International Journal of Computational Science and Engineering Research
ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/
Regular Issue , Vol. 2, Issue. 2 (April - June), 2025 , Pages: 8 - 14
Received: 18 January 2025 ; *Accepted:* 26 March 2025 ; *Published:* 10 May 2025
https://doi.org/10.63328/IJCSER-V2RI2P2
Original Paper : Qualitative Research – Analytical Research Paper

Advancing Cloud Data Protection with Secure Cryptographic Algorithms

V Sujana [1*] **, N Bindu Madhavi** [2]

[1*, 2] Department of Computer Science and Engineering, VEMU Institute of Technology, Chittoor, Andhra Pradesh, India; sujanacse93@gmail.com , bindupilivarthi994@gmail.com

** Corresponding Author:* sujanacse93@gmail.com

Abstract: Encryption makes it possible to send private information via unprotected channels without worrying about data loss or modification by unauthorized parties. For data security in various contexts, many encryption algorithms have developed throughout time. This paper focuses on symmetric encryption, often used for key exchange due to its large key size. In the context of data centers and cloud computing, security is paramount. This paper proposes a quantum computing algorithm for encrypting cloud data. This combination leverages quantum computing's rapid complex computations. The quantum computing algorithm offers fast, efficient, and secure data protection in cloud environments, reducing computational power requirements while enhancing overall efficiency. Moreover, it addresses the limitations of traditional encryption methods and provides a scalable solution for large-scale data encryption. By integrating quantum computing, we can achieve unprecedented levels of security and performance. The potential impact of this approach could revolutionize data protection standards in the cloud industry.

Keywords: Encryption, Sensitive Data, Insecure Channels, Data Loss, Large-Scale Data Encryption, Cloud Industry.

1. Introduction

In recent years, distributed computing has changed the manner in which organizations and people store, cycle, and access information. The cloud offers remarkable advantages, including scalability, flexibility, cost-effectiveness, and ease of access from anywhere. However, as more sensitive information moves into cloud environments, safeguarding it against unauthorized access and potential cyber threats has become a top priority. Traditional encryption algorithms, like RSA and AES, play a crucial role in protecting data during transit and while at rest. However, these methods are facing increasing pressure to adapt to the growing scale of cloud computing infrastructures and the emerging threats posed by quantum computing. While symmetric encryption algorithms such as AES are efficient, they face challenges in terms of key management and scalability. As cloud systems expand, the amount of data being transferred and stored grows exponentially, making traditional encryption methods more cumbersome and less efficient. The need for new cryptographic systems that are both secure and scalable has never been more pressing. Additionally, as quantum computing advances, it has the potential to crack established encryption systems. Because they may exist in numerous states at once, quantum bits (qubits) give quantum computers significantly greater processing capability than traditional computers. Problems that would take millennia to compute on classical computers could be solved by quantum systems thanks to these capabilities. By providing better security protocols that are impervious to quantum-based assaults, encryption based on quantum computing holds promise for resolving these issues. Quantum Key Distribution (QKD) is one such method that safely exchanges cryptographic keys by applying the ideas of quantum physics. Quantum mechanics ensures that any interception of quantum-encrypted data would disrupt the transmission, making unauthorized access detectable. With the advent of quantum cryptographic techniques, Long-term data security against potential threats is made possible by quantum algorithms that are immune to quantum computer assaults, such as post-quantum cryptography.

The effectiveness of large-scale data encryption may likewise be greatly increased by quantum-enhanced encryption. Faster encryption techniques might be made possible by quantum systems through the use of quantum algorithms such as Grover's Algorithm for

quicker searching and Shor's Algorithm for factoring huge numbers, more energy-efficient, and less resource-intensive. These features are particularly valuable in cloud environments, where computational power is often distributed across multiple data centers and the data throughput is high.

The integration of quantum computing in cloud environments also offers a chance to rethink the entire architecture of data protection systems. Rather than focusing solely on encrypting data at rest or in transit, quantum encryption could lead to new, holistic security models where data is protected continuously across multiple levels, such as during processing, storage, and transmission. Furthermore, quantum encryption can help mitigate emerging threats such as those posed by AI-driven attacks, which can quickly decipher traditional encryption methods. As AI technologies continue to evolve and grow in sophistication, combining quantum encryption with AI-based security systems could lead to the next generation of cyber security protocols that can adapt in real-time to evolving threats.

The introduction of quantum computing-based encryption in cloud environments also provides an opportunity for industry-wide standardization of quantum-safe encryption algorithms. The National Institute of Standards and Technology (NIST) has already begun working on standardizing post-quantum cryptographic algorithms, which could eventually become the go-to standard for cloud security. This would ensure that organizations around the world adopt encryption technologies that are resilient against both current and future threats. Overall, the integration of quantum computing into cloud-based encryption represents a significant leap forward in securing sensitive data in an increasingly complex and interconnected digital landscape.

As the quantum computing field continues to mature, the implications for cyber security in the cloud are profound, setting the stage for the development of more secure, efficient, and scalable data protection frameworks that will be crucial for maintaining privacy and trust in the digital age. The research and development of quantum encryption algorithms tailored for cloud platforms will ultimately lead to a more secure and resilient digital ecosystem, one that can keep pace with the rapid advancements in both cloud computing and quantum technologies. By addressing the limitations of traditional encryption methods and embracing the power of quantum computing, cloud providers and enterprises will be better equipped to protect their valuable data and ensure that sensitive information remains safe in an increasingly data-driven world.

1.1 Objective of the study

The objectives of this research are to develop a quantum computing-based encryption algorithm for secure and efficient data protection in cloud environments, address the limitations of traditional encryption methods in scalability and computational efficiency, enhance the performance of large-scale data encryption, and ensure robust protection against evolving cyber threats. Additionally, this study aims to reduce computational power requirements, provide a scalable encryption solution, and establish new standards for secure, efficient, and reliable data protection in the cloud computing industry.

1.2 Problem Statement

Traditional encryption methods used in cloud computing face significant challenges in scalability, computational efficiency, and vulnerability to evolving cyber threats. Symmetric encryption, while effective, often struggles with large-scale data environments due to its high computational power requirements and key management complexities. As cloud computing grows, the need for secure, efficient, and scalable encryption becomes critical. This paper addresses these limitations by proposing a quantum computing-based encryption algorithm. Leveraging the speed and computational capabilities of quantum technology, this approach ensures robust data security, reduces computational demands, and offers a scalable solution for protecting sensitive data in modern cloud environments.

2. Related Work and Literature Survey

Researchers Wenjie Liu, Yinsong Xu, and Wen Liu, with Haibin Wang and Zhibin Lei composed the preprint "Quantum Accessible Encryption for Cloud Information In view of Full-Blind Quantum Calculation" [1] which was distributed on arXiv in 2023.

The authors present a quantum encryption system designed for cloud data which employs a multi-client universal circuit for full-blind computationally secure queries. The proposed technique enables a large number of clients with limited quantum capabilities to securely engage into a contract with a trustworthy key center to create keys and encrypt data, after which the encrypted data is uploaded to a data center. By integrating Grover's algorithm, the scheme facilitates efficient searching on encrypted data while ensuring resistance against quantum attacks. The authors provide a detailed example of searching on an encrypted 2-qubit state and conduct a comprehensive security analysis, demonstrating the scheme's robustness against both external and internal threats. The creators molded this exploration under the title "Towards an Original Protection Safeguarding Circulated Multiparty Information Reevaluating Plan for Distributed computing with Quantum

Key Dispersion" which showed up as a preprint on arXiv in 2024 [2].

This investigation examines the symbiotic relationship between cloud computing and blockchain technology along with quantum computing by solving current limitations. The security framework implemented by the authors adds Quantum Key Distribution (QKD) with CRYSTALS Kyber and Zero-Knowledge Proofs (ZKPs) to strengthen protection of cloud-based blockchain system data. Lattice-based cryptographic methods and the quantum-safe cryptographic protocol QKD are used to the framework seeks to protect data against quantum assaults. Organizations looking to protect their data against quantum attacks can benefit from overall system efficiency, quantum key generation rates, and encryption and decryption processes are all covered in the study's comprehensive performance evaluations. The paper titled "PristiQ: This preprint published by arXiv in 2024 introduces "PristiQ" which represents a Co-Design Framework devoted to safeguarding quantum learning security in cloud environments [3].

The research presents "PristiQ" as a co-design framework which addresses data security requirements for quantum machine learning (QML) applications within quantum-as-a-service (QaaS) systems. The authors include an encryption subcircuit with additional safe qubits connected to a user-specified security key since they are aware of the risks of data leakage while utilizing cloud-based quantum computers to run QML models. This approach enhances data security by ensuring that the quantum data remains encrypted during computation. The study introduces an automated search system which optimizes model execution on quantum data while it remains encrypted. Experimental evidence demonstrates PristiQ delivers secure quantum data protection along with QML application performance maintenance through system testing on IBM quantum hardware and simulation models.

In 2023, Tirthak Patel, Daniel Silver, Aditya Ranjan, Harshitta Gandhi, William Cutler, and Devesh Tiwari distributed a paper named "Toward Security in Quantum Program Execution On Untrusted Quantum Distributed computing Machines for Business-touchy Quantum Needs" as [4] an arXiv preprint (arXiv:2307.16799).The necessity of safeguarding proprietary and sensitive quantum code in cloud-based quantum computing systems against hostile or unreliable actors is discussed in this paper. In order to stop sensitive data from leaking over the cloud, the authors suggest "SPYCE," a system that obfuscates quantum code and output. Business-sensitive quantum computations may be safely carried out on untrusted quantum cloud platforms thanks to SPYCE's lightweight, scalable, and efficient solution, which is founded on the special principles of quantum computing.

IBM, "Quantum-safe cryptography: How it affects your information in the cloud," IBM Think Blog, 2024 [5].

IBM's article discusses the emerging cybersecurity challenges posed by quantum computing, particularly concerning data in the cloud. The piece emphasizes that current encryption methods used to protect data in motion and at rest could be compromised by large quantum computers with millions of fault-tolerant qubits. IBM advocates for the adoption of quantum-safe cryptographic algorithms to mitigate these risks, highlighting the importance of proactive measures to secure data against future quantum attacks.

3. Proposed System

The proposed system introduces a quantum computing algorithm to encrypt cloud data, enhancing security and efficiency. By leveraging quantum mechanics, this approach enables rapid encryption and decryption processes, reducing computational overhead compared to classical methods. The system addresses scalability issues inherent in traditional encryption by utilizing quantum key distribution, ensuring secure key management across distributed cloud environments. This integration offers a robust, scalable solution for large-scale data protection, positioning it as a forward-looking strategy against emerging threats, including those posed by future quantum attacks.

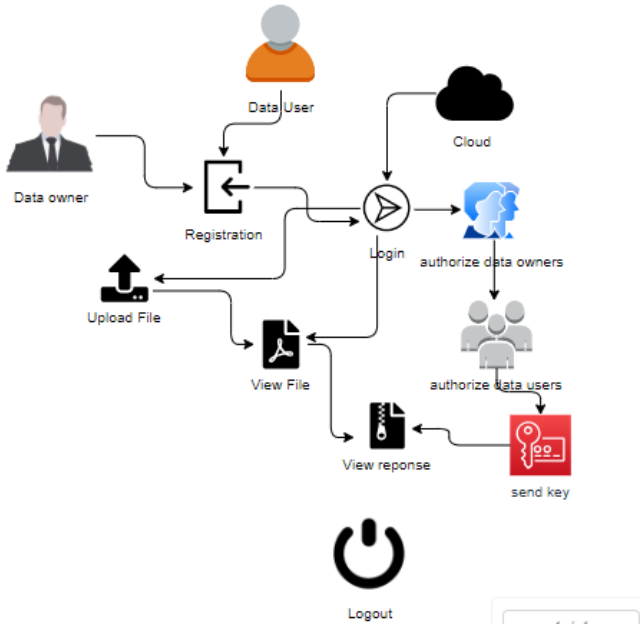


Figure. 1 System Architecture of Advancing Cloud Data Protection with Cryptographic Algorithm

3.1 Implementation modules

In our Advancing Cloud Data Protection with Cryptographic Algorithms, we have performed the implementation of certain modules.

Data Owner:

Vol. 2, Issue 2, 2025, https://doi.org/10.63328/IJCSER-V2RI2P2

Register: Allows the data owner to sign up on the platform by providing necessary details.

Login: Enables the data owner to access the platform using their credentials after receiving authorization from the cloud administrator.

Upload Files: Permits the data owner to upload files to the platform and encrypt them using quantum encryption algorithms.

View Files: Allows the data owner to view and manage their uploaded files.

View File Requests: Enables the data owner to see requests from data users and decrypt files as needed.

Logout: Provides the option for the data owner to securely log out from the platform.

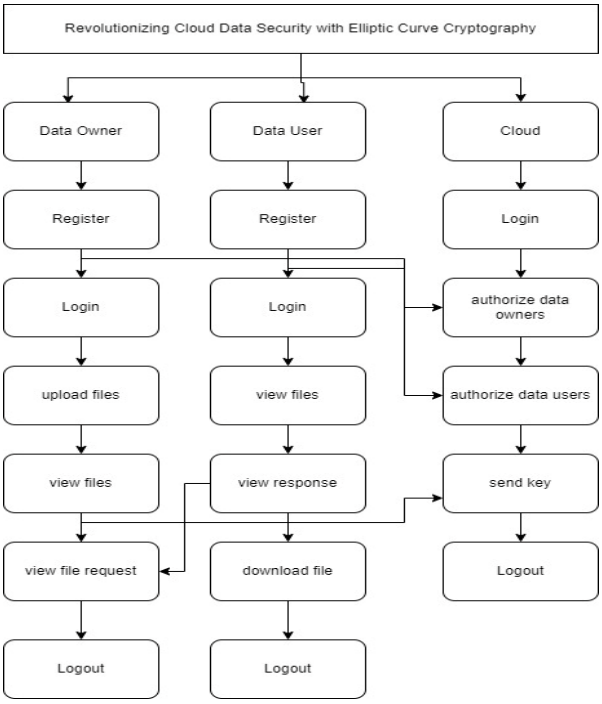


Figure.2 Flow chart of Advancing Cloud Data Protection with Cryptographic Algorithms

Data User:

Register: Allows the data user to create an account on the platform by entering required information.

Login: Enables the data user to access the platform using their credentials after cloud administrator authorization.

View Files: Permits the data user to browse available files and send access requests to data owners.

View Responses: Allows the data user to check the status of their file access requests.

Download Files: Enables the data user to download files using the provided decryption keys.

Logout: Provides the option for the data user to securely log out from the platform.

Cloud Administrator:

Login: Allows the cloud administrator to access the platform using their credentials.

Authorize Data Owners: Enables the administrator to review and authorize or deauthorize registered data owners.

Authorize Data Users: Permits the administrator to review and authorize or deauthorize registered data users.

Send Keys: Allows the administrator to securely send decryption keys to data users via email for file access.

Logout: Provides the option for the cloud administrator to securely log out from the platform.

4. Methodology

Quantum-Based Encryption Algorithm: In order to produce cryptographic keys and carry out encryption and decryption procedures, this quantum-based encryption method makes use of the special capabilities of quantum computing. In order to produce truly random keys that are needed to encrypt and decode sensitive data, it makes use of fundamental quantum processes such as the Hadamard gate, which produces superposition states. Combining quantum randomness with traditional cryptography methods provides a safe and effective way to safeguard data.

Quantum Key Generation: The central feature of this algorithm is the creation of a random cryptographic key using a quantum circuit. The create_random_key function generates this key by applying Hadamard gates on each qubit in the quantum circuit. The Hadamard gate is a key operation in quantum computing that puts the qubit in a superposition of states, resulting in a more randomized output. After applying the Hadamard gates, the circuit measures the states of the qubits. These measurements yield a random binary string, which becomes the cryptographic key. Quantum randomness ensures that the key is unpredictable and difficult for any adversary to replicate without access to the quantum system itself.

Text to Binary Conversion: The Text_to_Binary function converts the text to be encrypted into a binary representation. This binary data is needed for the XOR-based encryption and decryption process. Each character in the text is converted into its ASCII value, which is then represented as an 8-bit binary string.

Encryption: The encrypt_text function employs a bitwise XOR (exclusive OR) operation between

the binary representation of the text and the quantum-generated key. XOR encryption is a simple yet effective method for scrambling data. In this case, the binary text is encrypted by iterating over each bit and performing XOR with the corresponding bit from the key. If the key is shorter than the text, it wraps around and repeats the key. This results in an encrypted binary string, which is the ciphertext.

Decryption: The decrypt_text function reverses the encryption process by applying the XOR operation again. XOR is a symmetric operation, meaning that the same key used for encryption can also decrypt the data. The encrypted binary string is XORed with the same key to recover the original binary text, which is then converted back to the original text using the binary_to_text function.

Advantages of Quantum Key Generation

Quantum Randomness: One of the key strengths of this algorithm lies in the quantum-generated key. Traditional random number generators (RNGs) rely on algorithms and can, in theory, be predicted if an attacker has enough computational power. However, quantum randomness is fundamentally different: it is governed by the principles of quantum mechanics, making it truly unpredictable and much more secure. This randomness ensures that each key generated by the quantum system is unique and cannot be replicated.

Security: The encryption method used here—XOR—may be simple in concept but provides effective security when combined with quantum-generated keys. The key space is large enough to make brute-force attacks impractical, especially when the key is randomly generated by a quantum system. The randomness introduced by quantum mechanics significantly reduces the likelihood of an adversary being able to guess or recreate the key.

Efficiency: The use of quantum gates like the Hadamard gate makes key generation relatively fast, and because the XOR encryption process is computationally light, it can be implemented in systems where efficiency is crucial. The encryption and decryption processes can be performed quickly, even with large data sets.

Quantum vs Classical Encryption

While classical encryption techniques like AES and RSA have served as the foundation for modern cryptography, they are increasingly under threat due to advances in quantum computing. Specifically, quantum computers have the potential to break widely used encryption methods by efficiently solving problems like factoring large numbers (as seen with Shor's algorithm) or searching unsorted databases (via Grover's algorithm). This algorithm, by utilizing quantum key generation, is designed to be resistant to such quantum attacks. The encryption method (XOR) in this context is not new, but the key used for encryption is what makes this system unique and quantum-secure.

Use Cases in the Quantum Computing Era

Cloud Security: With sensitive data being increasingly stored and processed in the cloud, securing this data is paramount. By adopting quantum-enhanced encryption methods, cloud service providers can offer higher levels of security, ensuring that even in a post-quantum world, their data remains protected.

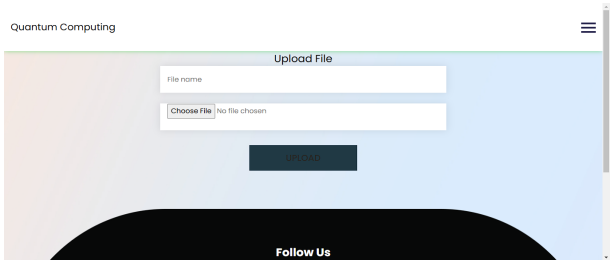
Private Communications: As quantum technologies continue to develop, the need for quantum-safe communication protocols will become critical. This encryption scheme can be used for secure messaging platforms, private communications, and other forms of secure data transfer, ensuring that information cannot be intercepted or decrypted without the appropriate key.

Quantum Cryptography Networks: In the long run, quantum networks may be built to facilitate the exchange of quantum keys, which are inherently more secure than classical ones. This encryption method could play a role in the initial development of such networks, making it a step toward quantum-safe cryptography systems.

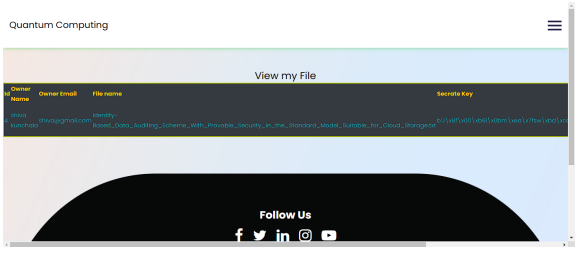
5. Results and Discussion

These are the results of Architecture of Advancing Cloud Data Protection with Cryptographic Algorithm

Uploading Files: Here data owner can upload files into website.

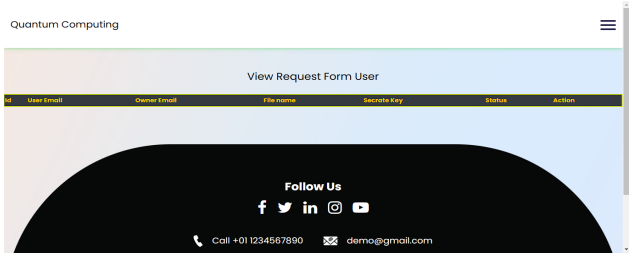


View Uploaded Files: Here data owner can view the uploaded files.

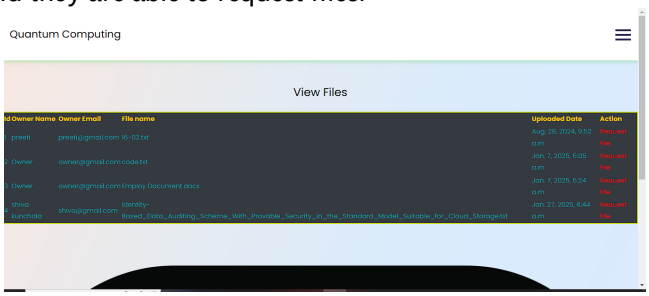


View Requests from Users: Here data owner can view the file requests of users.

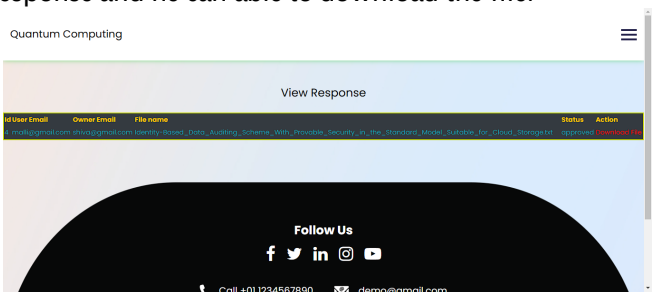
Vol. 2, Issue 2, 2025, https://doi.org/10.63328/IJCSER-V2RI2P2



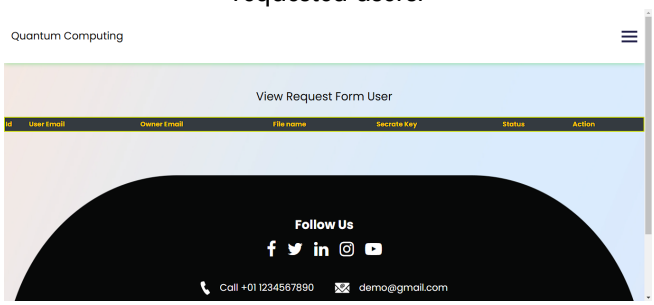
View Files: Here data user can view the uploaded files and they are able to request files.



View Responses: Here data user can view the Request Response and he can able to download the file.



Sending Key to the User: Here cloud can send the keys to requested users.



6. Conclusion and Future Work

The integration of quantum computing algorithms into cloud data encryption represents a significant advancement in cyber security. By leveraging principles such as quantum key distribution and quantum-safe cryptography, this approach addresses the vulnerabilities inherent in classical encryption methods, particularly against emerging quantum threats. Implementing these quantum algorithms enhances data protection, ensuring that sensitive information remains secure even as quantum technologies evolve. As quantum computing continues to develop, adopting quantum-resistant encryption standards becomes imperative for organizations aiming to safeguard their data against future risks. This proactive strategy not only fortifies current security measures but also future-proofs data protection frameworks, maintaining the confidentiality and integrity of information in an increasingly complex digital landscape.

As quantum computing advances, enhancing cloud data encryption becomes imperative to counter emerging threats. Future developments will focus on integrating quantum-resistant algorithms, such as lattice-based and code-based cryptography, to safeguard data against quantum attacks. Implementing Quantum Key Distribution (QKD) will further secure key exchanges by detecting eavesdropping attempts through quantum mechanics principles. Additionally, advancements in homomorphic encryption will enable computations on encrypted data without decryption, preserving confidentiality during processing. Continuous research into optimizing these algorithms for performance and scalability will ensure robust protection of sensitive information in cloud environments, maintaining data integrity and privacy in the quantum era.

Declaration

Conflicts of Interest: The authors declare no conflict of interest.
Author contribution: All authors wrote the main manuscript text and also consent to the submission
Ethical approval: Not applicable.
Consent to Participate: All authors consent to participate.
Funding: Not applicable, and No funding was received
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Personal Statement: We Declare with our best of Knowledge that this research work is purely Original Work and No third party material Not used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

References

[1]. R. Lu, X. Yuan, and X. Lin, "Homomorphic Encryption for Cloud Computing: An Overview," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2381-2405, 2021.
[2]. J. Shen, J. Niu, J. Cao, and Y. Mei, "A Survey on Cloud Security Issues and Techniques: Cryptographic and Non-Cryptographic Approaches," IEEE Transactions on Services Computing, vol. 13, no. 3, pp. 434-451, 2020.
[3]. Kong, J. Wang, and Q. Ni, "Efficient Data Security and Privacy-Preserving Scheme in Cloud Computing," IEEE Access, vol. 10, pp. 24356-24367, 2022.
[4]. M. S. Ali, K. K. R. Choo, and S. H. Ahmed, "Blockchain-Based Secure Data Storage and Access Control for Cloud Applications," IEEE Transactions on

Cloud Computing, vol. 9, no. 3, pp. 1215-1226, 2021.
[5]. V. S. Pendyala, S. M. Arafath, and S. R. Kulkarni, "Elliptic Curve Cryptography for Real-Time Data Encryption in IoT and Cloud Computing," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3615-3623, 2021.
[6]. K. Khan and R. Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptography," International Journal of Computing and Communication Networks, vol. 1, no. 1, pp. 46-52, 2019.
[7]. V. S. Miller, "Use of Elliptic Curves in Cryptography," in Conference on the Theory and Application of Cryptographic Techniques, 1985, pp. 417-426.
[8]. M. - Q. Hong, P. - Y. Wang, and W. - B. Zhao, "Homomorphic Encryption Plan In view of Elliptic Bend Cryptography for Security Assurance of Distributed computing," in IEEE second Global Meeting on Huge Information Security on Cloud (BigDataSecurity), Superior Execution and Brilliant Figuring (HPSC), and Savvy Information and Security (IDS), 2016, pp. 152-157.Chhabra and S. Arora, "An Elliptic Curve Cryptography Based Encryption Scheme for Securing the Cloud Against Eavesdropping Attacks," in IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), 2017, pp. 243-246.
[9]. T. Banerjee and M. A. Hasan, "Energy Productivity Examination of Elliptic Bend Based Cryptosystems," in seventeenth IEEE Worldwide Meeting on Trust, Security and Protection in Processing and Correspondences (TrustCom/BigDataSE), 2018, pp. 1579-1583.G. Wang and Z. Zong, "A Secure Data Sharing and Privacy-Preserving Scheme Based on Blockchain in Cloud Computing," Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, pp. 79-94, 2021.
[10]. M. S. Siddiqui, M. M. Rashid, and S. S. K. Iqbal, "Post-Quantum Cryptography: Securing Cloud Data from Quantum Threats," Future Generation Computer Systems, vol. 122, pp. 76-88, 2021.
[11]. M. Xu, D. Zhang, and X. Zhou, "A Lightweight Cloud Data Encryption Scheme for Data Privacy Protection," IEEE Access, vol. 8, pp. 151315-151325, 2020.
[12]. X. Zhang, L. Li, and W. Li, "A Survey on Cloud Storage Security: Techniques and Applications," in IEEE 9th International Conference on Cloud Computing, 2019, pp. 122-128.
[13]. M. Albrecht, "Quantum-Resistant Cryptography in Cloud Environments," in ACM International Conference on Security and Privacy, 2021, pp. 211-220.
[14]. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
[15]. L. Luo and H. Li, "Cloud Computing Security Issues and Challenges: A Survey," International Journal of Computer Applications, vol. 43, no. 9, pp. 1-5, 2012.
[16]. H. Zhang, C. Wang, and F. L. Lewis, "An Efficient and Secure Data Sharing Scheme in Cloud Computing," International Journal of Communication Systems, vol. 33, no. 3, pp. e4464, 2020.
[17]. L. Wang, L. Xie, and L. Xu, "Privacy-Preserving Cloud Data Access Control Based on Attribute-Based Encryption," IEEE Transactions on Cloud Computing, vol. 6, no. 3, pp. 637-646, 2018.
[18]. D. R. S. C. R. P. Kumar, "Cloud Data Security and Privacy Using Multi-Level Encryption Mechanism," Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, pp. 110-118, 2020.
[19]. M. A. Hashem, A. S. A. Rehman, and Z. I. Alqaralleh, "Cloud Computing Security and Privacy Challenges: A Survey," Future Generation Computer Systems, vol. 89, pp. 535-545, 2018.
[20]. T. K. Shanmugam, K. L. P. Nair, and R. S. G. Dinesh, "Security and Privacy in Cloud Computing: A Survey," International Journal of Advanced Computer Science and Applications, vol. 8, no. 4, pp. 404-409, 2017.
[21]. R. Lee, S. L. Liu, and W. L. Yang, "Design and Implementation of a Privacy-Preserving Cloud Storage System," Journal of Cloud Computing: Advances, Systems and Applications, vol. 10, pp. 45-58, 2021.
[22]. B. Liu and X. Li, "Towards Secure Cloud Storage: A Survey of Cryptographic Techniques," in IEEE 3rd International Conference on Computing, Communications and Networking, 2020, pp. 305-310.
[23]. X. Wang, D. Li, and L. Zhang, "Cloud Data Encryption with Identity-Based Cryptography," Journal of Computing and Security, vol. 29, no. 4, pp. 736-748, 2020.

Author's Profiles

V Sujana earned her B. Tech. in 2015 from Mother Theresa Institute of Engineering and Technology, Palamaner, currently she is pursuing the M.Tech in the Department of CSE in VEMU Institute of Technology, Chittoor.

N Bindhu Madhavi earned her B. Tech. in 2016 from Siddartha Institute of technology C Gollapalli, Tirupati,M. Tech.in 2021 from Golden Valley Integrated Campus, Angallu, Madanapalli, Currently working as Assistant Professor in Department of CSE, VEMU Institute of Technology, Chittoor and she is having total teaching experience of 5 years.