Recent Trends for Efficient and Secure Accessing Scheme for Cloud Database

Dr. Santosh S. Lomte[1], Swati V. Khidse[2]

[1]Principal VDF's School of Engineering & Technology, Latur, India, [2] PhD Student

[1, 2] Department of Computer Science & Engineering,

[2]Dr. B. A. M. University, Aurangabad, Maharashtra, India.

***Abstract* - Cloud computing provides an enormous amount of virtual storage, it provides access to servers, storage, databases and a broad set of application services over the Internet. Its popularity is growing day by day. Consequently, there is a need for strong authentication schemes for securing access to cloud database. Data protection and security are the primary factors in cloud database for gaining user's trust and making successful use of cloud technology. There are number of data protections and data security techniques that have been proposed in the research field of cloud computing. However, there is need for enhancing data protection techniques.**

***Index Terms*—Encryption, Data Protection, Confidentiality, Obfuscation;**

I. Introduction

Cloud computing allows their users to store and access computing resources and data over INTERNET rather than from the local hard drive. It also helps to increase the storage capacity because users can use more than one cloud services for storing their data and thus reduce the cost because there is no need for owning an expensive computer with larger memory. According to the US National Institute of Standards and Technology (NIST), cloud computing is a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

Now a day's many organizations data are being transferred and shared via devices from the cloud database .Figure 1 shows that how the user is using cloud services. With the increase in using services of the cloud computing, the security concern for cloud database is also increasing. Data of all the users are stored in cloud database, so the question arises to users like "how to access their data?", "how they should sure about privacy of their information?" and many more. It is very important to properly protect information. One of the method for protecting electronic messages and other types of data is encryption. Encryption method is used for protecting user's sensitive data. Only authorized users can read the original message, and it will be inaccessible to unauthorized users. Entirely encryption is not foolproof for complete security of information. Every encryption algorithm is having certain pros and cons, it is very important for users to select a particular encryption type to meet their security requirement.

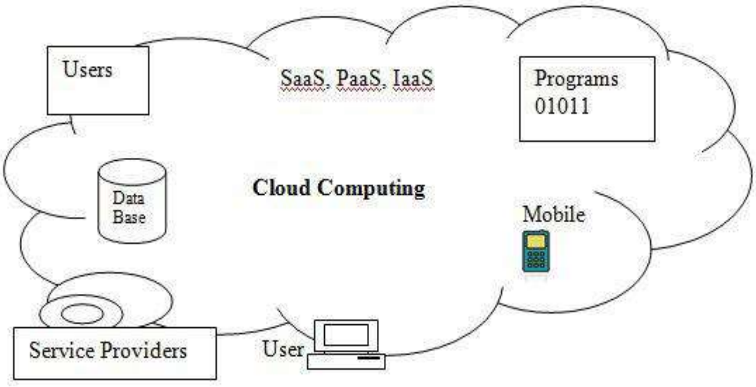

Figure 1: Cloud Services

Many companies are delivering their services from the cloud. Some examples are:

a) Google — It has having a private cloud that it used for delivering many different services, including email access, text translations, document applications, maps, web analytics, and much more.

b) Microsoft — Microsoft allows content and business intelligence tools to be moved to the cloud.

c) Salesforce.com —It runs application set for their customers in a cloud, and its Force.com and Vmforce.com products provide platform for building customized cloud services for their developers.

II. Literature Survey

Rapid development in cloud computing and services has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud database. Role-based access control (RBAC), model provides flexible controls and management by using two mappings, first users to roles and second roles to privileges on data objects. A Role-based encryption RBE integrates the cryptographic techniques with RBAC [2]. RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds.RBE scheme allows organization to store data securely in a public cloud and sensitive information related to the organization's structure is maintained in private cloud.

Two techniques for Data integrity or correctness in the cloud are achieved by using: Encryption, authentication at the client side and Data Obfuscation at server side. Encryption provides secrecy to data when it is transferred in the network. Data obfuscation will help service provider to secure data on his premises. User and Service provider will get maximum protection against intruders and unauthorized access by applying these two techniques [3]. A new scheme is proposed by using encryption and obfuscation technique works together. Firstly data will be encrypted before storing on cloud server and key is kept secret by user which provides security to data in transition. Encrypted format of data ensure about confidentiality. It provides confidentiality, Security and integrity of data.

Preserving privacy of data among the stored data shared in cloud storage is common. Some existing system uses fine grain access control with revoked user which protects prominent attacks for original data achieving security. Cloud Storage Controller (CSC) manages allocation of group of data and it is only referenced and cannot download any database from the cloud [4]. It provides helps in fast and highly secured datasets storage management in cloud storage system and also achieves efficient database privacy. It revokes user data swiftly and securely.

For ensuring confidentiality of data, most common technique used is encryption. But encryption alone doesn't guarantees maximum protection to data in cloud storage. To achieve efficient cloud storage confidentiality, encryption and obfuscation techniques are used to protect the data in the cloud storage [5]. Encryption is the process of converting readable text into unreadable form using an algorithm and a key. Obfuscation is also similar like encryption. Obfuscation disguises illegal users by implementing a particular mathematical function or using any programming techniques. Encryption and obfuscation techniques are applied based on type of data. Encryption is applied to alphabets and alphanumeric type of data and obfuscation to numeric type of data. By applying combination of encryption and obfuscation techniques on the cloud data, it will provide more protection against unauthorized access and thus confidentiality is achieved.

Without requiring the need of a secure channel between user and registration center, security at user side is achieved with two user-friendly authentication protocols. Second protocol guarantees unforgeability and non repudiation of the request [6]. The protocol uses elliptic curve operations, hashes and symmetric key encryption algorithms.

Database security is of prime importance in cloud computing. Different algorithms are used for protecting sensitive data. A review on different securing access techniques and various security issues of maintenance for cloud database is conducted [7].

III. Techniques Of Ensuring Secured Access To Cloud Database

There are various recent techniques that are used for ensuring secured access to cloud database.

Symmetric Encryption

This is the simplest kind of encryption. It involves only one secret key (either be a number, a word or a string of random letters) to cipher and decipher information. Symmetrical encryption is an old and best-known technique. Key is blended with the plain text of a message for changing the content in a particular way. Examples of symmetric encryption are: Blowfish, AES, RC4, DES, RC5, and RC6. AES-128, AES-192, and AES-256 are most widely used symmetric algorithm.

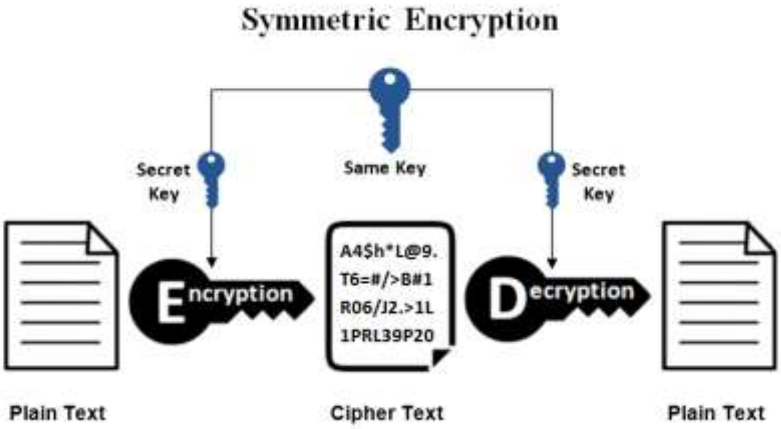

Figure 2: Symmetric Encryption

Asymmetric Encryption

Asymmetric encryption uses two keys for encrypting plain text. Secret keys are exchanged between users over the Internet or a large network. It eliminated the need to share the key. Popular asymmetric encryption algorithm includes EIGamal, RSA, DSA, Elliptic curve techniques, PKCS.

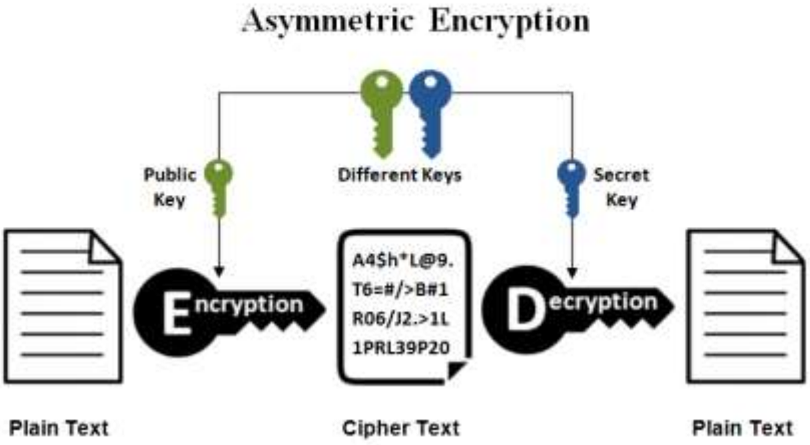

Figure 3: Symmetric Encryption

Biometric Authentication

In order to improve vulnerable identification process, bio-metrics techniques are used to strengthen the identification process in networked world [8]. Any human physiological or behavioral characteristic can be accounted as a bio-metric identification provided it should satisfies few properties:
i) universality - all human should possess it, ii) uniqueness – no two humans have the same, iii) permanence – it should not vary with time and iv)collectability- should be quantifiable. Fingerprint authentication is widely used for secured access to cloud database.

Two/Three Factor Authentication

Two/three-factor authentication ensures that claimant cloud users are authenticated by two or three methods as listed below [8]:
a) Claimant cloud users must remember - Password or PIN
b) Claimant cloud users must possess - Token or smart card (two-factor authentication)
c) Claimant cloud user's bio-metric characteristic - Such as a fingerprint (three-factor authentication)

Out-of band authentication

Out-of-band authentication is implemented in financial sectors or organizations that require higher security requirements. At the time of authentication process two or three connections are to be established between the cloud user and the cloud vendor. Each one of the channel will be used for exchange of user-id/password, another one for authentication plastic card data and the third one for exchange of bio-metrics data. When these channels are out-of band, trying to hack those channels becomes more difficult [8].

Bring Your Own Encryption (BYOE)

BYOE refers to a cloud computing security model which provides help to cloud service customers to use their own encryption software and manage their own encryption keys. It provides complete control over encryption of their data.

IV. CONCLUSION

Cloud computing model helps to speed up and increase the flexibility of data management with reduced cost. It is bringing a lot of benefits and becoming more and more popular now a days. Many large companies have started using cloud service in their business. While it is widely used, the security is becoming an important concern for everyone who use cloud services. There are different techniques with which accessing to cloud database is secured. There are a lot of security issue concerns increasing continuously, while there are improvements as well on the security model of the cloud.

V. FUTURE SCOPE

Cloud computing is relatively new and widely emerging domain in today's era and it must overcome security issues in order to be more and more prominent technology of the future. With the development of new technique for security, crackers are always fond of breaking it. So there is always need for making algorithm more secured.

REFERENCES

[1] Peter Mell ,Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology U.S. Department of Commerce, September 2011.

[2] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, pp.1947-1960, DECEMBER 2013.

[3] Krunal Suthar, Dr. Jayesh Patel, "EncryScation: A Novel Framework for Cloud IaaS, DaaS security using Encryption and Obfuscation Techniques," 2015 5th Nirma University International Conference on Engineering (NUiCONE)

[4] D. Seethalakshmi, Prof. Dr. G. M. Nasira, P. Thangamani, "Securing Cloud Database By Data Fusing Technique (DFT) Using Cloud Storage Controller (CSC)," 2016 IEEE International Conference on Advances in Computer Applications (ICACA), pp. 21-25, 2016.

[5] Dr. L. Arockiam S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security," 2014 International Conference on Computer Communication and Informatics (*ICCCI* -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.

[6] An Braeken and Abdellah Touhafi, "Efficient Anonymous User Authentication on Server Without Secure Channel During Registration," 2016 IEEE.

[7] Swati Vithal Khidse, Dr. Santosh S. Lomte, "A Survey on Securing Access and Security Issues of Maintenance for Cloud Database," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 1, pp. 1165-1169, January 2017.

[8] Dr. N. Venakatesan, M. Rathan Kumar," Finger Print Authentication For Improved Cloud Security," IEEE International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 434-439, 2016.