IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305433 |

Development of Various Data Access Control Techniques to Enhance Security in Cloud Computing

Anjan Kumar S, Anjum Afsana, Gagana Shree B N, Ganesh Babu Bakale, Prof. Ajay N

U.G. Student, Department of Computer Engineering, Sri Jagadguru Chandrashekaranatha Institue of Technology, Chickballapur, Karnataka, India

Associate Professor, Department of Computer Engineering, Sri Jagadguru Chandrashekaranatha Institue of Technology, Chickballapur, Karnatakat, India

ABSTRACT: With on-demand network access to a shared pool of reconfigurable computing resources including storage, applications, networks, services, etc., cloud computing is a current technology. It offers a variety of services that lower costs and management effort, such as software, platforms, infrastructure, etc. Different access control schemes, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Capability Based Access Control (CBAC), and Attribute Based Access Control (ABAC), are proposed in this paper. The experimental findings demonstrate that the suggested access control strategies, with enhanced performance and decreased computational complexity, more effectively address the problem of privacy and security issues throughout the cloud computing environment. Through these abstractions, security practitioners can create a robust foundation for enhancing data access control techniques in cloud computing, ensuring consistency, scalability, and resilience across diverse cloud environments.

KEYWORDS: MAC,ABAC,CBAC,DAC

I. INTRODUCTION

Cloud computing started a new promising era in the field of information technology, which has a new direction for the use of resources more efficiently with an optimum amount of payment for the service. As it allows the users to use the resources dynamically, according to their requirements from any remote location using the Internet connection. One of the biggest challenges in cloud computing is to provide the security and privacy of data to prevent it from any malicious attack. Security and privacy are thus gaining important consideration which needs to be solved in the cloud system. Users must authenticate themselves before accessing any data or performing transaction to prove it's a valid user for the required service. Many researchers addressed the key cloud security requirements such as confidentiality, authentication, integrity, etc. security is a framework with which an organization Cloud is highly adaptable and cost-effective for data storage and retrieval. In a cloud foundation, sensitive data of a client is kept on topographically scattered cloud stages, under the direct control of the cloud — not of the client. In spite of the advantages that an association appreciates in the wake of embracing distributed computing, there are security issues that are a prominent can direct and screen authorizations, or admittance to their business information by figuring different strategies. Hence, an integrated access control security approach that verifies the access rights to the cloud data while accessing is the primary focus of this research. This research work has the objective of developing a fine-grained efficient and access control policy that allows a reliable and secure exchange of information between different entities of the cloud environment. For achieving fine-grained access control, data confidentiality, integrity along with trust among different entities and efficient access control techniques are applied. Also, an efficient hierarchical access control technique will help in accomplishing reliability, stability, efficient key management and fine-grained protection. For cloud data security and low end-to-end delay, mitigating malicious attacks using third-party auditors is essential.

II. RELATED WORK

Security[1] of data stored in the cloud databases is a challenging and complex issue to be addressed due to the presence of malicious attacks, data breaches and unsecured access points. In the past, many researchers proposed security mechanisms including access control, intrusion detection and prevention models, Encryption based storage methods and key management schemes Cloud computing is used by many of the organizations for storing the huge amount of data on the clouds. Advantage: It introduces the importance of securing data in the cloud and the emerging nature of the cloud computing domain. Remark: While the abstract al introduction to the topic, it lacks specific details about the methodologies, findings, or contributions of the paper.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305433 |

A cloud computing environment[2] provides a cost-effective way for the end user to store and access private data over remote storage using some Internet connection. The user has access to the data anywhere and at any time. Many algorithms and protocols have been developed to maintain the security and integrity of the data using cryptographic algorithms such as the Elliptic Curve Cryptography (ECC). Secured Data Storage and Retrieval using Elliptic Curve Cryptography in Cloud. Security of data stored in the cloud databases is a challenging and complex issue to be addressed due to the presence of malicious attacks, data breaches and unsecured access points. Advantage: The abstract effectively highlights the complexity and importance of addressing security concerns in cloud databases. It acknowledges the presence of malicious attacks, data breaches, and unsecured access points, thereby emphasizing the urgency of the issue. Remark: While the abstract mentions several security mechanisms, it could be further improved by briefly indicating the advancements or innovations introduced by the proposed security measures.

Cloud computing [3] started a new promising era in the field of information technology, which has a new direction for the use of resources more efficiently with an optimum amount of payment for the service. It becomes a centre of attraction for many organizations like academics, healthcare and social organizations etc. Advantage: The abstract provides a clear and positive introduction to the significance of cloud computing in the field of information technology. It emphasizes its promise in terms of efficiency and cost-effectiveness, making it an attractive option for various organizations, including academia, healthcare, and social institutions. Remark: While the abstract effectively introduces the appeal of cloud computing, it lacks specific details about the focus of the paper. Readers may find it useful if the abstract briefly mentions the specific topics, issues, or contributions the paper will address within the context of cloud computing.

This paper [4] discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the - world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have security loopholes in them. Advantage: This abstract effectively addresses the importance of data security in cloud computing and outlines the scope of the paper. It mentions the focus on data protection methods and global approaches, which provides readers with a clear understanding of the paper's objectives. Remark: While the abstract touches on several important aspects of data security in cloud computing, it could be improved by briefly mentioning specific methodologies, technologies, or novel contributions that the paper brings to the field.

III. METHODOLOGY

1. Security: The techniques should be secure and able to protect data from a variety of threats,including unauthorized access, use, disclosure, modification, or destruction.
2. Usability**:** The techniques should be easy to use and manage, even for organizations with limitedresources and expertise.
3. Scalability**:** The techniques should be able to scale to protect large amounts of data in complex anddynamic cloud computing environments.
4. Privacy**:** The techniques should respect the privacy of users and ensure that their data is only usedand accessed in Accordance with their

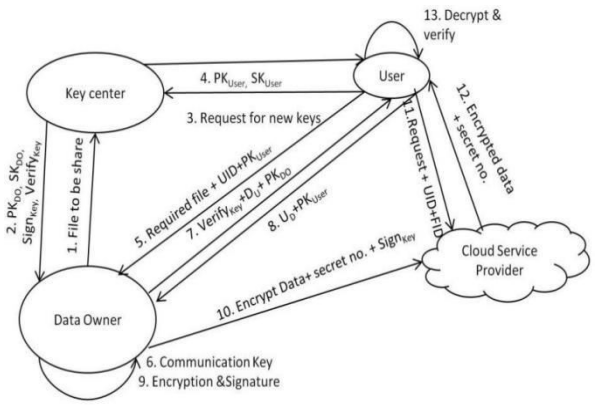


Figure 3.1: Communication among different entities

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305433 |

We aim to new enhanced techniques for security in cloud computing. First, we will study the literature and the real techniques are used for security cloud computing. This will be according to a study for many previous related works with cloud computing security in every possible field (authenticity, integrity and confidentiality). Then will suggest which technique of the cloud which we will work on it , we will suggest the needed standards and circumstances adopt the resulted model in order to have a cloud computing security . The final step will be to develop a sample example for the model and to test it to prove that it is applicable.

A new cryptography-based approach for faster computation and reduced resource consumption using Elliptical Curve Cryptography (ECC) is proposed, as shown in figure 2. An efficient approach for digital signature and verification which increases the speedup compared to other schemes is designed. Four entities are involved in the proposed framework: Data Owner, User, Cloud Service Provider & Key Centre. The complete procedure is divided into five phases: Key Generation, Data Encryption, Data Decryption, Hash code Generation and Hash code Verification.

Performance Evaluation- The designed protocol is compared with the following existing clustering protocols:

- ID-based digital signature scheme on the elliptic curve cryptosystem.
- ID-Based signature scheme using elliptic curve cryptosystem.
- Digital signature protocol based on elliptic curves.

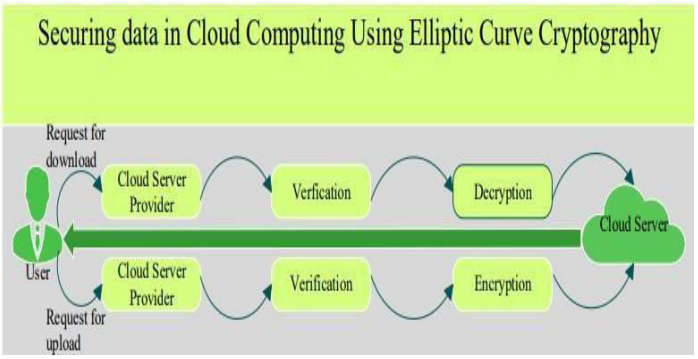


Figure 3.2: Elliptic curve cyrptography

ECC create the most advanced and efficient cryptographic technique over the cloud storage. ECC for encryption, key size is reduced, and performance is increased. ECC uses encryption and decryption key standards to reduce the key size and create the secured key system. ECC is the most appropriate technique to get the data secured from unauthorized use. Once the key size is set, then ciphertext will generate the encryption and decryption of data. The key generated by ECC. The ECC is suitable for the proposed technique at cloud storage to get the secured system.

This helps to reduce the storage size with secure data. Above, in Figure 3, is the block diagram of the proposed algorithm.

IV. EXPERIMENTAL RESULTS

The uniqueness and efficiency of the system by the ECC is enhanced in the different way that many of the data over cloud storage are secured and get the secured connections for the encryption and description of the data. This means that the user can get the original message easily by applying this techniques. Some advantages of ECC over RSA are presented in the following subsection.

ECC is used to ensure the security of the data over cloud storage. The maintenance of the data with reduced key size can help to optimize the storage space as well as get the desired results. It uses the same 3072 bits as the RSA. The most beneficial thing about the ECC is the reduced key size and the encryption of data through a public key, which is in an optimized manner. ECC is more beneficial compared to the RSA for using the latest algorithmic techniques applying to the encryption and decryption of data as well as the accuracy of the decrypted data. It is the widely used strategic algorithm over cloud computing to improve the security rules over cloud storage. The public key is known by rules over cloud storage. The public key is known by every person while the encryption and decryption process can also be done by the public key. Many advantages and key sizes of ECC and AES over RSA are given in the Table below.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

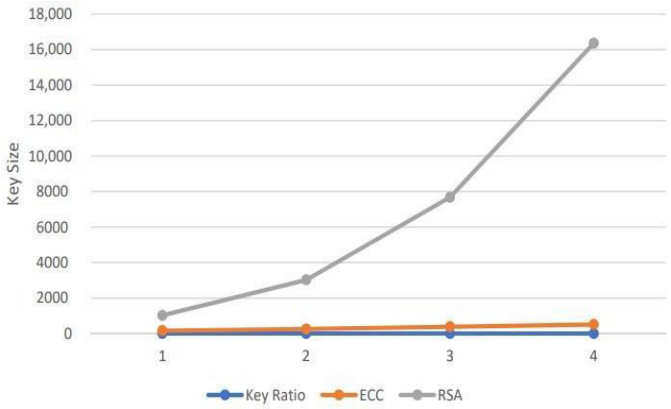
|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305433 |

ECC	RSA	Key Size Comparison
160 bits	1024 bits	1:6 bits
256 bits	3024 bits	1:12 bits
384 bits	7068 bits	1:20 bits
512 bits	16360 bits	1:20 bits

Table 1: ECC over RSA.

Explanation: As you can see in the Table 1 and Figure 4, a medium key size is required for ECC as compared to RSA. Because of this, it provides better security than RSA. ECC also provides better security with a smaller key size as compared to other cryptographic algorithms. It optimizes memory space and reduces computational complexity because of the smaller key size. Thus, by using a medium key size, a high level of data security can obtained.



Graphical representation of key sizes

V. CONCLUSION

IT-related services such as cloud computing provide efficient services regardless of the user's knowledge about technology. Data can be stored, managed, improved, and accessed through a cloud interface provided by third party cloud service providers via the Internet with minimal effort regardless of the location of the user. Cloud services provide many facilities to the user. Users are the people who are using the services depending on the kind of cloud services. Services are provided at low cost as well as being a beneficial thing for so many users to access their data from any place. Cloud services can be made available on any machine as there is no need to take your device along with you. However, the drawback of cloud services is the low data security which may be overcome through special strategies and must be secured. Specifically, for the generation of the key, ECC is used to reduce the complexity of the operations. Due to the low-key size, the enhancement of ECC is much better than other cryptographic techniques.

REFERENCES

1. Mrs. Anjali Sharma , Dr. Garima Sinha[2021]. An Efficient Approach on Data Security with Cloud Computing Environment.
2. Dhasarathan C., Thirumal V., and Ponnurangam D., "A Secure Data Privacy Preservation for onDemand Cloud Service," Journal of King Saud University-Engineering Sciences, vol. 29, no. 4,
3. pp. 144-150, 2017.
4. Dong B., Liu R., and Wang H., "Result Integrity Verification of Outsourced Frequent Itemset Mining," in Proceedings of IFIP Annual Conference on Data and Applications Security and Privacy, Newark, pp. 258-265, 2013.
5. Ge X., Yan L., Zhu J., and Shi W., "PrivacyPreserving Distributed Association Rule Mining based on the Secret Sharing Technique," in Proceedings of the 2nd International Conference on Software Engineering and Data

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305433 |

Mining, Chengdu, pp. 345-350, 2010.

6. Huang C., Lu R., and Choo K., "Secure and Flexible Cloud-Assisted Association Rule Mining over Horizontally Partitioned Databases," Journal of Computer and System Sciences, vol. 89, pp. 51-63, 2017.
7. Kantarcioglu M. and Clifton C., "PrivacyPreserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 9, pp. 1026-1037, 2004.
8. Kavin B., Ganapathy S., Kanimozhi U., and Kannan A., "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA," Wireless Personal Communications, vol. 115, pp. 1107-1135, 2020.
9. Krishnamurthy M., Kannan A., Baskaran R., and Kavitha M., "Cluster based Bit Vector Mining Algorithm for Finding Frequent Item sets in Temporal Databases," Procedia Computer Science, vol. 3, pp. 513-523, 2011.
10. Pradeep Suthanthiramani, Muthurajkumar Sannasy , Ganapathy Sannasi[2021]. Secured Data Storage and Retrieval using Elliptic Curve Cryptography in Cloud.
11. Kaushik, S., and Gandhi, C. "Cloud data security with hybrid symmetric encryption.", [2022] International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. 636-640, IEEE, Mar. 2022. (SCOPUS indexed).
12. J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secure., vol. 1, no. September 2020, pp. 3–22, 2020.
13. Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks (ICCSN), May 2021.p.245-249.
14. Kaushik, S., Gandhi, C. "Trust model in Cloud Computing: A Review", 2021 First International Conference on Recent Trends in Parallel and Distributed Processing Techniques IEEE, Jul. 2021. (SCOPUS indexed).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details