iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63457

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Securing Text Files: A Comprehensive Studyon AES and Diffie-Hellman Encryption

Sahil Mhatre[1], Omkar Khatode[2], Sargam Thakre[3], Sairaj Karche[4]
Department of CSE

Abstract: ***In today's digital landscape, data security is of utmost importance, and cryptography plays a crucial role in safeguarding sensitive information. This review papermeticulously examines recent developments in cryptographic methodologies, covering enhancements in the Playfair cipher, integration of cryptography with steganography for smart devices, advancements in Elliptic Curve Cryptography (ECC), and the efficacy of Advanced Encryption Standard (AES) in cloud computing. Additionally, it discusses innovative approaches to mitigating security vulnerabilities, such as RSA Diffie-Hellman integration, and explores the utilization of chaos theory in symmetric text cipher algorithms. Lastly, the paper examines advancements in text-to-image encryption-decryption algorithms, focusing on the utilization of CMYK mode. By synthesizing findings from diverse studies, this review offers valuable insights into emerging trends and future research directions in data security and encryption.***

Keywords: Data security, Encryption technique, AdvancedEncryption Standard (AES).

I. INTRODUCTION

In today's interconnected digital landscape, safeguarding sensitive information holds paramount importance.Cryptography, the art of securing data through encryption and decryption, emerges as a pivotal tool in protecting information from unauthorized access and interception. Over the years, researchers have explored various cryptographic algorithms and methodologies to tackle evolving security challenges. This review paper endeavors to present a comprehensive overview of recent advancements in cryptography, focusing on both theoretical frameworks and practical applications. By synthesizing insights from a diverse range of scholarly sources, we delve into the intricacies of cryptographic techniques utilized across multiple domains, encompassing mobile ad hoc networks(MANETs), text, and image encryption. The increasing adoption of mobile ad hoc networks underscoresthe necessity for robust cryptographic solutions to ensure secure data exchange. Our exploration delves into the importance of cryptography in MANETs, investigating the deployment of both symmetric and asymmetric key algorithms to mitigate inherent security risks in mobile communication. Moreover, the review delves into text and image encryption, shedding light on innovative approaches such as hybrid encryption methods and transposition techniques. Through the analysis of recent studies, we highlight the integration of cryptography with emerging technologies like DNA-based encryption and chaos theory, showcasing their potential to bolster data security. Furthermore, the review elucidates the fundamental principles ofcryptographic algorithms, emphasizing the critical role of key management and encryption protocols in fortifying information security. By examining modern encryption standards such as AES and RSA, we underscore the importance of balancing security robustness with computational efficiency.

II. HISTORY

In recent years, encryption has witnessed remarkable advancements, addressing diverse security challenges in digital communication. In 2014, a novel symmetric text encryption algorithm leveraging chaos theory integrated a 128-bit secret key and chaotic data into the encryption process, demonstrating potential for real-time applications. Concurrently, encryption was explored as a cryptographic function, emphasizing its role in converting data blocks into fixed-size bit strings to ensure integrity and confidentiality. By 2016, hybrid encryption methods emerged, combining Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), offering enhanced security through dynamic key selection and countermeasures against attacks like Cache Timing Attack. Meanwhile, in 2022, the integration of RSA encryption/decryption into the Diffie-Hellman Key Exchange protocol addressed Man in the Middle (MITM) attacks, significantly bolstering security during data transmission. Further innovations in 2022 introduced mechanisms for secure text transfer, emphasizing password-protected encryption for secure data exchange between sender and receiver. Subsequent developments in 2023 introduced multistage encryption techniques incorporating both cryptography and steganography, utilizing ciphers like Caesar and Vigenere, coupled with Morse code conversion and LSB steganography, to enhance data security through layered obfuscation.

These advancements reflect a dynamic evolution in encryption methodologies, driven by the imperative to ensure data confidentiality, integrity, and authenticity in an increasingly interconnected digital landscape.

III. LITERATURE REVIEW

The review paper [1]"A novel symmetric text encryption algorithm based on logistic map" by M. A. Murillo-Escobar, F. Abundiz-Pérez, C. Cruz-Hernández, R. M. LópezGutiérrez, published in the proceedings of the 2014 International Conference on Communications, Signal Processing and Computers, provides a comprehensive overview of encryption techniques and their applications. Beginning with an explorationof cryptography's fundamental role in securing data transmissionand storage, the authors delineate between symmetric and asymmetric encryption algorithms, highlighting established standards such as 3DES, AES, and RSA. They then delve into recent advancements, including DNA cryptography, where DNA sequences serve as secret keys, and chaos-based cryptography, leveraging chaotic systems' properties for algorithm design. The paper meticulously reviews existing chaos-based encryption algorithms, with a focus on logisticmaps, presenting a holistic perspective on encryption methodologies and their implications. This concise yet informative review serves as a valuable resource for researchersand practitioners seeking insights into the evolving landscape ofencryption techniques.

The review encapsulates the essence of the paper[2] "A SemanticApproach to Cloud Security and Compliance," shedding light onthe criticality of tackling security and compliance complexities within cloud computing. It aptly highlights the pervasive confusion arising from the lack of standardized security measures across cloud services and underscores the pressing need for cloud providers to adhere to stringent security and privacy protocols. At the heart of the paper lies a seminal contribution: the development of a sophisticated semantic approach, manifested through the construction of an ontology, which meticulously defines cloud security controls, identifies threats, and delineates compliance requirements. This innovative framework facilitates the automated determination ofsecurity policy controls tailored to specific threats, promising toalleviate barriers to cloud adoption while bolstering data protection through streamlined policy enforcement mechanisms. By advocating for a paradigm shift towards semantic-driven solutions, the paper not only offers a fresh perspective on cloud security challenges but also presents tangible pathways for advancing the secure adoption of cloud technologies. In essence,the review underscores the paper's significance as a pivotal resource for stakeholders invested in fortifying cloud security landscapes.

The review succinctly encapsulates the essence of the paper [3]"Challenges And Practices Identification Via A Systematic Literature Review In The Adoption Of Green Cloud Computing Client's Side Approach," which delves into the pivotal realm of green cloud computing adoption. It aptly underscores thesignificance of this burgeoning field in providing environmentally sustainable IT solutions and focuses on delineating the primary challenges and corresponding practices encountered by client organizations in embracing green cloudcomputing. The study meticulously identifies a spectrum of challenges encompassing technical, economic, and organizational barriers, thereby offering a comprehensive understanding of the hurdles impeding the adoption process. In tandem, it proffers a repertoire of practices aimed at surmountingthese obstacles and fostering the uptake of green cloud computing, including the adoption of energyefficient technologies, formulation of sustainable IT policies, and fostering collaborative partnerships with cloud serviceproviders. Importantly, the paper's findings not only advocate for the advancement of sustainable IT adoption but also serve asa cornerstone for policy and strategy development, equipping organizations with actionable insights to navigate the complexities of green cloud computing integration effectively. By bridging the gap between theory and practice, the paper heralds a pivotal stride towards ushering in a new era of environmentally conscious technological solutions. In conclusion, it stands as a commendable resource for stakeholders vested in championing environmentally friendly cloud computing paradigms.

The paper [4]"Text and Image Encryption Decryption Using Advanced Encryption Standard" presents a comprehensive exploration of the Advanced Encryption Standard (AES) and itsapplication in securing both textual and graphical data. Published in 2014, the study sheds light on the critical role of AES in bolstering data security in various contexts. It aptly highlights the importance of employing robust encryption mechanisms, especially in the transmission and storage of sensitive information. At the core of the paper lies a meticulousexamination of AES algorithms and their efficacy in safeguarding text and image data against unauthorized access and interception. By elucidating the practical implementation ofAES encryption and decryption processes, the paper offers valuable insights into enhancing information security practices. In essence, the review underscores the paper's significance as a pivotal resource for stakeholders vested in fortifying data protection measures against evolving cyber threats.

The paper titled [5]"AES Based Text Encryption Using 12Rounds with Dynamic Key Selection" by Nishtha Mathur and Rajesh Bansode, published in 2016, introduces a novel approach to enhancing data security in communication systems by combining Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC).

This extension of a public-key cryptosystem to support a private key cryptosystem eliminates the need for transmitting private secret keys before communication, simplifying key management while ensuring confidentiality. The approach offers advantages such as increased security and complexity of cryptography algorithms, achieved through more randomization in secret keys. Encrypting the AES key with ECC provides confidential key management akin to ECC, enhancing overall security without compromising efficiency. The paper suggests implementing an improved AES algorithm with a 192-bit key size and 12 rounds of iterations to further enhance data encryption efficiency and security, with future work focusing on implementing attacker modules and corresponding countermeasures, and exploring parameters such as key length and types of side channel attacks. Overall, the paper contributes to data security by proposing a hybrid encryption approach that combines AES and ECC, offering insights into key management, confidentiality, and avenues for future research and development.

The paper titled [6]"Android-Based Text Message Encryption and Decryption Application Using the Advanced Encryption Standard Algorithm" by Riski Adi Putra, Yupianti, and Eko Prasetyo R, published in 2023, introduces an Android application aimed at enhancing communication security through the implementation of the Advanced Encryption Standard (AES) algorithm. The application encrypts messages before storing them in a MySQL database, ensuring confidentiality during message exchange between users. With accessibility on Android smartphones with internet connectivity, the application presents significant potential utility, particularly in educational environments. Overall, the paper demonstrates the effective operation of the application, affirming its capability to maintain message confidentiality and serve as a practical solution for secure communication needs. Future work may focus on optimizing and expanding the application's features to cater to broader user requirements and contexts.

The paper titled [7]"Enhancement of Security of DiffieHellman Key Exchange Protocol using RSA Cryptography" by Chiradeep Gupta and N V Subba Reddy, published in 2022, presents a novel approach to bolster the security of the Diffie-Hellman Key Exchange Protocol by integrating RSA Cryptography. The proposed model addresses vulnerabilities such as the Man-in- the-Middle (MITM) attack, commonly associated with the classical Diffie-Hellman algorithm. By incorporating RSA into the key exchange process, the model enhances security and mitigates the risk of interception and manipulation. The paper concludes that the proposed model exhibits improved resistance against MITM attacks compared to the traditional Diffie- Hellman key exchange algorithm. Furthermore, the model demonstrates the combined utilization of both the Diffie- Hellman key-sharing protocol and the RSA cryptosystem. In terms of future work, the paper suggests extending the current model to incorporate additional security measures and exploring higher input values to ensure robust security during public key exchange.

The paper titled [8]"Secure Text Transfer Using DiffieHellman Key Exchange Based On Cloud" by L. Vijeeth Reddy and Mohd. Tajammul, published in 2022, explores a method for secure text transfer using cloud architectures. It employs Diffie-Hellman Key Exchange and AES encryption, ensuring confidentiality and preventing unauthorized access. The system adds an extra layer of security through password encryption. It concludes that the system effectively allows for secure text transfer, protecting private messages from external threats. Future work could focus on enhancing security features, improving user-friendliness, expanding capacity, and incorporating additional security measures.

The paper titled [9]"Multistage Encryption for Text Using Steganography and Cryptography" by Mohammed Majid Msallam and Fayez Aldoghan, published in 2023 in the Journal of Techniques, introduces a three-stage method for data security utilizing both cryptography and steganography. The approach entails dividing the message into two segments encrypted with Caesar Cipher and Vigenere Cipher, respectively, followed by encoding the ciphertext with Morse code and embedding it within a cover image using the Least Significant Bits (LSB) technique. The authors contend that this strategy enhances security and resilience by amalgamating both encryption techniques. Highlighted advantages include heightened security from the amalgamation of cryptography and steganography, the intricacy introduced by the three-stage encryption, and the stego image's quality reducing suspicion among hackers. The conclusion underscores the challenge for hackers in deciphering the message and the stego image's effectiveness in concealing crucial data. While the future research direction suggests potential for enhancing the system's robustness and security through further exploration of the combined steganography- cryptography approach.

The paper titled [10]"Cloud Computing Security Improvement using Diffie Hellman and AES" by Rameshwari Malik and Pramod Kumar, published in 2015 in the International Journal of Computer Applications, presents a data protection model addressing security issues in cloud computing. The model encrypts data using AES and authenticates it with the Diffie Hellman algorithm before uploading it to the cloud, ensuring confidentiality and security. The authors conclude that their proposed methods effectively secure cloud data from malicious users using the Diffie Hellman key exchange algorithm and address access control challenges through proper authentication mechanisms. Highlighted advantages include increased security from combining cryptography and steganography, complexity introduced by three-stage encryption, and reduced hacker suspicion due to the high quality of the stego image. Future research should aim at reducing memory area to enhance suitability for IoT devices.

The paper titled [11]"A Review of Encryption and Decryption of Text Using the AES Algorithm" authored by Assistant Professor Dr. P. Manikandaprabhu and Ms. M. Samreetha, published in April 2024, delves into the significance of encryption in safeguarding data privacy, with a specific focus onthe Advanced Encryption Standard (AES) for text data security.It offers an overview of AES encryption and decryption processes, delineating their strengths, weaknesses, and practical considerations. The conclusion underscores the pivotal role of encryption, particularly AES, in bolstering data privacy measures, emphasizing the necessity of robust encryption practices in the contemporary digital realm. It advocates for thecontinual refinement and adaptation of encryption techniques toaddress evolving security demands and uphold the integrity of sensitive information. The paper suggests that AES serves as a dependable method for data encryption and hints at the potentialfor further enhancing the AES algorithm and exploring its application across various domains in the future.

The paper titled [12]"Data Encryption to Decryption by Using Laplace Transform" by B. Ramu Naidu, K.P.K. Sastry, and D. M. K. Kiran, published in 2024, presents a novel encryption anddecryption technique employing Laplace transformation and itsinverse. The method, utilizing ASCII code conversion and two primes as primary keys, aims to ensure high-security data transmission. The conclusion, supported by an illustrative example, underscores the efficacy of the proposed approach in providing robust data security during transformation. The authors suggest future enhancements to the encryption and decryption process and explore its applicability across various domains. The paper implies that its key advantage lies in the highlevel of security achieved through the Laplace transformation and Inverse Laplace Transformation, preserving data integrityand confidentiality effectively.

IV. COMPARISON

1) DES, developed by IBM and based on a design by Horst Feistel, emerged as a widely used cryptographic system upon its release, eventually adopted by the National Institute of Standards and Technology (NIST). It operates as a symmetric-key algorithm for digital data encryption, utilizing a block size of 64 bits and employing the Feistel network structure. Despite its early prominence, DES's adoption waned due to its sluggish performance and susceptibility to security breaches, notably stemming from its short key length of 56 bits. Notably, in 1999,distributed.net demonstrated DES's vulnerability by breaking a key in just over 22 hours, prompting NIST to rescind its standardization. Subsequently, 3DES emerged as a response to address DES's shortcomings and enhance security.

2) Triple DES, also known as 3DES or TDES, officially referred to as the Triple Data Encryption Algorithm, operates as a symmetric-key block cipher, applying the DES algorithm three times to each block. With a block size of 64 bits and a key length of 112 or 168 bits, it retains the Feistel network structure inherited from DES. Despite its robustness initially, the advent of modern cryptology techniques and supercomputing revealed serious vulnerabilities within 3DES. Consequently, the National Institute of Standards and Technology (NIST) deprecated both DES and 3DES for new applications in 2017 and for all applications by 2023. This decision was influenced by the emergence of the Advanced Encryption Standard (AES), which supplanted these encryption algorithms due to its enhanced security features and efficiency.

3) Blowfish, developed by Bruce Schneier in 1993 as an alternative to DES, offers a significantly faster symmetric- key encryption technique with a better encryption rate. Featuring a key length of 446 bits, surpassing DES and 3DES, it poses a greater challenge for key cracking. With ablock size of 64 bits, Blowfish finds applicability in software due to its speed and efficiency. However, the advent of AES has shifted focus away from Blowfish,prompting Schneier to recommend Twofish as an alternative. Twofish, boasting a free license and availability for all uses, has garnered attention as a viable alternative to Blowfish in contemporary encryption practices.

4) AES, standing for Advanced Encryption Standard, stands out as one of the most robust encryption algorithms, effectively safeguarding data from malicious actors. Renowned for its strength and efficiency, AES ensures secure online activities without disruption by combining speed and security adeptly. Operating as a symmetric encryption method, AES employs the same key for both encryption and decryption processes. With key lengths available in 128, 192, and 256 bits, each offering varying levels of security, AES boasts a fixed block size of 128 bits or 16 bytes. Distinguished by its structure known as the substitution-permutation network, AES differs from other encryption algorithms, enhancing its resilience and effectiveness in protecting sensitive information.

5) RSA, or Rivest-Shamir-Adleman, is a widely-used asymmetric encryption algorithm renowned for its robust security features. Asymmetric encryption means it uses a pair of keys, one public and one private, for encryption anddecryption, respectively. The public key is shared openly, while the private key is kept secret. RSA's strength lies in the difficulty of factoring large prime numbers, upon whichits security relies. With RSA, secure communication isfacilitated without the need for both parties to share a secretkey beforehand, making it ideal for key exchange anddigital signatures. Key lengths for RSA typically range from

1024 to 4096 bits, with longer keys offering greater securityat the expense of computational overhead. Despite its security, RSA can be slower than symmetric encryption methods, particularly for large key lengths. Nonetheless, RSA remains a cornerstone of modern cryptography, enabling secure communication and data integrity verification in various applications.

6) Twofish, designed as a symmetric-key block cipher by Bruce Schneier and others in 1998, stands as a formidable encryption algorithm, providing robust protection against unauthorized access to data. Renowned for its security and versatility, Twofish offers a compelling alternative to otherencryption methods. With a variable key length, Twofish supports key sizes of 128, 192, or 256 bits, allowing for a wide range of encryption strengths to suit different security needs. As a symmetric encryption technique, Twofish utilizes the same key for both encryption and decryption processes, ensuring simplicity and efficiency in cryptographic operations. Notably, Twofish operates onblocks of data with a fixed size of 128 bits, maintaining consistency in its encryption structure. While AES remainsa popular choice in contemporary encryption practices,Twofish's free license and availability for all uses make it an attractive option recommended by Schneier as an alternative to other encryption algorithms.

	DES	3DES	Blowfish	Twofish	AES	RSA
Key Length	56 Bits	112 or 168 Bits	448 Bits	128, 192, or 256 Bits	128, 192, or 256 Bits	1024 bits to 4096Bits
Block Size	64 Bits	64 Bits	64 Bits	128 Bits	128 Bits	Does Not OperateOn Block
Developed In	1975	1978	1993	1998	2000	1977
Speed	Slow	Slow	Fast	Fast	Fast	Slow
Security	Not secure enough	Not secure enough	secure enough	secure enough	Excellent Security	Superior Security
Structure	Feistel	Feistel	Feistel	Feistel	Substitution, Permutation	mathematical properties
Time required to check all possible keys at 50 billion keys per sec	400 Days	800 Days	~3200 Days	5*10^21 Days	5*10^21 Days	Undefined

V. METHODOLOGY

A. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a widely adopted symmetric encryption algorithm designed to secure digital data. Established as a standard by the U.S. National Institute of Standards and Technology (NIST) in 2001, AES is celebrated for its robustness and efficiency. The algorithm encrypts data in fixed-size blocks of 128 bits and supports key sizes of 128, 192, or 256 bits, offering different levels of security. As a symmetric key algorithm, AES uses the same key for both encryption and decryption, which must remain confidential between the communicating parties to maintain security.

AES encryption involves a series of transformation rounds, with the number of rounds varying based on the key size: 10 rounds for 128-bit keys, 12 for 192-bitkeys, and 14 for 256-bit keys. The encryption process begins with an initial round where the plaintext is combined with the encryption key through an XOR operation. This is followed by multiple rounds of substitution, permutation, and mixing of the data, where bytes are substituted using a lookup table (S- box), rows are shifted, columns are mixed, and the round key is added again. The final round omits the column mixing step but includes all other transformations. Decryption reverses these steps usingthe same key schedule, ensuring data can be accurately retrieved.

AES is utilized across various applications due to its security and performance. It secures data transmission in communication protocols like TLS/SSL, protects sensitive information in file storage and transmission,and is integral to wireless security protocols such as WPA2 for Wi-Fi. Additionally, AES is employed in full disk encryption solutions like BitLocker, ensuringcomprehensive data protection. Its resistance to cryptographic attacks and ability to operate efficiently on both hardware and software platforms make AES acornerstone of modern data security.

B. Rivest-Shamir-Adleman (RSA)

The Rivest-Shamir-Adleman (RSA) algorithm is a cornerstone of modern public-key cryptography, widely used to secure sensitive data. Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is an asymmetric encryption algorithmthat relies on two keys: a public key for encryption and a private key for decryption. This key pair is generated based on the mathematical properties of large prime numbers, ensuring robust security. The public key can be freely distributed, while the private key must be kept secret to maintain the integrity of theencrypted data.

RSA encryption works by transforming plaintext into ciphertext using the recipient's public key, ensuring that only the corresponding private key can decrypt the message. The process involves modular exponentiation, where the plaintext is raised to the power of the public key exponent and then taken modulo a large composite number, typically the product of two large prime numbers. This transformation renders the ciphertext unreadable without the private key. Decryption reverses the process using the private key, restoring the original plaintext. The security of RSA relies on the computational difficulty of factoring large composite numbers, a problem currently infeasible to solve withexisting technology.

RSA has a wide range of applications, particularly in securing digital communications and ensuring data integrity. It is commonly used in secure web browsingthrough protocols such as SSL/TLS, where it helps establish secure connections between clients and servers. RSA also plays a crucial role in email encryption, digital signatures, and key exchange protocols, providing authentication and non- repudiation. Additionally, it is employed in secure filetransfer protocols and virtual private networks (VPNs). Despite its strength, RSA's computational intensity and the increasing threat of quantum computing have led to the exploration of alternative encryption methods, though RSA remains a fundamental component of contemporary cryptographic practices.

C. DEFFI-HELLMAN Key ExchangeAlgorithm

The Diffie-Hellman key exchange algorithm is a foundational protocol in the field of public-key cryptography, enabling secure key exchange over an insecure communication channel. Introduced by Whitfield Diffie and Martin Hellman in 1976, this algorithm allows two parties to generate a shared secret key, which can then be used for symmetric encryption of subsequent communications. The Diffie-Hellman algorithm relies on the mathematical difficulty of computing discrete logarithms, ensuring the security of the exchanged key even if the communication is intercepted. The key exchange process begins with both parties agreeing on a large prime number p and a base g , which are both publicly shared. Each party then selects a private key—let's call them a and b — whichare kept secret. Using their private key and the public base, each party computes a public value: $A = g^a$ modp and $B = g^b$ mod p. These public values are exchanged between the parties. Upon receiving the other party's public value, each party computes the shared secret key using their own private key: the firstparty computes $s = B^a$ mod p and the second party computes $s = A^b$ mod p . Due to the properties of modular arithmetic, both parties arrive at the same shared secret key, s, which can then be used for symmetric encryption. The Diffie-Hellman key exchange algorithm is widelyused in securing various communication protocols. It is a fundamental component of SSL/TLS, which underpins secure web browsing by enabling encrypted connections between web servers and clients. It is alsoemployed in secure shell (SSH) protocols, virtual private networks (VPNs), and other systems requiring secure key exchange. Despite its strengths, the Diffie-Hellman algorithm can be vulnerable to man-in-the- middle attacks if proper authentication mechanisms are not in place. Nevertheless, its ability to facilitate secure key exchange without prior shared secrets makes it an essential tool in the landscape of modern cryptography.

Sure, "the cloud" refers to the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Here are some key points:

*1) *Definition**

The cloud encompasses a variety of services including storage (like Google Drive or Dropbox), computing power (like Amazon Web Services or Microsoft Azure), databases (like MongoDB Atlas or Google Cloud SQL), networking (like content delivery networks), and more.

*2) *Types of Cloud Services**

- *Infrastructure as a Service (IaaS)*: Provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and networking infrastructure as needed.
- *Platform as a Service (PaaS)*: Provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.
- *Software as a Service (SaaS)*: Delivers software applications over the internet, on a subscription basis. Users can access applications through a web browser without needing to install or maintain the software themselves.

*3) *Benefits**

- *Scalability*: Cloud services can scale quickly to handle increasing workloads or user demands.
- *Cost-effectiveness*: Pay-as-you-go pricing models mean users only pay for what they use, reducing upfront costs.
- *Flexibility*: Accessible from anywhere with an internet connection, offering mobility and collaboration benefits.
- *Reliability*: Many cloud providers offer redundancy and backup options, reducing the risk of data loss.

*4) *Concerns and Considerations**

- *Security*: Data breaches and data loss are potential risks, although cloud providers invest heavily in security measures.
- *Compliance*: Depending on the industry, companies may need to adhere to specific regulations regarding data storage and handling.
- *Vendor Lock-in*: Moving data and applications between different cloud providers can be complex and costly.

*5) *Popular Cloud Providers**

- *Amazon Web Services (AWS)*: A comprehensive, evolving cloud computing platform provided by Amazon.
- *Microsoft Azure*: A cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services.
- *Google Cloud Platform (GCP)*: A suite of cloud computing services provided by Google.

Overall, the cloud has revolutionized the way businesses and individuals use computing resources, offering unprecedented flexibility, scalability, and accessibility compared to traditional on-premises infrastructure.

D. Future Enhancements

1) *Enhanced Security:* Consider implementing additional security measures such as digital signatures to authenticate communication parties.
2) *File Transfer:* Extend the application to support secure file transfer using the established encryption mechanisms.
3) *Cross-platform Compatibility:* Ensure the application can run seamlessly on different operating systems and devices.

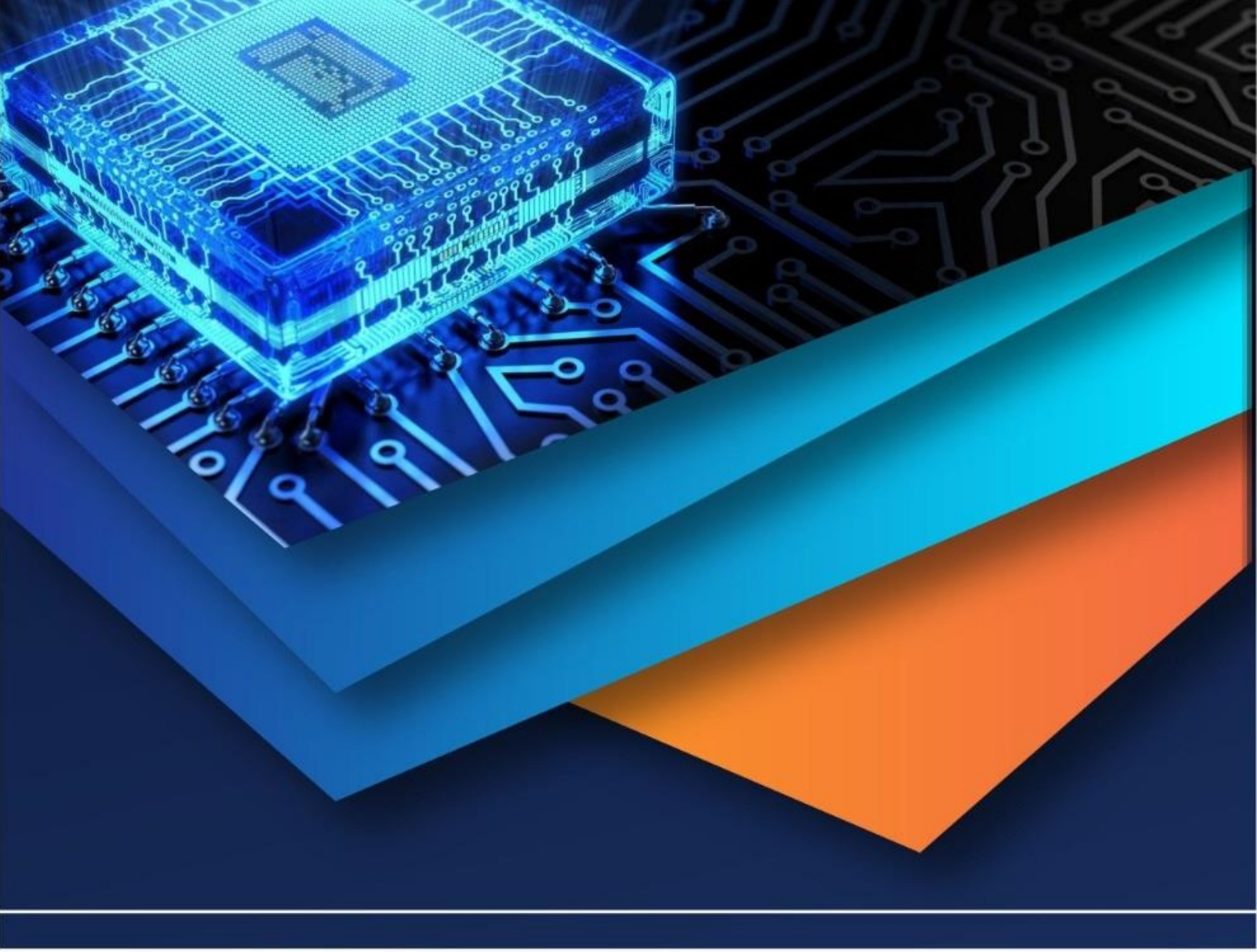
E. Result

Implementing "Secure Text Transfer Using Diffie-Hellman Key Exchange Algorithm" involves integrating cryptographic principles with robust programming techniques to ensure secure communication between parties. The project not only demonstrates practical knowledge of cryptography but also enhances understanding of network security and encryption protocols.

REFERENCES

[1] Msallam, M. M., & Aldoghan, F. (2023). “MultistageEncryption for Text Using Steganography and Cryptography. Journal of Techniques”, Vol. 5, No. 1, 38-43. https://doi.org/10.51173/jt.v5i1.1087
[2] Mathur, N., & Bansode, R. (2016). “AES Based TextEncryption Using 12 Rounds with Dynamic Key Selection”. Procedia Computer Science, 79, 1036-1043. 10.1016/j.procs.2016.03.131
[3] Ramu Naidu, B., Sastry, K.P.K., & Kiran, D.M.K. (2024). “Data Encryption to Decryption by Using LaplaceTransform”. Journal of Nonlinear Analysis and Optimization, Vol. 15(Issue. 4, No.1), 157-162.
[4] Mohammed Amin Almaiah1 , Ziad Dawahdeh2 , Omar Almomani3 , Adeeb Alsaaidah4 , Ahmad Al-khasawneh5, Saleh Khawatreh (2020), “A new hybrid text encryption approach over mobile ad hoc network”, (IJECE) Vol. 10, No. 6 pp. 6461~6471 DOI: 10.11591/ijece.v10i6.
[5] Rihartanto1 , Didi Susilo Budi Utomo1 , Herny Februariyanti2 , Arief Susanto3 , Wardatul Khafidhah (2023), “Bit-based cube rotation for text encryption”, (IJECE) Vol. 13, No.1 DOI:10.11591/ijece.v13i1.pp709717.
[6] Noor Sattar Noor 1 , Dalal Abdulmohsin Hammood 1, Ali Al-Naji 1,2,* and Javaan Chahl (2022) “A Fast Textto-Image Encryption-Decryption Algorithm for Secure Network Communication Volume 11 Issue3 ” https://doi.org/10.3390/computers11030039
[7] Marcin Lawnik 1,* , Lazaros Moysis 2,3 and Christos Volos“Chaos-Based Cryptography: Text Encryption Using ImageAlgorithms”. Electronics, 2022, 11, 3156. DOI: 10.3390/electronics11193156.
[8] M. A. Murillo-Escobar, F. Abundiz-Pérez, C. Cruz- Hernández, R. M. López-Gutiérrez. (2014). “A novel symmetric text encryption algorithm based on logisticmap”. Proceedings of the 2014 International Conference onCommunications, Signal Processing and Computers, Pages49-53.
[9] Gupta, Chiradeep and Reddy, N V Subba. (2022). “Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography.” Journal of Physics: Conference Series, 2161(1). DOI: 10.1088/1742- 6596/2161/1/012014
[10] Manikandaprabhu, P. and Samreetha, M. (2024). “A Review of Encryption and Decryption of Text Using the AES Algorithm”. International Journal of Scientific Research & Engineering Trends, Volume 10, Issue 2.
[11] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh (2015) , ”Implementation of Text Encryption using Elliptic Curve Cryptography” IMCIP2015 , Procedia Computer Science 54 (2015) 73 – 82.

[12] Malik, Rameshwari. (2015). "Cloud Computing SecurityImprovement using Diffie Hellman and AES". International Journal of Computer Applications, Volume118 - No. 1
[13] Thabit F, Alhomdy S, Jagtap S. (2021). "Security analysisand performance evaluation of a new lightweightcryptographic algorithm for cloud computing". Glob Transitions Proc, 2(1):100-110. DOI:10.1016/j.gltp.2021.01.014
[14] Gaurav Sharma, Priyanka Goyal, and Shivpratap Singh Kushwah. (2016). "Implementation of Modified Playfair CBC Algorithm". Int. J. Eng. Res., V5(06):679-684. DOI: 10.17577/ijertv5is060631
[15] Marzan RM, Sison AM, Medina RP.(2019). "Randomness ana 957-969". DOI: 10.32604/iasc.2023
[16] N. SugirthamR .Sherine Jenny B. Thiyaneswaran2 · S. Kumarganesh3 C. Venkatesan1 K Martin Sagayam4 · Lam Dang5 · Linh Dinh6 ·Hien Dang (2023), " Modifed Playfair for Text FileEncryption and Meticulous Decryption with Arbitrary Fillers by Septenary Quadrate Pattern", International Journal of Networked and Distributed Computing https://doi.org/10.1007/s44227-023-00019-4



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY