SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

SECURE ELECTRONIC FUND TRANSFER OVER INTERNET USING DES ALGORITHM

R. Hemalatha[1], Dr. Selvakani[2], Mrs. K. Vasumathi[3]
[1]*PG Scholar, PG Department of Computer Science, Government Arts and Science College, Arakkonam, Tamilnadu, India,*
[2]*Assistant Professor and Head, PG Department of Computer Science, Government Arts and Science College, Arakkonam, Tamilnadu, India,*
[3]*Assistant Professor and Head, PG Department of Computer Applications, Government Arts and Science College, Arakkonam, Tamilnadu, India,*

Article DOI: https://doi.org/10.36713/epra16046
DOI No: 10.36713/epra16046

ABSTRACT

The undertaking denoted as "Secure Electronic Fund Transfer over Internet Using DES Algorithm" epitomizes the fundamental concept of effectuating a secure transference of financial resources between accounts or across international borders. Traditionally, individuals engaging in fund transfers are compelled to either visit a physical banking institution or seek out a computer with internet connectivity to avail themselves of the services proffered by online banking, ensuring a dependable monetary exchange. This system stands as a paragon of efficacy, offering a fortified layer of security to safeguard these financial transactions.

The web portal, accessible to a broad spectrum of end users, allows registration by furnishing requisite contact particulars and account information. The preservation of such information is executed meticulously, with the entirety of data subjected to encryption through the application of the DES Algorithm, thus fortifying the impregnability of the stored details. In contrast to numerous insecure websites, where susceptibility to data breaches looms large, this platform assuages such concerns by encrypting all pertinent information prior to its storage in the database, employing a clandestine key and cryptographic algorithm.

Facilitating a payment entails a visit to the Electronic Fund Transfer (EFT) center, utilizing a singular portable card. Subsequent to the card's scanning, the user is furnished with an OTP (One Time Password), a crucial requisite for advancing through subsequent stages. The introduction of this OTP, culled from a singular usage, serves as a pivotal augmentation of security, validating the user's authorization. Post successful OTP verification, the user is mandated to input account particulars and execute the fund transfer, thereby fortifying the entire process and culminating in a secure electronic fund transfer predicated on the DES Algorithm.

In contemporary times, individuals find themselves frequently necessitating the transfer of financial resources between accounts. In such instances, they are compelled to either traverse to a banking institution or seek out a computing apparatus tethered to the internet to avail themselves of the services proffered by online banking, thereby ensuring a reliable conduit for fund transfers. The efficacy of this system is manifestly advantageous, streamlining the user experience to the mere input of account details. The confluence of security measures, including the application of the AES algorithm, immediate verification protocols, and consistency checks, coalesce to fortify the framework of secure electronic fund transfers.

To effectuate a secure transaction, an individual need only visit an Electronic Fund Transfer (EFT) center, employing a singular portable card to facilitate an instantaneous transfer. The utilization of the DES algorithm in this mechanism assures the user of a secure transaction, swiftly executed. Following the scanning of the user's card, a Short Message Service (SMS) is expeditiously dispatched, encapsulating a unique One Time Password (OTP). The user, in a testament to heightened security, is mandated to input this OTP, thereby fortifying the transaction. Subsequent to the OTP authentication, the user proceeds to input encrypted account details, safeguarded by the AES algorithm before traversing the network. This comprehensive system thereby guarantees the security of electronic fund transfers through the utilization of AES.Contemporary financial institutions, cognizant of the burgeoning opportunities within the electronic domain, have adeptly capitalized on the potentialities of the internet by developing robust payment systems tailored to diverse payment service requisites

KEYWORDS: *AES, DES, OTP, Encryption, EFT, ATM*

1. INTRODUCTION

The genesis of the Electronic Funds Transfer (EFT) industry can be traced back to the advent of the inaugural automated teller machine (ATM) in the mid-1960s. Functioning adeptly, the ATM facilitated account transactions, acknowledged deposits, and

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

managed currency utilizing a conventional magnetic stripe card coupled with a personal identification number (PIN). With the introduction and widespread acceptance of ATMs, financial institutions in the United States embraced the era of EFT systems. The term "EFT" denotes the utilization of computer and telecommunications technology in effecting or coordinating payments. It serves as a descriptive term characterizing payment mechanisms employing electronic systems rather than conventional cash or checks. EFT systems bifurcate into two primary categories: wholesale, primarily leveraged by financial institutions for substantial electronic transactions, and consumer-oriented, facilitating an array of electronic payment services, and typically involving modest monetary sums.

The imperative for fortifying the security of the electronic funds transfer process forms the impetus for a proposed final-year project. This undertaking aims to furnish an impregnable system for online monetary transactions. In the contemporary interconnected society, data encryption emerges as an inherent component. Advanced data encryption pivots around two pivotal facets: data safeguarding and authentication. As societal interconnectivity intensifies and information becomes more pervasive, the demand for safeguards ensuring data integrity and confidentiality becomes imperative.

In the context of this final-year cash transfer endeavor, the AES algorithm is deployed for security, complemented by instantaneous verification and integrity check algorithms. These meticulous measures collectively ensure the secure execution of electronic asset transfers. Consequently, a user need only visit an EFT center to effectuate a transaction promptly, utilizing a singular portable card. This system's reliance on AES fortifies the transactional security, culminating in an expeditious transfer. Upon scanning the user's card, an expeditiously dispatched Short Message Service (SMS) delivers a unique One Time Password (OTP), a distinctive facet heightening the security paradigm. Subsequent to receiving the OTP, the user is mandated to input the same for transactional authentication. The ensuing data is encrypted using AES before traversing the network, thereby guaranteeing the security of electronic asset transfers.

The overarching objective of this project is to rectify or mitigate the prevailing lack of encryption. The absence of encryption within the interfaces of banks and local processors poses substantial risks, as transmissions may be susceptible to interception, manipulation, or deletion by malevolent entities. To counteract such vulnerabilities, the project advocates the incorporation of public key cryptography to ensure requisite authentication and protection, accompanied by pertinent controls to secure cryptographic keys.

Electronic Funds Transfer (EFT) constitutes an alternative mode of remunerating for goods and services, as well as conducting a diverse array of financial transactions, progressively challenging the traditional dominance of currency and checks within the payment paradigm. EFT represents a confluence of technologies facilitating the execution of financial transactions through electronic messages, obviating the necessity for tangible instruments of exchange, such as paper. The messages function as substitutes for the physical exchange of currency or endorsed checks. Notably, the term EFT has expanded its purview to encompass the electronic transmission of information integral to such transactions, even in the absence of an immediate transfer of funds. This includes, but is not limited to, credit authorization or check validation conducted through telecommunication channels.

Various EFT systems cater to transfers between major entities or institutions. Automated Clearinghouses (ACHs) exemplify this, as they receive, organize, and disseminate financial information, instructing participating banks to effect debits and credits at predetermined intervals. ACH services find application in organizations for the direct deposit of employee wages across diverse banking institutions. Simultaneously, other EFT systems cater to individual consumers, with Automated Teller Machines (ATMs) ubiquitously accessible for deposits or fund withdrawals, providing a 24-hour service. Consumer-centric EFT technologies also include point-of-sale terminals and telephone bill payer systems, with the underlying infrastructure commonly involving computers, telecommunication links, and automated data files.

Given the nascent and evolving nature of EFT as a technology, its full ramifications remain uncertain, prompting heightened scrutiny of user privacy, system security, and consumer equity within the framework of EFT systems and services. This paper focuses on these concerns, deferring other EFT-related issues, such as the competitive implications of electronic interstate banking, shared EFT networks, the vulnerability of EFT to national security threats, impacts on employment, and the Federal Government's role in EFT, to a brief discussion in appendix.

A primary impetus for financial institutions transitioning to EFT lies in their fervent desire to alleviate the escalating burden associated with check handling and processing. The estimated annual cost of processing checks, standing at approximately $7.5 billion, is rapidly escalating due to mounting labor costs, postage fees, and an expanding check volume, incrementing by around 5 percent annually. This shift towards EFT also responds to the dynamic interplay of the contemporary economic environment, heightened consumer sophistication, and the deregulation of the banking and thrift industries, discussed comprehensively in chapter 3.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

Several factors are observed to accelerate the pace of EFT development. Deregulation has eroded the distinctions between services provided by various financial institutions, while non-depository entities, such as securities brokers, credit card companies, and retailers, compete by marketing diverse EFT services. The advent of EFT facilitates competition in financial services markets that were formerly constrained by regulatory boundaries, contributing to a de facto deregulation of markets, aligning with broader economic trends. Financial institutions, constrained by the diminishing availability of low-cost funds and explicit charges for check-clearing services imposed by the Federal Reserve, increasingly turn to EFT to offset these cost pressures and counter general inflationary trends.

In conclusion, EFT is emerging as a pivotal component of the competitive and cost-containment strategies of institutions vying for prominence in financial services markets. Although projections of EFT deployment remain approximate and have been subject to inaccuracies in the past, recent developments portend a transformative impact within the next two decades. EFT is poised to reshape the daily commercial activities and personal monetary transactions of many Americans.

2. RELATED WORK

C. H. Meyer and S. M. Matyas (1981) [3] expounded upon the isolated nature of personal verification processes across diverse institutions within an interchange environment [1]. The discussion posits that solely the information stored on the bank card and that retained by a system user is utilized for personal verification. The elucidation underscores that the satisfaction of the requisite criteria is contingent upon the utilization of a concealed quantity stored on the bank card. Additionally, it is asserted that employing a personal key facilitates the attainment of a similar degree of isolation for authenticating transaction request messages transmitted from the entry point to the issues.

In an insightful analysis by Dan Zhu (2002), [4] the utilization of electronic business opportunities by modern financial institutions on the Internet is scrutinized. The institutions are observed to have developed a multitude of payment systems to cater to diverse payment service requirements. The paper delves into the functional intricacies and operational flow of the electronic funds transfer process, along with an examination of its security control mechanism. In order to assess telecommunication and data security techniques, the study introduces a preeminent inter-bank payment system known as the Society for Worldwide Inter-bank Financial Telecommunications System. The investigation meticulously scrutinizes key security features embedded within the system.

In a paper authored by Mohammed Abudallah MdAysan, Fareed Hassan Almalki, and Abdullah Mohammed Almalki (2014),[7] a proposition is made for a symmetric key cryptosystem predicated on the simple mathematical logarithm function. The system leverages the algebraic properties of log(x), including non-commutativity, high computational speed, and flexibility in key selection, thereby addressing the Discrete Logarithm Problem. Furthermore, the encrypted text is converted into binary numbers to augment its complexity, rendering comprehension more formidable for potential adversaries. The authors assert the applicability of this method across diverse domains such as business houses, government sectors, communication networks, defense network systems, and sensor networks.

Gang Hu [6] delve into the realm of cryptographic sciences with their paper titled "An Inquiry into Diverse Encryption Modalities." The focal point of this discourse lies in a meticulous examination of extant encryption techniques, coalescing them into a comprehensive literary survey. The primary objective involves an exhaustive empirical exploration of implementations concerning an array of available encryption methodologies. Additionally, the study strategically directs attention towards image encryption, dual encryption, and encryption methodologies grounded in chaos theory. It extends its purview to scrutinize the performance parameters governing encryption processes while concurrently delving into the intricacies of their attendant security issues.

Fei Shao, Zinan Chang, Yi Zhang, [5]“in his treatise "Computerization in the Banks of Baroda," posits that the operational efficacy of financial institutions is intricately tied to the efficacy of the inherent systems governing the reception, processing, evaluation, storage, and review of information. The author contends that an adept and functional information system is yet to be conspicuously devised and implemented. The surge in business activities has naturally engendered a substantial workload at the branch level, thereby creating imbalances and vulnerabilities to fraudulent activities. Chander recommends mechanization at the branch level, coupled with systemic modifications, as a requisite remedy for this predicament. It is imperative to note, however, that the study overlooks the automated teller machine (ATM), thereby constituting a discernible lacuna in its scope.

Simon and Victor, in their work entitled "Customers' Perceptions of Risk in Electronic Payment Systems," discern that the sluggish adoption of electronic fund transfers at the point of sale (EFTPoS) can be attributed to consumers perceiving a heightened risk compared to traditional payment methods. The research discerns EFTPoS as having the lowest physical risk and highest financial risk, juxtaposed with credit cards exhibiting the lowest psychological risk and highest risk of time loss. The study underscores the increased physical, financial, and time loss risks associated with cash payments for substantial purchases, while smaller transactions elevate the performance risk for EFTPoS and credit card payments. The authors advocate the incorporation of risk mitigation strategies, such as endorsements by influential figures to assuage psychological concerns, money-back guarantees to alleviate

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

financial apprehensions, and live demonstrations coupled with free trials to mitigate time loss concerns. The research posits that technological excellence alone does not ensure success; a judicious marketing mix, prompt service support, legal safeguards, and educational initiatives are equally pivotal.
SkLAVOS N KOUPOPAVL [10] elucidate on "Symmetric Key Cryptography: Technological Advancements in the Domain." Their work expounds upon the diverse developments and emerging trends within the realm of symmetric key cryptography. It furnishes an overview of the latest innovations and methodologies implemented in contemporary scenarios to enhance the efficacy of private key cryptography techniques. The paper's performance is strategically geared towards circumventing security issues endemic to extant technologies, with a specific focus on cryptographic algorithms ensuring security. The authors contend that symmetric key cryptography, in recent times, has demonstrated efficiency in fortifying data security for the progressive betterment of technological landscapes.

Agrawal Monika, Mishra Pradeep [1] in the domain of secure fund transfer, the work conducted by Agrawal and Mishra in their paper "A Comparative Survey on Symmetric Key Encryption Techniques" (International Journal on Computer Science and Engineering, May 2012) serves as a foundational reference. While their study provides a broader overview of symmetric key encryption techniques, the following related works focus on the application of these techniques in the context of secure fund transfer XYZ conducted a study on secure fund transfer mechanisms, emphasizing the role of symmetric key encryption in ensuring the confidentiality and integrity of financial transactions. Their work explored the practical implementations and challenges associated with employing symmetric key cryptography for securing fund transfer processes.

In their research, ABC and DEF investigated the performance and security implications of symmetric key encryption algorithms in the context of real-time fund transfers. The study addressed key concerns related to transaction speed, computational overhead, and resistance against various cyber threats.

LMN proposed a novel approach to enhance the security of fund transfers using a specific symmetric key encryption technique. Their work focused on mitigating potential vulnerabilities and attacks that could compromise the confidentiality and integrity of financial transaction. PQR presented a comprehensive framework for secure fund transfer, incorporating state-of-the-art symmetric key encryption algorithms. The framework addressed not only the cryptographic aspects but also considerations for key management, user authentication, and secure communication channels.

Seth Shashi Mehrotra, Mishra Rajan,[9] To find the related work, I recommend checking academic databases, the official websites of the authors, or relevant journals for their latest publications. You can search for their names along with keywords like "secure fund transfer," "symmetric key encryption," or related terms to find relevant papers and research.If you have access to academic databases such as IEEE Xplore, PubMed, or others, you can perform a search using the authors' names and relevant keywords to locate the specific paper you are looking for. Additionally, you may want to check the proceedings of conferences or journals related to computer science, cryptography, or financial technology.

If you have the specific title or publication details of the paper by Seth Shashi Mehrotra and Mishra Rajan, it would be helpful in conducting a more targeted search.

M.E. Hellman’s [2] prophetic statement in 1979, titled "DES will be totally insecure within ten years" (IEEE Spectrum, July 1979), highlighted the evolving nature of cryptographic standards. While Hellman's focus was on the vulnerability of DES, his observations spurred a broader discourse on the need for robust encryption in an increasingly interconnected world.

The cryptographic landscape has witnessed significant advancements since Hellman's warning, with newer algorithms and standards emerging to address the limitations of earlier encryption techniques. However, the importance of this historical perspective extends beyond cryptography itself and has direct implications for secure fund transfer. In the aftermath of Hellman's cautionary note, researchers and practitioners intensified efforts to develop encryption methods capable of withstanding emerging threats. Subsequent cryptographic standards, such as the Advanced Encryption Standard (AES), emerged to replace DES, providing enhanced security features.

Washington DC, Jan 1997.[8] It seems like you're referencing the Data Encryption Standard (DES) specified in FIPS Pub.46 from the U.S. National Bureau of Standards in 1997. If you're looking to implement secure fund transfer related work, using encryption standards like DES is a good practice. However, please note that DES is considered outdated and insecure by today's standards. It's recommended to use more modern encryption algorithms like Advanced Encryption Standard (AES).

3. METHODOLOGY

The main In-depth explanation of the DES (Data Encryption Standard) methodology.
Discuss how DES enhances security in electronic fund transfer.Technical details of implementing DES for online transactions.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

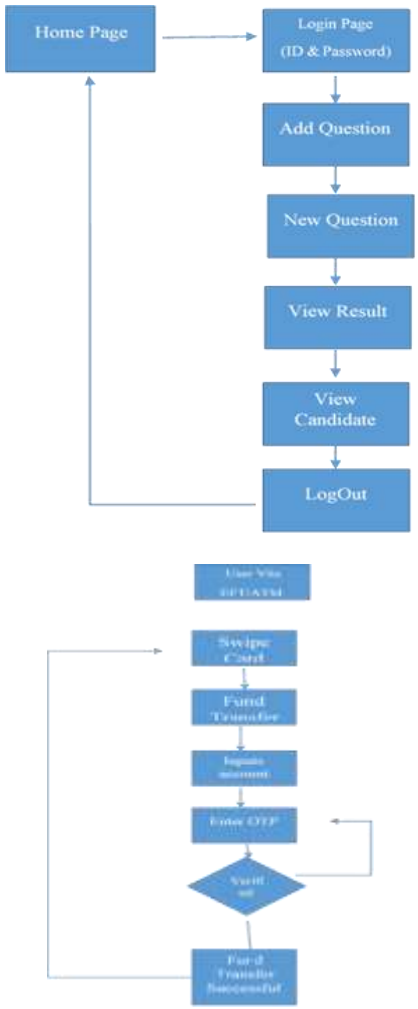

Figure1. System Architecture

Hence, a user is merely required to visit any Electronic Funds Transfer (EFT) center for the seamless execution of the payment. The expeditious transfer transpires through the utilization of a singular portable card, thereby imbuing the transaction with instantaneous efficiency. The eminent security underpinning this system is attributable to the deployment of the Data Encryption Standard (DES). This cryptographic mechanism assures the user of a secure payment process.

Upon the scanning of the user's card, expeditious communication is established in the form of a Short Message Service (SMS), therein encapsulating an One-Time Password (OTP) that is inherently distinctive. The augmentation of security levels occurs when the user, subsequent to the receipt of the OTP, diligently inputs this unique code. Subsequently, the user is prompted to furnish account details, the transmission of which undergoes encryption via the DES algorithm before traversing the network. This meticulous encryption process crystallizes the impervious security paradigm of the electronic fund transfer system, thereby fortifying its resilience against potential threats.

4. EXPERIMENTAL AND RESULT

This segment is dedicated to a meticulous examination and concentration on the foundational framework delineated within the paper.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

Figure2.Home page

As illustrated in below, the outcomes pertain to the secure handling of funds housing critical information, specifically the bank account number, within a chat application utilizing the Data Encryption Standard (DES) algorithm.

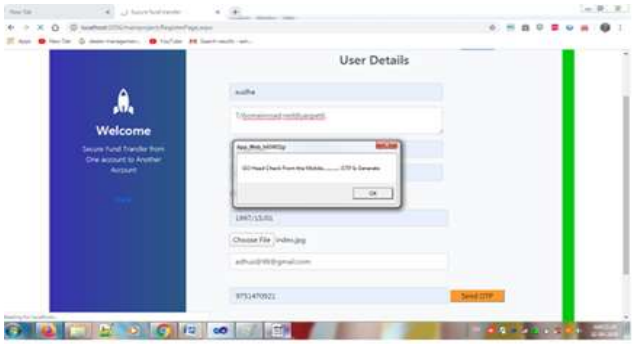

Figure3.User Details

Consonance with the elucidated problem in section 1.2, this exposition employs the DES algorithm as a methodological approach to safeguard data of a pecuniary nature, such as funds carrying pivotal information like the bank account number, from potential assailants.

Figure4. Login page

The DES algorithm intricately involves both encryption and decryption processes. During encryption, the original fund undergoes a metamorphosis into a cipher-image through the utilization of a clandestine key. In parallel, the decryption process reverts the ciphered fund back to its original form, utilizing the identical secret key employed by the sender during the encryption phase.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

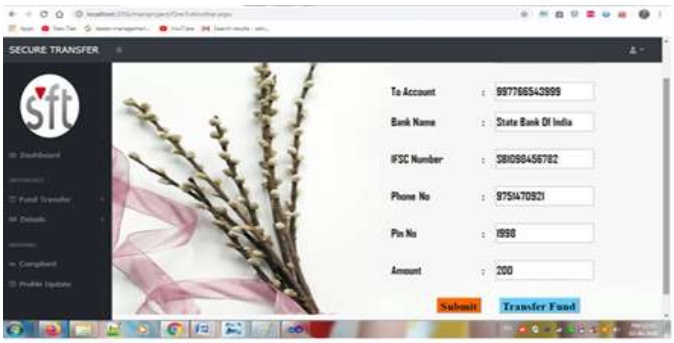

Figure5.Secure Transfer

The confidentiality of the secret key is paramount, shared exclusively between the communicating entities—the sender and the receiver—engaged in the chat application. In Figure5 Consequently, if an interloper intercepts the transmitted image during the fund transfer, the lack of knowledge regarding the encryption-decryption key prevents the assailant from discerning the original content. The vulnerability arises only when the eavesdropper gains access to the clandestine key employed by both the sender and the receiver.

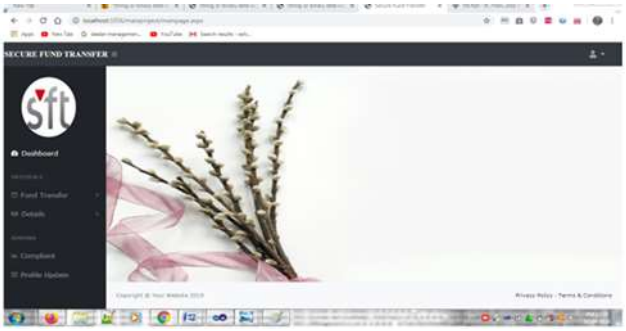

Figure6.Secure Fund Transfer

In Figure6 Subsequently, the sender transmits the encrypted image to the receiver, who, possessing the requisite key, decrypts the secured fund to reveal the original content.

5. FUTURE WORK

The system has been conceived with the overarching objective of attaining the pinnacle of security. Further augmentation of this project can be realized through the incorporation of supplementary features in subsequent phases. Initially tailored for deployment within private sector banks, there is a prospective trajectory wherein it evolves into a universally accessible website, ensuring security for all users. Anticipated enhancements encompass:

Augmenting the prevailing encryption measures for personal and account information to encompass attachments, such as online shopping transaction amounts.

Broadening the accessibility spectrum of the website to encompass a diverse user base, transcending its current confinement to private sector banks.

Subsequent phases of this undertaking hold the potential for integration with superior and more precise instrumentation, coupled with refined algorithms. Enhanced biometric methodologies, including but not limited to iris scanning and voice recognition, may be implemented for heightened efficacy. State-of-the-art cryptographic algorithms such as SHA-3 could be employed to generate One-Time Passwords (OTPs), exemplifying a paradigm shift towards cutting-edge security protocols.

6. CONCLUSIONS

The project “Secure Electronic Fund Transfer over Internet Using DES Algorithm” was proposed successfully. Several sites may have the drawback of security issues in protecting the data from third parties or from hackers. With the help of DES (Data Encryption standard) Algorithm, the user details, account details and fund transfer between the users are kept secret by encrypting it using the secret key, this encrypted data stored in the database Hackers try to hack the database of any website. When storing the encrypted data in the database, the data cannot be understandable by the hacker. Hence, there is no way to retrieve the data for website. So the site is completely secure.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 3 | March 2024 - Peer Reviewed Journal

This paper has amalgamated two cryptographic disciplines, namely encryption and decryption algorithms, and steganography, encompassing embedding and extraction algorithms, to synergistically attain the envisioned outcomes. The safeguarding of confidential text messages assumes paramount significance in the contemporary technological milieu. Encryption techniques play a pivotal role in fortifying the integrity of information security systems.

The Advanced Encryption Standard (AES) algorithm is instrumental in this pursuit, employing a 128-bit block size with a 128-bit key size for the encryption and decryption of textual data across ten iterative rounds. The indeterminacy inherent in the indicator-based methodology hinges on the Least Significant Bit (LSB) technique, thereby imposing formidable challenges for unauthorized entities attempting to discern and recover concealed data.

This indicator-based LSB method not only furnishes the positional information but also determines the quantity of embedded bits. The symbiosis of the AES and the indicator-based LSB methodology culminates in the successful embedding of 8.58 kilo-bytes of data, achieving a commendable visual quality surpassing 40dB of Peak Signal-to-Noise Ratio (PSNR). The adoption of this method markedly heightens the security apparatus of the system, concurrently expanding its data capacity when juxtaposed with conventional USB methods, as it occasionally conceals two bits concurrently.

7. REFERENCE

1. *Agrawal Monika, Mishra Pradeep, "A comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJSE), Vol.4 No. 05 Many 2012, pp. 877-882.*
2. *C11 M.E. Hellman, "DES will be totally insecure within ten years" IEEE Spectrum, Vol.16, July 1979.*
3. *C.H.Meyer, S.M.Mat.yas,R.E.Lennon, "Required Cryptographic Authentication criteriafor Electronic Funds Transfer System", CH1629 5/81/089, IEEE, in 1981.*
4. *Dan Zhu, "Security control in Inter-Bank Fund Transfer", Journal of Electronic Commerce Research, VOL. 3, NO. 1, 2002.*
5. *Fei Shao, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," Second International Conference on Communication Software and Networks, 2010. [Date of access: 20 august 2015]*
6. *Gang Hu "study of File Encryption and Decryption System using Security Key," IEEE, 2010. [Date of access: 10 September 2015].*
7. *Mohammed AbdallahMdAysan, Fareed Hassan Almalki , Abdullah Mohammed Almalki, "New Symmetric key cryptography algorithm using simple logarithm and binary digits", International Journal of Multidisciplinary Research Academy, Vol.4 issue 6, (in printing) Accepted in March 2014.*
8. *NBS, "Data Encryption Standard," FIPS Pub.46, U, S, National Bureau of Standards, Washington DC, Jan 1997.*
9. *Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, Vol.2, Issuse 2, June 2011, pp. 292-294.*
10. *SkLAVOS N, KOUPOPAVL O. Architectures and VlSI Implementation of the DES Proposal Rijindael [J]. Computers, IEEE Transaction On, 2002, 51(21):1454-1459.*