An Attribute-based Controlled Collaborative Access Control Scheme for Public Cloud storage (HCS)

Prof. Ankit sanghvi [1] Moiz Khot[2] SwapnilDhane[3] Umesh Lohot[4]
[1,2,3,4]Alamuri Ratnamala Institute of Engineering & Technology, A.S Rao Sapgaon, Shahapur Maharashtra, India

Abstract— A Fine-grained and immediate attribute decision is provided for key update. It uses P-ABE key management protocol which is secure and effective. Our construction is memory efficient as it stores private keys without adding any extra infrastructure. The collaborative mechanism helps it to reduce client decryption overhead by employing a decryption server to execute decryption process. It helps to optimize the clients' user experience since it helps additional tasks like decryption from user, and most of the work is done by the decryption server.

Keywords: Attribute-Based Encryption, Cloud Computing

I. INTRODUCTION

The adoption of cloud computing is increasing rapidly due to the scalability, flexibility, agility, and simplicity it offers to enterprises A recent cross-sectional survey by on the adoption rates of cloud computing by enterprises reported that 76.9% of large enterprises are adopting the cloud, whereas 72.9% of small and medium-sized enterprises (SMEs) are adopting the cloud. Cloud based encryption is important for different applications like business, military, medical and personal users. Everyone wants to know that their information is safe and secure and it is important for businesses to keep client data secure, with certain sectors having more stringent rules about data storage. So, the paper is based on how our cloud encryption works. But cloud computing has introduced security complications because cloud operators store and handle client data outside of the reach of clients' existing security measures. Various companies are designing new cloud encryption protocols tailored to cloud computing in an attempt to effectively balance security and performance. Most cloud computing infrastructures do not provide security against untrusted cloud operators, which poses a challenge for companies and organizations that need to store sensitive, confidential information such as military applications, medical applications, banking, or high-impact business data. As need of cloud computing increases, there are many cloud computing companies and experts who are pursuing cloud cryptography projects in order to address the business demands and challenges relating to cloud encryption. There are various approaches for encrypting cloud data. Many companies choose to encrypt data before uploading it to the cloud. This approach is beneficial because data is encrypted before it leaves the company's environment, and data can only be decrypted by authorized parties that have access to the appropriate decryption keys. Other cloud services are capable of encrypting data upon receipt, ensuring that any data they are storing or transmitting is protected by encryption by default. [1] Some cloud services may not offer encryption capabilities, but at the very least should use encrypted connections such as HTTPS or SSL to ensure that data is secured in transit. [1]

II. LITERATURE SURVEY

Cloud services offer various security options -- such as advanced configurations, automated encryption and access controls to protect your important information. However, many organizations still can't secure data in properly in cloud. We use Encrypt data Method to secure our data in cloud storage Encrypt data: To secure data in the cloud, it's important to encrypt it, whether in flight or at rest. To plan encryption needs, map out data flows through all applications and the tables that store the resulting data. Then, encrypt data the same way in storage and during send it. [1] For example, let's take the levels of data encryption in terms of T-shirt sizes: small, medium and large: Small: It is a very basic encryption plan for stored data, in which data may be compromised, but encryption ensures minimal damage. [2] Medium: It is a slightly better plan that encrypts data in flight and at rest to help deflect breaches. Large: A more improved plan that encrypts both data at rest and in flight, but also includes features such as tracking data usage by attributes and users and monitoring all changes to data. In general, to be sure we can use of third-party tools to test and verify cloud security configurations and to identify any gaps that need to be addressed.

III. METHODOLOGY

Cloud services offer various security options -- such as advanced configurations, automated encryption and access controls to protect your important information. However, many organizations still can't secure data in properly in cloud. We use Encrypt data Method to secure our data in cloud storage Encrypt data: To secure data in the cloud, it's important to encrypt it, whether in flight or at rest. To plan encryption needs, map out data flows through all applications and the tables that store the resulting data. [5] Then, encrypt data the same way in storage and during send it. For example, let's take the levels of data encryption in terms of T-shirt sizes: small, medium and large: Small: It is a very basic encryption plan for stored data, in which data may be compromised, but encryption ensures minimal damage. Medium: It is a slightly better plan that encrypts data in flight and at rest to help deflect breaches. Large: A more improved plan that encrypts both data at rest and in flight, but also includes features such as tracking data usage by attributes and users and monitoring all changes to data. In general, to be sure we can use of third-party tools to test and verify cloud security configurations and to identify any gaps that need to be addressed.

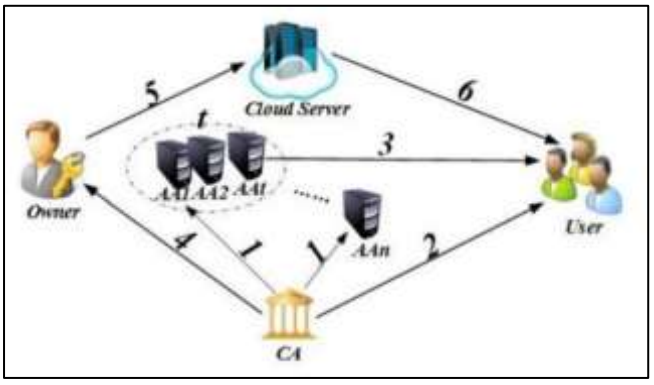

Fig. 1: System Architecture

IV. Result and Discussion

The collaborative mechanism helps markedly reduce client decryption overhead by employing a decryption server to execute most of decryption. [3] It helps to optimize clients' user experience since only a small amount of responsibility is taken by them for decryption. The proposed scheme performs better in cloud data sharing system serving massive performance-restrained front-end devices with respect to either security or efficiency. Data confidential was high.

V. Problem Definition

The main issues of cloud computing faces are maintaining confidentiality and integrity of data in data security. The only solution for these problems is encrypting data in the cloud. However, encrypting data can also bring up some new problems. Here is an overview of some of the main problems faced by cloud systems, Trust Issues, Legal Issues, Confidentiality and Authenticity. Trust Issues: -Trust Issues between the Service provider and the client are one of the main issues cloud computing faces today. There is no way for the client to be sure whether the management of the Service is trustworthy, and whether there is any risk of any possible attacks. This is a major issue and needs to be fixed. The only legal document between the client and service provider is the Service Level Agreement (SLA). [4] This document contains all the agreements between the client and the service provider, it contains what the service provider is doing and is willing to do. However, there is currently no clear format for the SLA, and as such, there may be services not documented in the SLA that the client may be unaware that it will need services later time. [6] Legal Issues: -There are several important requirements, privacy laws and data security laws that cloud systems need to adhere to. [3] One of the major problems with adhering to the laws is that laws vary from country to country, and users have no control over where their data is physically located. Confidentiality: -Confidentiality means the information should be confidential and should not be leaked. Preserving confidentiality is one of the major issues faced by cloud systems since the information is stored at various location that the Service Provider has full access to. Therefore, there has been some method of preserving the confidentiality of data stored in the cloud. The main method used to preserve data confidentiality is data encryption; however, encrypting data brings about its own issues, some of which are discussed later. Authenticity (Integrity and Completeness): -Integrity is preventing the improper modification of information. Just like confidentiality, integrity is also a major issue faced by cloud systems that needs to be handled, and is also mainly done by the use of data encryption.

VI. Conclusion

Cipher text policy attribute-based encryption is a promising cryptographic technique to realize fine-grained access control in secure cloud storage. We propose a novel collaborative key management protocol to enhance both security and efficiency of key management in cipher- text policy attribute-based encryption for cloud data sharing system.

VII. References

[1] A Survey on Ciphertext-Policy Attribute based Encryption and Time Specified Approach. Yugandhara L. Rothe, Prof. Vijay Gadicha, Prof.Y B Jadhao. M.E Student, Dept. of Computer Engineering, Padm. Dr VB Kolte College of Engineering and Technology, Malkapur, Buldhana (M.S.), India Asst. Professor, Dept. of Computer Science and Engineering, P.R.Pote College of Engineering and Management, Amravati, India Asst. Professor, Dept. of Computer Science and Engineering, Padm.Dr VB Kolte College of Engineering and Technology, Malkapur, Buldhana (M.S.), India

[2] A Survey Report on Attribute Based Encryption Methodologies to Secure Cloud Storage Sadanand H Bhuse Santosh N Shelke ME Student Assistant Professor Department of Computer Engineering Department of Computer Engineering Sinhgad Academy of Engineering Pune Sinhgad Academy of Engineering Pune

[3] Ciphertext-Policy Attribute based Data-Sharing with Enhanced Productivity and Security Kavita Patil1 ,Vidya Chitre2 M.E. Student, Information Technology, Vidyalankar Institute of Technology, Mumbai, India1 Assistant Professor, Information Technology, Vidyalankar Institute of Technology, Mumbai, India2

[4] Attribute Based Encryption for Secure Access to Cloud Based EHR Systems Maithilee Joshi, Karuna P. Joshi and Tim Finin University of Maryland, Baltimore County, Baltimore, MD 21250.

[5] A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing Guofeng Lin, Hanshu Hong, and Zhixin Sun

[6] A Survey on Ciphertext-Policy Attribute-based Encryption (CP-ABE) Approaches to Data Security on Mobile Devices and its Application to IoT

