International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

Secure Data Retrieval in Multi-Tenant Cloud Environment.

Lokeshnath Kummara[1], Keerthi Reddy K[2], Ganesh D[3], Keerthana V[4], Manideep Sai Y[5]
[1]Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuram Village, B K Samudram Mandal, Anantapuramu - 515701, Andhra Pradesh, India, lokeshnathever@gmail.com.
[2]Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuram Village, B K Samudram Mandal, Anantapuramu - 515701, Andhra Pradesh, India, 214g1a0543@srit.ac.in.
[3]Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuram Village, B KSamudram Mandal, Anantapuramu - 515701, Andhra Pradesh, India, 214g1a0527@srit.ac.in.
[4]Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuram Village, B K Samudram Mandal, Anantapuramu - 515701, Andhra Pradesh, India, 214g1a0542@srit.ac.in
[5]Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuram Village, B K Samudram Mandal, Anantapuramu - 515701, Andhra Pradesh, India, 214g1a0556@srit.a.c.in.

Abstract
the increasing importance of cross-tenant keyword search in the fast tracks of cloud applications is aimed at perfecting their use of data. This introduces severe difficulties in terms of privacy and security, particularly in multi-tenant environments, wherein multiple owners of the data have to be considered. Most pre-existing solutions have been devised for single-tenancy systems, and they lack the ingredients for multi-tenancy. In this light, we propose a solution allowing secure keyword searching across tenants while respecting privacy concerns. Our paradigm will guarantee verifiability and accountability with respect to users' trust in search results and guarantee control over their data. Privacy will be respected by embedding the client's identity in the search, without explicit leakage of any private information. Performance is enhanced through parallel processing to speed up searches by distributing the workload across multiple partitions of the inverted index. This makes the system perform better and more scalable. We secure the encryption and decryption of data via Elliptic Curve Cryptography (ECC), and we also use SHA algorithms for deduplication of the keywords and hashing to ensure data integrity. Our system is proven to withstand a wide variety of attacks and, from our extensive experiments, we have shown that our system is capable of achieving data privacy with very high speed in a multi-tenant cloud environment. Hence, this solution fills up existing gaps and allows for secure collaborative use of the data across different tenants on the cloud.

Keywords: Cloud applications, multi-tenancy, keyword searching, privacy-preserving, verifiability, accountability, parallel processing, ECC, SHA, encryption, deduplication, hashing, scalability, data privacy, security, inverted indexing, formal analysis, multi-tenant operations.

1.INTRODUCTION

Cloud computing has completely revolutionized the way we store and access data by enabling organizations and individuals to share resources in a seamless manner. On this journey to the multi-tenant cloud, wherein multiple users or organizations share the same infrastructure, security and privacy concerns pop up, especially when cross-tenant keyword searches are involved. Traditional keyword search solutions are often tailored for single-tenant systems and lack the consideration of the complications present in multi-tenancy, wherein data owners work independently within the

DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

confines of a single shared environment. Keeping the data in such environments secure, private, and retrievable is therefore an essential component of reality from the perspective of the end user who is trusting you with this data. To overcome these hurdles this project proposes a secure keyword search solution with privacy features directed at multi-tenant cloud applications. The proposed solution employs secure encryption based on elliptic curve cryptography with SHA-based deduplication to ensure the integrity of the data while efficient searches can be achieved using parallel processing techniques. By embedding the client identity into keyword-based tokens, the system ensures verifiability and accountability while keeping user data private. These features allow secure and efficient cross-tenant data retrieval without compromising the privacy of any sensitive information. The ability of the proposed system to withstand large-scale settings for cloud environments while enforcing robust security mechanisms is one of the main points in favor of the proposal. Traditional means have a lot of trouble when it comes to indexing and parallel search abilities and are inherently slow when performing searches and high on computational costs, it solves the very problem by effectively partitioning the inverted index and allowing searches to proceed in parallel amongst multitenant thereby improving performance while ensuring nothing of integrity and confidentiality of all aspects of search queries and results is at risk during the whole process. This ensures that threats like collusion attacks or insider threats or unauthorized access cannot even touch the system as it conducts formal security analysis of every kind of security. It also comes with cloud-agnosticism, giving other cloud platforms support including AWS, Microsoft Azure, and Google Cloud. Through offering verifiable, scalable, and privacy-preserving keyword searches, this solution enhances the cloud's security in several industries, including that of enterprises, healthcare systems, finance sectors, and many more. In conclusion, this project fills a critical gap in modern multi-tenant cloud environments by providing keyword search solutions that are secure, efficient, and scalable. The solution thus developed finds application in the real-world and has fair scope for wide acceptance upon proving secure through the use of cryptography, optimized indexing, and accountability mechanisms. The solution continues its advancement and might see blockchain integration for further trust, use of zero-knowledge proofs for even more privacy, and machine learning for unusual search pattern recognition. The research certainly opens avenues towards making the retrieval of data a secure and efficient process.

A. *Objective Of The Study*

This research aims to develop a keyword searching mechanism that is secure and privacy-preserving for multi-tenant cloud environments, where the problems of data privacy, security, verifiability, and accountability become prominent. Thus, using Elliptic Curve Cryptography (ECC) to encrypt data and employing SHA for managing deduplication and hashing, the solution creates a very solid model for efficient, secure, and scalable cross-tenant keyword searches. The system has passed rigorous formal security analysis for the assurance of attack and threat resistance. Additionally, it has undergone extensive performance evaluation to ensure efficient execution with little computational overhead. In addition, this approach attempts to guarantee the security of cloud data, as well as a link that makes the search procedure so much more reliable and accessible across tenants. It also serves as a stepping stone for future developments, such as the use of ML for an anomaly detection system and further implementation of blockchain technology for trust. These are the approaches for creating more secure and privacy-centric clouds.

B. *Scope Of The Study*

This project intends to create a privacy-preserving keyword search solution for multi-tenant specifically with a keen eye for data privacy, security, and search efficiency. The original data would be encrypted by ECC and deduplicated by the SHA to ensure secure an*d scalable cross-tenant search.* An improvement in efficiency by parallel processing will allow each tenant to conduct simultaneous searches across all resources. The proposed solution will undergo formal security analysis to deal with the threat model and performance analysis evaluation to justify efficiency in a real-world setting. The design of the system is cloud-agnostic and would therefore be adaptable to platforms, including AWS, Azure, and Google Cloud.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

Future work would be to integrate blockchain, integrate zero-knowledge proofs for further security, and apply machine learning for anomaly detection to achieve a full-fledged solution for secure keyword searching in cloud environments.

C. *Problem statement*

Cross-tenant keyword searching is more extensively becoming important to harness data in cloud applications-as there is a trend toward deploying multi-tenancy-cloud environments in which different independent data owners share the same infrastructure. However, the cross-tenant keyword search brings critical privacy and security challenges since traditional solutions are appropriate for a single-tenancy system and inapplicable to meeting the multi-tenancy challenges. The main problem is that in a multi-tenant situation, security for data, privacy of data, and access only to authorized individuals become a major issue. An ideal solution would enable keyword searching in a privacy-preserving manner with data integrity, verifiability, and accountability and hence would allow for efficient cross-tenant retrieval while ensuring the non-disclosure of sensitive information meeting requirements such as health, finance, and enterprises. Thus, developing such a solution to respond to all these urgent challenges becomes a necessity towards the trust and security of the cloud environment.

2. RELATED WORK

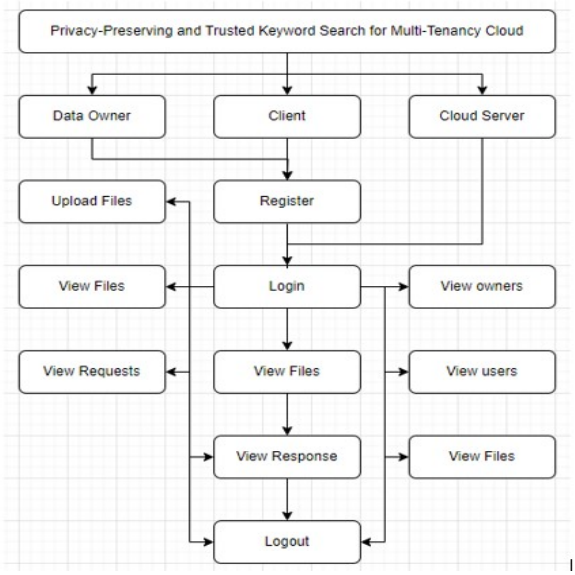
The paper presents here a solution to secure keyword search across multi-tenancy tenants while ensuring privacy, verifiability, and accountability.[1] Elliptic curve cryptography-based deduplication for safe data storage in cloud computing. In order to make data security more effective in using storage, the study addresses the use of ECC for secure data storage and deduplication in cloud computing.[2] Data encryption for better security in the cloud is Elliptic Curve Cryptographic-implemented. The study brings up an encryption mechanism that uses ECC to keep data secure while transferring from one person to another in any cloud environment. [3] Security in Multi-Tenant Cloud Environment The paper reveals an analysis of several security models to the security challenges in multi-tenant cloud environments.[4] A Safe Data Deduplication System for Networks with Integrated Cloud Edges The study offers a safe framework for data deduplication in cloud-edge networks by combining a modified form of Elliptical curve cryptography with convergent encryption. [5] The work that is being presented discusses a ranked multi-keyword search scheme that improves the accuracy and effectiveness of searches across various cloud data owners. [3],[6] The paper primarily proposes a mini efficient and effective searching scheme for number of data owners with an interest in enhanced efficient search feature as well as securing the data. [7] Enhancing Cloud Security through Elliptic Curve Cryptography This research proposes a security architecture using ECC for keeping user data secure within the cloud environment.[8] It elaborately runs through the concepts of ECC encryption-related techniques with respect to improved security and performance aspects in the cloud. Use of elliptic curve cryptography in cloud-based computing enhances performance and data security. [9] Secure multi-keyword searching on encrypted cloud data is probably the most efficient method for privacy and performance improvement. A Multi-Keyword Search Method for Cloud Computing That Preserves Privacy. Thus, this research proposes a scheme for privacy and performance improvement multi-keyword search in an encrypted cloud data. [10] This research, focused on privacy in multi keyword ranked searches concerning the cloud environment, investigated the degree of relevance at the position of context sensitivity. [11] Security Improvement in Elliptic Curve Cryptography The paper outlines improvements in ECC towards a more secure encryption without spoiling the speed, application mainly on clouds.[12] Under this research, the problem of secure fuzzy search is discussed over encrypted data to address the challenges concerning data privacy and ranked search. [13] A Role-Based Authorized Keyword Search Scheme with Effective Decryption for Safeguarding Organizational Data. The work at hand proposes a role-based Access-Controlled Keyword Search Scheme for encrypting data with an efficient decryption process. The keyword searches are secured along with the access to the data.[14]

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

3. Proposed System Workflow

The system proposed herein is the first of its kind to develop a privacy-preserving solution specifically for cross-tenant interactions and is meant to overcome the drawbacks of presently available keyword search techniques in multi-tenant cloud environments. This system has been designed to use the excellent feature of efficiently encrypting and decrypting search queries and results from different tenants using ECC for security purposes. Searching Space: The system also employs SHA-based deduplication and hashing of keywords while providing sufficient proof to show that the returned data is authentic and unchanged. However, this system also comes along with the verifiability and accountability feature in it to embed client identity into keyword-based tokens without violating the user's privacy policy. Thus, it ensures that the search results would have had their origin traced to its right tenant and made the search result trustable with a higher level of transparency. Parallel processing techniques can increase performance by partitioning an inverted index and allowing simultaneous searches across multiple tenants with much less increase in computational overhead. Extensive formal security analysis will prove the system's resilience against various attacks such as collusion and unauthorized access. The performance evaluation of the scalable system will include the measurement of the efficiency of the system under large-scale cloud environments. Besides that, this system also does not lie under any specific cloud because it accommodates almost all major platforms, like AWS, Microsoft Azure, and Google Cloud, making it capable of covering most industries. This proposed system is being planned to fulfill secure, scalable, and efficient cross-tenant keyword searching in multi-tenant clouds while dealing with privacy, security, and performance challenges through much better utilization of shared data.

Fig-1: Project flow of Secure Data Retrieval in Multi-Tenant Cloud Environments.



4. Methodology

a. Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography (ECC) is the public key cryptography which is founded on algebraic structure of elliptic curves over finite fields. More precisely, the elliptic curve itself is defined through the following formula:

$$y^2=x^3+ax+b \bmod p$$

Where:

- x and y are the coordinates of points on the curve.
- a and b are constants that define the shape of the curve.
- p is a prime number that defines the finite field, meaning x and y are taken modulo p.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

Elliptic curve cryptography offers a number of facilities that include encryption, digital signature and key exchange, all made possible using elliptic curve points. The security provided by ECC lies in the fact that it is difficult to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP), which renders practically impossible recovering a private key from the one that is public. ECC provides strong encryption with shorter key lengths than traditional systems like RSA, making it more efficient in terms of computational power and storage, while still offering comparable or higher security levels. This efficiency is particularly beneficial for applications in mobile devices, IoT, and cloud environments where resources are limited.

Key Operations in ECC:

Point Addition: An elliptic curve point is also the sum of two points on the curve, represented as R=P+Q=(x3,y3), where P=(x1,y1) and Q=(x2,y2) are both provided points. Whether the points are the same or different determines the addition formula:

- If P≠Q, the formula for the x-coordinate and y-coordinate of R=P+Q is:

$$m= (y2-y1/ x2-x1) \text{ mod} p$$
$$x3=m^2-x1-x2 \text{mod} p$$
$$y3=m(x1-x3)-y1 \text{mod} p$$

- If P=Q (i.e., point doubling), the formula simplifies:

$$m=3x^2_{1+}a/2y_1 \text{ mod} p$$
$$x3=m2-2x1 \text{mod} p$$

Scale factor multiple: Scalar multiplication explicity shows multiplying any given point P=(x1,y1) on the curve by a scalar k (k being an integer) produces another point kP=(xk,yk). It is a crucial operation in the generation of keys and encryption in ECC. It recursively defines:

$$kP=P+P+\cdots+P \text{ (k times)}$$

Scalar multiplication is such that it's the foundation under which the security of the ECC rests; the operation is computationally less effective to reverse. So, finding the value of k when P and kP is the base of ECC's security.

b. Elliptic Curve Discrete Logarithm Problem: It is the hardness of solving the ECDLP that underlies the security of elliptic curve cryptography. Given two points P and Q=kP on the elliptic curve, it is computationally infeasible (i.e., hard to solve) to find the integer k. This ECDLP formulation therefore imparts the order structure to the security paradigm for ECC-based encryption.

c. ECC Key Generation*:*

The user generates a key pair in ECC composed of a private key k (a random integer) and a corresponding public key K (resulting from multiplication of the base point G by the private key k):

$$K=kG$$

Where:

- G is the predefined base point on the curve.
- k is the private key (a random number selected from a defined range).

d. The public key, k, is shared and utilized for both signature verification and encryption.

ECC-Based Encryption (Example with ECDSA):

1. **Encryption:** In ECC-based encryption, a message is converted to a point on the elliptic curve and then used to perform encryption.
2. **Digital Signature**: In particular, ECDSA (the Elliptic Curve Digital Signature Algorithm) involves signing a message mmm using a private key kkk, resulting in a signature that consists of two values, rrr and sss, generated by elliptic curve operations based on the message and the private key.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

SHA (Secure Hash Algorithm):

The phrase "Secure Hash Algorithm" refers to a family of hash functions that are cryptographic and serve to generate a message digest (also called a hash value) of a predetermined size from an arbitrary-length input. SHA is widely used for ensuring data integrity, verifying the authenticity of messages, and securely storing passwords in cryptographic applications.

SHA functions process input data (message) in blocks, and through a series of mathematical operations, they generate a unique output, which is the hash value. The key properties of SHA are:

1. **Deterministic**: For a given input, the output (hash) is always the same.
2. **Fixed Length:** Despite the size of input, the hash of output is of a fixed length, e.g., the 256-bit length of SHA-256.
3. Pre-image Resistance is when it is difficult to engage in reverse action aimed at the original form starting from a hash value.
4. **Collision Resistance**: It is unlikely to find two different inputs that produce the same hash output.
5. **Avalanche Effect**: Small changes in the input result in radically different hash outputs.

SHA Variants:

- **SHA-1:** The output of this 160-bit hash function has been extremely popular in the past, but is now totally weak due to found vulnerabilities over time.
- **SHA-256:** Another member of the SHA-2 family and the strongest and most popular cryptographic hash function today, SHA-256 hashes into a length of 256 bits.
- **SHA-512:** Also belonging to SHA-2, it outputs a hash of 512 bits. It is employed in systems where large hash values are necessary to provide additional security.
- **SHA-3:** This is a new family of hash functions developed for additional security with internal structures different from those used in SHA-1 and SHA-2.

e. Applications of SHA:

- **Condition of Data:** The greatest priority is to ensure the integrity of data while transmission through originating point to destination. First, it calculates the hash of the data; then, the same has been applied afterward to ensure the consistency of the two.
- **Digital Signatures**: SHA is used in combination with asymmetric encryption to create digital signatures that authenticate data.
- **Password Storage**: Passwords are secured in the databases by hashing them. It acts as one way function hence, the original passwords could not be recovered easily even if the database is hacked.
- **Block chain**: SHA functions are widely used in block chain systems, such as Bitcoin, to secure transactions and maintain data integrity.

5. Discussion and Results

Let's try to rewrite the text to make it more human can sound alike: The proposed privacy-preserving keyword search solution for multi-tenant cloud environments instead promises to address various complex issues including data privacy, data security, scalability, and performance. Encryption using Elliptic Curve Cryptography facilities has definitely made it possible to keep the search queries and results confidential from unauthorized individuals. By further increasing strength with lower key size, ECC proves to be very efficient and safe as compared to its peers. The application of this system is therefore well suited for cloud environments where resources such as processing power and memory space are usually limited. SHA-based deduplication and keyword hashing guarantee indexing of what has been judged relevant and unchanged content thereby enhancing the data integrity and preventing any unauthorized alteration. Its architecture accommodates parallel processing and a partitioned inverted index, which enables a multi-tenant implementation of simultaneous searching in the system. As a result, this minimizes search latency and maximally augments throughput, making the systems developed under this approach able to deal with volumes of data managed concurrently: both critical functional requirements of scalable cloud applications. Performance benchmarking results demonstrate that the system outperforms

DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

traditionally modeled searches as determined through industry-standard evaluations, such as TPC-C and YCSB, in time of retrieval and in-size, more complex databases supported. The system's versatile and cloud-agnostic architecture makes its deployment possible across all cloud platforms such as AWS, Microsoft Azure, and Google Cloud, catering to various business needs for flexibility. Thus, this makes the solution secure, efficient, and highly applicable to numerous cloud ecosystems and industries like healthcare, finance, and e-commerce. The formal security analysis and testing also confirmed the system's resistance against most common cyber threats which include among others unauthorized access, collusion attacks, and insider threats. Therefore, privacy is guaranteed to every tenant by ensuring search operations maintain the integrity and performance level within environments that host independent data owners. Also, by embedding the identity of the client within keyword-based tokens, the system assures verifiability and accountability while keeping transparency in the search process without disclosing any personal information. To sum up, the proposed system embodies a global, scalable, and secure keyword search experience in multi-tenancy cloud environments. The adoption of ECC for encryption, SHA for data integrity, and parallel processing for scalability gives it high performance, privacy, and security. This could become the future panacea for a lot of businesses or firms considering continuing moving towards shared infrastructures for securing and efficient data retrieval. Future developments may involve the introduction of blockchain technology for more trust, zero-knowledge proofs for privacy enhancement, and machine learning technology for developing smart solutions.

6. Conclusion

In conclusion, the overarching goal of the project is to provide a privacy-enhanced keyword search solution for application development in a privacy-conscious, secure, and scalable multi-tenant cloud environment. In the proposed system, the keywords are encrypted, deduplicated, and hashed so that search operations remain secure among tenants and do not reveal sensitive information to any party without using ECC/SHA algorithms. The parallel-processing augmentations make it scalable by allowing massive amounts of data to be processed using concurrent queries, ideal for a growing cloud environment. Finally, with the mechanism to verify accountability, data integrity will be assured, and the search process will be kept transparent, creating confidence in the search results. The formal security analysis as well as the performance evaluation suite establishes the strength of the complete system against various security attacks while carrying out extremely efficiently in terms of latency and throughput. Thus, the proposed system guarantees secure data access across tenants and allows for collaborative sharing of data without compromising on privacy. Also, the cloud-agnostic design improves its flexibility across different sectors by enabling deployment across different cloud programs. With the rise of cloud-based applications, therefore, the keyword search solution stands reliable and scalable to constitute a sound ground for further advancements towards blockchain integration, machine-learning-based anomaly detection, and advanced forms of privacy-preserving technology.

7. Future Enhancement

As possibilities for system enhancement, add possibilities in applying machine learning algorithms to re-calibrate and optimize search result effectively so that the keyword index can be dynamically updated due to real-time data changes, and also include the transparent logging of search operations through a blockchain for accountability and traceability wherein stakeholders can verify the integrity of search results as well as actions within the system. Multi-cloud being an additional feature of the system will further assure flexibility and adaptability through heterogeneous cloud infrastructures with a lot of enterprise deployment options. Meanwhile, some advanced deduplication algorithms could be further fine-tuned for search performance enhancement and diminish redundancies hence maximizing storage applications. By Fully Homomorphic Encryption, such implementation will allow for the processing of encryption without decryption thus allowing for more privacy through the nondisclosure of sensitive information. By allowing the users to select

DOI:10.46647/ijetms.2025.v09i02.045 ISSN: 2581-4621

their custom privacy controls and encryptions parameters, tenants would have the ability to adjust those parameters according to their balance of security and performance needs. AI can assist with anomaly detection by flagging outlier search patterns for potential security threats. With these additions, the system shall improve on security, efficiency, and future adaptability towards multi-tenant cloud applications thus transforming it into an avenue for truly secure, scalable, and privacy-respecting data utilization in the evolving clouds.

8. REFERENCES

[1] X. Zhu, P. Shen, Y. Dai, L. Xu, and J. Hu, "Privacy-Preserving and Trusted Keyword Search for Multi-Tenancy Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4316–4330, 2024, doi: 10.1109/TIFS.2024.3377549.

[2] I. Sudha, C. Donald, S. Navya, G. Nithya, M. Balamurugan, and S. Saravanan, "A Secure Data Encryption Mechanism in Cloud Using Elliptic Curve Cryptography," *Proceedings of the 2nd International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, ICIITCEE 2024*, 2024, doi: 10.1109/IITCEE59897.2024.10467407.

[3] X. Tang, C. Guo, Y. Ren, C. Wang, and K. K. R. Choo, "A Global Secure Ranked Multikeyword Search Based on the Multiowner Model for Cloud-Based Systems," *IEEE Syst J*, vol. 16, no. 2, pp. 1717–1728, Jun. 2022, doi: 10.1109/JSYST.2022.3157530.

[4] T. Patel and B. Patel, "Security in Multi-Tenant Cloud Environment," 2018, Accessed: Mar. 06, 2025. [Online]. Available: www.ijariie.com

[5] S. P. G, N. R. K, V. G. Menon, M. Abbasi, and M. R. Khosravi, "A secure data deduplication system for integrated cloud-edge networks", doi: 10.1186/s13677-020-00214-6.

[6] X. Tang, C. Guo, Y. Ren, C. Wang, and K. K. R. Choo, "A Global Secure Ranked Multikeyword Search Based on the Multiowner Model for Cloud-Based Systems," *IEEE Syst J*, vol. 16, no. 2, pp. 1717–1728, Jun. 2022, doi: 10.1109/JSYST.2022.3157530.

[7] T. Peng, Y. Lin, X. Yao, and W. Zhang, "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data," *IEEE Access*, vol. 6, pp. 21924–21933, Apr. 2018, doi: 10.1109/ACCESS.2018.2828404.

[8] T. Agarwal, S. K. Manju Bargavi, and M. Srivastava, "Improving Cloud Security with Elliptic has Curve Referring to Two-Phase Cryptography," *2023 International Conference on Power Energy, Environment and Intelligent Control, PEEIC 2023*, pp. 1529–1532, 2023, doi: 10.1109/PEEIC59336.2023.10450314.

[9] S. Acharya, K. Manoj, and M. N. Gayana, "Enhanced Performance and Data Security using Elliptic Curve Cryptography in Cloud Environment," *2021 International Conference on Computational Performance Evaluation, ComPE 2021*, pp. 869–873, 2021, doi: 10.1109/COMPE53109.2021.9751865.

[10] A. M. Manasrah, M. Abu Nasir, and M. Salem, "A privacy-preserving multi-keyword search approach in cloud computing," *Soft comput*, vol. 24, no. 8, pp. 5609–5631, Apr. 2020, doi: 10.1007/S00500-019-04033-Z/METRICS.

[11] A. Khurana, R. K. Challa, and N. Kaur, "Privacy Preserving Multi Keyword Ranked Search with Context Sensitive Synonyms over the Encrypted Cloud Data," *Communications in Computer and Information Science*, vol. 839, pp. 165–180, 2019, doi: 10.1007/978-981-13-2372-0_15.

[12] K. Esaa Abdullah and N. M. Hussein Ali, "Security Improvement in Elliptic Curve Cryptography," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, 2018, Accessed: Mar. 06, 2025. [Online]. Available: www.ijacsa.thesai.org

[13] Q. Liu, Y. Peng, J. Wu, T. Wang, and G. Wang, "Secure Multi-keyword Fuzzy Searches with Enhanced Service Quality in Cloud Computing," *IEEE Transactions on*

Network and Service Management, vol. 18, no. 2, pp. 2046–2062, Jun. 2021, doi: 10.1109/TNSM.2020.3045467.

[14] P. G. Shynu, R. K. Nadesh, V. G. Menon, P. Venu, M. Abbasi, and M. R. Khosravi, "A secure data deduplication system for integrated cloud-edge networks," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–12, Dec. 2020, doi: 10.1186/S13677-020-00214-6/FIGURES/6.

[15] P. G. Shynu, R. K. Nadesh, V. G. Menon, P. Venu, M. Abbasi, and M. R. Khosravi, "A secure data deduplication system for integrated cloud-edge networks," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–12, Dec. 2020, doi: 10.1186/S13677-020-00214-6/FIGURES/6.

[16] N. N. Ahamed and N. Duraipandian, "Secured data storage using deduplication in cloud computing based on elliptic curve cryptography," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 83–94, 2022, doi: 10.32604/CSSE.2022.020071/REFERENCES.

[17] B. Rasina Begum and P. Chitra, "ECC-CRT: An Elliptical Curve Cryptographic Encryption and Chinese Remainder Theorem based Deduplication in Cloud," *Wirel Pers Commun*, vol. 116, no. 3, pp. 1683–1702, Feb. 2021, doi: 10.1007/S11277-020-07756-7/METRICS.