Survey on Cryptographic Data Security over Cloud

Er. Lalit Gehlod
Asst.Professor, Dept.Of Computer Engineering,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

Govind Patidar
Dept. Of Information Technology,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

Abstract—in cloud computing, clients usually outsource their data to the cloud storage servers to reduce the management costs. While those data may contain sensitive personal information, the cloud servers cannot be fully trusted in protecting them. Encryption is a promising way to protect the confidentiality of the outsourced data, but it also introduces much difficulty to performing effective searches over encrypted information. Most existing works do not support efficient searches with complex query conditions. In this paper, we propose new scheme to solve the problem searching data on cloud because on the cloud data is stored in encrypted format. When the data search easily provides and also provides sharing between users. Data security is biggest issue on cloud. At that time provide safe searching and sharing between trusted users. Using these search results, cloud server will send encrypted document to the end user and at the user end perform decryption of data and get to original data.

Keywords--- Cloud Computing, Privacy, Sharing, Security Search, Trusted users, Encryption and Decryption.

I. INTRODUCTION

Cloud computing means store and access data and programs over the internet. In cloud data can be easily stored and fetch by anyone without any effort is used.Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

In cloud data is save and retrieve from storage. Mainly cloud storage has three types. It can be private, public or hybrid. **Public cloud**: The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations. **Private cloud**: The computing infrastructure is dedicated to a particular organization and not shared with other organizations. **Hybrid cloud:** its usage of both private and public clouds together is called hybrid cloud [1].

Cloud computing offers IT resources, including storage, networking, and computing platforms, on an on-demand and pay-as-you-go basis. Cloud resources are available over the network in a manner that provides platform independent access to any type of clients. Cloud Computing offers on-demand self-service. It does not require installing specific software to access or manipulating cloud services [2].

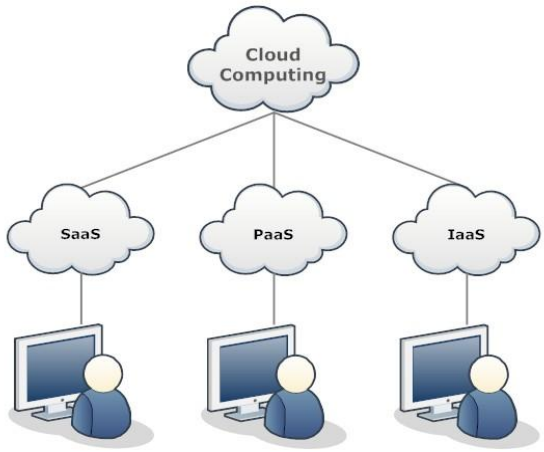
Infrastructure as a Service (IaaS) abstracts hardware (server, storage) into a pool of computing, storage, and connectivity capabilities that are delivered as services for a reliable cost. Its goal is to provide anable to be easily modified, standard, and virtualized operating environment that can become a user friendly.Virtualization means data is run own platform but it's exactly run on main server. [3]

Platform as a Service (PaaS) delivers application execution services, such as application runtime, storage, and combining, for applications written for a pre-specified development framework. PaaS provides an efficient and agile approach to operate scale-out applications in a predictable and cost-effective manner. PaaS can be defined as a computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath It[3] [4].

Software as a Service (SaaS) delivers business processes and applications, such as CRM, collaboration, and e-mail, as standardized capabilities for a reliable cost at an agreed, business-relevant service level. SaaS provides significant efficiencies in cost and delivery in exchange for minimal customization and represents a shift of operational risks

ISSN: 2278 – 1323

from the consumer to the provider. All infrastructure and IT operational functions are abstracted away from the consumer. [3].



Data access, share, and transfer from one place to another place at that time need the higher security for data protection.Data share, if one client wants to share his data to another client at that time data is moved from source to destination machine. If sharing policy is weak at transfer time unauthorized person easily break the data and steal the useful information. So at the data sharing time use a highly secure medium between trusted parties.

Data access refers to a user's ability to access or fetch the data, those stored in a database. Users who have the permission for data access also perform the fetching or transfer the data from one place to another place. At the moment of data if the security is weak easily trap the data.

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from intruder [5]. Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized user's access. The security mechanism involves the file sharing and transfer utility for demonstrating the working of the designed technology. In this system a secure infrastructure is developed for providing security and data protection. In addition of that the data is preserved from the intruder and malicious users using the concept of cryptographic approach. Cryptographic approach helps to hide data from the untrusted users with using encryption and decryption technique.

II. BACKGROUND

Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information. Confidentiality providing unauthorized access from secretes conversation it's provide secure data transaction. When the communication perform between two parties at that time hide the data from unauthorized user with the help of confidentiality. Confidentiality achieves a better privacy of the data. Security is an essential part in network communication and file hosting. The untrusted network hosts and lake of security in network can harm the data security and user privacy. If the security is weak easily vulnerable the data and steal the data. Cryptography is performing major role in security of data when the data transaction is perform between two sources use cryptographic technique. In cryptography technique data is encrypts and decrypt with the help of encryption and decryption algorithm. When the data is transfer from one source to another source encrypt the data with the help of encryption algorithm, when the data receive from another source decrypt the data with the help of decryption algorithm. In this process sending and receiving time data is in unreadable form, nobody can read the data only authorized person can read the data. Data security is basically protecting the data from intruder or unauthorized user. If unauthorized person access our data it can easily alter delete or update. Data is stored on the cloud storage so at the time of data fetching and saving is easily captured if security is weak. So protect the data from intruder we use high security.

Mainly three type of cryptographic technique is used at the time of data encryption and decryption.

- Secret Key Cryptography (SKC): In this cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. When user wants to send his file to another user at that time encryption and decryption is performed. Sender perform encryption at own end with the help of secret key. At the receiver end receive the data and perform the decryption. At decryption time use same key (used encryption time). Both the key (encryption and decryption) is generated with the same algorithm.
- Public Key Cryptography (PKC): In this cryptographic system we use two keys one for encryption and another key for decryption. This key is calledas private key and public key. Public is known for every

ISSN: 2278 – 1323

person but private key is own key and hide to everyone authorized or unauthorized person. When sender wants to send the data use encryption and at the encryption time use public key. With the help of public key data encrypt and send to receiver. At the receiver end receive data in encrypted format then apply decryption technique. Decryption is perform with the help of own private key. Both the end different key are generated with same algorithm is used.

- Hash Functions: A cryptographic hash function is a hash function which takes an input or message and returns a fixed-size alphanumeric string, which is called the hash value or message digest. At the sender end hash function is apply and then send to receiver. At the receiver end, receive the message and then apply the same hash function and get original message.

III. RECENT STUDIES

In The Privacy-Assured and Searchable Cloud Data Storage Services, we identify the system requirements and challenges toward achieving privacy-assured searchable outsourced cloud data services. We present a general methodology for this using searchable encryption technique, which allows encrypted data to be searched by users without leaking information about the data itself and users' queries. We discuss three desirable functionalities of usable search operations: supporting result ranking, similarity search, and search over structured data. In this paper, we identify the problem and challenges of enabling privacy-assured searchable cloud data storage services. Which suggest that achieving functionally rich, usable, and efficient search on encrypted data is possible without sacrificing privacy guarantee too much. The steady evolution of this field will need to bring expertise from the cryptography, database, and information retrieval communities [6].

In Techniques for Efficient Keyword Search in Cloud Computing, we solve the problem of exact keyword match by providing searching with fuzzy keyword. We also propose two more techniques called gram based technique which is useful for reducing the time, providing fast searching and increase the performance by considering substring from the given string. And Symbol-based tree traverse search scheme where a multi way tree structure is built by using symbols, which works for more than one keywords entered by the user. By providing security, we show that the proposed solution is secure and privacy-preserving. In this paper, we try to formalize and solve the problem of providing efficient fuzzy search for remotely stored data in cloud computing. We design two more advanced techniques (i.e., Gram based and Symbol-based tree traverse search techniques) to construct efficient fuzzy keyword sets. By providing security, we show that the proposed solution is secure and privacy-preserving. Experimental results demonstrate the efficiency of our proposed solution [7].

In Searching Encrypted Data on Cloud, Data Encryption on cloud as well as corresponding security issues has been addressed. The proposed method incorporates two main phases: indexing and searching. Trapdoor and code word are the two security parameters applicable in this technique. This paper concentrates on safe and secure searching of unstructured data in cloud. In this technique trapdoor and code word are two security levels for both indexing and searching. Bloom Filter (BFAH) has been used to make the code word more secure and confidential. The evaluation of experimental results indicates that searching encrypted data on Cloud proposed is secure and protective from hackers. The method is proposed for cloud environment where a large amount of unstructured data is stored in encrypted form [8].

In Security on Cloud Using Cryptography mainly focus on core secured cloud storage services i.e. Cryptography to provide cryptographic techniques for securing data and computation in a cloud environment. Cryptography in cloud computing is a new secure service regarding security and privacy in cloud. The Cloud computing as a technology would be adopted if the areas of concerns like security of the data will be covered with full proof mechanism. The strength of cloud computing is the ability to manage risks in particular to security issues. Our suggested model will present an outline sketch of architecture to be adopted by architects involved in implementing the cloud computing. Security algorithms mentioned for encryption and decryption and ways proposed to access the multimedia content can be implemented in future to enhance security framework over the network [9].

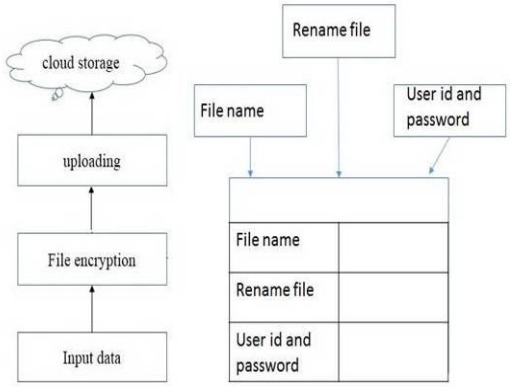
In Accessing Secured Data in CloudComputing Environmentcan be used for secure access to and storage of data on public cloud server, moving and searching encrypted data through communication channels while protecting data confidentiality. This method ensures data protection against both external and internal intruders. Data can be decrypted only

ISSN: 2278 – 1323

with the provided by the data owner key, while public cloud server is unable to read encrypted data or queries. Answering a query does not depend on it size and done in a constant time. Data access is managed by the data owner. The proposed schema allows unauthorized modifications detection. In this study each data record is encrypted with a different symmetric key generated from the secure index so that flexible cryptography-based control can be accomplished; and confidentiality of the outsourced data against the cloud service provider and unauthorized users is guaranteed [10].

IV. PROPOSED WORK

In this section, we are proposed a new cloud storage based data security and searching system. In this system we provide a better utilization for the secure data hosting and sharing systems. This system provide better security at the time of data transfers between parties, it's protects the data from intruder or illegal access. And it's providing easily searching and sharing between authorized users.



[11]

When Upload the data on cloud, firstly confirm authorization. For authorization enter valid user id and password. After authorization youselect the input data, in the input data phase select the file or data those wants to upload on cloud. After the select of file you will go in file encryption phase. In this phase data is encrypted then send to uploading phase. In encryption process we use AES(Advance Encryption Standard) technique with the helpof key generation SHA(Secure Hash Algorithm) technique. When the encryption performed successfully uploading process is performed. In this process data is converted in to bytes form then it is uploaded on the cloud storage. After the successfully stored data on cloud any authorize person can fetch the data on cloud. All the process handled by third party.
In the Hash table includes the file name, rename file, and user id for performing search and shearling of file. The file name is extracted particular data file between lots of file. Rename file name, when the two file is same in the database we used concept of Rename file and extract the file. Its provide a uniqueness for data searching.

Downloading data at cloud server firstly download the main chunk also download the all related chunk of file. If we download the data get into encrypted form. So at the downloading time we use decryption process for decrypt the data. Downloading and decryption process work simultaneously. In the decryption process we also used AES algorithm with the help of SHA algorithm for the data decryption. SHA generate secret key in decryption process. After decryption is performed successfully file is converted into original file.

V. CONCLUSION

We have proposed an efficient cryptographic data (encryption, decryption) algorithm for the data security. When the data transection time if the security is weak easily break and steal the data or information. In this paper we are propose a new way for data security at the encryption and decryption time. And we also provide easily data searching and sharing of data between two trusted parties. When user wants to search data on cloud at that time stored data is in encrypted form, so searching is not an easy concept on that. We provide searching and sharing concept on encrypted data.

VI. ACKNOWLEDGEMENT

We thank immensely our management for extending their support in providing us infrastructure and allowing us to utilize them in the successful completion of our paper.

VII. REFERENCES

1. http://thecloudtutorial.com/cloudtypes.html
2. https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&sqi=2&ved=0CCgQFjAA&url=http%3A%2F%2Fwww.tutorialspoint.com%2Fcloud_computing%2Fcloud_computing_tutorial.pdf&ei=MAUMVaOZNM-GuASn34GYBA&usg=AFQjCNF1r8qXUp3wsivdCuJ9csoonAs-Sg
3. https://technet.microsoft.com/enus/magazine/hh509051.aspx
4. http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas

ISSN: 2278 – 1323

5. http://www.techopedia.com/definition/26464/data-security
6. https://www.google.co.in/search?q=services+in+cloud+computing&biw=1366&bih=667&source=lnms&tbm=isch&sa=X&ei=jE2EVYDEPMKxuAS4zYCwDg&sqi=2&ved=0CAYQ_AUoAQ#tbm=isch&q=services+cloud+computing+diagram&imgrc=6T0RHi5kHlLJFM%253A%3BkabzkFsLEHgoRM%3Bhttp%253A%252F%252Fwww.exigotechnology.com%252Fwp-content%252Fuploads%252Fcloudcomputing.jpg%3Bhttp%253A%252F%252Fwww.exigotechnology.com%252Findex.php%252Fsolutions%252Fexigo-cloud%252F%3B550%3B456 [image cloud service]
7. http://www.ijarcsse.com/docs/papers/Volume_4/12_December2014/V4I12-0206.pdf
8. http://www.ijcsit.com/docs/Volume%204/Vol4Issue1/ijcsit2013040116.pdf
9. http://ijcsi.org/papers/IJCSI-10-6-1-230-233.pdf
10. http://www.ijarcsse.com/docs/papers/Volume_5/3_March2015/V5I3-0321.pdf
11. http://ijarcet.org/wp-content/uploads/IJARCET-VOL-4-ISSUE-3-953-957.pdf

ISSN: 2278 – 1323