

**INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH
TECHNOLOGY****A SURVEY ON CLOUD DATA SECURITY****Mukesh Kumar Jha*, Veerendra Shrivastava***M.Tech Research Scholar, IES College of Technology, Bhopal
Asst. Prof. CSE Department, IES College of Technology, Bhopal

DOI: 10.5281/zenodo.168843

ABSTRACT

Cloud computing gives customers the illusion of infinite computing sources which are available from anywhere, anytime, on demand. However the capability of selectively sharing encrypted data with distinctive users thru public cloud storage can also greatly ease security concerns over inadvertent information leaks inside the cloud. The desired flexibility of sharing any group of particular selected documents with any group of users demands different keys for encryption to be used for any different documents. So many trapdoors are created in the cloud. In this paper review helps the research how to secure data in cloud environment.

KEYWORDS: Cloud Storage, Data Sharing, Cloud Storage, Data Encryption, Aggregate Key**INTRODUCTION**

Cloud storage also **on-demand storage** has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to huge amounts of document shared over the world wide web. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization

However, whereas enjoying the convenience of sharing knowledge via cloud storage, users also are progressively involved concerning accidental knowledge leaks within the cloud. Such knowledge leaks, caused by a malicious human or a misbehaving cloud operator, will typically result in serious breaches of non-public privacy or business secrets (e.g., the recent status incident of celebrity photos being leaked in iCloud). To handle users' issues over potential knowledge leaks in cloud storage, a standard approach is for the info owner to write in code all the info before uploading them to the cloud, such later the encrypted knowledge is also retrieved and decrypted by those that have the secret writing keys. Such cloud storage is commonly known as the crypto logic cloud storage. However, the cryptography of knowledge makes it difficult for users to go looking and so by selection retrieve solely the info containing given keywords. a standard answer is to use a searchable cryptography (SE) theme within which {the knowledge the info the information} owner is needed to write in code potential keywords and transfer them to the cloud at the side of encrypted data, such that, for retrieving knowledge matching a keyword, the user can send the corresponding keyword trapdoor to the cloud for acting search over the encrypted data.

CLOUD STORAGE FRAMEWORK

Cloud storage offers enterprise organizations the potential to dramatically decrease storage costs. Various cloud services provide cloud storage to consumers at no charge, while others charge some type of subscription-based fee [3]. There are also private clouds that are owned and controlled by an organisation, providing a secure network for sharing critical software and data. They can create their own cloud archive solution. In addition, hospitals can pool their budgets and resources to create a shared private cloud consortium or group. Private clouds are created using hardware, software and other tools from different vendors, where the actual servers are managed either onsite or offsite. Hybrid clouds, as the name suggests, combine various public and private cloud resources into a service or solution [13].

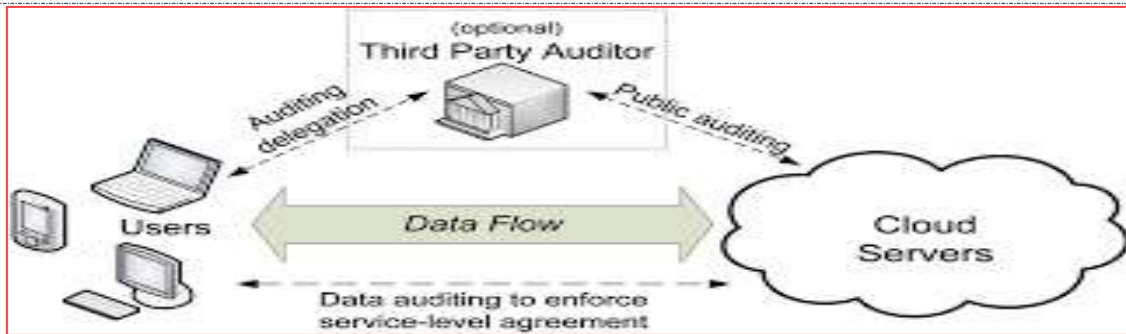


Figure 1: Cloud Data Storage

In the Figure (1) when any user want store or access any data/file from cloud then first user need to authenticated by third party auditor then after direct communicate from cloud servers[2]. At the heart of legacy IT, hosting, managed service provider (MSP) and clouds are common building blocks, which include networking, processing and storage technologies. Different types of servers, networks and storage technologies meet various cloud computing and cloud storage requirements (for example, dense rack and blade servers with different numbers of sockets and cores at various GHz speeds, threads, amount of memory and I/O expansion capabilities). Networking options include fast 40GbE and 100GbE for backhaul or trunk circuits, along with the more common 10GbE and 1GbE for virtual private networks (VPN) and bandwidth optimisation[4][5].

Data storage options or tiers include ultra-fast SSDs, as well as fast medium- and high-capacity HDDs. Storage management features include data protection — high availability (HA), backup (BC) and disaster recovery (DR) — as well as footprint reduction (DFR) for space optimisation, such as compression, de-duplication and thin provisioning, which enables more information to be stored for longer periods at lower costs [7].

Software tools are also very important in creating services and solutions, and include APIs, middleware, databases, applications, hypervisors for creating virtual machines (VMs) and virtual desktop infrastructures (VDI), along with cloud stack ware, such as Open Stack, and associated management tools. Examples of VMs and VDI hypervisors include Citrix/Xen, KVM, Microsoft Hyper-V, Oracle and VMware ESX/sphere.

CLOUD SERVICE MODEL

Cloud computing is a term that describes a broad range of services. Since the cloud is a collection of services, organizations choose where, when, and how they use cloud computing. In this paper we explain the three different types of service models: [4]

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a service (IaaS)

1. Software as a Service (SaaS) model SaaS is software that is developed over internet. It is a delivery model where the software and the associated data are hosted in a cloud environment by a third party such as Cloud Service Provider (CSP).

2. Platform as a Service (PaaS) model Is a computing platform that allows creation of web applications easily without the complexity of maintaining the software. Is a delivery model where a CSP provides an online software development platform for an organization?

3. Infrastructure as a Service (IaaS) model: This model is used to access essential IT resources. These essential IT resources include services that are linked to resources of computing, data storage and the communications channel.

CHALLENGES FACING THE CLOUD

Ensuring data storage security in cloud computing with effect of Kerberos

The problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, and correctness of users who can access to the cloud server , we proposed an effective and flexible distributed scheme with explicit dynamic data support, including Kerberos and authentication service. Kerberos provides a centralize authentication service whose function is to authenticate user to cloud server and cloud server to user. any user to access the cloud server first should make the profile and password. Then it can use the cloud server with gain the qualify [11].

A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security

To ensure data security in cloud data storage, a novel triple encryption scheme is proposed. In the triple encryption scheme, HDFS files are encrypted by using the hybrid encryption based on DES and RSA, and the user's RSA private key is encrypted using IDEA. The triple encryption scheme is implemented and integrated in Hadoop-based cloud data storage [10].

Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

The practical downside of privacy conserving information sharing system supported public cloud storage which needs an information owner to distribute an oversized range of keys to users to change them to access his/her documents we tend to for the primary time propose the thought of key-aggregate searchable cryptography (KASE) and construct a concrete KASE theme in an exceedingly KASE theme, the owner solely must distribute one key to a user once sharing several documents with the user, and also the user solely must submit one trapdoor once he queries over all documents shared by constant owner [8].

Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage

We explored proxy re-encryption from both a theoretical and realistic perspective. We outlined the traits and security guarantees of previously recognised schemes, and as compared them to a set of stepped forward re-encryption schemes we gift over bilinear maps. These pairing-primarily based schemes understand crucial new capabilities, consisting of safeguarding the master secret key of the delegator from a colluding proxy and delegatee. One of the maximum promising applications for proxy re-encryption is giving proxy capabilities to the key server of a confidential distributed record system; this manner the key server need not be absolutely relied on with all the keys of the device and the name of the game storage for every consumer also can be reduced [15].

Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

Finegrainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. In this paper we propose a scheme to achieve this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed Scheme is secure under standard cryptographic models [12]

Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption

Bearing in mind the matter-of-fact difficulty of privacy preserving information distribution organization based on public cloud storeroom which necessitates an information proprietor to share out a bulky numeral of keys to users to facilitate them to right of entry his or her credentials, we for the foremost time recommend the perception of key aggregate searchable encryption [KASE][4].

Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature

To share data flexibly is an important role in cloud computing. Users prefer to upload their data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Key Aggregate Cryptosystems provides delegation of secret keys for different files stored in cloud storage in the form of single aggregate key. The proposed work additionally includes digital signature to provide integrity towards the user's data [5].

A Paper On secure multi-owner group data search by using aggregate key

Considering the pragmatic issue of security saving information sharing framework taking into account open cloud stockpiling which obliges an information proprietor to appropriate a substantial number of keys to clients to empower them to get to his/her records, we surprisingly propose the idea of key-aggregate searchable encryption (KASE) and develop a solid KASE plan [6].

Group Data Searching And Sharing Using Key Aggregate Cryptosystem

In this paper, we reviewed the existing systems papers of sharing the data securely in the cloud. The existing systems based on key encryption may suffer from certain problems such as; these systems are impractical and inefficient as they may require many keys over the cloud data for encryption as well as decryption. Therefore in this paper we are analyzing these problem and aims to overcome them by proposing a novel system called as KASE. In this system, we define general framework for KASE system. Then we describe functional and non-

functional requirements of KASE scheme. After describing the KASE scheme we establish its security by detailed analysis [1].

Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to perform keyword queries and update operations on the encrypted file collections. DSSE has several important applications such as privacy-preserving data outsourcing for computing clouds. In this paper, we developed a new DSSE scheme that achieves the highest privacy among all compared alternatives with low information leakage, non-interactive and efficient updates, compact client storage, low server storage for large file-keyword pairs with an easy design and implementation [2].

Dynamic Authentication for Client Side Deduplication in Cloud Storage Environment

The growing need for secure cloud storage services and the attractive properties of the convergent cryptography lead us to combine them, thus defining an innovative solution to the data outsourcing security and efficiency issues. The proposed work provides space saving as well as security to the data, but still there are various aspects which need to be address in future. Proposed work addresses only three types of file txt file, doc file and pdf file, we can extend this work for different types of file such as image and sound files and video files in future. We can also apply some searching technique that speed-up the operation by separating the hash key according to the file type [3].

RESEARCH SCOPE

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents. Many key aggregation scheme are available also discuss in this paper but if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting this is also a research work in cloud computing.

CONCLUSION

Cloud computing is a new paradigm of computing utilities that promises to provide more flexibility, less expense, and more efficiency in IT services to end users. In this paper presents how the cloud services can be deployed and many challenges to access data from cloud. In this paper we found that when we to upload and download multi owner file then many trapdoor are created in the cloud in order to perform search over the shared data. So this region security level of shared data in the cloud is decreases. Then how to reduce the number of trapdoors under multi-owners setting is a research work

REFERENCES

- [1] Wakchaure Sonali Pandharinath. "Group Data Searching And Sharing Using Key Aggregate Cryptosystem" IJARIE-ISSN (O)-2395-4396 Vol-2 Issue-1 2016.
- [2] E. Seetha1, D. Ponniselvi "A Dynamic Authentication for Client Side Deduplication in Cloud Storage Environment" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2015
- [3] Sharayu.J.Lande, Prof. N.B.Kadu "A Review of Research on An Aggregate Key Sharing Mechanism For Sharing Data Between Different Groups Via Cloud" IJEDR | Volume 3, Issue 4 2015.
- [4] K. Rajasrika1, P.S. Smitha2 "Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015.
- [5] G. Suganyadevi1 S. PunithaDevi "Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Special Issue 6, May 2015.
- [6] Salman Mujawar "A Paper On secure multi-owner group data search by using aggregate key" Innovation in engineering science and technology (NCIEST-2015).
- [7] M.R. Kalai Selvi1 "Secure Data Sharing for Dynamic and Large Groups in the Cloud" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014 .

- [8] Baojiang Cui, Zheli Liu_ and Lingyu Wang “Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage” IEEE TRANSACTIONS ON COMPUTERS, VOL. 6, NO. 1, JANUARY 2014.
- [9] Harshitha. K. Raj “A Survey on Cloud Computing” International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, July 2014.
- [10] Chao YANG, Weiwei LIN*, Mingqi LIU “A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security” Fourth International Conference on Emerging Intelligent Data and Web Technologies 2013.
- [11] Mehdi Hojabri “Ensuring data storage security in cloud computing with effect of Kerberos” International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5 , July - 2012 ISSN: 2278- 01 81.
- [12] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing” IEEE INFOCOM 2010.
- [13] Ayad F. Barsoum and M. Anwar Hasan “Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems.
- [14] Attila A. Yavuz and Jorge Guajardo “Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware”.
- [15] GIUSEPPE ATENIESE KEVIN FU MATTHEW GREEN and SUSAN HOHENBERGER “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage” ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006, Pages 1–30.