**IMPLEMENTATION OF HYBRID ENCRYPTION TECHNIQUES IN DATA TRANSMISSION**

Dr. S. Venkatramulu   
Associate Professor  
Computer Science & EngineeringKakatiya Institute of Technology and Science  
svr.cse@kitsw.ac.in

Chandu Kuchanapally  
Computer Science & EngineeringKakatiya Institute of Technology and Science  
b20cs023@kitsw.ac.inRahul Gattu  
Computer Science & EngineeringKakatiya Institute of Technology and Science  
b20cs048@kitsw.ac.in

Karthik Rendla  
Computer Science & EngineeringKakatiya Institute of Technology and Science  
b20cs021@kitsw.ac.in Manideep Dugyala  
Computer Science & EngineeringKakatiya Institute of Technology and Science  
b20cs031@kitsw.ac.in

*Abstract*— This paper presents a unique approach for assuring the security of digital communication that combines the Asymmetric key algorithms - RSA algorithm, Diffie-Hellman algorithm for key exchange and Symmetric key algorithm - AES algorithm. The primary goal is to increase the confidentiality while transmitting the data and security of data in modern communication networks. Ciphertext is created using the symmetric key algorithm - AES from plaintext. The RSA encryption technique is then used to further encrypt this ciphertext using the public key of receiver. The recipient's public key and the AES key are encrypted simultaneously using the Diffie-Hellman technique to create a shared secret key. When the message is received, the encrypted text is decrypted using the RSA technique, and the AES key is decrypted using the Diffie-Hellman algorithm. This AES key is used to decode the ciphertext and hence disclose the plaintext. Our technique improves communication security and contributes significantly to the creation of safe data transmission methods. By doing simulations and comparative analysis, we demonstrate the efficiency and reliability of our combined encryption and key exchange architecture. We highlight its advantages over traditional ways for eliminating potential flaws and ensuring secure communication routes. This study demonstrates the efficiency of seamlessly merging AES, RSA, and Diffie-Hellman in an encryption and key exchange process, therefore contributing to the advancement of secure communication protocols and data security mechanisms.

Keywords— AES, RSA, Secret Key, Diffie-Hellman, private key, public key, symmetric key, asymmetric key.

# Introduction

In today's linked world, when digital communication has grown pervasive, preserving the security and confidentiality of our sensitive information has never been more vital. Every day, we share personal and financial data via the internet, from emails and instant messaging to online purchases and cloud storage. Protecting sensitive information from unwanted access and hostile assaults is vital, and encryption plays a crucial role in attaining this aim. This research project digs into the world of encryption and key exchange protocols, concentrating on how the combination of Rivest-Shamir-Adleman algorithm and Diffie-Hellman with Advanced Encryption might strengthen the security of digital communications.

## The Importance of Encryption

Encryption is analogous to a secret language that converts our messages into unintelligible nonsense, save to those who know the key to decipher them. It works as a digital lock, shielding our data from prying eyes and unwanted access during transmission and storage. Without encryption, sensitive information including passwords, financial details, and intimate interactions would be subject to interception and exploitation by hackers and enemies.

## Understanding AES, RSA, and Diffie-Hellman:

***Advanced Encryption Standard (AES):*** AE**S** encryption algorithm is a symmetric key encryption method which is noted for its strength, speed, and broad usage. It functions by splitting data into blocks and executing a series of sophisticated mathematical operations using a secret key. AES is like the fortified vault that securely keeps our digital assets, guaranteeing that only those with the necessary key may open and access the contents.

***Rivest-Shamir-Adleman (RSA):*** RSA is an asymmetric key encryption method that utilizes a pair of keys – a public key and a private key. For encryption, public key is used and for decryption private key used which is kept secret and utilized for decoding. RSA is like having a secure mailbox where anybody can drop a message (with the public key), but only the intended recipient with the private key can access and read it.

***Diffie-Hellman Key Exchange*:** Diffie-Hellman is a key exchange technique that enables two entities to establish a shared secret key across an unsecured channel. It is like a secure meeting when two persons agree on a secret code without disclosing it to eavesdroppers. Diffie-Hellman assures that even if someone intercepts the conversation, they cannot decode the secret key without the assistance of the parties involved.

Our study strives to establish a strong encryption and key exchange paradigm by synergizing the characteristics of AES, RSA, and Diffie-Hellman. Our specific target is establishing an integrated encryption method employing AES for data encryption and RSA for encrypting AES keys. Implementing a secure key exchange system utilizing Diffie-Hellman to establish shared secret keys between communication entities.

# Literature Survey

A novel approach to generating digital signatures and public-key cryptosystems was presented in the field of hybrid encryption techniques for data transmission, which transformed the field of cryptography and established the groundwork for contemporary hybrid encryption techniques [1]. Furthermore, a thorough analysis of the Advanced Encryption Standard (AES) demonstrated its broad use in numerous cryptographic applications and its importance in guaranteeing safe data transfer [2]. Recent developments in cryptography have led to an exploration of emerging patterns and new possibilities that could lead to improvements in hybrid encryption methods for data transfer [3]. Hybrid techniques are successful in safeguarding data transmission in cloud environments, as demonstrated by a novel hybrid encryption mechanism that combines the RSA, AES, and Blowfish algorithms [4]. Also, in order to improve data security during network transmission, innovative hybrid encryption algorithms that make use of RSA and Diffie-Hellman techniques were created [5]. These algorithms present interesting options for safeguarding data exchange in communication networks. The need for strong encryption mechanisms in cloud-based data storage and sharing platforms was addressed by a hybrid encryption scheme that combines the RSA and AES algorithms for secure data sharing in cloud environments [6]. The effectiveness of a hybrid encryption algorithm based on the Diffie-Hellman and RSA methods was shown in improving data security in communication networks, especially in situations when safe data transfer between entities is necessary [7].

A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare leveraged hybrid encryption techniques to secure multimedia data transmission in IoT-enabled healthcare systems, addressing critical security concerns associated with healthcare data exchange [9]. Furthermore, a secure data sharing framework for cloud-assisted industrial IoT integrated hybrid encryption techniques to ensure secure online/offline data sharing in industrial IoT environments, contributing to the advancement of secure data transmission in industrial settings [10]. Finally, a performance analysis of encryption algorithms in a satellite communication network based on H-ARQ evaluated the effectiveness of encryption schemes in ensuring secure data transmission over satellite communication networks, providing insights into the performance of encryption algorithms in satellite communication systems [11].

In comparison to a comparative examination of hybrid models, our proposal includes all three algorithms (AES, RSA, Diffie-Hellman) into a single integrated model, stressing the need of safe key exchange methods with data encryption. This integrated technique provides increased security for data transfer compared to typical hybrid systems.   
Furthermore, our project's triple-layer encryption strategy and end-to-end security concerns separate it from research concentrating on specialized fields like cloud computing or IoT communication security. While linked with the purpose of strengthening key exchange security, particularly in cloud environments, our model's adaptability and greater breadth make it adaptable to different communication scenarios beyond specialized domains.

The current study [12] suggests a trust-based authentication technique using a security algorithm that collectively forms a hybrid security algorithm in VANET to provide a secure platform for vehicle communication. In providing a trustworthy authentication of vehicles in VANET, the technique provides a generally more secure and safe vehicular network. [13] Study delivers a security paradigm to protect vital scholarly information that is conveyed over infrastructures of fog computing for security in eLearning systems. When two entangled encryption mechanisms are combined, security in eLearning systems is improved. The study ensures the security and privacy of eLearning platform and its users. It also helps to protect the instructions given and subjective information by using multiple encryption mechanisms for protection in e-learning. Multiple encryption techniques combined improve e-learning platform security, protecting user privacy and instructional information. In addition, a strong hybrid lightweight cryptosystem was created to guard IoT smart devices and solve security flaws in IoT ecosystems [14]. In IoT contexts, this cryptosystem ensures data security and integrity by providing effective encryption algorithms designed for devices with little resources. Additionally, a hybrid cryptography system's effectiveness and efficacy in securing data transfer were evaluated by performance evaluation [15]. The study helps in the selection and application of appropriate encryption techniques for a variety of applications by offering insights into the performance characteristics of hybrid encryption systems. Hybrid cryptography has also been proposed to address security issues in resource-constrained sensor environments for safe data transmission in wireless sensor networks [16]. The study helps to understand the performance characteristics of hybrid cryptography mechanisms to guard against any chances of intrusion, deception or security breach during data transmission. The study is proposed for secure data transmission on resource-constrained sensor- environments to overcome security issues faced by narrow spectrum wireless environment used is Wireless sensor network [16].

This method protects the confidentiality and integrity of sensor data transferred over wireless channels, improving data security in wireless sensor networks. Furthermore, in order to improve data security in fog computing environments, data encryption utilizing hybrid cryptography with validity check was investigated [17]. In order to mitigate security vulnerabilities, fog computing systems use hybrid cryptography with integrity check techniques to ensure data integrity and authenticity. Also, a comparative examination of several encryption algorithms was carried out to assess the suitability and performance of different encryption methods for secure data transfer [18].

The study provides valuable insights into the strengths and weaknesses of different encryption techniques, aiding in informed decision-making for secure data transmission applications. Additionally, the security of cloud computing was enhanced using hybrid cryptography algorithms, addressing security concerns in cloud-based environments [19]. The proposed hybrid cryptography algorithms enhance data security in cloud computing systems, ensuring confidentiality and integrity of cloud-hosted data. Investigating financial information security using a hybrid encryption technique on multi-cloud architecture was conducted, enhancing the security of financial data transmission [20]. This approach ensures robust security measures for financial information exchanged over multi-cloud architectures, safeguarding sensitive financial data from unauthorized access. Finally, a novel hybrid cryptographic approach for secure communication was proposed, offering enhanced security measures for data transmission [21]. This hybrid cryptographic approach ensures secure communication channels, protecting sensitive information exchanged between entities. Additionally, a comprehensive study on data security in cloud environments using hybrid encryption techniques was conducted, focusing on enhancing confidentiality and reliability of cloud-hosted data [22]. This study provides valuable insights into the effectiveness of hybrid encryption techniques in improving data security in cloud environments, contributing to the development of robust security measures for cloud-based data storage and transmission.

Additionally, although other studies focus on specialized applications like mobile banking or multimedia communication, our project's applicability extends to general digital communication, emphasizing its adaptability and greater breadth. The integration of AES, RSA, and Diffie-Hellman into a complete encryption architecture provides an extra degree of security and dependability to key management operations, assuring safe data transfer and communication channels.

The suggested integrated encryption approach guarantees safe communication across numerous platforms, complementing existing security measures and offering increased protection for data storage, transport, and sharing. The triple-layer encryption technique and the integration of key exchange mechanisms contribute to a complete security strategy appropriate for varied communication scenarios, making our project a significant achievement in the field of secure communication and cryptography.

## Why this approach?

This research presents an innovative technique by merging AES, RSA, and Diffie-Hellman in a seamless encryption and key exchange scheme. This integrated paradigm attempts to promote data confidentiality, security, and reliability in digital communication networks. The innovation lies in many crucial aspects:

***Triple Layer Encryption:*** Unlike standard systems that may use either AES or RSA for encryption, our solution incorporates a triple layer of encryption. The plaintext is initially encrypted using AES, providing strong symmetric encryption. The AES key and the ciphertext are then individually encrypted using RSA using the recipient's public key, offering an extra degree of protection. Finally, the AES key is encrypted using Diffie-Hellman, producing a shared secret key for safe key exchange.

***Hybrid Cryptographic Techniques:*** By integrating AES, RSA, and Diffie-Hellman, our project exploits the capabilities of each technique while limiting their own flaws. AES provides fast and efficient symmetric encryption, RSA provides safe asymmetric encryption and digital signatures, and Diffie-Hellman enables exchanging keys securely without broadcasting the key over the network.

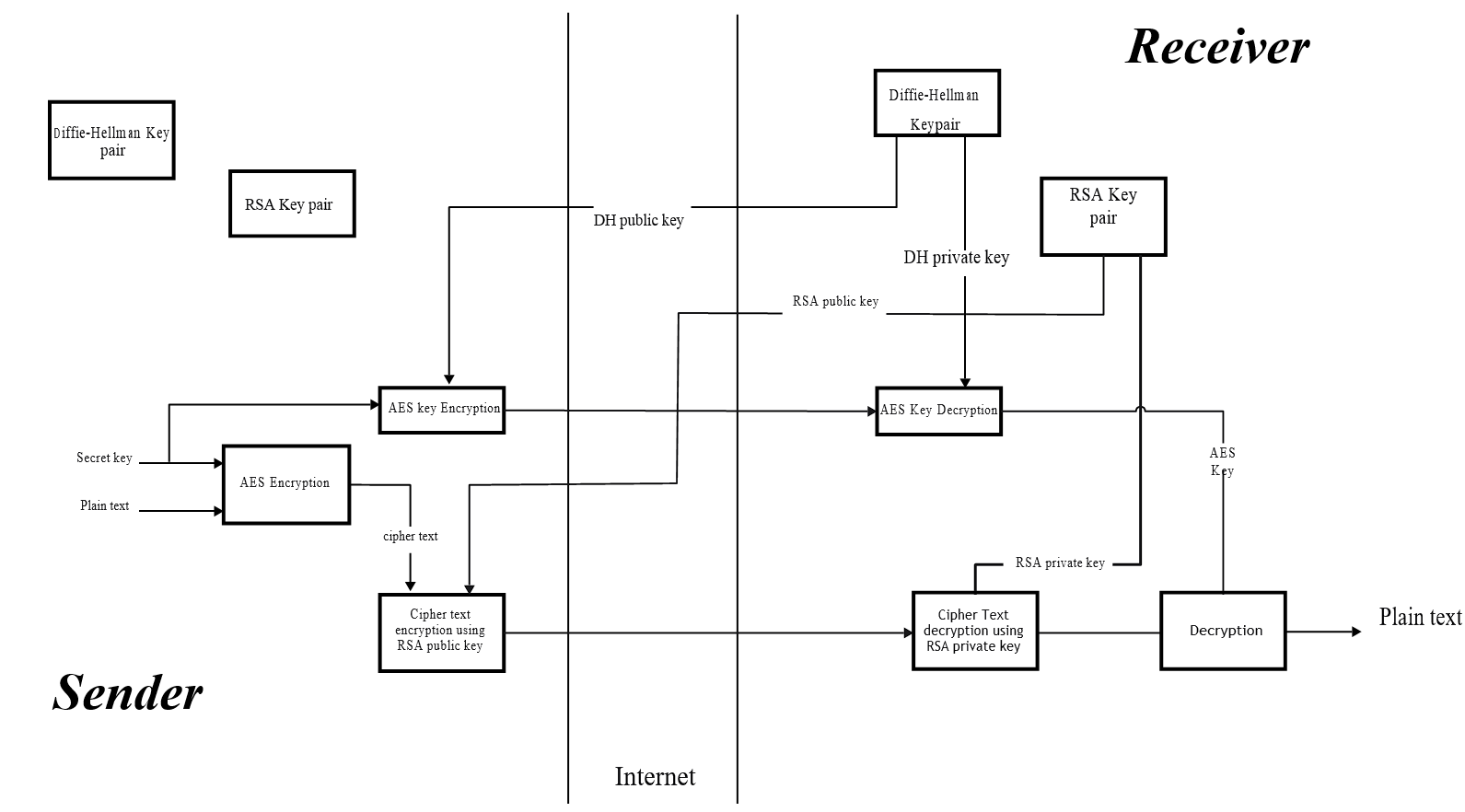
***Safe Key Exchange Mechanism:*** The incorporation of Diffie-Hellman enables a safe key exchange procedure, solving difficulties connected to key management and distribution. This strategy increases the overall security of the communication channel by establishing a shared secret key between the sender and recipient without disclosing the key during transmission.

***End-to-End Security****:* The suggested paradigm assures end-to-end security by encrypting both the message content (by AES) and the encryption keys (via RSA and Diffie-Hellman). This complete encryption technique safeguards against illegal access, interception, and alteration of data during transmission.   
  
Our approach distinguishes itself by focusing on combining AES, RSA, and Diffie-Hellman in a triple-layer encryption and key exchange paradigm, which provides an additional layer of security when compared to typical hybrid methods. While comparable to prior research in integrating these algorithms for security objectives, our effort expands the use beyond specialized fields like IoT security, intending to better security in general digital communication systems. The complete strategy of encrypting both message content and encryption keys promotes security across numerous communication channels.

# implementation

In our encryption and transmission process, the initial step involves encrypting plaintext using the Advanced Encryption Standard (AES) algorithm, utilizing a specific AES key to generate ciphertext. This ciphertext is then subjected to an additional layer of encryption, this time using the public key of receiver in the Rivest-Shamir-Adleman (RSA) encryption algorithm. Concurrently, the AES key utilized in the first encryption step is separately encrypted using the Diffie-Hellman key exchange technique and the receivers Diffie-Hellman public key. Both the RSA-encrypted ciphertext and the Diffie-Hellman-encrypted AES key are securely shared with the intended receiver.

Fig 1 Encryption and Decryption



Upon receiving these encrypted components, the recipient proceeds with the decryption process. Initially, the RSA private key, corresponding to the public key used for encryption, is employed to decrypt the RSA-encrypted ciphertext, revealing the original ciphertext generated by the AES algorithm. Simultaneously, the recipient utilizes their private Diffie-Hellman key, paired with the sender's public Diffie-Hellman key shared during key exchange, to decrypt the Diffie-Hellman-encrypted AES key. This step effectively retrieves the original AES key used for encryption. Finally, armed with the decrypted AES key, the recipient proceeds to decrypt the previously obtained ciphertext from the AES encryption phase. This decryption process completes the sequence, resulting in the recovery of the original plaintext message. Through this intricate encryption and decryption process, our system ensures robust security and confidentiality in transmitting sensitive information between sender and recipient parties.

## Methodology

In our project, the methodology involves a multi-step process to ensure secure communication and data encryption. The following steps outline the methodology implemented:

*AES Encryption:* The process begins with the encryption of plaintext using the Advanced Encryption Standard (AES) algorithm. This algorithm employs a symmetric encryption technique where the same key is used for both encryption and decryption. The AES key is generated and applied to the plaintext, resulting in the generation of ciphertext.

*Cipher Text=EAES key(Plain Text)* (1)

*RSA Encryption:* Next, the ciphertext produced by AES encryption is further encrypted using the RSA algorithm. RSA is an asymmetric key encryption algorithm which generates a pair of keys: a public key for encryption and a private key for decryption. In this step, the recipient's public key is used to encrypt the ciphertext, adding an additional layer of security to the data.

*Ts=ERSA-Public key (Cipher Text)* (2)

*Diffie-Hellman Key Exchange:* Simultaneously, the AES key generated during the AES encryption phase is encrypted using the Diffie-Hellman key exchange technique. Diffie-Hellman is a key exchange algorithm that allows two entities to create a shared secret key over an insecure communication channel. The sender and receiver exchange public keys and perform computations to derive a shared secret key without explicitly transmitting the key over the network. In this step, the AES key which is used for AES encryption is encrypted using Deffie-Hellman public key which is exchanged from recipient to the sender. And the encrypted AES key is sent to the recipient.

*Tk = EDH-Public Key (AES Key)* (3)

*Sharing Encrypted Data:* Both the RSA-encrypted ciphertext and the Diffie-Hellman-encrypted AES key are shared with the recipient securely. The encrypted data is transmitted over the communication channel to the intended recipient.

*Ts and Tk are exchanged over the internet* (4)

*Decryption Process:* Upon receiving the encrypted data, the receiver initiates the decryption process. First, the RSA-encrypted ciphertext is decrypted using the recipient's private RSA key. This step reveals the original ciphertext generated by the AES encryption phase.

*Cipher Text=DRSA-Private Key(Ts)* (5)

*AES Key Decryption:* Simultaneously, the Diffie-Hellman shared secret key is used to decrypt the Diffie-Hellman-encrypted AES key. Here, this process ensures that only the receiver who possess the corresponding intended Diffie-Hellman private key, can be able to decrypt the AES key securely.

*AES Key=DDH-Private Key(Tk)* (6)

*Final Decryption:* Finally, the decrypted AES key obtained from the Diffie-Hellman decryption process is used to decrypt the original ciphertext generated by AES encryption. This step completes the decryption process, resulting in the recovery of the original plaintext message.

*Plain Text = DAES Key(Cipher Text)*  (7)

# RESULT

The proposed project adopts a sophisticated approach to data security by integrating AES, RSA, and Diffie-Hellman in a triple-layer encryption and key exchange model, which sets it apart from previous papers focusing on individual or dual-layer encryption methods. The project's core strategy involves encrypting plaintext using AES, then encrypting the AES-encrypted ciphertext using RSA, and encrypting the AES key itself using Diffie-Hellman. This multi-layer encryption scheme significantly enhances security by creating multiple barriers that unauthorized entities must overcome to access sensitive data. Unlike single-layer encryption methods, which may be susceptible to decryption attacks, our project's combination of symmetric (AES) and asymmetric (RSA, Diffie-Hellman) encryption provides a robust defence mechanism against accessing data unauthorized and tampering of data.

One of the key strengths of our approach lies in the combination of RSA for secure key exchange and initial encryption, and AES for efficient bulk data encryption. This blend of asymmetric and symmetric encryption techniques maximizes security without compromising performance. Furthermore, the use of Diffie-Hellman for key exchange adds an additional layer of security by establishing a shared secret key without transmitting the actual key over the network, thwarting potential key interception attacks. Additionally, our project prioritizes secure transmission protocols such as HTTPS or TLS/SSL during data transmission, further safeguarding data integrity during transit.

The decryption process in our model involves RSA private key decryption and Diffie-Hellman key decryption, ensuring end-to-end security. Only authorized recipients possessing the correct private keys can decrypt and access the original plaintext message, thereby ensuring confidentiality throughout the communication process. Overall, our project's comprehensive and multi-layered encryption approach aims to provide a robust security framework for data transmission, addressing vulnerabilities present in traditional encryption methods and enhancing data confidentiality, integrity, and authenticity.

# conclusion

The integration of AES, RSA, and Diffie-Hellman in our triple-layer encryption and key exchange model marks a significant stride in data security for digital communication. This approach combines symmetric and asymmetric encryption methods to fortify defenses against unauthorized access and data interception. By leveraging RSA for secure key exchange, AES for efficient data encryption, and Diffie-Hellman for key security without direct transmission, our project ensures robust protection throughout data transmission. The emphasis on secure transmission protocols further enhances data integrity and confidentiality, making our solution a reliable safeguard for sensitive information exchange.

##### References

[1] Rivest, R. L., Shamir, A., & Adleman, L. (1978, February). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

[2] Heron, S. (2009, December). Advanced Encryption Standard (AES). *Network Security*, *2009*(12), 8–12. https://doi.org/10.1016/s1353-4858(10)70006-4

[3] Cao, Z. (2012, December 6). *New Directions of Modern Cryptography*. https://doi.org/10.1201/b14302

[4] Singh, G., & Garg, D. M. (2018, November 6). Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP. *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, *18*, 7364–7380. https://doi.org/10.24297/ijct.v18i0.7898

[5] A Hybrid Algorithm For Enhancement of the Data Security during Network Transmission Based on RSA and DH. (2023). *International Journal of Intelligent Engineering and Systems*, *16*(3), 614–624. https://doi.org/10.22266/ijies2023.0630.49

[6] RSA and AES Based Secure Data Sharing in Cloud Based Environment. (2017, February 18). *International Journal of Computing, Communication and Instrumentation Engineering*, *4*(1). https://doi.org/10.15242/ijccie.h1216011

[7] Gupta, S., & Sharma, J. (2012, December). A hybrid encryption algorithm based on RSA and Diffie-Hellman. *2012 IEEE International Conference on Computational Intelligence and Computing Research*. https://doi.org/10.1109/iccic.2012.6510190

[8] Quist-Aphetsi, K., & Xenya, M. C. (2019, May). Node to Node Secure Data Communication for IoT Devices Using Diffie-Hellman, AES, and MD5 Cryptographic Schemes. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*. https://doi.org/10.1109/icsiot47925.2019.00022

[9] Taloba, A. I., Elhadad, A., Rayan, A., El-Aziz, R. M. A., Salem, M., Alzahrani, A. A., Alharithi, F. S., & Park, C. (2023, February 1). *A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare*. Alexandria Engineering Journal /Alexandria Engineering Journal. https://doi.org/10.1016/j.aej.2022.09.031

[10] Miao, Y., Tong, Q., Choo, K. K. R., Liu, X., Deng, R. H., & Li, H. (2019, October). Secure Online/Offline Data Sharing Framework for Cloud-Assisted Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(5), 8681–8691. https://doi.org/10.1109/jiot.2019.2923068

[11] Jeong, W. H., Yeo, B. G., Kim, K. H., Park, S., Yang, S. W., Lim, J. S., & Kim, K. S. (2015, February 28). *Performance Analysis of the Encryption Algorithms in a Satellite Communication Network based on H-ARQ*. the Journal of the Institute of Internet, Broadcasting and Communication. https://doi.org/10.7236/jiibc.2015.15.1.45

[12] E, P. V., & W, K. T. (2021, May 13). *Trusted Authentication using hybrid security algorithm in VANET*. arXiv.org. https://arxiv.org/abs/2105.06105.

[13] Alshambri, H. A., & Alassery, F. (2021, January 1). *Securing Fog Computing For E-Learning System Using Integration of Two Encryption Algorithms*. Journal of Cyber Security. https://doi.org/10.32604/jcs.2021.022112

[14] Ragab, A. A. M., Selim, G. M., Wahdan, A. M., & Madani, A. (2019, January 1). *Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices*. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-030-24900-7\_1

[15] Shaikh, E., & Patil, S. (2017, December 25). Performance Evaluation of Hybrid Cryptography System. *International Journal of Engineering Trends and Technology*, *54*(4), 255–263. https://doi.org/10.14445/22315381/ijett-v54p235

[16] Prakash, S., & Rajput, A. (2018). Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks. *Advances in Intelligent Systems and Computing*, 589–599. https://doi.org/10.1007/978-981-10-7386-1\_50

[17] Ejim, S., Gital, A. Y., Chiroma, H., Lawal, M. A., Abubakar, M. Y., & Kubi, G. M. (2023). Data Encryption in Fog Computing Using Hybrid Cryptography with Integrity Check. *Soft Computing for Problem Solving*, 627–638. https://doi.org/10.1007/978-981-19-6525-8\_48

[18] Mota, A. V., Azam, S., Shanmugam, B., Yeo, K. C., & Kannoorpatti, K. (2017, September). Comparative analysis of different techniques of encryption for secured data transmission. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. https://doi.org/10.1109/icpcsi.2017.8392158

[19] Taha, A. A., Salama, D. D., Abdelminaam, S., & Hosny, K. (2017, December 1). *Enhancement the Security of Cloud Computing using Hybrid Cryptography Algorithms*. ResearchGate. https://www.researchgate.net/publication/324877911\_Enhancement\_the\_Security\_of\_Cloud\_Computing\_using\_Hybrid\_Cryptography\_Algorithms

[20] Rashid, M. N., Abed, L. H., & Awad, W. K. (2022, December 1). Financial information security using hybrid encryption technique on multi-cloud architecture. *Bulletin of Electrical Engineering and Informatics*, *11*(6), 3450–3461. https://doi.org/10.11591/eei.v11i6.3967

[21] Arora, G., Hirolikar, D. S., Deore, S. S., Bajaj, K. K., Gupta, P. K., Jaleel, U., & R, V. (2024). *A Novel Hybrid Cryptographic Approach for Secure Communication*. https://ijisae.org/index.php/IJISAE/article/view/4118

[22] Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability. (2024, April 30). *International Journal of Intelligent Engineering and Systems*, *17*(2), 159–170. https://doi.org/10.22266/ijies2024.0430.14