DASINYA JOURNAL for engineering and informatics

https://doi.org/00.0000/xxxxx
Dasinya Journal for Engineering and Informatics. **2025**, 1, 4.

Review

Cryptography in Cloud Computing: Ensuring Data Confidentiality and Integrity

Shivan Hussein Hassan* [1, 2], **Wafaa Mustafa Abduallah** [3]

[1] Department of Information Technology, Technical College of Duhok, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq. [1]; shivan.hassan@dpu.edu.krd
[2] Department of Mathematics, College of Basic Education, University of Duhok, Duhok, Kurdistan Region, Iraq.[2]; shivan.hassan@uod.ac
[3] Department of Cyber Security Engineering, Technical College of Engineering, Duhok Polytechnic University, 4200, Kurdistan Region, Iraq. [3]; wafaa.abduallah@dpu.edu.krd
* Correspondence: shivan.hassan@dpu.edu.krd

Abstract

Cloud computing revolutionized the storage and management of information in organizations with the provision of elastic and inexpensive services. These benefits bear major risks, notably guaranteeing confidentiality and integrity of sensitive information. In this article, cryptography as a solution to the aforementioned concerns and to offer security for cloud systems is taken into consideration. Cryptography provides techniques that protect information against unauthorized usage and render information accurate and reliable. And presents the role of cryptography in cloud computing, with special focus on its application in ensuring data confidentiality and integrity. It highlights various cryptographic techniques, including symmetric and asymmetric encryption, hashing, and digital signatures, and their weaknesses and strengths. The other new techniques, like lightweight cryptography, hybrid schemes, and zero-knowledge authentication encrypted storage, have potential future impacts but are not yet unscalable or practical. Nevertheless, despite all this, encryption is still the foundation of cloud security through confidentiality and integrity protection. Ongoing innovation and better processes for verification should stem from an ability to contend with dynamic cyber threats and increase trust in cloud computing services.

Keywords: Cloud Computing; Cryptography; Data Confidentiality; Encryption Techniques; Cloud Security.

1. Introduction

Cloud computing has revolutionized the organizational life of information processing, management, and storage in the last few years. Cloud computing offers unprecedented flexibility, scalability, and economics through the provision of access to titanic computational power without compelling organizations to raise enormous amounts of capital in the initial stage. These advantages go hand-in-hand with tremendous risks, particularly safeguarding sensitive information. With data breaches and cyberattacks becoming more and more sophisticated every day, a sound set of security controls is more critical than ever. Cryptography, or coding information for the sake of safeguarding it, has emerged as a significant technique for storing data in the cloud computing platform [1].

In this review essay, the significance of the role played by cryptography in cloud computing, i.e., its application for the maintenance of confidentiality and integrity of data, is discussed. Confidentiality provides access to data to only

Received: August 27, 2025; Revised: September 8, 2025; Accepted: September 15, 2025; Published: October 12, 2025; Available online: October 12, 2025.
Citation: To be added by editorial staff during production.

authorized staff, whereas integrity will not permit corruption or tampering of data and will permit identification of any unauthorized change. These two pillars for data security are key in ensuring trust in cloud services, especially with more and more sensitive information being kept and processed over cloud infrastructure [2].

The essay explains various cryptographic techniques, such as symmetric and asymmetric encryption, hashing, and digital signatures, and their operations when used in cloud computing. Symmetric encryption is usually used for fast encryption of large volumes of data, while asymmetric encryption provides robust key exchange and authentication methods. Hash functions ensure integrity by producing fixed-length representations of data that support quick identification of changes, and digital signatures use these methods to offer both authenticity and integrity [3][4].

Also highlighted are novel cryptographic techniques addressing particular challenges of cloud computing. They include homomorphic encryption, by means of which computation can be conducted on encrypted data without decrypting to maintain confidentiality, and attribute-based encryption to ensure fine-grained access control based on the user's attributes. The paper also highlights the role of secure multi-party computation, by means of which multiple parties can compute data cooperatively without compromising privacy [5].

The subsequent sections of this review paper are organized as follows: Section 2 covers the background, Section 3 delves into methodologies, Section 4 reviews the literature review, Section 5 covers the discussion, and Section 6 talks about conclusions.

2. Background

This research explored the applications of quantum cryptography in mobile cloud computing, highlighting benefits like unconditional security and effective sniffing detection but noting challenges in practical scalability and real-world applicability. The New Lightweight Cryptographic Algorithm (NLCA) outperformed existing algorithms in encryption/decryption times and security [6], though it lacked vulnerability analysis. Comparisons of encryption algorithms showed AES as the fastest and most secure. AES 128-bit cryptography and LSB steganography enhanced data security for cloud services, despite potential detection by advanced steganalysis tools. The study proposed secure communication methods for IoT devices using ECC and hybrid cryptography. An efficient two-stage cryptography scheme improved security and reduced processing times. Enhanced security in multi-cloud environments was achieved through encryption techniques and access control mechanisms. RSA was identified as the most widely used encryption algorithm, with the importance of robust validation practices emphasized. Advanced multilevel user authentication protocols using hybrid CAPTCHA codes were introduced [7], enhancing security by incorporating cognitive features. Finally, new encrypted storage approaches using Cocks IBE and AES-256 CBC with zero-knowledge authentication were proposed to enhance trust and security in cloud storage [8].

3. Methodology

This review was conducted by integrating a systematic search of literature in order to prevent gaps and ensure methodological precision. The primary databases sought were IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar, and they were charged with peer-reviewed articles in the time frame of 2019 to 2024. Potential sources were accessed by applying diverse combinations of keywords (cloud computing, cryptography, data confidentiality, encryption methods, and cloud security). Inclusion was accorded to research targeting particularly cryptographic methods applied in cloud computing with particular emphasis on confidentiality, integrity, and security concerns. Nevertheless, exclusion criteria excluded pure theory papers lacking practical or comparative assessment, non-English publications, and unrelated literature on cryptographic strategies in cloud environments. The selected literature was critically analyzed by comparing cryptographical methods, taking into consideration their pros and cons, and marking their limitations in scalability, practical application, and usability. The systematic approach made the review a thorough, reliable, and balanced integration of the existing knowledge of cryptographic solutions in cloud computing.

4. Literature Review

This research explored applications of quantum cryptography in mobile cloud computing, including the DARPA Network, IPSEC implementation, and twisted light HD implementation. The study highlighted the benefits of quantum cryptography, including unconditional security and decent sniffing detection, making it suitable for future internet applications. However, key areas in the theory of quantum cryptography remained complex and poorly understood. Quantum key distribution and some quantum elements like photon yield and propagation were utilized in the experiment, demonstrating the feasibility of using quantum encryption for virtual private networks. The experimental investigation demonstrated that quantum cryptography could address critical internet security issues, ushering in greater security for smart cities, the internet, and tomorrow's cyberspace. Although promising, practical scalability and real-world applicability were still difficult [9]. The research is limited by high implementation costs, restricted transmission speed and distance, environmental vulnerabilities, scalability issues in mobile cloud integration, and unresolved system-level security gaps. To reduce this limitation, we suggest combining hybrid classical-quantum systems and quantum repeaters for scalable and resilient security.

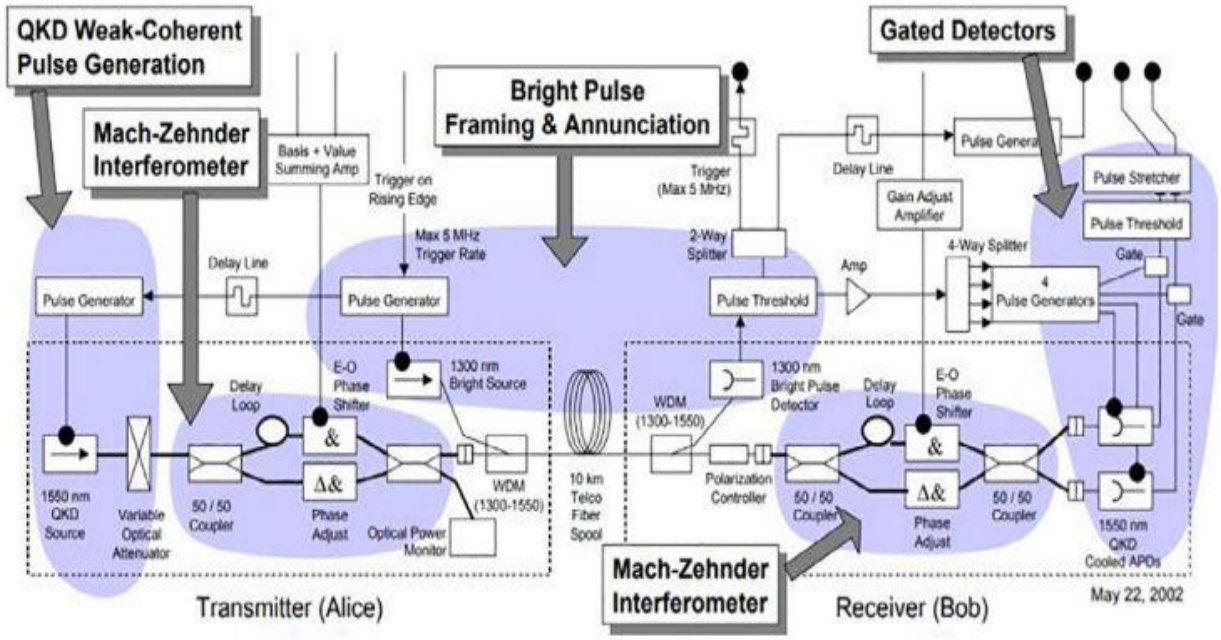

Figure 1. (QKD) setup with (Mach Zehnder) interferometer, showing pulse generation (Alice), framing, and gated detection (Bob) for secure key exchange [9].

The authors proposed the New Lightweight Cryptographic Algorithm (NLCA) to enhance data security in cloud computing. NLCA was a 128-bit block cipher using symmetric cryptography and logical operations like XOR and XNOR to ensure high security and efficiency. It outperformed existing algorithms (DES, AES, HIGHT, Blowfish, and LED) in encryption/decryption times and security levels. However, the study lacked a detailed analysis of potential vulnerabilities and real-world performance. Future hardware implementation was suggested for better results. NLCA offered significant benefits, including adaptability in key lengths and turns, making it suitable for fast data processing in cloud environments [6]. The research is restricted by limited datasets, privacy risks, high computational demands, and clinical adoption barriers; these can be reduced through standardized datasets, federated learning, explainable lightweight models, and stronger regulatory-clinical collaboration.

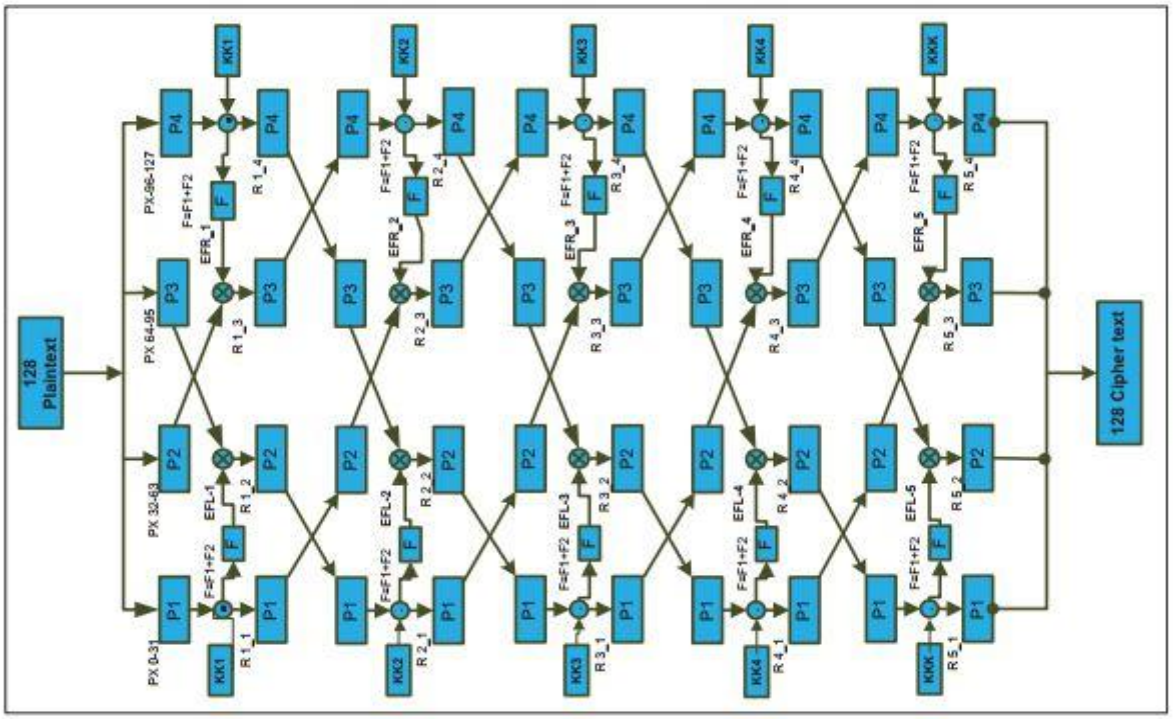

Figure 2. Block diagram of the 128-bit encryption process showing key mixing, substitution, and permutation operations [6].

The researchers compared encryption algorithms (AES, DES, Blowfish, RSA, and IDEA) to find the best for securing cloud information. AES, Blowfish, and DES proved more secure than RSA and IDEA, with AES being the fastest and Blowfish using the least memory. RSA was less efficient due to high memory use and long execution time. The study included a literature review on cloud security issues and encryption techniques. It emphasized enhanced security, better cloud adoption guidance, and reduced hacking. Hybrid algorithms like AES and Blowfish were recommended for increased security. This research offers valuable insights for cloud data protection [8]. Cloud systems face data privacy and security vulnerabilities, lack of trust in third-party providers, and challenges in data availability, integrity, and regulatory compliance; these can be addressed by strengthening encryption and authentication, establishing transparent service level agreements (SLAs), and implementing auditing, compliance monitoring, and advanced intrusion detection.

The study on implementing the AES 128 algorithm for cryptography and LSB steganography for message hiding revealed several key findings and limitations. Using cloud computing services (Platform as a Service —PaaS), the research successfully encrypted messages and embedded them into JPG/JPEG images. The results showed that the encryption process increased the file size proportionally with the number of characters inserted. Tools like Stegspy were used to assess data, confirming the effectiveness of the steganography. Despite these successes, the increase in file size and potential detection by advanced steganalysis tools were noted as limitations. The research demonstrated that AES 128-bit cryptography and LSB steganography enhanced data security, making messages difficult to read and detect. Leveraging cloud services for these processes indicated their feasibility and scalability, offering practical applications in secure digital communication [10]. The study's main restrictions are that encrypted and hidden JPG/JPEG files become significantly larger than the originals, some encrypted images can still be detected by tools like StegSpy, and the method is limited to JPG/JPEG formats only. To reduce these issues, compression can be applied to control file size, more advanced or hybrid steganography techniques (such as adaptive or histogram-preserving methods) can be used to improve undetectability, and the approach can be extended to other image formats or media types like PNG, video, and audio for broader security coverage.

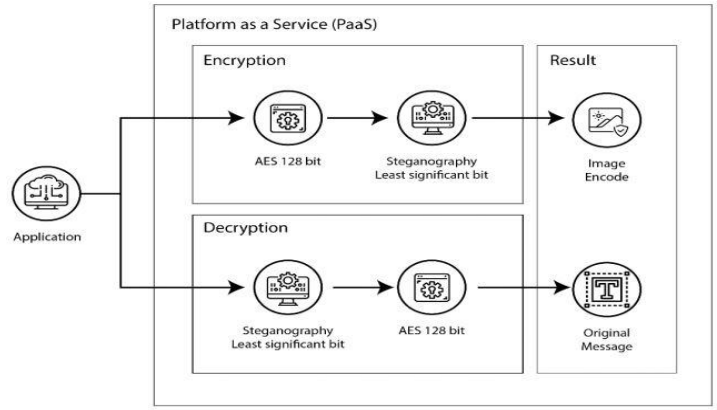

Figure 3. PaaS-based encryption and decryption model using AES-128 and steganography for secure image communication [10].

This study found flaws in cutting-edge cryptographic techniques for cloud computing and Internet of Things devices, namely in terms of non-repudiation, availability, and service reliability. It used technologies such as lightweight cryptography for IoT devices with limited resources and Elliptic Curve Cryptography (ECC) for secure communication. The effectiveness of homomorphic cryptography for encrypted calculations, hybrid cryptography for fusing symmetric efficiency and asymmetric security, and ECC for secure key exchange were among the main conclusions. The paper proposed the use of DNA computing in cryptography. Strong security, efficient use of resources, sharing of hardware and software, and prevention of data loss were among the advantages. It was suggested that future studies look into other measures and current solutions that were not discussed in this study [11]. Cryptography techniques in cloud computing face restrictions such as high computational complexity, storage overhead, long encryption/decryption times, key management challenges, and limited suitability for resource-constrained devices; these can be reduced by adopting lightweight and hybrid cryptography for efficiency, using blockchain and machine learning to strengthen key management and data integrity, and exploring quantum-based methods to enhance speed and security.

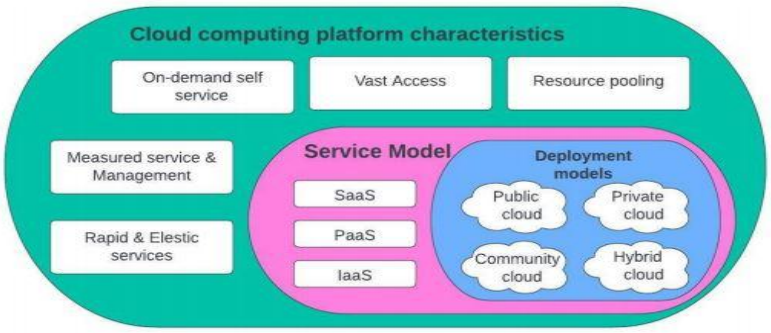

Figure 4. Cloud computing characteristics, service models (SaaS, PaaS, IaaS), and deployment models (public, private, community, hybrid) [11].

The researchers proposed an efficient two-stage cryptography scheme for secure cloud data access and storage, enhancing user authentication and encryption efficiency. The scheme used a two-factor authentication mechanism and logistic chaos model theory for key generation, aiming to improve security and reduce encryption and decryption times. Potential limitations included reliance on user-entered parameters and scalability issues. Key results showed high security, reduced ciphertext size, and lower processing times. Tools likely used were simulation software, cryptographic libraries, and mathematical software. The scheme offered enhanced data security, efficient processing, practicality, and improved user authentication without needing extra hardware, making it suitable for real-world applications [12]. Traditional cloud cryptography schemes often face restrictions such as high complexity, longer encryption/decryption times, extra storage overhead, and weaker security when relying on hybrid or third-party key management; these issues

can be reduced by using the proposed two-stage scheme that splits files, applies chaos-based keys, and integrates two-factor authentication, while further improvements could focus on optimizing multi-server storage and refining lightweight encryption for faster performance.

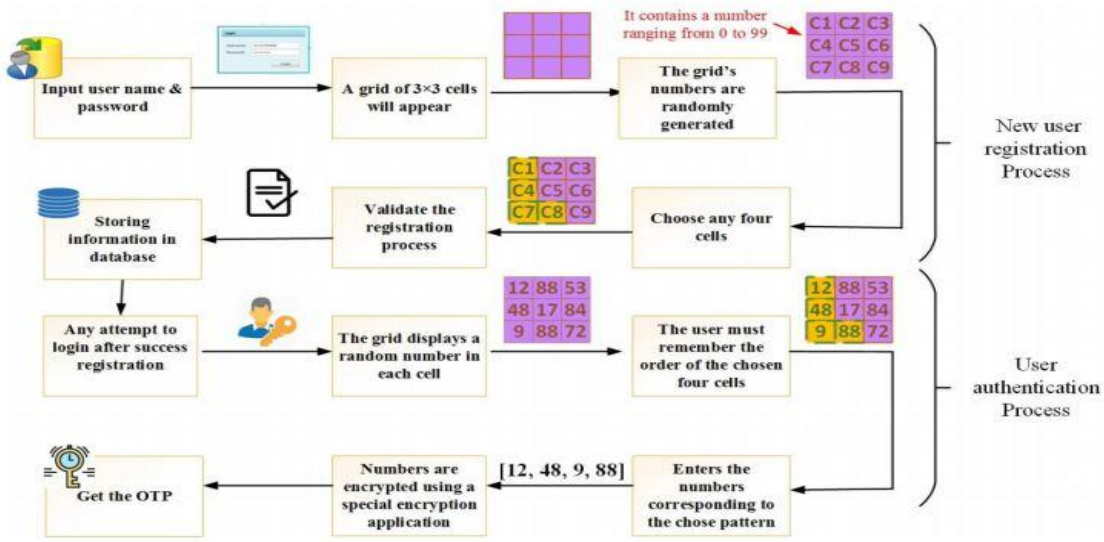

Figure 5. Graphical password-based authentication framework using a 3×3 grid with OTP encryption[12].

The authors had emphasized the importance of cloud computing in secure, reliable, and friendly data storage and urged the encryption of data for protecting outsourced data. Potential limitations included reliance on encryption algorithms, performance overhead, and challenging key management. They discussed cloud computing and symmetric and asymmetric approaches to encryption. Probable hardware included encryption algorithms and cloud storage systems. Primary results showed that data encryption enhanced security and confidentiality, whereas cloud storage ensured efficient data management. The benefits included efficient data management, security enhancement, simple solutions with on-demand availability, and a secure, reliable platform to store and retrieve data [13]. The main limitations are dependence on encryption algorithms, performance overhead, and challenges in key management. Suggestion: These restrictions can be reduced by adopting more efficient or lightweight encryption to lower overhead, improving or automating key management systems, and designing user-friendly security solutions that balance strong protection with ease of use.

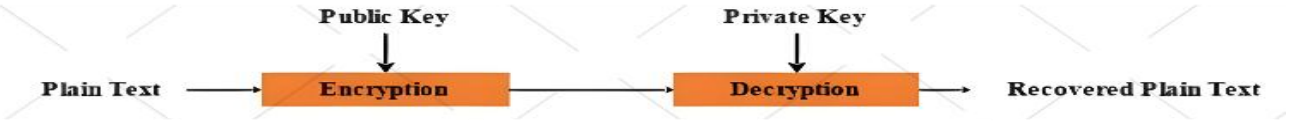

Figure 6. Asymmetric encryption and decryption process using public and private keys [13].

This research focused on reviewing information security strategies for data protection in cloud computing, analyzing various cloud data storage solutions and security challenges. Limitations included a potentially narrow scope, lack of practical implementation details, and the rapidly evolving nature of cloud security. The study used distributed computing technologies, cloud storage solutions, and data security models, employing tools such as literature reviews, analytical frameworks, and comparative analysis. Key findings included the identification of security challenges, analysis of threats and privacy risks, and evaluation of data security models. The benefits of this research included enhanced understanding of cloud security, informed decision-making for organizations, a framework for future research, and encouragement for adopting robust security practices in cloud environments [14]. The main restrictions in this research

are trust management issues, performance overhead, complex key management, uncertain data location, insider threats, data loss/leakage, and risks from attacks like DDoS, spoofing, and floods; these can be reduced by using advanced cryptographic methods such as quantum key distribution and biometric-based encryption, improving key management systems, and integrating blockchain, fuzzy logic, and multi-layered verification to enhance overall security and trust.

This research focused on enhancing security and privacy in multi-cloud settings through encryption techniques and access control mechanisms. Limitations included interoperability issues and evolving security threats. The study utilized multi-cloud technologies and detailed analyses of security protocols, privacy measures, disaster recovery strategies, and continuous monitoring. Key findings identified advanced encryption, AI, ML for threat detection, and privacy-enhancing technologies for regulatory compliance as critical resilience strategies. The research provided valuable insights into fortifying multi-cloud environments against threats and vulnerabilities. Benefits included improved flexibility, scalability, and security in multi-cloud architectures. Future research should address interoperability, edge and quantum computing impacts, and secure data sharing, with best practices recommended for defense-in-depth, identity and access management, and incident response procedures [15]. The main limitations for this study are interoperability, compliance difficulties, data sovereignty issues, and limitations of current encryption techniques. The proposed solutions focus on open standards, advanced privacy-preserving technologies, strong access control, governance frameworks, resilience strategies, and future-oriented research (AI, ML, and quantum security).

This research aimed to examine and compare the predominant encryption methods used in protecting data within cloud systems, focusing on RSA and AES algorithms, and evaluate the validity of these methods using previous literature. The study showed that the most used was RSA, an asymmetric-key algorithm, with 28% of the studies reviewed employing it for protection of data, and 16% of the studies employing AES, which is a symmetric-key algorithm. However, the biggest limitation was that 16% of the methods proposed were not yet tested, demonstrating there was a need for improved validation processes. The research, which was grounded on a systematic literature review, provided valuable advice to business customers in the selection of appropriate encryption algorithms and recommended RSA as the preferable choice. Through the identification of widely adopted and proven encryption methods, this research enhanced cloud-based system security and highlighted the importance of sound validation processes in encryption research [16]. The main limitations are the overuse of RSA, limited validation, underutilization of emerging encryption schemes, and the lack of multi-layered security integration. The proposed solutions include adopting hybrid and emerging encryption techniques, conducting real-world validation, preparing for quantum-era threats, and integrating encryption with broader security measures.

This research introduced a symmetric key encryption algorithm that encrypted files locally on the client-side before cloud upload and decrypted them after downloading using a generated key. The algorithm employed a specific key calculation method, enhancing security and performance for text files. However, it was limited to text files and showed low performance for large files. Future implementations could explore asymmetric key encryption and social media platform adaptation. The algorithm added an extra security layer, addressing public cloud security concerns and reducing data loss, theft, and interference during transit. The study highlighted the need for improved cloud security measures, offering a reliable solution for text files while acknowledging the potential for broader applications and performance improvements [17]. The main limitations of this research are its restriction to text files, reduced performance for large data, reliance only on symmetric encryption, lack of standardization across cloud providers, and narrow application scope. The proposed solutions include expanding file support, optimizing performance for large files, adopting hybrid encryption, establishing cross-platform encryption standards, and extending usability to multiple cloud services and contexts.

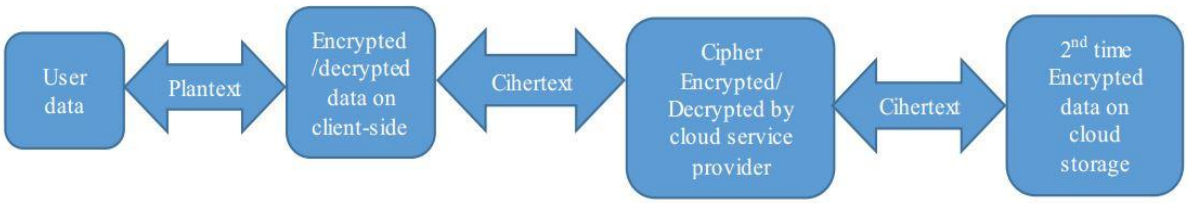

Figure 7. Client-side and cloud-based encryption process for secure cloud data storage [17].

The researchers developed advanced multilevel user authentication protocols using hybrid CAPTCHA codes, requiring specific skills and expertise for proper authentication. This method aims to provide data access only to expert groups, introducing a new class of cognitive CAPTCHAs that combine pattern recognition with semantic understanding. While the approach may be limited in broader applicability, it enhances security by incorporating cognitive features and expert knowledge. The research involves CAPTCHA development, cognitive testing, and cryptographic protocols. Key results include new cognitive CAPTCHAs and expanded security protocols, establishing cognitive cryptography. This research proposes more secure authentication methods tailored for expert groups, integrating human mental characteristics into security technologies [7]. The main limitations of the proposed cognitive cryptography are its dependence on expert knowledge, reduced usability due to complex multistage CAPTCHAs, scalability challenges, and limited empirical validation. To address these issues, future work should integrate hybrid authentication methods, adopt adaptive difficulty levels, design more general cognitive tasks, provide error-tolerant and inclusive alternatives, and conduct large-scale validation studies to ensure both usability and security.

This paper aimed to enhance cloud computing security using cryptography. It addressed new security challenges due to resource sharing in cloud environments, focusing on data sensitivity. The authors introduced encryption techniques to solve security problems from both client and provider perspectives. The research provided encryption-based solutions to enhance security. Benefits included improved data protection and solutions beneficial to both clients and providers. Limitations involved the effectiveness of encryption techniques in addressing all security risks and potential performance overheads. Specific tools and technologies used were not detailed [18]. The main limitations are data security vulnerabilities, outdated or computationally heavy encryption algorithms, inefficiency of Fully Homomorphic Encryption (FHE), and fragmented solutions, while the proposed solutions include adopting modern algorithms such as AES and ECC, using hybrid cryptography, optimizing homomorphic encryption, strengthening key management, and moving toward integrated multi-layered frameworks.

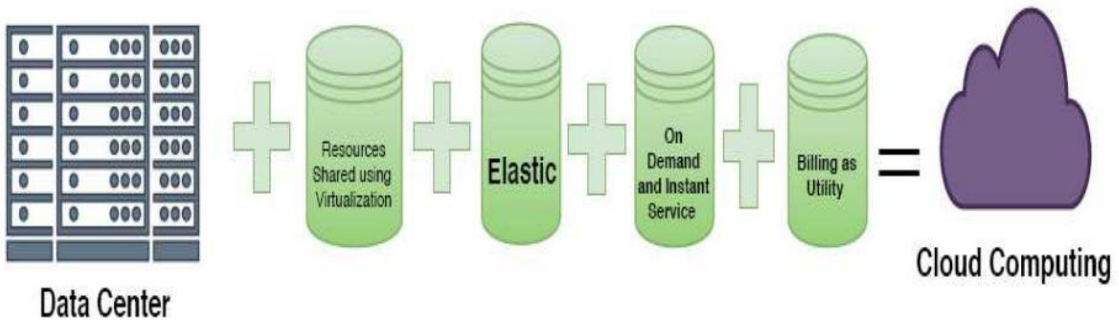

Figure 8. Key components that transform traditional data centers into Cloud Computing: virtualization, elasticity, on-demand services, and utility based billing [18].

The study evaluated the impact of cryptography techniques on cloud computing in the information technology sector using secondary data gathering and thematic data analysis of peer-reviewed journals since 2019. The study focused on cryptography utilization for data storage and transmission security, examining confidentiality, integrity, authentication, and authorization of encrypted data. The study encompassed benefits and limitations of various cryptographic methods, including symmetric and asymmetric cryptography and hash functions. Even as it identified the complexity of cryptographic techniques as a drawback, it noted that they were cost-saving and time-saving. It concluded that encryption reduced data loss risk and improved data security. Limitations included reliance on secondary data, focus on recent literature, and challenges in generalizing results. The research had practical implications for IT practitioners regarding data security controls [19]. The research identifies cryptographic complexity, performance inefficiency, system vulnerabilities, cost, and poor design as major limitations. The proposed solutions include hybrid encryption, stronger authentication, frequent algorithm updates, advanced cryptographic standards, and integration into unified security frameworks.

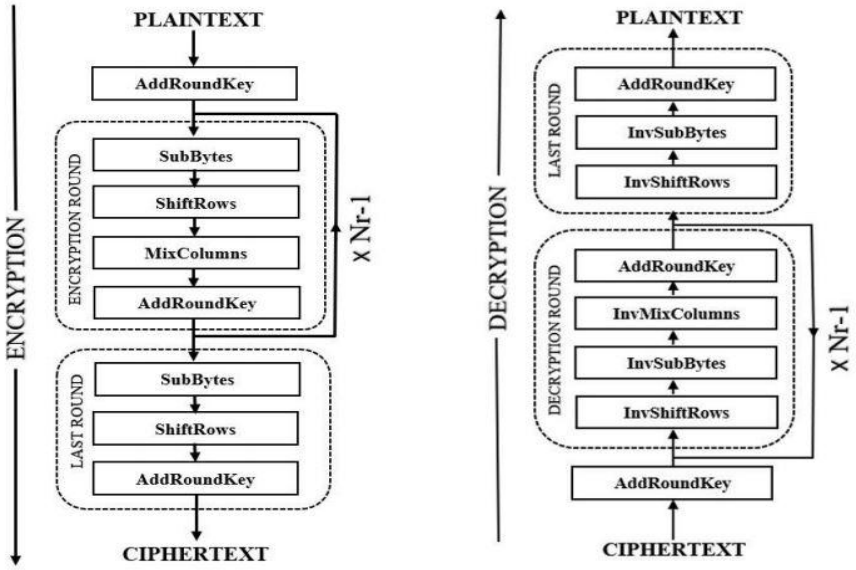

Figure 9. AES encryption and decryption rounds: transforming plaintext to ciphertext and back [20].

The research identified limitations in cloud storage and cryptographic systems, such as trust issues due to providers' access to data, complex key management, and limited security information. It evaluated the security of cloud storage options like Microsoft Azure, Tresorit, Amazon S3, and Google Cloud, noting vulnerabilities such as Tresorit's phishing risks. The study proposed a new encrypted storage approach using Cocks Identity-Based Encryption (IBE) and AES-256 Cipher Block Chaining (CBC), with zero-knowledge Fiat-Shamir authentication to enhance trust. It suggested replacing IBE with a decentralized approach to improve privacy, despite challenges like re-encryption. Solutions like using a pseudorandom number generator for IVs or replacing Boneh-Franklin IBE with Cocks IBE aimed to improve efficiency and security, though storage concerns persisted. The research's benefits included improved security, increased trust, and potential enhancements in privacy and efficiency [21]. The research has several limitations, such as provider access risks, limited cryptographic system usability, complex key management, weak authentication, imbalanced trust, and reliance on documentation over experiments. These can be addressed by improving transparency with access notifications, enhancing usability via searchable encryption, simplifying key management, implementing user-controlled encryption, strengthening authentication with zero-knowledge methods, and validating results experimentally for real-world reliability.

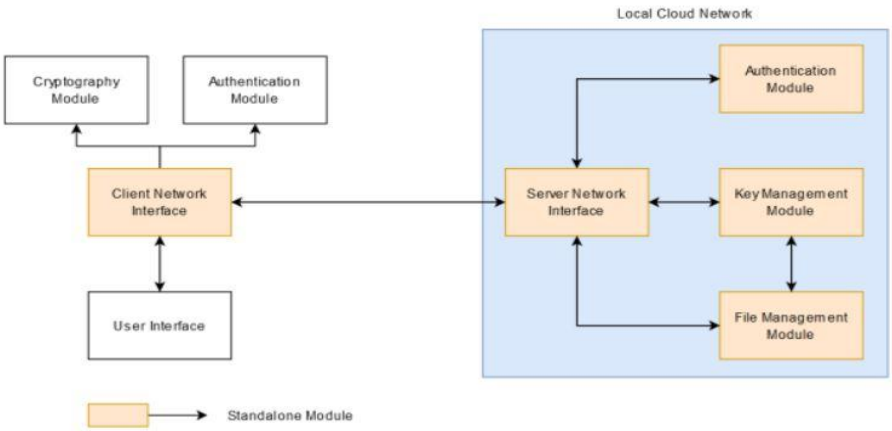

Figure 10. Cloud network architecture showing client interaction with authentication, key management, and file management modules [21].

Table 1. Overview of cryptographic techniques for cloud security.

Ref.	Method Name	Technique Used	Advantage	Limitation	Result
[9] 2021	Quantum Cryptography Technique	Quantum key distribution, photon yield and propagation	Unconditional security, effective sniffing detection	Complexity, not fully understood	Enhanced security for smart cities, internet, and future cyberspace
[6] 2021	New Lightweight Cryptographic Algorithm (NLCA)	128-bit block cipher, symmetric cryptography, XOR, XNOR	High security and efficiency, outperforms DES, AES, HIGHT, Blowfish, LED	Lack of detailed analysis of vulnerabilities, real-world performance	Significant adaptability in key lengths and turns, suitable for fast data processing in cloud environments
[8] 2023	Comparison of Encryption Algorithms	AES, DES, Blowfish, RSA, IDEA	AES is fastest, Blowfish uses least memory, better security guidance	RSA is less efficient due to high memory use and long execution time	Valuable insights for cloud data protection, recommended hybrid algorithms like AES and Blowfish
[10] 2020	AES 128 and LSB Steganography	AES 128-bit cryptography, LSB steganography	Enhanced data security, practical application in secure digital communication	Increased file size, potential detection by advanced steganalysis tools	Successfully encrypted messages and embedded them into JPG/JPEG images
[11] 2024	Advanced Cryptographic Methods for Cloud Computing and IoT	ECC, homomorphic cryptography, hybrid cryptography	Strong security, effective resource utilization	Service dependability, availability, non-repudiation issues	Suggested DNA computing's potential in cryptography
[12] 2020	Two-Stage Cryptography Scheme	Two-factor authentication, logistic chaos model theory	High security, reduced ciphertext size, lower processing times	Reliance on user-entered parameters, scalability issues	Enhanced data security and user authentication without extra hardware
[13] 2024	Data Encryption in Cloud Storage	Symmetric and asymmetric encryption techniques	Improved data management, enhanced security	Reliance on encryption algorithms, performance overhead, complex key management	Enhanced security and confidentiality for cloud data storage
[14] 2021	Information Security Strategies for Cloud Computing	Distributed computing technologies, cloud storage solutions, data	Enhanced understanding of cloud secu-	Narrow scope, lack of practical implementation details	Identified security challenges and evaluated data security models

		security models	**rity, informed decision-making**		
[15] 2024	**Security and Privacy in Multi-Cloud**	**Multi-Cloud technologies, encryption, AI, ML**	**Improved flexibility, scalability, security**	**Interoperability issues, evolving security threats**	**Valuable insights into fortifying Multi-Cloud environments**
[16] 2021	**Key Encryption Methods for Cloud-Based Systems**	**RSA, AES**	**Widely used and validated encryption methods**	**16% of proposed encryption approaches not validated**	**RSA recommended as optimal choice, enhanced security for cloud-based systems**
[17] 2021	**Symmetric Key Encryption for Cloud**	**Local client-side encryption**	**Enhanced security and performance for text files**	**Limited to text files, low performance for large files**	**Reliable solution for text files, potential for broader applications**
[7] 2020	**Cognitive Cryptography for Cloud Computing**	**Hybrid CAPTCHA codes, cognitive testing**	**Enhanced security by incorporating cognitive features**	**Limited broader applicability**	**New cognitive CAPTCHAs and expanded security protocols**
[18] 2020	**Cryptography for Cloud Computing Security**	**Encryption techniques**	**Improved data protection**	**Effectiveness in addressing all security risks, potential performance overheads**	**Encryption-based solutions beneficial to both clients and providers**
[19] 2022	**Impact of Cryptography Techniques on Cloud Computing**	**Symmetric and asymmetric techniques, hash functions**	**Cost-effectiveness, time-saving benefits**	**Complexity of cryptographic techniques**	**Reduced risk of data loss, improved data security**
[21] 2023	**Encrypted Storage Approach**	**Cocks IBE, AES-256 CBC, zero-knowledge Fiat-Shamir authentication**	**Improved security, increased trust**	**Storage concerns, re-encryption challenges**	**Enhanced trust and privacy, potential efficiency improvements**

5. Discussion

Cloud computing has transformed the manner in which data is handled by enabling on-demand access to computational services without having to make huge capital investments. Such advantages notwithstanding, security of sensitive information remains at the top of the agenda due to increasing instances of data breaches and cyberattacks. Cryptography becomes the focus of maintaining confidentiality and data integrity within cloud systems.

Data is shielded against unwanted reading and disclosure by confidentiality, which guarantees that information is only accessible to those who are allowed to view it. While asymmetric encryption (like RSA) is used for high security for key exchange in addition to digital signatures, symmetric encryption (like AES) is generally used because it is effective at encrypting massive volumes of data. By creating fixed-length unique representations of the data, hash algorithms like SHA-256 ensure data integrity by making it easier to identify any changes. Asymmetric encryption and hashing are combined in digital signatures to confirm the integrity and origin of data.

New cryptographic protocols are being developed with the cloud environment's specific problems in mind. Homomorphic encryption, for example, allows computations to be made directly on encrypted data without needing decryption, thus preserving secrecy during processing. Attribute-based encryption allows access to be granted at a fine level of granularity using user attributes, which is more secure. Secure multi-party computation cryptographic protocols allow multiple data processing through collaboration without compromising any individual's privacy.

The research further indicates advancements in quantum cryptography, which offers unconditional security and effective detection of eavesdropping. Quantum key distribution (QKD) and other quantum elements illustrate the potential of quantum encryption in securing virtual private networks (VPNs) and offering enhanced security in the use of the future internet.

6. Conclusions

Cryptography plays a crucial role in protecting sensitive information as cloud computing progresses. Cryptographic technique development and utilization on cloud platforms are crucial in the building of confidence and trust in cloud computing. The review is critical of the central role of cryptography in mitigating cloud computing security threats and therefore the necessity for continued innovation and collaboration. In the future, effort must go into developing such approaches in order to render them more applicable in real-world situations and practically scalable without compromising hard data protection. Specific areas of research are (i) the design of lightweight cryptographic primitives for resource-constrained devices, e.g., for the Internet of Things (IoT); (ii) the design of hybrid modes of encryption appropriate for multi-cloud environments for interoperability, performance, and security; (iii) the use of artificial intelligence and machine learning for anomaly detection and adaptive encryption; and (iv) an investigation into privacy-preserving cryptographic methods, such as zero-knowledge proofs, to enable authentication and trust without revealing sensitive information. With the evolution of these guidelines, cryptographic research will be in a position to transition from theoretical breakthroughs to effective, scalable, and resilient security systems.

Abbreviations

The following abbreviations are used in this research:

Abbreviation	Full Form
AES	**Advanced Encryption Standard**
RSA	**Rivest–Shamir–Adleman**
SHA	**Secure Hash Algorithm**
CBC	**Cipher Block Chaining**
IBE	**Identity-Based Encryption**
QKD	**Quantum Key Distribution**
VPN	**Virtual Private Network**
IPSec	**Internet Protocol Security**
ECC	**Elliptic Curve Cryptography**
NLCA	**New Lightweight Cryptographic Algorithm**
DES	**Data Encryption Standard**
IDEA	**International Data Encryption Algorithm**
HIGHT	**Highly Secure and Lightweight Block Cipher**
LSB	**Least Significant Bit (Steganography)**
IoT	**Internet of Things**
AI	**Artificial Intelligence**
ML	**Machine Learning**
PaaS	**Platform as a Service**
SaaS	**Software as a Service**
CAPTCHA	**Completely Automated Public Turing test to tell Computers & Humans Apart**

References

[1] R. Adee and H. Mouratidis, "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography," Sensors, vol. 22, no. 3, pp. 1–23, 2022, doi: 10.3390/s22031109.

[2] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[3] H. C. Ukwuoma, G. Arome, A. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing," Open Comput. Sci., vol. 12, no. 1, pp. 142–153, 2022, doi: 10.1515/comp-2022-0235.

[4] Oluwatoyin Ajoke Fayayola, Oluwabukunmi Latifat Olorunfemi, and Philip Olaseni Shoetan, "Data Privacy and Security in It: a Review of Techniques and Challenges," Comput. Sci. IT Res. J., vol. 5, no. 3, pp. 606–615, 2024, doi: 10.51594/csitrj.v5i3.909.

[5] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security," Cluster Comput., vol. 24, no. 2, pp. 739–752, 2021, doi: 10.1007/s10586-020-03157-4.

[6] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Glob. Transitions Proc., vol. 2, no. 1, pp. 91–99, 2021, doi: 10.1016/j.gltp.2021.01.013.

[7] U. Ogiela, "Cognitive cryptography for data security in cloud computing," Concurr. Comput. Pract. Exp., vol. 32, no. 18, pp. 1–4, 2020, doi: 10.1002/cpe.5557.

[8] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, "Cloud data security and various cryptographic algorithms," Int. J. Electr. Comput. Eng., vol. 13, no. 2, pp. 1867–1879, 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.

[9] S. Abidin, A. Swami, E. Ramirez-Asís, J. Alvarado-Tolentino, R. K. Maurya, and N. Hussain, "Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)," Mater. Today Proc., vol. 51, no. xxxx, pp. 508–514, 2021, doi: 10.1016/j.matpr.2021.05.593.

[10] N. R. D. P. Astuti, E. Aribowo, and E. Saputra, "Data security improvements on cloud computing using cryptography and steganography," IOP Conf. Ser. Mater. Sci. Eng., vol. 821, no. 1, 2020, doi: 10.1088/1757-899X/821/1/012041.

[11] K. Sasikumar and S. Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," IEEE Access, vol. 12, no. April, pp. 52325–52351, 2024, doi: 10.1109/ACCESS.2024.3385449.

[12] R. F. Abdel-Kader, S. H. El-Sherif, and R. Y. Rizk, "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," Int. J. Electr. Comput. Eng., vol. 10, no. 3, pp. 3295–3306, 2020, doi: 10.11591/ijece.v10i3.pp3295-3306.

[13] S. R. Gudimetla, "Data Encryption in Cloud Storage," Int. Res. J. Mod. Eng. Technol. Sci., no. April, pp. 4–7, 2024, doi: 10.56726/irjmets50637.

[14] K. Gupta, D. Gupta, S. K. Prasad, and P. Johri, "A Review on Cryptography based Data Security Techniques for the Cloud Computing," 2021 Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2021, pp. 1039–1044, 2021, doi: 10.1109/ICACITE51222.2021.9404568.

[15] N. Mohammad, "Multi-Cloud Environments : a Comprehensive Study on Encryption Techniques and Access Control," Int. J. Comput. Eng. Technol., vol. 12, no. 2, pp. 51–63, 2024.

[16] A. Rajab, S. Aqeel, M. S. Al Reshan, A. Ashraf, S. Almakdi, and K. Rajab, "Cryptography based techniques of encryption for security of data in cloud computing paradigm," Int. J. Eng. Trends Technol., vol. 69, no. 10, pp. 1–6, 2021, doi: 10.14445/22315381/IJETT-V69I10P201.

[17] A. Musa and A. Mahmood, "Client-side Cryptography Based Security for Cloud Computing System," Proc. - Int. Conf. Artif. Intell. Smart Syst. ICAIS 2021, pp. 594–600, 2021, doi: 10.1109/ICAIS50930.2021.9395890.

[18] S. Zaineldeen and A. Ate, "Review of Cryptography in Cloud Computing Review of Cryptography in Cloud Computing," vol. 9, no. 3, pp. 211–220, 2020.

[19] L. G. De Lazo and D. P. V. S. Kumar, "Role and Importance of Cryptography Techniques in Cloud Computing," Technoarete Trans. Internet Things Cloud Comput. Res., vol. 2, no. 2, 2022, doi: 10.36647/ttitccr/02.02.art005.

[20] B. Sarkar, A. Saha, D. Dutta, G. De Sarkar, and K. Karmakar, "A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography," Int. J. Comput. Sci. Mob. Comput., vol. 13, no. 4, pp. 68–87, 2024, doi: 10.47760/ijcsmc.2024.v13i04.008.

[21] C. Manthiramoorthy, K. M. S. Khan, and N. A. A, "Comparing Several Encrypted Cloud Storage Platforms," Int. J. Math. Stat. Comput. Sci., vol. 2, pp. 44–62, 2023, doi: 10.59543/ijmscs.v2i.7971.