International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 07 | July - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

The Future of Cryptography and Encryption Techniques

R. Ramakrishnan[1], M. Gowthomen Raj[2], J. Hareesh[3]
[1]Associate Professor, Department of Master of Computer Application, Sri Manakula Vinayagar Engineering College, Puducherry – 605 107. India
ramakrishanamca@smvec.ac.in
[2] Student, Department of Master of Computer Application, Sri Manakula Vinayagar Engineering College, Puducherry – 605 107. India
gowthomenrajmca@gmail.com
[3]Student, Department of Master of Computer Application, Sri Manakula Vinayagar Engineering College, Puducherry – 605 107. India
haresshmasters@gmail.com

ABSTRACT:

As the importance of information security grows in our digitally connected world, the field of cryptography and encryption techniques continues to expand at a rapid pace. This review paper looks at the future of cryptography, highlighting cutting-edge advances and emerging paradigms that have the potential to revolutionized the industry. The paper begins with a discussion of post-quantum cryptography, which addresses the immediate threat that quantum computers represent to standard encryption techniques. Post-quantum cryptography entails creating new encryption techniques that are immune to quantum computer attacks. The paper examines lattice-based encryption, code-based cryptography, multivariate cryptography, and other promising techniques that have demonstrated resistance to quantum attacks.

With the development of technology and the sophistication of data security threats, cryptography and encryption methods have a bright future. This essay examines future advancements in the area and the effects they might have on secure communication and data protection.

The requirement for quantum-resistant cryptography is the first topic covered. Traditional cryptography algorithms may become susceptible as quantum computing develops, requiring the development of new encryption techniques that can withstand quantum attacks. Among the possible techniques that could be used are multivariate cryptography, lattice-based cryptography, and code-based encryption.

As a crucial piece of technology, homomorphic encryption permits computations on encrypted data without the need for decryption. This capacity creates opportunities for safe data processing in industries like healthcare, finance, and government.

KEY WORDS: Cryptography, Encryption, Confidentiality, Integrity, Validity

1.INTRODUCTION:

The relevance of cryptography cannot be stressed in today's interconnected society, when massive volumes of data are generated and transmitted across networks. Encryption preserves the confidentiality, integrity, and validity of data by transforming plaintext to ciphertext using cryptographic techniques. It enables safe online transactions**.** In the digital age, cryptography and encryption techniques have played a critical role in protecting sensitive information and ensuring secure communication. As technology advances at an unprecedented rate, the future of cryptography becomes increasingly important in addressing

rising security concerns and protecting data from ever evolving threats. This introduction lays the groundwork for further investigation into the future of cryptography and encryption techniques, emphasizing the need for novel approaches and breakthroughs to satisfy the needs of a linked and data-driven world**.** It is impossible to overstate the importance of cryptography in the highly connected society of today, where networks are used to generate and transfer enormous amounts of data. Data's secrecy, integrity, and validity are maintained by encryption by converting plaintext to ciphertext using cryptographic methods. It allows for secure internet transactions. In the digital age, safe communication and the protection of sensitive data have been made possible through cryptography and encryption systems. The future of cryptography is crucial for resolving growing security issues and safeguarding data from ever developing dangers as technology develops at an unparalleled rate. This introduction establishes the framework for additional research into the potential applications of cryptography and encryption methods, highlighting the need for innovative solutions and technological advancements to meet the demands of a networked and data-driven society.

2.LITERATURE SURVEY:

The research cited above suggests dividing files into separate portions and applying hybrid cryptography to each part.

The technique stores keys using LSB steganography and encrypts and decrypts data using symmetric cryptographic algorithms**.**

3.PROPOSED SYSTEM :

in this proposed system, we present a hybrid cryptography-based approach for secure file storage and communication. The system aims to provide robust protection for sensitive data, ensuring confidentiality, integrity, and availability. By combining the strengths of symmetric and asymmetric encryption algorithms, the proposed system offers an efficient and secure solution for both local file storage and network communication.

Encryption Module:

The encryption module employs a hybrid cryptography approach, combining symmetric encryption algorithms such as AES (Advanced Encryption Standard) with asymmetric encryption algorithms like RSA (Rivest-Shamir-Adleman).

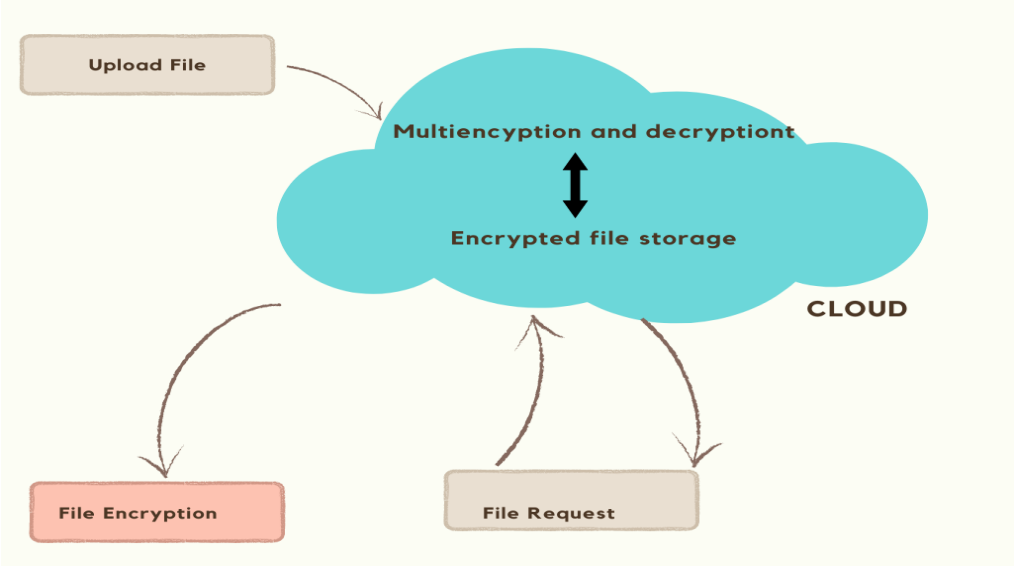

Fig.no.1: Cryptography Architecture

Symmetric encryption is used for fast and efficient encryption of large files, while asymmetric encryption is utilized for secure key exchange and management.

Key Management:

The system incorporates a robust key management mechanism to ensure the secure generation, storage, and distribution of encryption keys. Public keys and private keys are generated using RSA, and symmetric encryption keys are derived using a secure key derivation function. The key management component includes functionalities for key generation, key storage, and key sharing among authorized users.

Secure File Storage:

The secure file storage component provides a secure repository for storing encrypted files. Files are encrypted using AES with a randomly generated symmetric key, ensuring their confidentiality. The encrypted files are then stored on local or remote storage with appropriate access controls and authentication mechanisms. The system also supports efficient file retrieval and management operations, ensuring the integrity and availability of stored files.

4.CLOUD COMPUTING IN CRYPTOGRAPHY:

Through the provision of a scalable and adaptable infrastructure for the implementation and management of cryptographic systems, cloud computing plays a vital role in the field of cryptography and encryption. Following are some benefits and uses of cloud computing in encryption and cryptography

High computational power and resources are available through cloud computing, which can be used to carry out difficult encryption and decryption procedures. This is especially advantageous for cryptographic algorithms that need a lot of work, like post-quantum cryptography or homomorphic encryption.

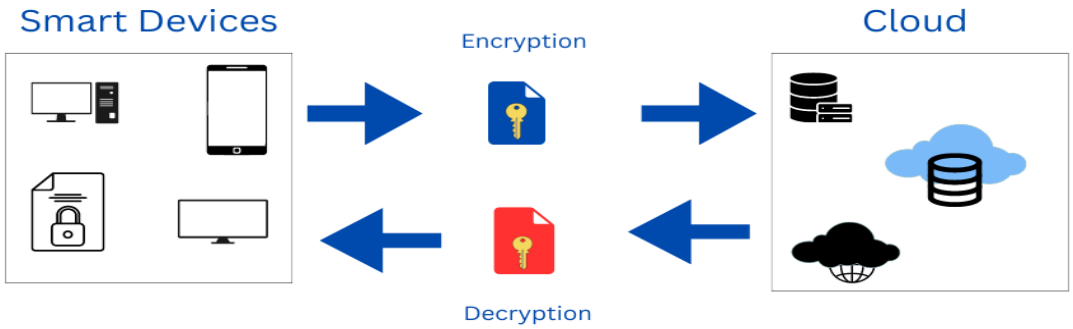

Fig. no. 2: cloud computing in cryptography

Cryptographic keys can be stored securely and centrally using cloud-based key management solutions. Organizations can benefit from strong key protection tools like hardware security modules (HSMs) and secure the integrity and secrecy of cryptographic keys by using cloud-based key management services.

5.ADVANTAGES:

Data security will be improved via cryptography and encryption methods in the future. Both post-quantum and quantum-resistant encryption offer defence against attacks from potent quantum computers, preserving the confidentiality and integrity of sensitive data.

By enabling computations on encrypted data without first needing to decrypt it, homomorphic encryption offers secure data processing while preserving privacy.. In industries like healthcare and finance where sensitive data must be analysed without jeopardising privacy, this technology is essential.

Post-quantum cryptography is used to ensure long-term security in the face of advances in quantum computing. Data and communications may be kept secure even as quantum computing technology develops by using algorithms that fend off both classical and quantum attacks.

6.IMPLEMENTATION:

The implementation begins with the generation of public and private keys using the RSA algorithm. The system generates a pair of RSA keys for each user, storing the private keys securely and distributing the public keys to other authorized users. Additionally, symmetric encryption keys are derived using a secure key derivation function from user-defined passphrases or randomly generated values. The key management component ensures secure storage and access to the generated keys.

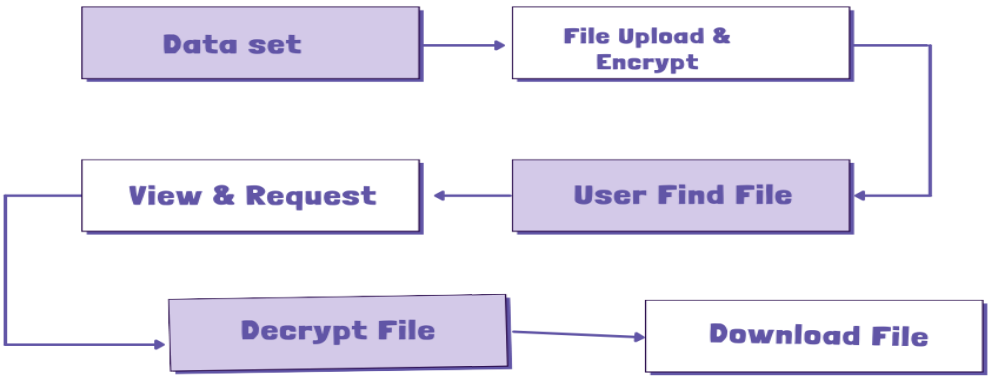

Fig.no.3: Implementation of Cryptography

The implementation provides a secure file storage mechanism, where files are encrypted using the Advanced Encryption Standard (AES) algorithm. When a user uploads a file, the system generates a unique symmetric encryption key for that file and encrypts it using the recipient's public key. The encrypted file, along with the encrypted symmetric key, is then stored securely in local or remote storage. Access controls and authentication mechanisms are implemented to restrict unauthorized access to stored files.

The system enables secure communication between users over a network. When a user wants to send a file or message to another user, the system retrieves the recipient's public key and encrypts the data using AES with a randomly generated symmetric key. The symmetric key is then encrypted using the recipient's public key and transmitted securely over the network. The recipient can decrypt the received symmetric key using their private key and use it to decrypt the encrypted file or message.

To enhance the security of the system, additional security measures can be implemented. Digital signatures can be employed to verify the authenticity and integrity of files. Secure hash functions can be used to calculate file hashes and detect any tampering or modifications. Data integrity checks, such as checksums or message authentication codes (MACs), can be implemented to ensure the integrity of transmitted and stored data.

The implementation addresses the scalability and performance considerations. Efficient algorithms and data structures are employed to handle large files and a significant number of users. Proper indexing and caching mechanisms are implemented to optimize file retrieval and storage operations. The system is designed to handle high throughput and provide low latency for secure file storage and communication.

7.CONCLUSION:

The future of cryptography and encryption techniques is poised to shape the landscape of information security in our increasingly digital world. This paper explored various aspects and advancements in the field, highlighting key concepts and technologies that will play a crucial role in ensuring the confidentiality, integrity, and availability of sensitive data.

Traditional cryptographic techniques, such as symmetric encryption algorithms like AES and asymmetric encryption schemes like RSA and ECC, continue to serve as the foundation of secure communication. Efforts are underway to enhance their efficiency, security, and adaptability to evolving threats.

The advent of quantum computing poses a significant challenge to existing cryptographic methods. Post-quantum cryptography, which focuses on developing encryption schemes resilient against attacks from quantum computers, has emerged as a critical area of research. Among the promising techniques being investigated in this context are multivariate cryptography, lattice-based cryptography, and code-based cryptography.

Homomorphic encryption has the potential to revolutionize secure data processing and privacy preservation. Fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE) enable computations to be performed on encrypted data without decryption, opening up possibilities for secure data sharing, cloud computing, and privacy-preserving machine learning.

REFERENCE :

Al-Riyami, S., & Paterson, K. G. (2003). Certificateless public key cryptography. In Advances in Cryptology – ASIACRYPT 2003 (pp. 452-473). Springer Berlin Heidelberg.

Boneh, D., & Shoup, V. (2000). A graduate course in applied cryptography. Retrieved from https://crypto.stanford.edu/~dabo/cryptobook/

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2017). Post-quantum cryptography (1st ed.). Springer International Publishing.

Gentry, C. (2009). A fully homomorphic encryption scheme. In Proceedings of the 41st annual ACM symposium on Theory of Computing (pp. 169-178). ACM.

Yao, A. C. (1982). Protocols for secure computations. In Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (pp. 160-164). IEEE.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

Azarderakhsh, R., Bagheri, N., & Karakoç, F. (2017). Blockchain-based key management: A review. Cryptography and Communications, 9(6), 875-903.

Bos, J., Lauter, K., & Naehrig, M. (2013). Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics, 46(3), 430-440.

Ateniese, G., Fu, K., Green, M., & Hohenberger, S. (2017). Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security (TISSEC), 9(1), 1-30.

Döttling, N., Garg, S., & Malavolta, G. (2016). Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Annual International Cryptology Conference (pp. 637-667). Springer.

Canetti, R., Goldreich, O., & Halevi, S. (2010). The random oracle methodology, revisited. Journal of the ACM (JACM), 51(4), 557-594.

Kumar, A., & Sharma, S. K. (2021). Blockchain-enabled secure sharing and provenance of medical images: A systematic review. Journal of Medical Systems, 45(1), 1-19.

Shumow, D., & Ferguson, N. (2007). On the possibility of a back door in the NIST SP800-90 Dual Ec Prng. In Proceedings of the 48th annual IEEE Symposium on Foundations of Computer Science (pp. 61-70). IEEE.

Du, Y., Wei, X., & Luo, Y. (2017). Practical attribute-based encryption with access control for sharing electronic health records. IEEE Journal of Biomedical and Health Informatics, 22(6), 1731-1742.

Rijmenants, D. (2016). History of cryptology—Part 2: Modern cryptographic algorithms. Cryptologia, 40(2), 97-136.