JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Hybrid Cryptographic System for Secure, Scalable File Encryption and Decryption Using RSA and AES: A Review

[1] Mohit Kumar Malviya, [2]Prof. Dr Shekhar Nigam,
[1]M.Tech Scholar, [2] Professor & H.O.D,
[1,2]Department of Information Technology (IT)
[1,2] NRI Institute Of Information Science And Technology, Bhopal (Mp), India

Abstract : A Hybrid Cryptographic System integrates the strengths of both symmetric and asymmetric encryption techniques to ensure secure and scalable file encryption and decryption. This paper reviews AES (Advanced Encryption Standard), a symmetric key algorithm, is utilized for its high-speed performance and efficiency in encrypting large volumes of data. However, symmetric encryption alone lacks secure key distribution mechanisms, which is where RSA (Rivest–Shamir–Adleman), an asymmetric key algorithm, plays a crucial role. RSA is leveraged to encrypt the AES session key, ensuring that only the intended recipient with the correct RSA private key can access it. This combination optimizes both security and performance: the fast encryption speed of AES for bulk data and the robust key management capabilities of RSA. the hybrid system ensures that data remains confidential, while also being scalable and efficient for various applications, making it a suitable solution for modern secure communication and data storage needs.

Keyword **- AES (Symmetric Encryption), Chunk-Based Encryption, Distributed Key Management, File Encryption and Decryption, Hybrid Cryptography, RSA (Asymmetric Encryption), Secure Key Exchange.**

I. INTRODUCTION

A Hybrid Cryptographic System integrates the strengths of both symmetric and asymmetric encryption techniques to ensure secure and scalable file encryption and decryption. In this approach, AES (Advanced Encryption Standard), a symmetric key algorithm, is utilized for its high-speed performance and efficiency in encrypting large volumes of data. However, symmetric encryption alone lacks secure key distribution mechanisms, which is where RSA (Rivest–Shamir–Adleman), an asymmetric key algorithm, plays a crucial role. RSA is leveraged to encrypt the AES session key, ensuring that only the intended recipient with the correct RSA private key can access it. This combination optimizes both security and performance: the fast encryption speed of AES for bulk data and the robust key management capabilities of RSA. By combining these cryptographic techniques, the hybrid system ensures that data remains confidential, while also being scalable and efficient for various applications, making it a suitable solution for modern secure communication and data storage needs.

the hybrid approach ensures data integrity and confidentiality, as unauthorized users cannot access the encrypted content or manipulate it without detection. The combined strength of RSA and AES not only enhances the encryption process but also simplifies compliance with data protection regulations, such as GDPR and HIPAA, by ensuring that sensitive information remains secure during transmission and storage. As a result, this hybrid cryptographic solution addresses both current and future challenges in secure data management, making it a resilient choice for enterprises seeking robust encryption mechanisms to protect against the ever-increasing threat of cyber attacks.

A. **Hybrid Cryptographic System**

The Hybrid Cryptographic System combines the strengths of two powerful encryption methods, RSA and AES, to provide a secure, scalable solution for file encryption and decryption. RSA, an asymmetric encryption technique, leverages two separate keys—a public key for encryption and a private key for decryption—to securely distribute AES keys to intended recipients. AES, on the other hand, is a symmetric encryption method known for its speed and efficiency, particularly with large data volumes. By first using RSA to securely encrypt the AES key and then using AES for fast data encryption, this hybrid approach ensures both high-level security and practical performance. The system is designed to protect sensitive information against unauthorized access while also enabling scalability across diverse file sizes and encryption needs. This blend of RSA and AES addresses the limitations of each technique on its own, achieving an ideal balance between security and speed for modern data protection requirements

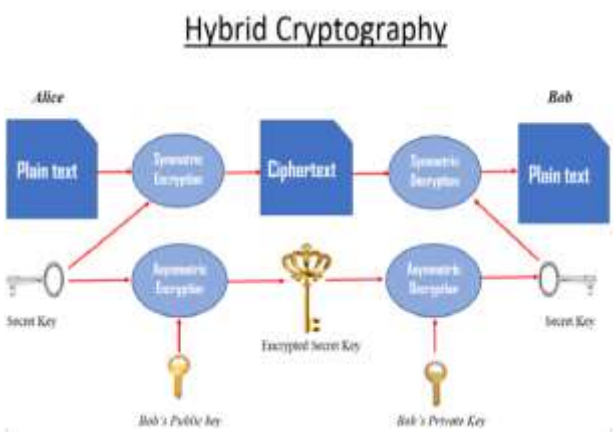

Fig 1 Hybrid Cryptography

In a Hybrid Cryptographic System, RSA handles the secure exchange of keys, mitigating the risk of key interception during transmission. Once the AES key has been securely shared via RSA, AES efficiently encrypts and decrypts large volumes of data, making it highly suitable for scalable applications, such as cloud storage, secure file sharing, and large-scale data processing. The combination also enhances security by separating the key management process from data encryption, reducing the chance of exposing critical information.

This layered security model reinforces the system's robustness, as any compromise in one layer requires breaching the other to access the underlying data. Consequently, hybrid cryptographic systems leveraging RSA and AES meet both security and scalability demands, making them ideal for environments where data privacy and speed are paramount.

B. Encryption and Decryption

Encryption and decryption are fundamental processes used to protect data and ensure privacy in the digital world. Encryption involves converting readable data, known as plaintext, into an unreadable format, called ciphertext, using a specific algorithm and an encryption key. This process ensures that only authorized individuals with the correct key can access the original data. On the other hand, decryption is the reverse process where ciphertext is transformed back into its original plaintext form. This requires the use of a decryption key, which is typically kept secret to prevent unauthorized access. These techniques are widely used in various applications, such as securing online communications, protecting sensitive information in databases, and ensuring the confidentiality of transactions over the internet.

Organizations frequently use encryption to comply with privacy regulations and standards, such as the GDPR or HIPAA, which mandate strict data protection practices. However, while encryption provides robust security, it also requires proper management of keys. Losing access to encryption keys can render data permanently inaccessible, emphasizing the need for effective key management systems.

Providing a critical layer of protection against unauthorized access, data breaches, and identity theft. As technology advances and cyber threats become more sophisticated, the adoption of strong encryption practices continues to be crucial for safeguarding digital assets and maintaining trust in online platforms and services.

Fig 2 Encryption-Decryption process

Encryption and decryption are fundamental processes in securing digital information. Encryption is the process of converting plain, readable data into an encoded format using a specific algorithm and an encryption key. This ensures that only authorized parties, who possess the correct decryption key, can access the original data. For instance, when you send a message over the internet, it might be encrypted to prevent hackers from reading it during transmission.

The decryption process is the reverse of encryption. It involves converting the back into its original plaintext from using a decryption key

II. LITERATURE REVIEW

Renuka Shone Durge et.al. (2024) - As cyber attacks are getting more complex and sophisticated, stringent, multi-layered security measures are required. Existing approaches often rely on tokenization or encryption algorithms, both of which have drawbacks. Previous attempts to ensure data security have primarily focused on tokenization techniques or complex encryption algorithms. While these methods work well on their own, they have proven vulnerable to sophisticated cyber attacks. This research presents new ways to improve data security in digital storage and communication systems. We solve data security issues by proposing a multi-level encryption strategy that combines double encryption technology along with tokenization. The first step in the procedure is a byte-level byte-pair encoding (BPE) tokenizer, which tokenizes the input data and adds a layer of protection to make it unreadable. After tokenization, data is encrypted using Rivest–Shamir–Adleman (RSA) to create a strong initial level of security. To further enhance security, data encrypted with RSA has an additional layer of encryption applied using the advanced encryption standard (AES) method. This article describes how this approach is implemented in practice and shows how it is effective in protecting data at a higher level than single-layer encryption or tokenization systems [01].

Chidi Ukamaka Betrand et al. (2024) - The goal of this project was to develop a hybrid encryption scheme that will only allow authorized users to access and download files stored online, thus enhancing file storage security in the cloud. Rapid Application Development (RAD) methodology was used to create the proposed system, allowing for modifications to be made to the system as it was being developed. The hybrid encryption scheme employs both symmetric and asymmetric encryption. The AES (Advanced Encryption Standard) algorithm and RSA (Rivest–Shamir–Adleman) algorithm were combined to develop the proposed hybrid encryption system. PHP, JavaScript and Laravel were the programming languages and web framework used to implement the system. The proposed system was tested and evaluated by users. The experimental results show that the proposed hybrid encryption scheme was fast and provided a high level of security but had some drawbacks which include increase in file size after it was encrypted and inability to sort files in the web app. Overall, the proposed system enhances confidentiality and data protection in cloud environments, guarding against potential breaches and unauthorized access [02].

LE L, et.al, (2023) - Author are study a n the current era of information explosion, users' demand for data storage is increasing, and data on the cloud has become the first choice of users and enterprises. Cloud storage facilitates users to backup and share data, effectively reducing users' storage expenses. As the duplicate data of different users are stored multiple times, leading to a sudden decrease in storage utilization of cloud servers. Data stored in plaintext form can directly remove duplicate data, while cloud servers are semi-trusted and usually need to store data after encryption to protect user privacy. Secure de-duplication and recover data in ciphertext for different users, and determine whether the indexes of public key searchable encryption and the matching relationship of trapdoor are equal in ciphertext to achieve secure de-duplication. For the duplicate file, the data user's re-encryption key about the file is appended to the ciphertext chain table of the stored copy [03].

Tashara Solomon et. al (2023) - Cloud storage is an integral part of modern computing; however, the associated data security concerns have hindered its widespread adoption. This paper proposes a triple phase hybrid security model for cloud storage using Advanced Encryption Standard (AES) that can address these security concerns. In the first phase, the AES algorithm is used to encrypt the data using a shared key between the user and the cloud server. In the second phase, a data integrity verification algorithm is applied to guarantee that the data being stored in the cloud are not tampered with. Lastly, a transmission security layer is employed to protect data transmissions between the user and the cloud server. The data is encrypted using AES during the encryption process using 16-bit key. The encrypted data is inserted into a cover image during the steganography stage. The data is once more encrypted using AES and stored in the cloud during the hybrid phase. The effectiveness of the suggested model was assessed using a variety of security measures. The proposed triple phase hybrid security model is evaluated in an extensive security experiment. The results demonstrate that the proposed security model is able to effectively protect data stored in the cloud from threats such as unauthorized access, data manipulation and data leakage. Furthermore, the proposed model is also able to effectively minimize the transmission overhead and reduce the total computational cost required for data encryption and decryption [04**].**

Moses Kazeem Abiodun et.al (2023) - Network users have been scared of storing sensitive information, such as bank details, health records, and other vital information, on the Internet because it is vulnerable to attack by a third party. Several threat models are impacting the security of the cloud. Having a secure cloud system will help to be at ease in using cloud computing facilities. This study aims at providing a cryptography approach to eliminating the vulnerabilities in the cloud-based system, and making access and data storage in the cloud very safe. The system uses Rivest-Shamir-Adleman (RSA) to encrypt files and the Advanced Encryption Standard (AES) key to encrypt the encrypted files. The hash function is used for extra key security, and Python programming language was used to implement the system, and for cloud storage, MongoDB was used. Generally, results indicate that the Double Stage Encryption (DSE) takes an average time for encryption of 83% and decryption of 75% compared to RSA and AES singly. The RSA is 68% faster than AES during the encryption process, but there is no significant difference between

the two during decryption. The Avalanche effect testing showed the DSE to be 17% higher than singly testing AES and RSA, which implies it is more secure than RSA and AES as single encryption schemes [05].

III. **Bijeta Seth, et. al (2022) -** Authors presented Cloud computing has emerged as one of the most groundbreaking technologies to have redefined the bounds of conventional computing techniques. It has ushered in a paradigm shift and pushed the frontiers of how computing assets, inclusive of infrastructure resources, software, and applications can be used, adopted, and purchased. The economic benefits or rather the fundamental economic shift offered by cloud computing in reducing capital expenditure and converting it to operational expenditure has been a primary motivating factor for early adopters. However, despite its inherent advantages that include better access and control, there exist several reservations around cloud computing that have impeded its growth. The control, elasticity, and ease of use that cloud computing is associated with also engender many security issues. Security is considered to be the topmost hurdle out of the nine identified challenges of cloud computing as underlined by the study conducted by the International Data Corporation [06].

Udochukwu Iheanacho Erondu et.al (2022) - Author are study the advancement of network and multimedia technologies in recent years, multimedia data, particularly picture, audio, and video data, has become increasingly frequently used in human civilization. Some multimedia data, such as entertainment, politics, economics, militaries, industries, and education, requires secrecy, integrity, and ownership or identity protection. Cryptology, which looks to be a viable method for information security, has been used in many practical applications to safeguard multimedia data in this regard. Traditional ciphers based on number theory or algebraic ideas, such as data encryption standard (DES), advanced encryption standard (AES), and other similar algorithms, which are most commonly employed for text or binary data, do not appear to be appropriate for multimedia applications. As a result, this research examines effective algorithms for data security [07].

Sultan Almakdi et. al (2021) – This paper reviews has presented the database users have begun to use cloud database services to outsource their databases. The reason for this is the high computation speed and the huge storage capacity that cloud owners provide at low prices. However, despite the attractiveness of the cloud computing environment to database users, privacy issues remain a cause for concern for database owners since data access is out of their control. Encryption is the only way of assuaging users' fears surrounding data privacy, but executing Structured Query Language (SQL) queries over encrypted data is a challenging task, especially if the data are encrypted by a randomized encryption algorithm. Many researchers have addressed the privacy issues by encrypting the data using deterministic, onion layer, or homomorphic encryption. Nevertheless, even with these systems, the encrypted data can still be subjected to attack [08].

Reece B. D'Souza et. al (2021) - Protection of sensitive or confidential data is one of the major security concerns in this day and age, for an organization or individual, be it a government body or a business corporation. Cryptography, which initially was designed for military or diplomatic use, can now be publicly utilized by anyone to achieve data security. Encryption is being seen as the best way to make data secure and ensure its protection [6]. Therefore, the utilization of hybrid cryptography can ensure an additional layer of protection to any security system. The main aim of this paper is to securely store and retrieve files stored on the cloud. Data security is achieved using the combined techniques of AES and RSA Algorithms. Furthermore, the AES algorithm was enhanced with the use of threads. This concept of multithreading reduces the time of completion as the file size increases. It also consists of OTP verification via the RSA digital signatures methodology. Therefore, a system with high security, better performance, data integrity was designed and implemented [09]].

.

III. METHOD

A. System Architecture Overview

The secure file storage system is designed to offer a robust and efficient mechanism for users to upload, encrypt, store, and later decrypt and restore files. It employs the Flask web framework to create a seamless front-end interface, allowing users to interact with the system intuitively. A key feature of this architecture is its hybrid encryption mechanism, which combines the strengths of both asymmetric and symmetric encryption to safeguard data throughout its lifecycle.

B. File Upload and Handling

The first step in the secure file storage process is the user uploading a file through the web interface. Users interact with a straightforward and user-friendly interface, enabling them to select files for upload effortlessly. The system performs file validation to check for permissible file types, such as .pem and .txt. This validation ensures that only safe and suitable files are processed, mitigating potential security risks. Once a file is validated, it is temporarily stored in a designated upload directory on the server, which is essential for managing files prior to encryption.

C. File Splitting and Chunk-Based Encryption:

Once the file is uploaded, it undergoes a process of splitting into smaller segments or chunks. This chunking enhances security and improves manageability during encryption and decryption. Large files are divided into smaller, fixed-size chunks, allowing for efficient processing of data. Each chunk can be handled independently, facilitating parallel processing and minimizing memory usage. Additionally, the system creates a metadata file that contains vital information about the original file, including its name and the number of chunks produced. This metadata is crucial for accurately reassembling the file during the decryption phase.

D. Hybrid Cryptography

The system's security framework relies on a hybrid cryptographic approach, which utilizes both asymmetric and symmetric encryption techniques. RSA (Rivest-Shamir-Adleman) is implemented for the secure transmission of symmetric encryption keys. RSA employs a public-private key pair, where the public key encrypts the AES key, ensuring that only the holder of the corresponding private key can access it. In parallel, the Advanced Encryption Standard (AES) algorithm is used to encrypt each chunk of the file. AES is preferred due to its high speed and robust security features, making it well-suited for handling large datasets. Each file benefits from a unique AES key, further bolstering security.

E. Encryption Process:

The encryption process is meticulously designed to uphold the highest standards of data security. A random AES key is generated for each file upload, which is essential for the encryption and decryption of the file chunks. Each chunk is then encrypted using this AES key, ensuring that unauthorized access to the chunks does not compromise data integrity, as the chunks cannot be decrypted without the correct AES key. The AES key itself is subsequently encrypted with the RSA public key, ensuring that it can only be decrypted by an individual with the associated RSA private key. This layered encryption approach enhances overall security significantly.

Encryption is the process of converting data into a coded format to prevent unauthorized access. It typically involves the use of an algorithm and an encryption key. When data, such as a message or a file, is encrypted, it is transformed into an unreadable format called ciphertext. Only individuals with the corresponding decryption key can reverse the process and convert the ciphertext back into its original, readable form (plaintext). Encryption is essential for securing sensitive information during transmission across networks, such as in online banking, messaging, and file storage. There are different types of encryption methods, including symmetric encryption (where the same key is used for both encryption and decryption) and asymmetric encryption (where different keys are used for encryption and decryption).

In symmetric encryption, both the sender and receiver use the same secret key to encrypt and decrypt the data. The key must be securely exchanged between the parties before communication begins, but the main challenge is ensuring the secrecy of the key during transmission. Common algorithms that use symmetric encryption include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

On the other hand, asymmetric encryption, also known as public-key encryption, utilizes a pair of keys: a public key and a private key. The public key is used to encrypt the data, while the private key is used to decrypt it. This system eliminates the need for key sharing between parties, as the public key can be openly distributed without compromising security. One popular asymmetric encryption method is the RSA algorithm.

Encryption not only protects data during transmission but also ensures data integrity, preventing tampering or alteration. It is a fundamental technology used in securing communications on the internet, including activities like email encryption, secure browsing (SSL/TLS), and cryptocurrency transactions. The continuous advancement of encryption techniques and key management systems is crucial in maintaining privacy and security in an increasingly digital world.

The effectiveness of encryption largely depends on the strength of the encryption algorithm and the length of the encryption key. A longer key generally increases security, making it exponentially harder for attackers to decrypt the information through brute force (trying every possible key combination). However, with increased security comes higher computational costs, as longer keys require more processing power for encryption and decryption operations.

Another aspect of encryption is key management, which involves generating, storing, distributing, and revoking encryption keys in a secure manner. Poor key management can lead to vulnerabilities, even in strong encryption systems. For example, if a key is compromised, an attacker could potentially decrypt sensitive data or impersonate the rightful owner of the key. To mitigate this risk, organizations often use additional layers of security, such as hardware security modules (HSMs) or secure key storage solutions.

In addition to encryption for protecting data in transit or storage, encryption is also vital for authentication and digital signatures. Digital signatures ensure that the sender of a message is who they claim to be and that the message has not been altered during transmission. This adds a layer of trust and integrity to online transactions, further emphasizing the significance of encryption in securing communications and protecting privacy in the digital age.

As the demand for security grows, encryption continues to evolve with new algorithms and approaches, such as quantum-resistant encryption, which is being researched to counter the potential threat posed by quantum computers. This continuous evolution ensures that encryption remains a crucial component of cyber security in a rapidly changing technological landscape.

F. Decryption Process:

The decryption process is essentially the inverse of the encryption steps, allowing for the restoration of the original file. To initiate decryption, the system retrieves the RSA-encrypted AES key, which requires the user to provide the private key linked to the public key used during encryption. Once the AES key is decrypted, the system decrypts each encrypted chunk of the file, ensuring that the order of the chunks is preserved as indicated in the metadata. After all chunks have been decrypted, the system reconstructs the original file by combining the chunks in the correct order, restoring it to its pre-encrypted state.

Encrypted data back into its original, readable form. It is the reverse of encryption, where information is transformed into an unreadable format to protect it from unauthorized access. Decryption typically requires a decryption key, which is often the

inverse of the encryption key used in the encryption process. This key may be private, symmetric (same key for both encryption and decryption), or asymmetric (using a pair of public and private keys). Decryption ensures that only authorized users with the correct key can access the sensitive data, making it a vital step in securing communications and information in various digital systems.

During the decryption process, the encrypted data, also known as ciphertext, is processed using the decryption algorithm. The algorithm, when applied to the ciphertext with the correct decryption key, converts it back to plaintext, the original, unencrypted data. In symmetric encryption, the same key is used for both encryption and decryption, so anyone with access to the key can decrypt the data. In contrast, asymmetric encryption uses a public key to encrypt the data and a private key for decryption. The private key is kept secret, ensuring that only the intended recipient, who possesses the private key, can decrypt the message.

The strength of encryption and decryption processes relies heavily on the length and complexity of the encryption keys. The longer and more complex the key, the harder it is to decrypt the data without the correct key. This is why encryption methods like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are widely used for securing sensitive information, as they provide robust protection against unauthorized access. Decryption, when done correctly with the right key, ensures data privacy, integrity, and security, especially in scenarios like online banking, secure messaging, and data storage.

The decryption process also plays a critical role in more advanced cryptographic techniques, such as digital signatures and public key infrastructure (PKI). In these systems, decryption is not only about retrieving data but also ensuring its authenticity and integrity. For example, a digital signature involves encrypting a message or document with a private key, and the recipient can decrypt it using the corresponding public key to verify that the message was indeed sent by the claimed sender and has not been altered.

Moreover, decryption is central to the field of secure communication protocols. In systems like SSL/TLS (Secure Sockets Layer/Transport Layer Security), decryption ensures that data exchanged between a client and a server is securely transmitted over the internet. The process involves multiple layers of encryption and decryption, with session keys being exchanged during the handshake phase. These keys allow for efficient encryption and decryption of the actual data being transmitted, ensuring that unauthorized parties cannot intercept or read the communication.

The complexity of decryption also contributes to the strength of the security system. In many cases, the longer and more intricate the encryption, the more computationally intensive the decryption process becomes, making brute force attacks (where an attacker tries every possible key combination) practically infeasible. However, with the rise of quantum computing, there are concerns that certain encryption methods might become vulnerable, prompting the development of quantum-resistant encryption algorithms that would still ensure secure decryption in the future.

Ultimately, decryption is not just a technical process but a fundamental aspect of maintaining confidentiality, trust, and security in the digital world. It enables businesses, governments, and individuals to protect sensitive information, safeguard privacy, and foster secure interactions online.

G. Security Protocols:

The secure file storage system incorporates multiple security measures to protect the integrity and confidentiality of the files. Confidentiality is ensured through the use of AES for chunk encryption, which keeps data unreadable even if intercepted. The additional RSA encryption of the AES key provides an extra layer of security during key transmission. Each chunk is encrypted independently, making any tampering detectable during decryption, as tampered chunks will fail to decrypt properly. The system enforces strict key management practices, keeping private keys secure and avoiding their transmission over the network to minimize interception risks.

H. Error Handling and Logging

To maintain operational efficiency and facilitate troubleshooting, robust error handling mechanisms are integrated into the system. The system is designed to detect and respond to potential errors, such as unsupported file types or incorrect decryption keys, providing users with informative feedback through the web interface to assist in resolving issues. Additionally, detailed logging mechanisms track all actions within the system, including uploads, downloads, encryption, and decryption attempts. These logs serve critical auditing purposes and are instrumental in identifying any security anomalies or breaches.

IV. CONCLUSSION AND FUTURE SCOPE

Conclusion

The secure file storage system developed using a hybrid cryptographic approach successfully provides a robust mechanism for secure file encryption, storage, and retrieval. By combining the efficiency of symmetric encryption (AES) for bulk data handling with the security of asymmetric encryption (RSA) for key exchange, the system ensures both high-performance processing and strong data protection. The architecture, which splits files into chunks for independent encryption, enhances manageability and performance, particularly for large files. Additionally, chunk-based encryption with associated metadata enables precise reassembly during the decryption process, further ensuring the integrity of the restored file.

Security measures, including the encryption of AES keys with RSA, the prevention of unauthorized access, and robust error handling mechanisms, make the system resilient against potential attacks. The integration of detailed logging and file validation processes reinforces security and allows for traceability in case of errors or security breaches.

Future Scope

The future scope of a hybrid cryptographic system that combines RSA and AES for secure, scalable file encryption and decryption is promising, with significant potential for enhancing data protection in various domains. RSA, a public-key algorithm, provides robust security for key exchange and digital signatures, while AES, a symmetric-key algorithm, offers high efficiency for encrypting large volumes of data. The hybrid system leverages the strengths of both algorithms, ensuring high-speed encryption and decryption, coupled with the security of RSA's key management. As the need for secure data transmission grows, particularly in cloud computing, Internet of Things (IoT), and enterprise-level applications, such hybrid systems are likely to become more prevalent. Innovations may focus on improving performance, reducing computational overhead, and ensuring adaptability in the face of emerging threats such as quantum computing.

REFERENCES

[1] Renuka Shone Durge, Vaishali M. Deshmukh "Advancing cryptographic security: a novel hybrid AES-RSA model with byte-level tokenization" Vol. 14, No. 4, August 2024, pp. 4306~4314 ISSN: 2088-8708, DOI: 10.11591/ijece.v14i4.pp4306-4314.

[2] Chidi Ukamaka Betrand, Chinwe Gilean Onukwugha, Mercy Eberechi Benson-Emenike, Christopher ifeanyi Ofoegbu, Nneka Martina Awaji "File Storage Security in Cloud Computing Using Hybrid Encryption" 2024; 12(1): 1-9 http://www.sciencepublishinggroup.com/j/iotcc doi: 10.11648/j.iotcc.20241201.11 ISSN: 2376-7715 (Print); ISSN: 2376-7731.

[3] Narendra Shyam Joshi, Kuldeep P. Sambrekar , Abhijit J. Patankar , Archana Jadhav and Prajakta Khadkikar. "Optimizing Encrypted Cloud Data Security and Searchability through Multi-Keyword Ranking Search Methods." ISSN (2210-142X) (2024) Int. J. Com. Dig. Sys. , No. (Mon-20..).

[4] Narendra Shyam Joshi, Kuldeep P. Sambrekar , Abhijit J. Patankar , Archana Jadhav and Prajakta Khadkikar. "Optimizing Encrypted Cloud Data Security and Searchability through Multi-Keyword Ranking Search Methods." International Journal of Computing and Digital Systems, ISSN (2210-142X) (2024).

[5] Le Li , Dong Zheng, Haoyu Zhang And Baodong Qin. "Data Secure De-Duplication and Recovery Based on Public Key Encryption With Keyword Search." VOLUME 11, 24 March 2023.

[6] Tashara Solomon, Yusuf Musa Malgwi, Molta Danlami Eli and Carroll Sermeje Pius "A Triple Phase Hybrid Security Model for Cloud Storage Using Advanced Encryption Standard" ISSN: 2762-4585X, Vol. 11, No. 1 2023.

[7] Moses Kazeem Abiodun, Agbotiname Lucky Imoize, Joseph Bamidele Awotunde, Cheng-Chi Lee, Abidemi Emmanuel Adeniyi , Ugbaja Chioma, Chun-Ta L "Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems" December 2023 pp.1-26 https://doi.org/10.6182/jlis.202312_21(2).001.

[8] Kalvikkarasi S, Dr.Saraswathi A "An Empirical study of Hybrid Cryptographic Algorithms" Int. J. of IT, Research & Applications, Vol.2, No.1, March 2023, pp. 22~32, ISSN: 2583-5343.

[9] Avaneesh Kanshi, Rajkumar Soundrapandiyan, V. S. Anita Sofia, Rajasekar V. R "Hybridized Cryptographic Encryption and Decryption Using Advanced Encryption Standard and Data Encryption Standard" Volume 23, No 4, ISSN: 1311-9702; Online ISSN: 1314-4081 DOI: 10.2478/cait-2023-0036

[10] Aviral Srivastava, Aryaman Kumar "A Robust Approach to Secure Data Encryption: AESRSA Hybrid with Kernel Key Protection" November 16th, 2023.

[11] M. Suganya and T. Sasipraba. "Comparison and Analysis of Transformer-less Topologies for Grid-Connected PV Systems." Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment, 09 May 2023.

[12] Bijeta Seth, Surjeet Dalal, Vivek Jaglan, Dac-Nhuong Le, Senthilkumar Mohan, Gautam Srivastava. "Integrating encryption techniques for secure data storage in the cloud." Citations: 27, Volume33, Issue4 04 September 2022.

[13] Udochukwu Iheanacho Erondu, Nehemiah Adebayo, Micheal Olaolu Arowolo, Moses Kazeem Abiodun. " Different Encryption and Decryption Approaches for Securing Data."2022.

[14] Muhammad Bilal Qureshi, Muhammad Shuaib Qureshi , Saqib Tahir , Aamir Anwar, Saddam Hussain, Mueen Uddin and Chin-Ling Chen, Volume 14, Issue 4 , 28 March 2022

[15] Bello A. Buhari, Aliyu Mubarak, Bello A. Bodinga, Muazu D. Sifawa "Design of a Secure Virtual File Storage System on Cloud using Hybrid Cryptography" Volume: 13 Issue: 05 Pages: 5143-5151(2022) ISSN: 0975-0290.

[16] Samson Michael Khamis Wani, Abhay Kumar "Secure File Storage on Cloud Using a Hybrid Cryptography Algorithm" Volume 5, Issue 5, May 2022 https://www.ijresm.com | ISSN (Online): 2581-5792.

[17] Anjana1 , Dr. Ajit Singh "Hybrid Cryptographic solution using RSA, Blowfish and MD5 for Information Security in Cloud Computing" Vol. 71 No. 3s (2022), Page Number: 1250-1268, ISSN: 2094-0343.

[18] Sultan Almakdi, Brajendra Panda, Mohammed S. Alshehr " An Efficient Secure System for Fetching Data From the Outsourced Encrypted Databases. Volume 9" June 4, 2021.

[19] Reece B. D'Souza1, Dr. Ruby D "Secure File Storage on Cloud using Enhanced Hybrid Cryptography" Volume: 08 Issue: 03 | Mar 2021 p-ISSN: 2395-0072.

[20] Noha E. El-Attar , Doaa S. El-Morshedy and Wael A. Awad "A New Hybrid Automated Security Framework to Cloud Storage System" Volume 5 Issue 4, 2021, 5, 37. https://doi.org/10.3390/ cryptography5040037, 20 December 2021.