A Survey on Cryptographic Security over Cloud

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

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

Abstract - Privacy and security are the most important issues in cloud computing. To achieve high flexibility and to reduce cost, many data owners are outsourcing their data management system to public cloud. Data must be encrypted locally before outsourcing to protect data privacy. The data encryption reduces the data utilization based on simple keyword search. Consider large numbers of documents are outsourced on cloud by large number of cloud users. In this paper, we propose new scheme to solve the problem of multi keyword search over encrypted data using trusted third party in cloud computing. User will encrypt their data locally. Before encrypting data, the index will be created. Trusted third party will use all these indexes to search data similar to the search query of user. Using these search results, cloud server will send encrypted document to the user and at the user end perform decryption of data. In this paper implement secure keyword search over encrypted cloud data.

Keywords--- Cloud Computing, Privacy Preserving, Trusted Third Party, Keyword Search, Encryption

I. INTRODUCTION

Cloud computing is computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources.

Cloud computing is a result of computational revolution, that is derived from the distributed computing approach. Therefore that is working on the basis of plug and play manner. That is basically a huge computational and storage infrastructure that provides support for various computing applications.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people.

Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

Cloud computing offers IT resources, including storage, networking, and computing platforms, on an on-demand and pay-as-you-go basis. The high usability of today's cloud computing platforms makes this rapidly emerging paradigm very attractive for customers who want to instantly and easily provide web-services that are highly available and scalable to the current demands[1].

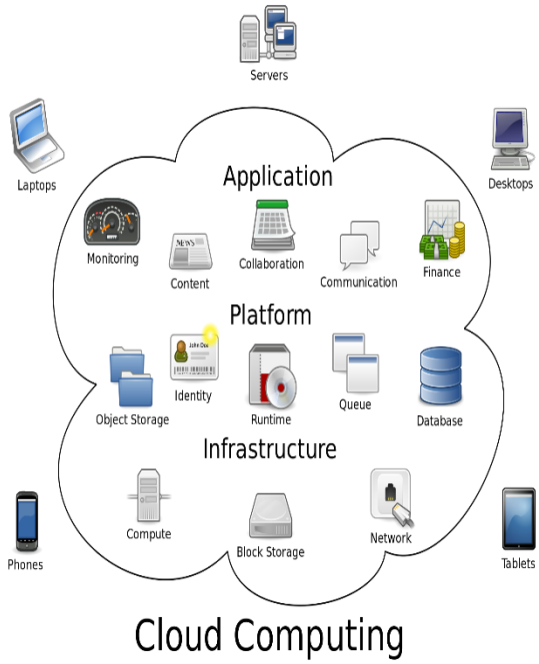
Cloud resources are available over the network in a manner that provides platform independent access to any type of clients. Cloud Computing offers on-demand self-service. The resources can be used without interaction with cloud service provider [2].

Application or Software as a service complete application for a given purpose which we use with or without customization.

Platform as a service is server along with a software environment is provided. We can use the environment to build our application and deploy it for use by our organization.

Infrastructures as a service are providing the physical infrastructure by a vendor which we can access over internet and use to install our software, build or deploy our applications. [3]

ISSN: 2278 – 1323



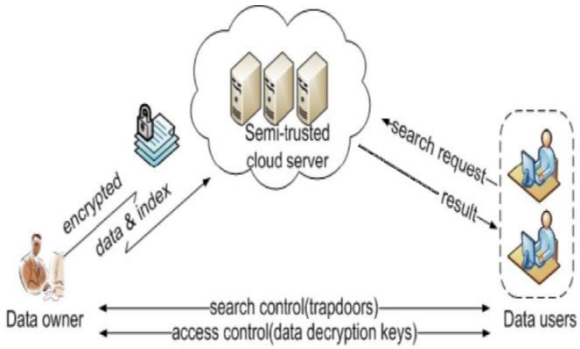
Data access, share, and transfer from one place to another place at that time need the higher security. Data access refers to a user's ability to access or retrieve data stored within a database or other repository. Users who have data access can store, retrieve, transfer or update stored data, which can be stored on a wide range of hard drives and external devices. At the accessing time security is major concern, an unauthorized person also seeing the data if the security is weak [4].

Data share, if one party wants to share the data to another party at that time if sharing policies weak easily break the data. Transfer of file from server to client or client to server at that time if security is vulnerable easily to break. So in whole process if our security is strong anyone can't be break easily at sent and receiving time.

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 owner management. In addition of that the data is preserved from the untrusted and malicious users using the concept of cryptographic approach. The cryptographic approach helps to hide data from the outside the world and using decryption the data, data owner is identified for secure and authenticated access.

Data owner: wishes to outsource data onto a cloud provider server. The data owner module is responsible for encrypting the data. After encrypting the data by the proposed technique, the data owner sends data to cloud storage server. The data are stored in the public part of the data storage server. Data owner needs access to the cloud server only for loading and updating encrypted data.

Data user: Trusted parties wishing to access the cloud data by means of encrypted identifier provided by the data owner. Only the legitimate clients are allowed to access and store data with confidence [5].



In addition of that the encrypted data is not searchable for other cloud user, thus the proposed approach incorporate the security mechanism is such way by which any user can search the data availability on cloud storage.

Firstly data owner encrypt the data with indexing then store the data on cloud storage. Data user want to search the data in the cloud storage research request is sent then the result is came.

II. BACKGROUND

Aspect of data security

The confidentiality of a system is guaranteed providing it avoid unauthorized accessing of information. When communication performs between two sources, the whole communication is hidden from intruder. Confidentiality achieves a better privacy of the data. To protect confidentiality use Cryptographic and access controls technique for strong authentication. Security is an essential aspect 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 vulnerable anyone breach the security and steal the data. Cryptography is a method of storing and transmitting data in a particular form so that only authorized person can read and process it. The term is most often associated with scrambling plaintext (ordinary text) into ciphertext (a process of encryption), then process again (known as decryption) [6]. Cryptography technique is used for

ISSN: 2278 – 1323

data encryption and decryption. Implement a new algorithm for perform cryptographic technique, it's also increase the data security because security on cloud is poor. In the cryptography use a hybrid of algorithm and design a new algorithm for better data security. Cryptographic storage services are that manages the data by the customer and the security properties are derived from cryptography, as opposed to legal mechanisms, physical security or access control. [7]. Data security is basically protecting the data from intruder or unauthorized person. Data is stored on the cloud server so at the time of fetching data easily trappable if security is weak. So protect the data from intruder use high security.
Any new design of Cryptographic technique must accomplish the above requisites. Cryptography not only protects data from theft or alteration, but can also be used for user authentication

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

- Secret Key Cryptography (SKC): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (used algorithm) to encrypt the plaintext into ciphertext and sends the ciphertext to the receiver. The receiver applies the same key (same algorithm) to decrypt the message and recover to the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. Secret key are generated both the end and used same algorithm for secret key generation [8].
- Public Key Cryptography (PKC): with the public key cryptography, different – different key is used for encryption and decryption. And this key is called private key and public key. Public key is known but private key is hidden at both ends. Use public key for data encryption and the decryption we used own private key. Both the end generate own different-different private key with the help of algorithm. After key generation only exchange his public key.
- Hash Functions: hash function, also called massage digest. It's convert the input message in to shorter from also says compression of data. It is a one way encryption, means at the sender end hash function is apply and then send. At the receiver end, same hash function is apply and then match the both hash function if same accept otherwise discard the message.

III. RECENT STUDIES

In Privacy Preserving Data Search, we propose new scheme to solve the problem of multi keyword search over encrypted data using trusted third party in cloud computing. User will encrypt their data locally. Before encrypting data, the index will be created. Trusted third party will use all these indexes to search data similar to the search query of user. Using these search results, cloud server will send encrypted document to the user. In this paper, the method is proposed to perform the multi-keyword ranked search over cloud data. The proposed system will perform secure search over encrypted data in cloud computing [9].

In cloud the data search arises only with the plain data. But it is essential to invoke search with the encrypted data also. The specialty of cloud data storage should allow copious keywords in a solitary query and results the data documents in the relevance order. This paper focuses on multi keyword search based on ranking over an encrypted cloud data (MRSE). The search uses the feature of similarity and inner product similarity matching. The experimental results show that the overhead in computation and communication are considerably low. For meeting the challenge of supporting multi-keyword semantic without privacy breaches, MRSE framework is proposed using secure inner product computation. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset shows our proposed scheme introduces low overhead on both computation and communication [10].

In Secure and privacy preserving keyword searching for cloud storage services paper, we investigate the characteristics of cloud storage services and propose a secure and privacy preserving keyword searching (SPKS) scheme, which allows the CSP to participate in the decipherment, and to return only files containing certain keywords specified by the users, so as to reduce both the computational and communication overhead in decryption for users, on the condition of preserving user data privacy and user querying privacy. It is provable that the proposed scheme has semantic security against adaptive chosen plaintext attacks. By performance analysis, we show that our scheme outperforms the scheme proposed by Boneh when applied to a cloud environment [11].

ISSN: 2278 – 1323

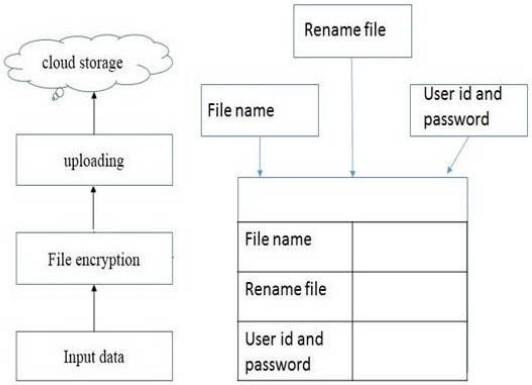
In this paper we propose an efficient privacy preserving keyword search scheme in cloud storage, the scheme satisfies the multi-user requirement with low computational overhead and flexible key management, and it is proved to be secure and feasible. It meets the needs of multi-user and the conjunctive keyword search, and the efficiency is improved as well [12].

In this article, we identify the system requirements and challenges toward achieving privacy-assured searchable outsourced cloud data services, especially, how to design usable and practically efficient search schemes for encrypted cloud storage. 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. Recent research advances in this field are surveyed, 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 [13].

In An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data paper, we propose a semantic multi-keyword ranked search scheme over the encrypted cloud data, which simultaneously meets a set of strict privacy requirements. Firstly, we utilize the "Latent Semantic Analysis" to reveal relationship between terms and documents. The proposed scheme could return not only the exact matching files, but also the files including the terms latent semantically associated to the query keyword [14].

IV. PROPOSED WORK

In this section, we are proposed a new cloud based data security and searching system which is utilized for the secure data hosting and sharing systems. In this system provide a better security at data hosting on server and sharing the data, no one unauthorized person can steal the information. Interact with user data from anywhere in the world using internet, when data are stored at server its views as public and provide easily searching on network. Anyone can search and easily download the data from the server in the world.



Uploading the data firstly, inter user id and password then select the input data, the input data is processed first for storing in the cloud storage. After selecting data file encryption phase is used, in this phase encryption is performed. Encryption is hybrid of AES (Advance Encryption Standard) and SHA(Secure Hash Algorithm)technique. After conversion of the file is transmitted on hosting server, where a chunk recovery mechanism works for re-organizing the file chunks into encrypted format. Cloud storage that is a cloud based storage server which provides the hosting space Cloud storage that is a cloud based storage server which provides the hosting space. Whole the data is store on cloud and all the process handled by third party.
The Hash table includes the file name, rename file, and user id for performing search and handling file owner. The file name is extracted to keep preserve during file search. Multiple file are stored in one cloud server so file name provide a unique name to each file. Rename file, two different file contents may have the same file name for purpose of uniqueness the file is renamed. After rename the file searching is easily.

Downloading data at cloud server firstly download the main chunk also download the all related chunks. After download chunks combine the chunks into a file that the file called main file. After file creation decryption process is apply to the data for decryption. For the decryption process use algorithm of hybrid of AES and DES. In this technique both algorithm are combine and use as a decryption algorithm. After decryption is performed file converted into original file.

V. CONCLUSION

In this paper, we have proposed an efficient data encryption and data decryption algorithm to protect the outsourced sensitive data in cloud computing

ISSN: 2278 – 1323

environment. In this paper we are focus mainly in the data searching on the cloud storage. In the cloud storage data are stored in the encrypted format so searching is applied on the encrypted data. On the other hand, to reduce the burden of data owner, trusted third party is introduced for verification of authorized users to access the data from cloud server.

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://drops.dagstuhl.de/opus/volltexte/dagrep-complete/2011/dagrep-v001-i012-complete.pdf
[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]http://en.wikipedia.org/wiki/Cloud_computing#/media/File:Cloud_computing.svg
[4]http://www.techopedia.com/definition/26929/data-access.
[5]https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=39&cad=rja&uact=8&ved=0CFAQFjAIOB4&url=http%3A%2F%2Fwww.ijsr.net%2Farchive%2Fv3i3%2FMDIwMTMxMTI4.pdf&ei=jkAMVbj6JsOVuASktYDYAg&usg=AFQjCNF6YsdWmXNCMfofjfP10xnbvZvn4g&bvm=bv.88528373,d.c2E
[6]http://searchsoftwarequality.techtarget.com/definition/cryptography
[7]http://research.microsoft.com/en-us/people/klauter/cryptostoragerlcps.pdf
[8]http://www.cs.princeton.edu/%7Echazelle/courses/BIB/overview-crypto.pdf
[9]http://www.ijarcsse.com/docs/papers/Volume_4/11_November2014/V4I11-0412.pdf
[10]http://www.ijarcsse.com/docs/papers/10_October2012/Volume_2_issue_10_October2012/V2I10-0028.pdf
[11]http://www.cis.temple.edu/~wu/research/publications/Publication_files/Secure%20and%20Privacy%20Preserving%20Keyword%20Search%20for%20Cloud%20Storage.pdf
[12]http://www.meeting.edu.cn/meeting/UploadPapers/1281520889828.pdf
[13]http://www.ijarcsse.com/docs/papers/Volume_4/12_December2014/V4I12-0206.pdf
[14]http://www.sersc.org/journals/IJSIA/vol8_no2_2014/33.p

ISSN: 2278 – 1323