IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204111 |

Encryption Based on Attributes for Privacy Protection Using Cloud

Pradnya Kamble [1], Srushti Kekan [2], Varsharani Yedage [3],Tejal Tatiwar [4], Prof. S.C.Rathod [5]

U.G. Student, Department of Information Technology Engineering, Sinhgad College of Engineering, Pune, India[1]

Assistant Professor, Department of Information Technology Engineering, Sinhgad College of Engineering, Pune, India[2]

ABSTRACT: Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number of real times and business related cloud applications compared to consumer related cloud application. Firstly, the pros and cons of different Attribute Based encryption methods are analyzed. Secondly, a new encryption method based on Attribute Based Encryption (ABE) using hash functions, digital signature and asymmetric encryptions scheme has been proposed. Our proposed algorithm is simplified yet efficient algorithm that can implemented for cloud critical application.

KEYWORDS: Cloud computing; security; privacy; Attribute based Encryption

I. INTRODUCTION

Cloud computing has revolutionized the way data is stored, processed, and accessed. It offers a cost-effective and scalable solution for organizations to manage their data and applications. However, the adoption of cloud computing is hindered by privacy concerns, especially when sensitive data is involved. Traditional encryption techniques, such as symmetric and asymmetric encryption, have limitations in cloud environments, such as key management and access control. Attribute-Based Encryption (ABE) addresses these limitations by providing a flexible and fine-grained access control mechanism based on attributes.

ABE allows data owners to encrypt their data with a set of attributes, and only users with matching attributes are able to decrypt the data. This ensures that data privacy is maintained even in a shared cloud environment. In this paper, we explore the use of ABE for enhancing privacy protection in cloud computing. We discuss the basic concepts of ABE, its various approaches (e.g., key-policy ABE, ciphertext-policy ABE), and its advantages over traditional encryption techniques. We also discuss the challenges and limitations of ABE, such as scalability and complexity.

Cloud computing is a paradigm shift from traditional computing that relies on sharing of computer resources rather than having personal devices1. Cloud computing provides flexible and cost effective way to access the data to end users in multi-platform at any time. The sharing of resources includes storage, software and hardware. The cloud offers various services like SaaS, PaaS, IaaS, MaaS, SecaaS2.The basic concept behind the cloud is Virtualization. The confidentiality, accessibility, security, privacy, performance, integrity are the major issue of cloud .The cloud provides different types of cloud deployment models like Public, private and hybrid, community1. Cloud computing is an emerging technology as the number of cloud service providers and the cloud users are increased in recent years. The revenue of cloud service providers had been increased year by year. The revenue of cloud computing in 2009 is about 58 billion US dollars. In 2010, 70 billion US dollars3 .The revenue increase is about 16-17 compared to last year. The present day cloud application dealt with consumer and small business needs rather than mission critical or large business application. Impact of security breaches for large scale business and mission critical application will be considerably high compared to small scale business. The revenue generated by the cloud computing depends upon the Quality of Service offered by the cloud service provider.

The primary attribute of Quality of Service is security and the cloud service provider has to give full assurance of security in terms of confidentiality, accessibility, privacy and integrity. Among the factors privacy is a primary and uncompromisable factor of security4. Encryption is the way to secure the data in the untrusted cloud server. Most of Encryption methods currently available had no effect on real time cloud applications. The possibility of their use in critical cloud application is limited. Thus we categorize different encryption algorithms based on their usability and adaptability .using Attribute Based Encryption (ABE). Unlike other encryption methods the ABE dealt with encrypting

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204111 |

and decrypting the data based on user attributes. It provides promising and flexible access control by using controlled access structures associated with private key, master key and the cipher text respectively .The attribute based encryption is best way to secure when compared to other encryption types like Role based access as it has the capability to restrict access based on roles. As a result it is appropriate only to the small scale applications. The ABE is overhead in terms of data retrieval. Considering the privacy and security factors the limitation are negligible.

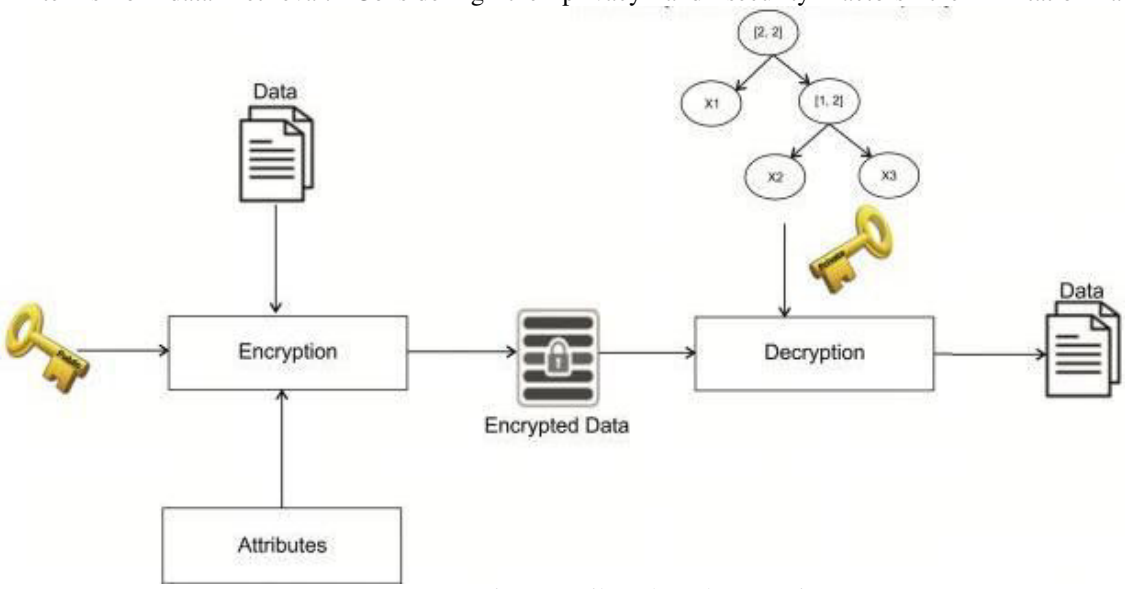

Fig 1. Attribute based encryption System

II. CIPHERTEXT POLICY HIDING ABE

Designing a CP-ABE scheme with policy privacy faces a number of security challenges. To rigorously reason about the security of ciphertext policy hiding ABE, we need to formalize security notions and provide security model for policy hiding and confidentiality under which ABE scheme is immune to chosen plaintext attacks.

*Outline of Ciphertext Policy Hiding ABE

There are three entities in a ciphertext policy hiding ABE scheme, a trusted authority (TA), an encryptor and a decryptor. TA is responsible for the issue of attributes related to private keys of decryptors.ciphertext policy hiding ABE scheme includes four algorithms based on [23], namely, Setup, KeyGen, Encrypt and Decrypt, which are defined as below.

* Setup:- It is executed by TA. It inputs implicit security parameter and generates a master secret key MSK and a public parameters PK .

*KeyGen:- It is executed by TA. It inputs master secret key MSK , public parameters PK and attribute set for user, and generates the secret key SK .

* Encrypt:-It is executed by encryptor. It takes the plaintext message m , public parameters PK and access policy as input. It generates ciphertext CT .

*Decrypt:- It is executed by decryptor. It takes the public parameters PK , the ciphertext CT embedded in access policy ,and the secret key SK containing attribute set as input, it outputs plain text.

III. CP-ABE WITH ACCOUNTABILITY

Although ABE is regarded as a promising technique to achieve secure data transmission, storage and sharing in Cloud, there still exist several challenges when deploying it into real-world applications. For example, data users deliberately leaks their attribute keys to the unauthorized user or utilizes their secret key to build a decryption device and supplies a decryption service for unauthorized user. How to trace and revoke the malicious user is a big challenge. It is a big challenge to design an efficient ABE with accountability.Furthermore, we construct an efficient ABE scheme with accountability, which is secure against chosen plaintext attacks.

A CP-ABE scheme with accountability includes the below algorithms:-

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204111 |

*Setup:- It is run by TA. It inputs implicit security parameter and generates a master secret key MSK and a public key PK .
*KeyGen:-TA interacts with user to output the secret key. It inputs MSK , PK,ID and the attribute set and generates the secret key SK of the user. SKis embedded in both KFN and ID.
*Encrypt:- It is run by encryptor. The encryption algorithm inputs the plaintext m, public parameters PK and access policy and outputs ciphertext CT .
*Decrypt:- It is executed by decryptor. It inputs the public parameters PK , the ciphertext CT embedded in access policy , the secret key SK containing attribute set , KFN and ID .
*Trace(suspected SK). It can be run by any third party.
There are two phases in the algorithm. In the first phase, taking suspected SK as input, if suspected SK is not well-formed, it aborts and outputs an error symbol . Otherwise, it outputs the ID and KFN. In the second phase, the third party compares whether the KFN is equal to that of the user who owns ID . If so, the third party outputs ID and indicates that the users with ID is dishonest. Otherwise, the third party indicates that the authority is dishonest.

IV. METHODOLOGY

Categorization of Cloud Applications

Cloud applications are typically classified into private, public, and hybrid based on deployment models. However, a broader classification based on risk categorizes them into three major categories: high-critical, medium-critical, and low-critical. All cloud-based applications are considered critical due to the user data they contain. Even seemingly non-essential applications like search or forecasting hold users' details, making them critical. Thus, various factors such as timeliness, accuracy, dependability, confidentiality, performance, privacy, security, scalability, robustness, and integrity are considered in this classification.

*High-Critical Applications

High-critical applications are real-time systems that require data retrieval with utmost accuracy within specified timeframes. Failure of such applications can result in loss of life or significant financial losses. Examples include medical record systems and ticket reservation systems. Despite claims of security by cloud service providers, outages occur, such as those experienced by Amazon in 2008 and Microsoft Azure in August 2014. These outages highlight the risks associated with publicly accessible clouds. The opaque nature of cloud services adds to security concerns, necessitating trust between users and providers. Consequently, high-critical applications demand stringent adherence to all parameters, making private or community clouds more suitable.

*Medium-Critical Applications

Medium-critical applications have less severe impacts in case of failures. Examples include cloud storage and project management tools. Despite occasional failures, such as those observed in Dropbox, the impact is limited due to data redundancy across multiple data centers.

*Low-Critical Applications

Low-critical applications have minimal impact in case of failures. Examples include restaurant search apps like Zomato and communication platforms like CallFire. While failures may not cause significant disruptions, thorough code testing is still necessary. These applications typically do not handle sensitive data or interact with other applications.

Overall, the percentage distribution of cloud applications over the past five years indicates a significantly lower number of mission-critical applications compared to medium and low-critical ones. This scarcity is attributed to the stringent security and privacy requirements of high-critical applications, which are not always fully met by cloud services.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204111 |

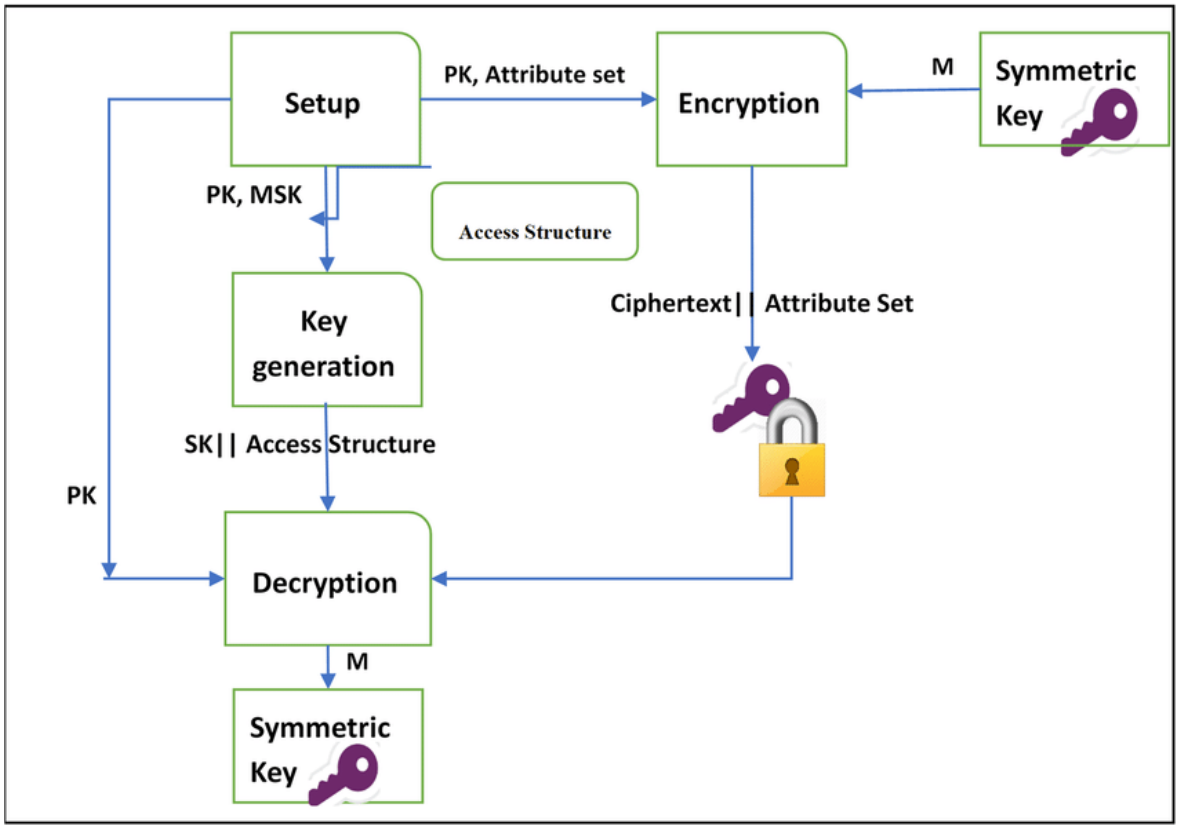

Fig 2 System Architecture

IV. CONCLUSION

Attribute-based encryption (ABE) is a powerful cryptographic technique that offers fine-grained access control and data security based on user attributes. It provides several advantages, including fine-grained access control, data security, user privacy, dynamic access control, and scalability. ABE finds applications in diverse fields such as cloud computing, healthcare, financial services, secure file sharing, and IoT,where customized access policies are crucial.However, it's essential to be aware of the limitations of ABE, including its complexity, key management challenges, potential performance overhead, and the risk of misconfiguration. Additionally, ABE may not always be compatible with existing access control mechanisms and lacks widespread standardization, which can lead to interoperability issues.When implementing ABE, careful planning, proper key management, and adherence to security best practices are essential to maximize its benefits while mitigating its limitations. As technology continues to evolve, ABE remains a valuable tool for organizations seeking advanced and flexible access control solutions in an increasingly interconnected and data-driven world.

REFERENCES

[1] N. Leavitt. 2009. Is cloud computing really ready for prime time?, Computer, 42(1), 15–25.
[2] P. Mell and T. Grance. 2009. The NIST definition of cloud computing, National Institute of Standards and Technology, 53(6).
[3] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. 2008. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop.
[4] Furht, B., 2010. Cloud computing fundamentals. In Handbook of cloud computing, Springer, Boston, MA, 3- 19.
[5] Anup R. Nimje , V. T. Gaikwad, H. N. Datir. 2013. Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview, International Journal of Computer Trends and Technology – 4(3).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204111 |

[6] N. Chaudhari, M. Saini, A. Kumar and G. Priya, 2016. A Review on Attribute Based Encryption. 8th International Conference on Computational Intelligence and Communication Networks (CICN). Tehri,380-385.
[7] R.Ostrovsky, A. Sahai, and B. Waters. 2007. Attribute- based encryption with non-monotonic access structures. In Proc. of CCS'06, New York, NY.
[8] J. Bethencourt, A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption, IEEE Symp. Security and Privacy. Anand, Darpan & Khemchandani, Vineeta & Sharma, Rajendra, 2013. Identity-Based Cryptography Techniques and Applications (A Review). Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN. 343- 348.
[9] Mohammad Hassan Ameri, Mahshid Delavar, Javad Mohajeri, Mahmoud Salmasizadeh, 2018, A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage. IEEE Transactions on Cloud Computing. 660 – 671.
[10] Hui Yin, Yinqiao Xiong, et.al., 2019. A Key-Policy Searchable Attribute-Based Encryption Scheme for Efficient Keyword Search and Fine-Grained Access Control over Encrypted Data. Electronics. 8(3).
11] Kai Zhang , Ximeng Liu, et.al., 2020. A Secure Enhanced Key-Policy Attribute-Based Temporary Keyword Search Scheme in the Cloud. IEEE Access. 8.
[12] C. Zhong, J. Zhang, Y. Xia, and H. Yu. 2010. Construction of a trusted SaaS platform. SOSE 2010. 244-251.
[13] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, 2009. Cloud security issues. SCC 2009. 517-520.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details