International Journal of Computer Applications (0975 - 8887)
Volume 186 - No.48, November 2024

Advanced Encryption Techniques for Securing Data Transfer in Cloud Computing: A Comparative Analysis of Classical and Quantum-Resistant Methods

Koushik Kumar Ganeeb
Salesforce Inc
North Carolina, USA

Vivekananda Jayaram
JPMorgan Chase
Texas, USA

Manjunatha Sughaturu Krishnappa
Oracle America Inc
California, USA

Pankaj Gupta
Discover Financial Services
Illinois, USA

Akshay Nagpal
IEEE Senior Member
Newyork, USA

Amey Ram Banarse
IEEE Senior Member
California, USA

Seema G Aarella
University of North Texas
Texas, USA

ABSTRACT

As cloud computing becomes increasingly prevalent, the need for robust security measures to protect data during transfer is critical. This paper provides a thorough examination of advanced encryption techniques designed to ensure secure data transmission in cloud environments. Traditional methods, including Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), are evaluated alongside emerging approaches such as homomorphic encryption and quantum key distribution (QKD). These techniques are assessed based on their security strength, performance, and suitability in addressing contemporary challenges, particularly those posed by quantum computing. The analysis highlights the practical applications of these methods in cloud security and their potential for future advancements in securing data transfers. The insights provided will aid in developing resilient encryption strategies to protect sensitive information in the evolving landscape of cloud computing.

Keywords

Secure Data Transfer, Cyber Security, Data Integration, Distributed Systems, Encryption, Digital Signatures, Data Confidentiality, Cryptographic Techniques

1. INTRODUCTION

Cloud computing has revolutionized the way businesses and individuals store, process, and access data. It offers unparalleled scalability, flexibility, and cost efficiency, making it an integral part of modern IT infrastructure. However, the convenience of cloud computing comes with significant security challenges. As data is transferred across potentially insecure networks and stored in remote locations, it becomes vulnerable to a wide range of threats, including interception, unauthorized access, and data breaches.

Ensuring the security of data during transfer is crucial to maintaining the confidentiality, integrity, and availability of sensitive information. Encryption, the process of converting plaintext into ciphertext using algorithms and keys, is a fundamental technology in protecting data from unauthorized access. Traditional encryption methods like the Advanced Encryption Standard (AES) [1] and Rivest-Shamir-Adleman (RSA) [13] have been widely used to secure data transfer. AES, a symmetric encryption algorithm [2], is known for its efficiency and strong security, while RSA, an asymmetric encryption algorithm, is valued for its secure key distribution capabilities, as shown in Figure 1. Despite their effectiveness, traditional encryption techniques face challenges in the context of evolving security threats and advanced computing capabilities. The rise of quantum computing, for instance, poses a significant threat to classical encryption algorithms, necessitating the development of quantum-resistant techniques. Additionally, the increasing complexity of cloud computing environments requires more advanced encryption methods that can ensure data security without compromising performance. In response to these challenges, new encryption techniques have emerged. Homomorphic encryption [6] allows computations to be performed on encrypted data without decrypting it, thus preserving data confidentiality during processing. Quantum Key Distribution (QKD) [19] on the other hand, leverages the principles of quantum mechanics to provide provably secure key exchange, making it a promising solution against future quantum threats.

This paper aims to provide a comprehensive review of both traditional and advanced encryption techniques employed for secure data transfer in cloud computing. By examining their effectiveness, advantages, and limitations, insights are offered into their practical applications and future potential. Understanding these techniques is essential for developing robust security strategies that protect sensitive data in increasingly complex and dynamic cloud environments. The discussion also extends to future directions of en-

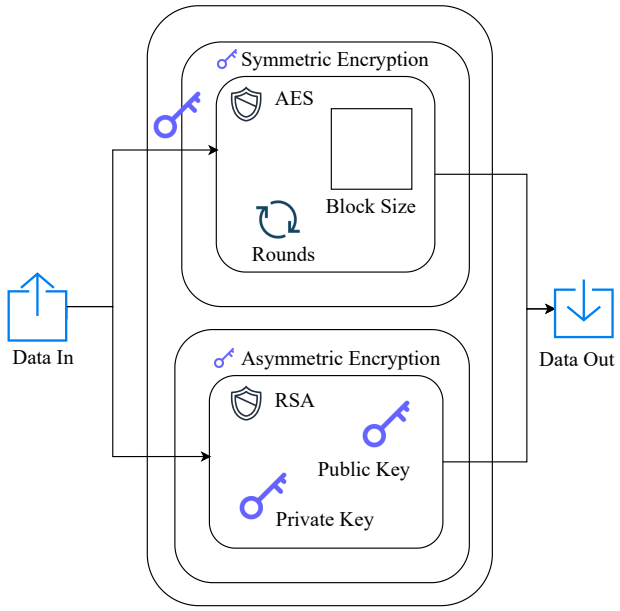

Fig. 1: Encryption techniques

cryption research, emphasizing the need for continued innovation to stay ahead of emerging security threats.

2. BACKGROUND

Distributed systems consist of multiple autonomous computers communicating through a network to achieve a common objective. Examples include cloud computing environments, distributed databases, and peer-to-peer networks. The distributed nature of these systems involved in Cloud Computing introduces several challenges, including latency, fault tolerance, and security. Data breaches and cyber attacks can have severe consequences, including financial loss, reputational damage, and legal repercussions. Secure data transfer is essential to protect sensitive information and maintain trust in distributed systems. Ensuring data confidentiality, integrity, and availability is paramount in mitigating these risks.

3. LITERATURE REVIEW

Research on secure data transfer in distributed systems encompasses various cryptographic techniques, protocols, and frameworks. This section reviews key contributions in the field.

Symmetric encryption is known for its efficiency and is commonly used for encrypting large datasets. Algorithms such as the Advanced Encryption Standard (AES) are favored for their strength and speed, making them a cornerstone of secure data transfer methodologies [11]. However, symmetric encryption's simplicity and speed come with the challenge of key distribution, which can be a significant vulnerability if not managed properly. Asymmetric encryption addresses the key distribution problem by using a pair of keys—one public and one private. [14]

Algorithms like RSA and Elliptic Curve Cryptography (ECC) [3] are well-regarded for their robust security features, particularly in scenarios requiring secure key exchange and digital signatures. ECC offers the advantage of providing strong security with smaller key sizes, beneficial in resource-constrained environments. Digital signatures ensure data integrity and authenticity. They are created using the sender's private key and verified using the sender's public key, providing a reliable method for confirming the data's authenticity and the sender's identity. Algorithms such as RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) [8] are commonly used for generating digital signatures, ensuring that data has not been tampered with during transit. Cryptographic hashing functions create a fixed-size hash value from input data, which is unique to the original data. Hash functions [15], such as SHA-256 and SHA-3, must be collision-resistant and irreversible to ensure data integrity and authenticity. These hashing functions play a crucial role in various security protocols and data verification processes.

Hybrid encryption combines the strengths of both symmetric and asymmetric encryption to enhance security and efficiency. The process typically involves generating a symmetric key for data encryption, encrypting the data with this symmetric key, and then encrypting the symmetric key with the recipient's public key. This method ensures that the symmetric key is securely transmitted, while the actual data encryption remains efficient. Hybrid encryption is particularly useful in scenarios where large volumes of data need to be securely transferred without compromising performance. The goal is to build a comprehensive comparison of Traditional and Advanced Encryption Techniques [7] to secure data in the Cloud Computing and AI adapted technologies.

4. TRADITIONAL ENCRYPTION TECHNIQUE

4.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) [9] is a symmetric encryption algorithm known for its strong security and widespread adoption across industries. AES operates on fixed block sizes of 128 bits and supports key sizes of 128, 192, and 256 bits, offering flexibility in encryption strength. Its robustness against cryptographic attacks, including brute force, has established it as a reliable choice for securing data in diverse applications. A comparative analysis of encryption techniques addressed in this research is shown in Figure 2.

Key Features

- SubBytes Transformation and ShiftRows: This involves nonlinear substitution of bytes using a substitution box (S-box), which provides resistance to linear and differential cryptanalysis. The rows of the state matrix are cyclically shifted to increase diffusion.
- MixColumns Transformation: Bytes within each column of the state matrix are mixed by multiplying them with a fixed polynomial matrix, further enhancing diffusion and resistance to cryptographic attacks.
- AddRoundKey Transformation: A round key, derived from the main key, is XORed with the state matrix, adding confusion and ensuring the encryption process depends on the input key.
- Key Expansion: AES generates round keys through a key scheduling process, ensuring that different parts of the data are encrypted using distinct keys, thereby adding another security layer.

Strengths

- High Security: AES offers strong protection against most cryptographic attacks.

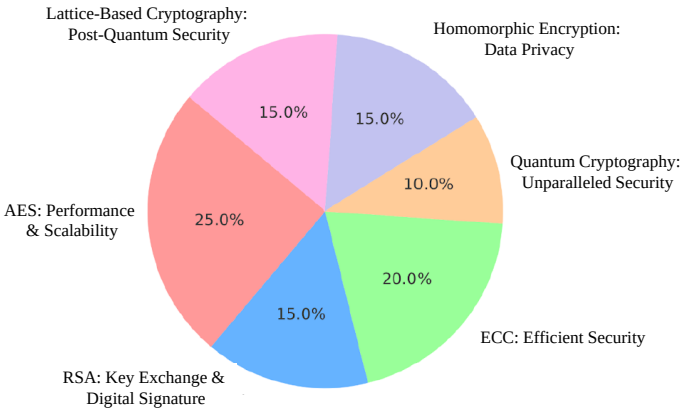

Fig. 2: Comparitive analysis of encryption techniques

- Efficiency: It performs well on both hardware and software platforms, allowing for fast encryption and decryption, making it ideal for real-time applications such as financial transactions and communications.
- Widespread Use: AES is trusted across numerous industries, ensuring its reliability and proven effectiveness.

Limitations

- Fixed Block Sizes: AES operates on a block size of 128 bits, which may require padding or other techniques for handling data that doesn't fit neatly into 128-bit blocks.
- Side-Channel Attacks: Physical implementation characteristics can be exploited in side-channel attacks, making secure implementation critical.
- Key Management: The overall security of AES heavily depends on proper key management; insecure handling of keys can compromise encryption, regardless of the algorithm's inherent strength.

4.2 Rivest-Shamir-Adleman (RSA)

RSA, an asymmetric encryption algorithm, relies on a pair of keys—one public and one private—for encryption and decryption. Its security is based on the mathematical difficulty of factoring large prime numbers, making it a fundamental algorithm in cryptography.

Key Features

- Strong Security: RSA's security relies on the hardness of factoring large integers, a problem that becomes increasingly difficult as key sizes grow.
- Digital Signatures: RSA supports the generation of digital signatures, ensuring authentication, data integrity, and non-repudiation in communications and transactions.
- Interoperability: Standardization of RSA ensures that it is compatible across different platforms and systems, enabling secure communication in distributed environments.

Strengths

- Robust Security: RSA is considered highly secure under current computational models, particularly for key exchange and digital signatures.
- Widely Used: RSA's long-standing reputation and interoperability make it a popular choice for secure data transfers and digital signature generation.

Limitations

- Performance: RSA is computationally intensive, especially during key generation, encryption, and decryption processes, making it slower than symmetric encryption algorithms such as AES.
- Quantum Vulnerability: RSA's security is potentially at risk with the development of quantum computers, which could factor large integers much more efficiently, thereby breaking RSA encryption.
- Limited Use for Large Data: Due to its slower performance, RSA is typically used for encrypting small amounts of data, such as keys, rather than large datasets.

5. ADVANCED ENCRYPTION TECHNIQUES

5.1 Elliptic Curve Cryptography (ECC) and Quantum Cryptography

Elliptic Curve Cryptography (ECC) shown in Figure 3 is a public-key cryptographic technique based on the algebraic structure of elliptic curves over finite fields. ECC offers the same level of security as RSA but with much smaller key sizes, resulting in faster computations and reduced power consumption, making it ideal for resource-constrained environments like mobile devices and embedded systems [18].

The security of ECC comes from the elliptic curve discrete logarithm problem, which is mathematically complex and resistant to attacks.

- Applications: ECC is widely employed in secure communication protocols (e.g., SSL/TLS), cryptocurrencies (e.g., Bitcoin), and mobile security.
- Strengths: Smaller key sizes, faster computation, lower power consumption.
- Weaknesses: Implementation can be more challenging due to the complexity of elliptic curve arithmetic.

Quantum Cryptography, on the other hand, leverages the principles of quantum mechanics to ensure secure communications. A key application is Quantum Key Distribution (QKD) as shown in Figure 4, which allows two parties to securely share a secret key [12].

Quantum cryptography offers unconditional security because it relies on the fundamental laws of physics, making it immune to computational attacks that threaten classical encryption techniques.

- Eavesdropping Detection: Any attempt to intercept a quantum key changes its quantum state, alerting the communicating parties to the presence of an eavesdropper.
- Applications: Quantum cryptography is used in high-security environments, including government and military communications, financial transactions, and critical infrastructure protection.

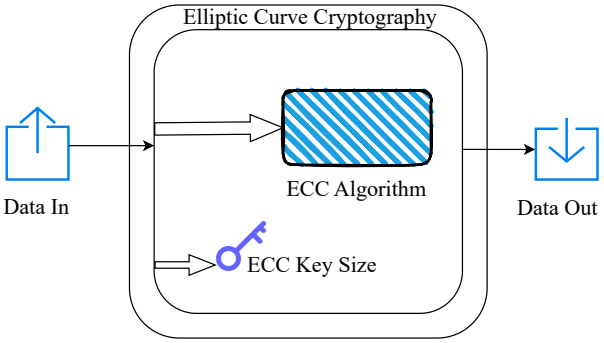

Fig. 3: Elliptic curve cryptography

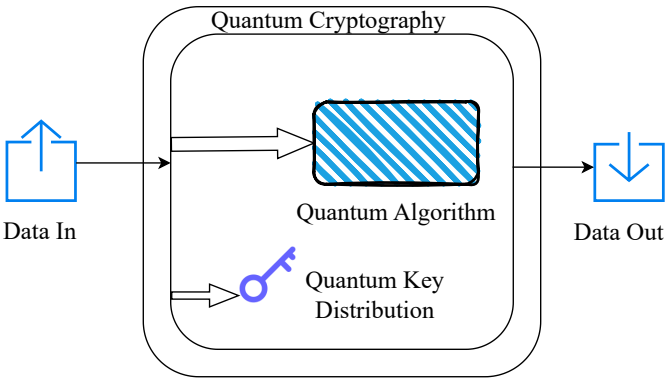

Fig. 4: Quantum cryptography

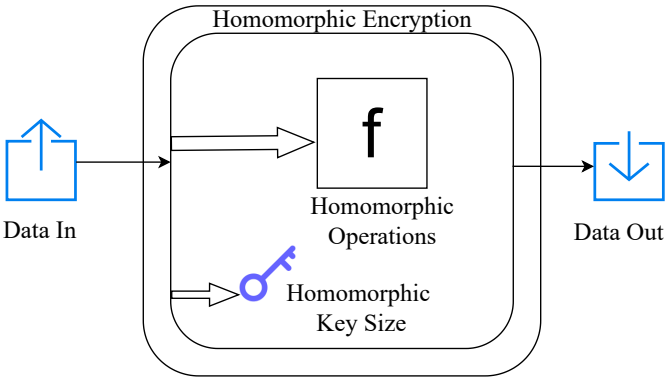

Fig. 5: Homomorphic Encryption

5.2 Homomorphic Encryption and Lattice-Based Cryptography

Homomorphic Encryption allows computations to be performed directly on encrypted data without needing to decrypt it. This means that data privacy is preserved while still allowing for meaningful analysis and operations. The result, once decrypted, will match the outcome of operations performed on the plaintext. Homomorphic encryption shown in Figure 5 is particularly useful for secure cloud computing and data analysis, allowing sensitive data to be processed without exposing it [10].

- Applications: Secure cloud services, encrypted databases, and privacy-preserving computations.
- Strengths: Enables secure data processing without decryption, ensuring data privacy in outsourced environments.

Lattice-Based Cryptography Shown in Figure 6 relies on the hardness of mathematical lattice problems, which are believed to be resistant to quantum attacks [16]. This makes it a strong candidate for post-quantum security, a field focused on developing encryption methods that remain secure in the face of future quantum computers. Lattice-based cryptography is versatile and can be used to construct various cryptographic primitives, including encryption schemes, digital signatures, and more.

- Applications: Post-quantum cryptography standards, securing future communications against quantum threats.

5.3 Attribute-Based Encryption (ABE) and Identity-Based Encryption (IBE)

Attribute-Based Encryption (ABE) is a public-key encryption method where access to encrypted data is determined by the attributes of the user and a predefined policy, is depicted in Figure 7. This allows for detailed and flexible access control mechanisms based on user roles or characteristics. ABE is scalable and well-suited to environments with large numbers of users and varying access rights [17].

- Applications: Secure data sharing in cloud environments, health information systems, and enterprise data management.
- Strengths: Granular access control, scalability for managing large user groups.

Identity-Based Encryption (IBE) shown in Figure 8 simplifies key management by deriving public keys from known identifiers, such as an email address [5]. This eliminates the need for complex key distribution systems, making it easier to establish secure communications.

IBE is particularly useful in secure messaging and network authentication protocols.

- Applications: Secure email communication, secure messaging, network authentication.
- Strengths: Simplifies key management, and reduces complexity in public key infrastructure.

5.4 Functional Encryption (FE) and Multi-Party Computation (MPC)

Functional Encryption (FE) allows users to compute specific functions on encrypted data, revealing only the result of the com-

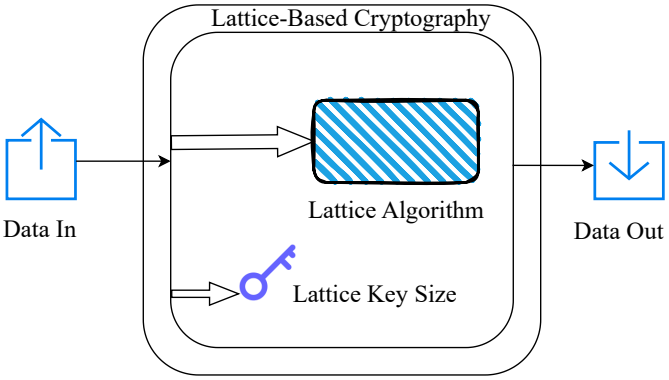

Fig. 6: Lattice based cryptography

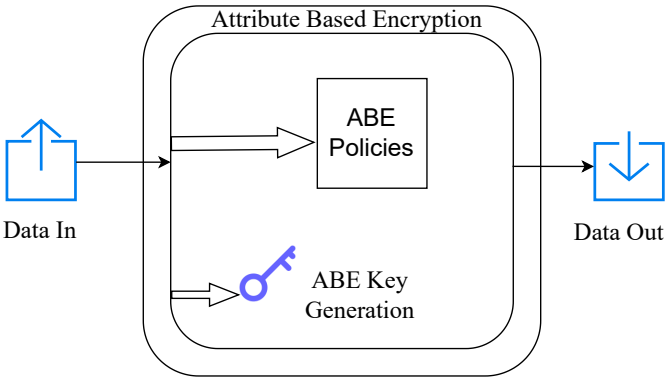

Fig. 7: Attribute based encryption

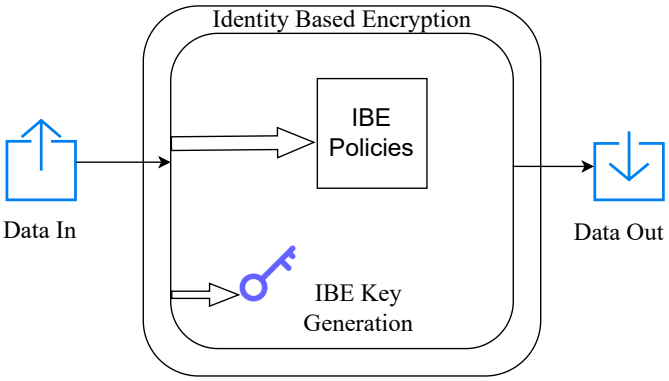

Fig. 8: Identity Based Encryption

putation while keeping the underlying data hidden. This technique shown in Figure 9 ensures that only authorized computations are performed, providing controlled access to data [4].

- Applications: Secure data sharing, privacy-preserving data analysis, secure multiparty computations in sectors like healthcare and finance.
- Strengths: Controlled data access, and tailored data-sharing policies.

Multi-Party Computation (MPC) Shown in Figure 10 enables multiple parties to compute a function over their inputs while keeping those inputs private from each other [20]. This is essential for collaborative environments where parties need to analyze data without revealing sensitive individual inputs.

- Applications: Secure collaborative data analysis, secure voting systems, privacy-preserving machine learning.
- Strengths: Enhanced privacy, secure joint computations without revealing full datasets.

6. COMPARATIVE ANALYSIS

Security AES and RSA are foundational in cryptographic security, offering robust defenses against classical computational attacks. AES, in particular, provides symmetric encryption with high speed and security, while RSA excels in asymmetric encryption, though it requires larger key sizes. However, both are potentially vulnerable to future quantum computing attacks. Advanced techniques like Homomorphic Encryption ensure privacy during data processing, making it ideal for scenarios where data needs to be encrypted even while being analyzed. Quantum Key Distribution (QKD) goes beyond conventional security by leveraging quantum mechanics to guarantee eavesdropping detection and future-proof security against quantum attacks, offering unmatched protection.

Performance and Practicality In terms of speed and efficiency, AES stands out, making it optimal for real-time applications due to its lightweight computational requirements. On the other hand, RSA, though secure, is slower and more resource-intensive, making it better suited for tasks like secure key distribution and digital signatures. Despite being a staple in encryption, RSA's efficiency drops with larger key sizes, especially when compared to ECC which offers the same security with smaller key sizes, resulting in faster operations and lower resource consumption.

Homomorphic Encryption, while offering privacy-preserving computation, faces significant performance challenges due to its heavy computational overhead, making it less practical for real-time applications.
However, it is invaluable in scenarios requiring secure processing of sensitive data, such as outsourced cloud computing. QKD, though providing superior security, is still in its early stages and requires specialized infrastructure, limiting its use to high-security environments like military and financial institutions.

Applications
AES is the go-to for large-scale data encryption, due to its scalability and efficiency, making it a favored choice in systems where performance is key, such as data storage and real-time communication. RSA, with its ability to securely exchange keys and provide digital signatures, is indispensable in applications requiring authentication and secure key management.

Table 1. : Comparison of Encryption Techniques

Encryption Technique	Strengths	Limitations
AES	• Highly efficient • Ideal for real-time applications • Strong security and performance	• Limited key size options • May introduce performance overhead in high-speed scenarios • Vulnerable to potential future quantum computing threats
RSA	• Secure key exchange • Digital signatures • Well-established	• Performance limitations • Vulnerable to future quantum computing
ECC	• Efficient alternative to RSA • Smaller key sizes with the same level of security	• Limited to resource-constrained environments
Quantum Cryptography	• Unparalleled security • Quantum Key Distribution (QKD)	• Current technology limitations • Scalability issues
Homomorphic Encryption	• Privacy-preserving data processing without decryption	• Challenges in computational efficiency
Lattice-Based Cryptography	• Security against quantum computing threats • Crucial for post-quantum standards	• Still in development • Limited by practical applications today

Elliptic Curve Cryptography (ECC) is gaining traction as a viable alternative to RSA, offering similar security but with smaller key sizes, which makes it ideal for mobile devices, IoT, and environments with limited computational resources.

Quantum Cryptography, particularly QKD, is targeted toward environments where unconditional security is a necessity, though its adoption is limited due to infrastructure demands.
Homomorphic Encryption shines in privacy-preserving cloud services and encrypted data analysis, while Lattice-based cryptography holds promise for post-quantum security, addressing future concerns about quantum computing vulnerabilities.

7. RESULTS

The analysis compared traditional encryption techniques, such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), with advanced methods including Elliptic Curve Cryptography (ECC), Homomorphic Encryption, Quantum Key Distribution (QKD), Lattice-Based Cryptography, Attribute-Based Encryption (ABE), and Identity-Based Encryption (IBE). Each technique was assessed based on security strength, performance, and practicality in real-world applications.
Security and Resilience: AES and RSA are foundational algorithms in cryptography, offering robust defenses against classical computational attacks. AES demonstrated high security, particularly effective in symmetric encryption scenarios where rapid processing is critical. RSA excelled in key distribution and digital signatures, but its vulnerability to quantum computing poses significant future challenges. ECC emerged as a strong alternative to RSA, providing comparable security with smaller key sizes, making it more efficient for environments with limited resources.

Quantum cryptography, especially QKD, showcased unparalleled security due to its reliance on quantum mechanics, which inherently alerts parties to eavesdropping attempts. Homomorphic encryption also offered a significant advantage by allowing computations on encrypted data, preserving data confidentiality during processing. Lattice-based cryptography proved essential for post-quantum security, standing out for its resilience against quantum threats, which is crucial for long-term encryption strategies.

Performance Benchmarks: AES was the most efficient in terms of speed and performance, ideal for real-time applications such as financial transactions and secure communications. It showed minimal computational overhead, making it suitable for high-speed scenarios. In contrast, RSA, while reliable for secure key exchanges and digital signatures, had slower performance due to the complexity of its operations, especially with larger key sizes. ECC provided faster operations compared to RSA due to its smaller key sizes,

making it an attractive option for mobile devices and IoT environments.

Homomorphic encryption, although beneficial for privacy-preserving computations, faced significant performance limitations due to its computational intensity, rendering it less practical for real-time applications but valuable for secure cloud computing and data analysis. QKD, while offering unmatched security, was limited by current technological and infrastructural constraints, making it suitable primarily for high-security sectors like government and financial institutions.

Practical Applications: AES proved to be highly scalable and was preferred for large-scale data encryption where speed and reliability are paramount. RSA's use was more specialized, serving critical functions such as secure key distribution and digital signatures. ECC found practical use in scenarios demanding efficient security with lower power consumption, making it ideal for mobile devices and secure web communications.

Homomorphic encryption excelled in privacy-preserving data processing, suitable for applications requiring secure computations on outsourced data. Lattice-based cryptography emerged as a key player for future-proof encryption, crucial for maintaining security in the advent of quantum computing. Quantum cryptography's current use cases were limited to specialized fields requiring the highest level of security, such as military communications.

8. CONCLUSIONS

This research presents a comparative analysis of various encryption techniques, including AES, RSA, ECC, Quantum Cryptography, Homomorphic Encryption, and Lattice-Based Cryptography, highlighting their respective strengths and limitations as listed in Table 1:

AES (Advanced Encryption Standard): AES stands out for its high efficiency and robustness, making it suitable for encrypting large volumes of data in real-time applications. Its combination of strong security and performance makes it a preferred choice for many applications requiring fast and reliable encryption.

RSA (Rivest-Shamir-Adleman): RSA is well-regarded for its capabilities in secure key exchange and digital signatures. However, it faces performance constraints, especially with larger key sizes, and is vulnerable to future quantum computing threats, which could potentially compromise its security.

ECC (Elliptic Curve Cryptography): ECC provides a compelling alternative to RSA, offering comparable security with smaller key sizes. This efficiency is particularly advantageous in environments with limited computational resources, improving performance and reducing overhead.

Quantum Cryptography: Quantum Cryptography, especially Quantum Key Distribution (QKD), promises unprecedented levels of security by leveraging quantum mechanics. However, it is constrained by current technological limitations and scalability issues, making widespread adoption challenging at present.

Homomorphic Encryption: This technique enables data processing while preserving privacy, allowing computations on encrypted data without decryption. Despite its promising capabilities, Homomorphic Encryption is currently hampered by challenges related to computational efficiency and practical implementation.

Lattice-Based Cryptography: As a key component in the development of post-quantum cryptographic standards, Lattice-Based Cryptography offers resilience against potential quantum computing attacks. It is crucial for the advancement of encryption methods designed to withstand future technological developments.

In conclusion, each encryption technique possesses unique attributes that make it suitable for different use cases. By leveraging the strengths of these various methods and fostering ongoing innovation, the field of cryptography can ensure robust and scalable security solutions to protect sensitive information in an increasingly interconnected digital world. Continued research and development in these areas will be essential to address emerging challenges and enhance the overall security landscape.

By utilizing these distinct strengths and continuing innovation, the cryptographic field can ensure robust and scalable security solutions to protect sensitive information in an interconnected digital world.

9. FUTURE SCOPE OF WORK

As cloud computing continues to evolve, the need for advanced encryption techniques will become increasingly critical to address emerging security challenges. Future research and development in this domain could explore several key areas:

Quantum-Resistant Algorithms: With the advent of quantum computing, traditional encryption methods like AES and RSA face potential obsolescence. Research into quantum-resistant algorithms, such as lattice-based cryptography and post-quantum cryptographic methods, will be essential for developing encryption techniques that can withstand quantum attacks.

Enhanced Homomorphic Encryption: While homomorphic encryption offers significant advantages in privacy-preserving computations, its current implementations can be resource-intensive. Future work could focus on optimizing these techniques to reduce computational overhead and improve practical applicability for large-scale cloud environments.

Integration of Machine Learning in Encryption: Machine learning algorithms could be employed to enhance encryption techniques, such as through predictive analytics for threat detection and automated key management. Research could explore how AI can be integrated into encryption processes to create adaptive security measures.

Secure Multi-Party Computation (MPC) Innovations: As collaborative data analysis and secure voting systems become more prevalent, advancements in MPC techniques will be crucial. Future research could aim at improving the efficiency and scalability of MPC protocols to handle complex data sharing scenarios with enhanced security guarantees.

Attribute-Based Encryption (ABE) Optimization: ABE is promising for fine-grained access control, but its implementation can be complex. Future work could focus on simplifying ABE systems, enhancing their scalability, and integrating them with emerging cloud services to better manage large datasets and diverse access policies.

Quantum Key Distribution (QKD) Scaling: Although QKD offers groundbreaking security, its deployment is currently limited by practical constraints. Future research could investigate ways to scale QKD technologies for broader adoption, including integrat-

ing them with existing communication infrastructures and reducing implementation costs.

Improved Key Management Systems: As encryption techniques evolve, the management of cryptographic keys will become increasingly important. Research could focus on developing robust key management systems that address vulnerabilities in current practices and support new encryption methods.

Regulatory and Compliance Considerations: As encryption technologies advance, there will be a need to ensure they align with evolving regulatory requirements and standards. Future work could involve exploring the impact of regulations on encryption practices and developing strategies for compliance in diverse jurisdictions.

By addressing these areas, future research will contribute to the development of more secure and efficient encryption techniques, ensuring that data remains protected in the ever-changing landscape of cloud computing and beyond.

10. REFERENCES

[1] S. Al-Kuwari, O. Al-Sakran, and J. Al-Muhtadi. Comparative analysis of aes and rsa algorithms in cloud computing. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(2):65–72, 2020.

[2] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad. Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, 12(2):105–115, Aug. 2020.

[3] Moncef Amara and Amar Siad. Elliptic curve cryptography and its applications. In *International Workshop on Systems, Signal Processing and their Applications (WOSSPA)*, pages 247–250, 2011.

[4] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *Theory of Cryptography*, pages 253–273, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[5] S. Chatterjee and P. Sarkar. *Identity-Based Encryption*. SpringerLink: Bücher. Springer US, 2011.

[6] S. Cui, J. Zhang, and X. Wu. Practical challenges and solutions in homomorphic encryption. *Journal of Cryptographic Engineering*, 9(3):183–200, 2019.

[7] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 169–178, 2009.

[8] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1):36–63, Aug 2001.

[9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, revised edition, 2019.

[10] Kundan Munjal and Rekha Bhatia. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex Intelligent Systems*, 9(4):3759–3786, Aug 2023.

[11] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback. Report on the development of the advanced encryption standard (aes). *Journal of Research of the National Institute of Standards and Technology*, 106(3):511–577, Jun 2001.

[12] Petar Radanliev. Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, 15(1):4, Feb 2024.

[13] Hengki Tamando Sihotang, Syahril Efendi, Elvyawati M Zamzami, and Herman Mawengkang. Design and implementation of rivest shamir adleman's (rsa) cryptography algorithm in text file data security. *Journal of Physics: Conference Series*, 1641(1):012042, nov 2020.

[14] D. M. Tank, A. Ganatra, Y. P. Kosta, and C. K. Bhensdadia. Speeding etl processing in data warehouses using high-performance joins for changed data capture (cdc). In *Proceedings of the IEEE International Conference*, 2010.

[15] Urs Wagner and Thomas Lugrin. *Hash Functions*, pages 21–24. Springer Nature Switzerland, Cham, 2023.

[16] Xiaoyun Wang, Guangwu Xu, and Yang Yu. Lattice-based cryptography: A survey. *Chinese Annals of Mathematics, Series B*, 44(6):945–960, Nov 2023.

[17] T. Williams. Challenges in implementing ai-powered crm systems. *Journal of Information Systems*, 2022.

[18] Yuhan Yan. The overview of elliptic curve cryptography (ecc). *Journal of Physics: Conference Series*, 2386(1):012019, Dec 2022.

[19] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. Advances in device-independent quantum key distribution. *npj Quantum Information*, 9(1):10, Feb 2023.

[20] Chuan Zhao, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu an Tan. Secure multi-party computation: Theory, practice and applications. *Information Sciences*, 476:357–372, 2019.

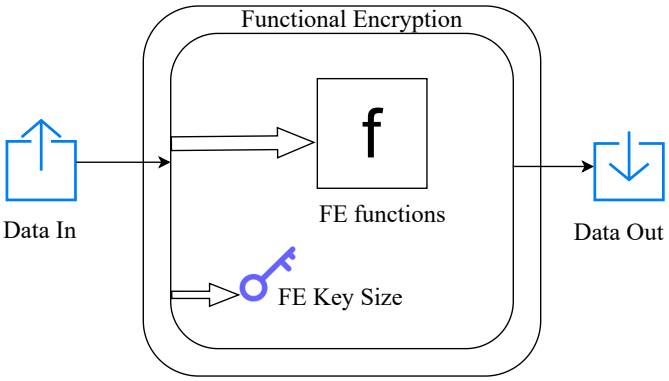

Fig. 9: Functional Encryption

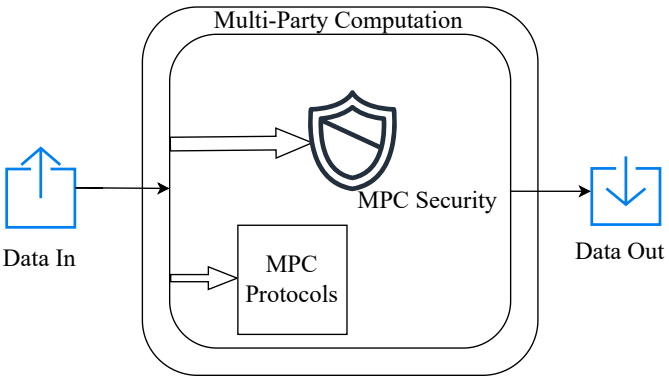

Fig. 10: Multi-party computation