array(

'verify\_peer' => false,

'verify\_peer\_name' => false,

'allow\_self\_signed' => true

)

);

$mail->isSMTP(); //Send using SMTP

$mail->Host = 'smtp.gmail.com'; //Set the SMTP server to send through

$mail->SMTPAuth = true; //Enable SMTP authentication

$mail->Username = 'mogith.p2021@vitstudent.ac.in'; //SMTP username

$mail->Password = 'vgbd xoyz ifgn epwa '; //SMTP password

$mail->SMTPSecure = PHPMailer::ENCRYPTION\_SMTPS; //Enable implicit TLS encryption

$mail->Port = 465;

use 587 if you have set SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS

$mail->setFrom('mogith.p2021@vitstudent.ac.in', $name);

$mail->addAddress($email); //Add a recipient

$mail->isHTML(true); //Set email format to HTML

$mail->Subject = $subject;

$mail->Body = $r;

$mail->AltBody = 'This is the body in plain text for non-HTML mail clients';

$mail->send();

?>

<script>

window.location.href="otpverify1.php";</script>

<?php

//echo 'Message has been sent';

}

catch (Exception $e) {

echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

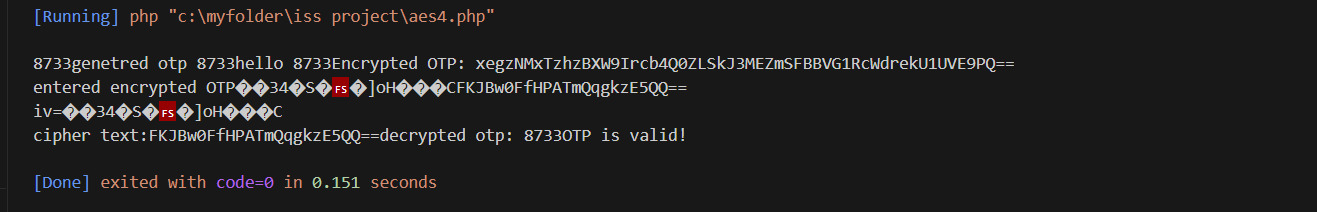
}

?>

</html>

**Performance metrics and Run Results:**

**AES with valid OTP:**



Exited in 0.151 seconds.

**AES with invalid OTP:**

A computer screen with white text

Description automatically generated

Exited in 0.135 seconds.

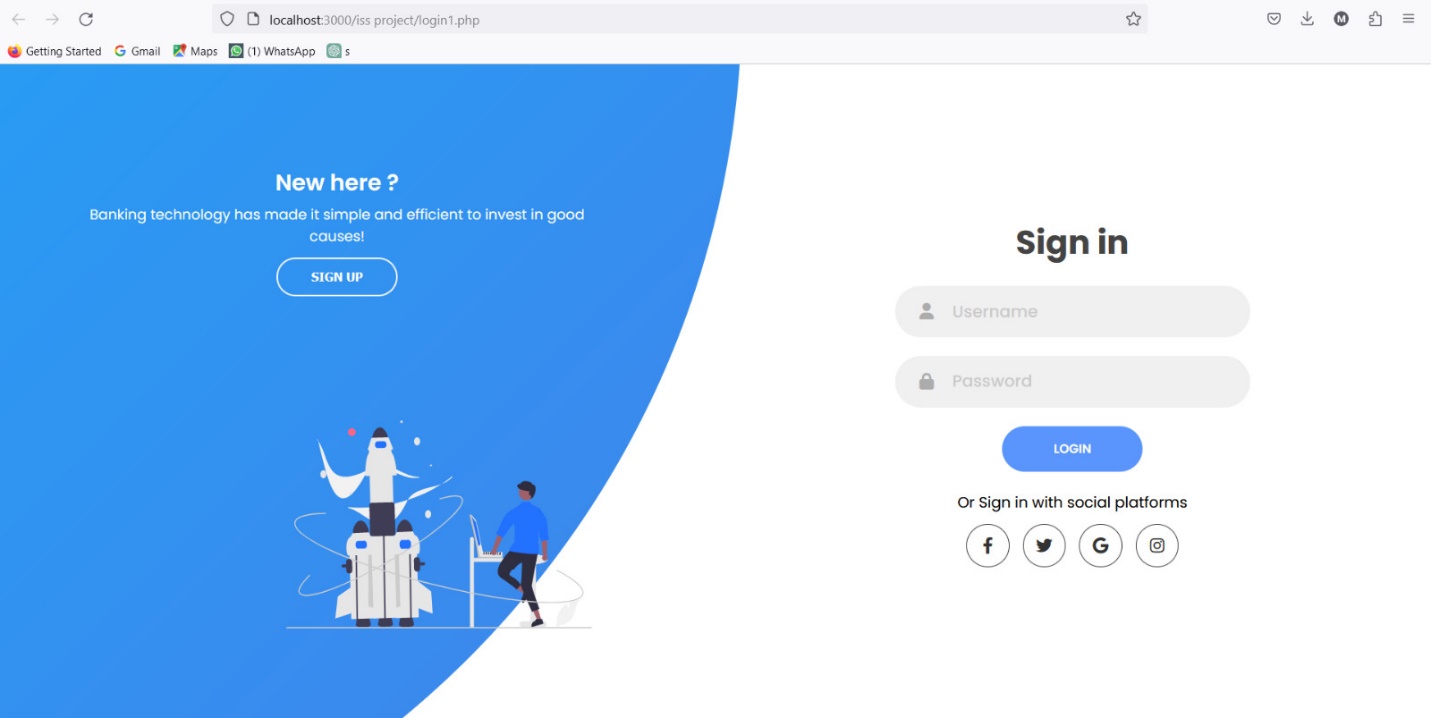
**Database connectivity:**

A black screen with white text

Description automatically generated

Exited in 0.145 seconds.

**Demo Screenshot:**



A screenshot of a computer

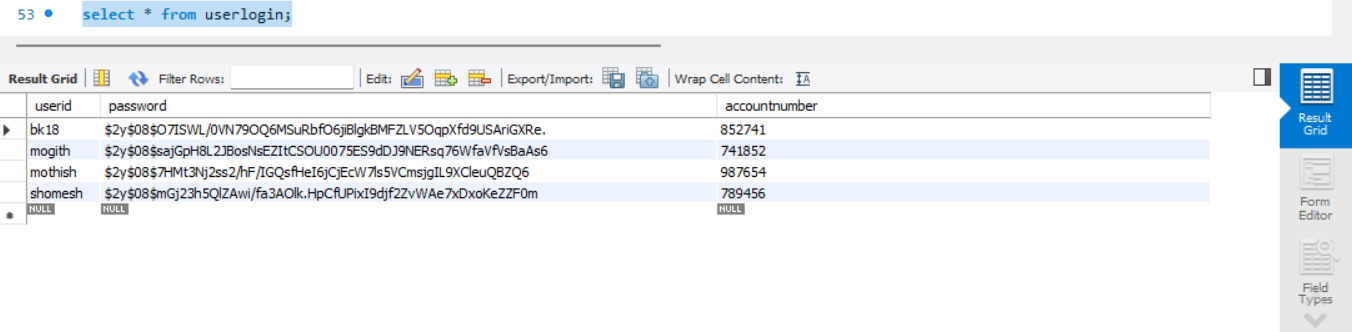
Description automatically generated

A person standing in front of a screen

Description automatically generated

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

**Conclusion:** In conclusion, an Electronic Fund Transfer (EFT) website serves as a dynamic and secure platform that revolutionizes financial transactions by providing users with the convenience of managing their funds online. This digital solution not only facilitates swift and efficient transfers between accounts but also extends its functionality to support cross-border transactions, bill payments, and scheduled transfers. With user-friendly interfaces and robust security measures, EFT websites empower users to take control of their finances with confidence. The integration of encryption protocols, multi-factor authentication, and real-time transaction monitoring ensures the integrity and security of every financial interaction. Moreover, the continuous evolution of technology presents an opportunity for EFT websites to stay at the forefront of innovation, offering users an ever improving and seamless experience in the realm of digital finance. As these platforms become integral to modern banking practices, their ability to adapt to user needs, technological advancements, and stringent security standards will define their success in shaping the future of electronic financial transactions**.**

**References:**

https://en.wikipedia.org/wiki/Data\_Encryption\_Standard https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/  
https://www.geeksforgeeks.org/advanced-encryption-standard-aes/  
https://www.geeksforgeeks.org/rsa-algorithm-cryptography/  
https://www.geeksforgeeks.org/sha-1-hash-in-java/  
https://www.geeksforgeeks.org/implement-secure-hashing-algorithm-512-sha-512-as-functional-programming-paradigm/  
https://www.geeksforgeeks.org/sha-in-python/  
https://en.wikipedia.org/wiki/HTTP  
https://scholar.google.com/  
https://www.researchgate.net/  
https://www.sciencedirect.com/