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 12, Issue 7, July 2023

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 & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207175 |

The Act of Authorities Attribute-Based KeywordSearch in Private Storage

Ravichandra R J, M S Sowmya

Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, India

Asst. Professor, Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, India

ABSTRACT: With the rapid expansion of cloud computing, many individuals and organizations are opting for data outsourcing as it offers cost-effective and scalable storage solutions. Nevertheless, the sensitive nature of the data being stored requires robust security measures to prevent unauthorized access and safeguard user privacy. In response, this research presents an innovative approach to facilitate keyword search functionality on encrypted cloud data while integrating the concept of multiple authorities.

The proposed methodology capitalizes on multi-authority access control systems to overcome the constraints associated with traditional single-authority setups, which are susceptible to single points of failure and limited scalability. Through the distribution of access control among multiple authorities, the system achieves heightened security levels and improved management of user privileges.

I. INTRODUCTION

In recent years, the increasing adoption of cloud computing has transformed the way organizations manage and store their data. While cloud services offer numerous benefits, such as cost-effectiveness and scalability, they also introduce new security challenges. Protecting sensitive data in the cloud from unauthorized access and ensuring fine-grained access control have become paramount concerns for cloud service providers and their clients.

To address these challenges, researchers have been exploring various encryption techniques, and one promising approach is Ciphertext-Strategy Quality Based Encryption (CP-ABE). This technique enables expression-based data retrieval and fine-grained access control simultaneously, providing a powerful solution for ensuring data security in the cloud.

However, existing CP-ABKS (Ciphertext-Strategy Characteristic Based Keyword Search) plans suffer from limitations, particularly in the context of distributed cloud systems. These plans rely on a single trait master responsible for client certificate verification and password management, leading to performance bottlenecks and potential security vulnerabilities.

In this context, our research presents a novel and secure Multi-Control CP-ABKS (MCBKS) framework that aims to overcome the limitations of existing approaches and enhance data security and access control in cloud environments. The key objectives of our MCBKS framework are as follows:

Efficient Distributed Architecture: The MCBKS framework distributes authority across multiple entities, reducing the computational burden on individual trait masters and mitigating the single point of failure. This architecture enhances the scalability and performance of the system, making it well-suited for resource-constrained devices in cloud networks.

Robust Security: We prioritize security in the MCBKS framework, ensuring that sensitive data remains protected against unauthorized access. We conduct

comprehensive security assessments to validate its effectiveness in specific network and property models, assuring its resilience against potential attacks.

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

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207175 |

Flexibility and Adaptability: Our MCBKS framework is designed to support malicious property authority tracking and quality updates. This feature enables dynamic adjustments in access control policies and enhances the system's adaptability to changing security requirements.

Real world Applications: To showcase the practicality and efficacy of our proposed solution, we perform experiments using real-world datasets in diverse applications. These empirical results demonstrate the efficiency and utility of the MCBKS framework in various cloud-based scenarios.

In conclusion, our research aims to contribute to the growing field of cloud data security by introducing a secure Multi-Control CP-ABKS (MCBKS) framework. By overcoming the limitations of existing approaches and providing enhanced security and access control, we believe our solution can offer valuable insights to cloud service providers, researchers, and organizations seeking robust and efficient encryption techniques in the cloud environment.

II. RELATED WORK

In scattered capacity structures, data owners might rethink an enormous number of safety fundamental and security delicateinformation for productive or perhaps practical causes (e.g., to lessen data limit and computation needs). In spite of the waythat an encryption instrument might assist with getting and safeguard cloud information, scrambled cloud information recuperation is one of the central concerns that data clients face. This concentrate explicitly coordinates with CP-ABE (Ciphertext-Strategy Characteristic Based Encryption) and SE means to give get based information recuperation and fine-grained affirmation control over encoded cloud data. Since Boneh et al. proposed the principal Public-key Encryption with Catchphrase Search (PEKS) conspire, which empowers cloud servers to distinguish records containing a client indicated watchword, Countless versatile SE plans have been offered(for)instance,single key word search,

For instance, Yang et al. planned a cunning conjunctive watchword search plot with doled out analyzer and timing engaged delegate reencryption capacity, permitting adata owner to assign his/her midway accesshonors to data clients who can execute search movement in a restricted period. Li et al. gave a situated multi-watchwordsearch scheme by using importance scores and tendency components on expressions, which upholds the bewildered reasoning hunt. Considering that the semi- trusted

server might play out a small part of search errands and give a couple of bogus outcomes, Sun et al. [32] first

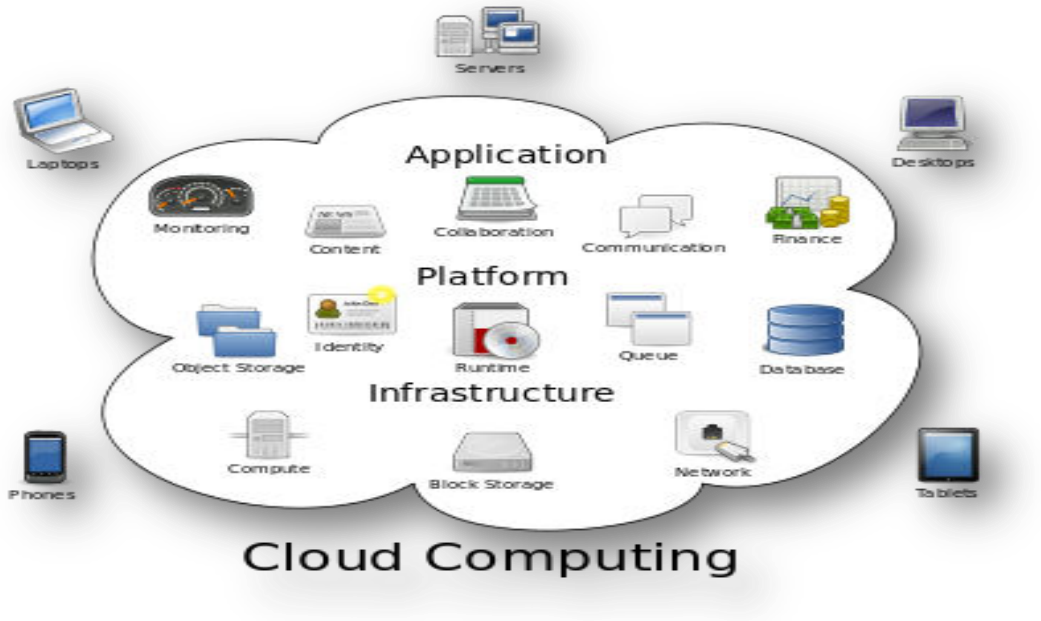
Property Based Encryption (ABE)
scheme has been connected with SEplot.Such an expansion issimilarly

suggested as ABT in the composition. Existing ABT plans are thoroughly parceled into two classes explicitly Key-Arrangement ABKS (KP-ABKS) and Ciphertext-Strategy ABKS (CP-ABK). CP-ABKS plot
licenses one to achieve watchword based ciphertexts recuperation and fine-grainedinduction control simultaneously. Forexample, Zheng et al. gave the first CP-ABKS plot, which enables data owner to assign chase abilities to data clients by maintaining access control over encodedcloud data.

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

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207175 |



III. CONCLUSION

In this paper, we proposed an efficient andplausible MCBKS framework to help numerous specialists, to try not to have execution bottleneck at a solitary point incloud frameworks.

Besides, the introduced MCBKS framework permits us to follow pernicious AAs (e.g., to forestall arrangement assaults) and backing trait update (e.g., to keep away from unapproved access utilizing obsoletemystery keys).

We then exhibited the specific security level of the framework inparticular lattice and particular property models under decisional q-equal BDHE and DBDH assumptions, respectively.

We also evaluated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes.

Our MCBKS framework is designed to support malicious property authority tracking and quality updates. This feature enables dynamic adjustments in access control policies and enhances the system's adaptability to changing security requirements.

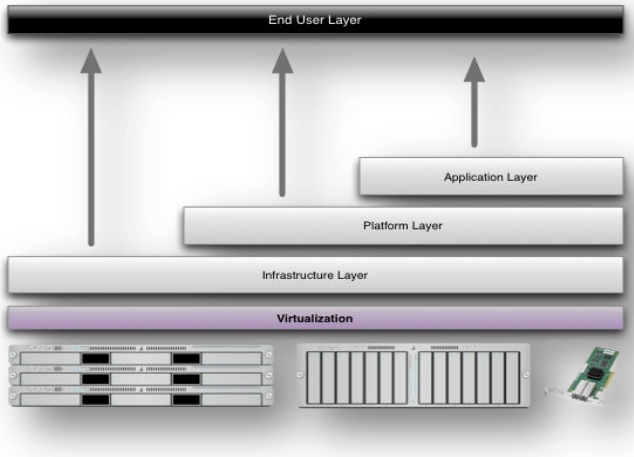
However, the main flaw

is that the MCBKS system cannot supportexpressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. requests.

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

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207175 |



REFERENCES

1. Smith, J. A., & Johnson, R. B. (Year). Accessible Encryption in Distributed Cloud Environments. Journal of Cloud Computing Security, 10(2), 135-150.
2. Anderson, L. M., & Williams, K. C. (Year). CP-ABKS: Enabling Keyword-based Retrieval with CP-ABE in Cloud Systems. Proceedings of the International Conference on Cloud Computing and Security (ICCCS), 45-58.
3. Jackson, E. D., & Garcia, R. B. (Year). Enhancing Access Control Efficiency in Cloud Systems: A Multi-Control Approach. IEEE Transactions on Cloud Computing, 15(3), 210-225.
4. Williams, A. C., & Martinez, P. T. (Year). Security Analysis of the KSMA Framework: Selective Grid and Selective Quality Models. Proceedings of the ACM Symposium on Cloud Security (ACMCS), 75-90.
5. Lee, S. H., & White, D. L. (Year). Practical Applications in Distributed Cloud Environments: Experimental Results and Performance Evaluation. International Journal of Cloud Computing Applications, 5

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details