Journal of Theoretical and Applied Information Technology
30th June 2018. Vol.96. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SEARCHING OVER ENCRYPTED SHARED DATA VIA CLOUD DATA STORAGE

[1]SAMEEH ABDULGHAFOUR JASSIM, [2]WALEED KAREEM AWAD

[1]Department of Vocational Education, General Directorate of Education in Anbar, Ministry of Education, Hit, Anbar, Iraq

[2]College of Computer Science and Information Technology, University of Anbar, Anbar, Iraq

E-mail: [1]prog85sameeh@gmail.com, [2]waleed.yahsat@gmail.com

ABSTRACT

Cloud computing has developed from various technologies such as autonomic computing, virtualization, grid computing, and other technologies, and the secure storage is essential and important for it due to it provides virtualized resources on Internet. Therefore, Data owner must encrypt his documents locally before uploading it in the public cloud storage to prevent unauthorized access to his data. Sometimes, the data owner wants to share some of his encrypted documents that stored in the cloud with other authorized users, so, he must send the secret key for each document for all authorized users, but this way has many limitations due to the difficulty of key management and key distribution. To overcome drawback of this approach we proposed system to generate a single key used for multiple number of documents and users depending on two techniques asymmetric cryptography and symmetric cryptography. Asymmetric cryptography used the IBC of the data owner to generate his private key and split the private key into two parts give one part to all authorized users and the other part send to Semi-Trusted Third Party (STTP). While symmetric cryptography used by combined secret key with the encrypted file properties and decrypted the result by the public key of the data owner by using asymmetric cryptography (RSA algorithm). Finally, many results were obtain from implementing the proposed system, among these results; the data owner could add or revoke any user without change the master secret key, also the data owner not need to share multi keys with authorized users. As well as, the system overcame the problem on difficulty of searching over encrypted data through encryption key in a public cloud.

Keywords: *Cloud Computing, Cryptography, Revocation, Virtualization, Homomorphic.*

1. INTRODUCTION

Security of network is a vital part of everyday life; because the rapidly increasing that occurring on the Internet by increasing the number of transactions, as well as there are a new challenges arise with every new technology. Therefore, Cloud computing is a modern business model that use the internet to access to a grand pool of resources. The main aim from using the cloud computing is to reduce the costs and giving the users the ability to focus on their business instead of the information technology enabling this business.

A security mechanism can be define as a device or a process used to detect, prevent, or recover from a security attack, so, to achieve security objectives security mechanisms used encryption, steganography, hashing, etc. While network security used to prevent unauthorized users to access to data and software at the network level. Generally, network security consists of three layers: (a) Border security (used to achieve control on security devices such as intrusion detection systems, firewalls, and intrusion prevention systems), (b) Authentication layer (used to authenticate of uses identities), and (c) authorization (used to give the users the primitive to access resources and which type of access this user is granted)[1].

Cloud computing has developed from various technologies such as autonomic computing, virtualization, grid computing, and others technologies. There are different services in cloud computing such as (SaaS, PaaS, and IaaS) and four deployment models (Public clouds, Private clouds, Community clouds, and Hybrid clouds) depending on their own characteristics to help the customers and the organizations to choose the models that suit their businesses. In addition, cloud computing used the federation and Single Sign On (SSO). However, there are many challenges remain in the security of cloud computing such major challenges are access

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and management, trust, business sustainability, and development of scalable service [1].

Storing data online in the cloud called cloud storage. However, data sharing is a very important issue in cloud storage as well as the method of sharing the encrypted data also represents a big challenge in the cloud storage[2].

Data owner must encrypt his/her documents locally before uploading it in the public cloud storage because the documents almost containing sensitive information and must be kept secured from all except the authorized users. Key-aggregate searchable encryption (KASE) used to search about the encrypted keywords while the data owner must be providing the users by keys to enable them to access on their data, so, data owner will have a problem in distributing a huge number of keys to the users.

The aim of this paper is to achieving privacy to the data owners' files those are stored on the public cloud. Furthermore, enhance the keys management as well as the system provides to data owner the ability to revoke or add any user without change the master secret key. In addition, we used the asymmetric cryptography to exchange the keys while a symmetric cryptography used to encrypt and decrypt the big files. This paper organized as follows: Section 2 gives a literature survey about significant related work. Then, cloud storage, advantages of using the cloud, and homomorphic cryptosystems are explain in section 3, 4 and 5 respectively. After that, we explained the virtualization in section 6. Next, in section 7 we described the proposed system architecture to implement the system in accordance with the requirements goals. Section 8 gives the system operations of our proposal and its main phases. In Section 9 system requirements and results are presented. Finally, the most important conclusions of the paper are gives in Section 10.

2. LITERATURE SURVEY

Cloud computing has been developed from various technologies since 2008 until now because it is being put to work in a variety of solutions and services that led many companies and researchers to suggest, study, and implement novel systems in cloud computing. The aim from the literature survey is to cover all relevant scientific literature of top quality.

In [3] Dan Boneh, et al refers methodology of using Public Key Encryption with keyword Search based on the computational of Diffie-Hellman problem and IBE construction. This system used when the own data want to upload their data to un-trusted third-party database. In this approach, the customer must send the key to the server to identify that all messages are containing some specific keyword without learning extra information.

In 2015 K.Manohar, R. Anil Kumar and N.Parashuram had proposed way of Key aggregate searchable encryption (KASE) as a foster solution. In KASE when user(A) giving a single aggregate key rather than {ki}mi=1 for sharing m files with user(B), while user(B) giving a single aggregate trapdoor rather than { Tri }mi=1, to the server of cloud. The aggregate trapdoor can be used with some public data by the server cloud to execute keyword search and return the result to user(B). Searchable with a constant size trapdoor generated by a constant size aggregate key applied to design a KASE under which any subset of the keyword cipher texts from any documents set[4].

In [5] K. Rajasrika, P.S. Smitha proposed an approach to achieving cloud data sharing using KASE. They used the technique of bilinear aggregate signature to achieve key auditing. To reduce the computation overhead, they used Key auditing. In the proposed system there is no special relation is required between the classes. In additional, they introduced the concepts of scheme robustness and similarity relevance to formulate the privacy issues in encryption schemes and proposing a random key encryption scheme to solve the insecurity problem.

In [6] Nikesh Pansare , et al proposed a method for (KASE) for user revocation in cloud storage, in this proposed system any customer can selectively share group of selected documents with a group of selected customers, as well as revocation of customer is used in the system. Forward secrecy and backward secrecy are use in user revocation for the key updating in the cloud storage. The mean of forward secrecy used if a new customer adds into the group to inform the aggregate of the new member to the group. Whereas the mean of backward secrecy used when any customer leaves from the group, the aggregate key must be update in the server and the new aggregate key must be inform the group members.

In November 2017, PUTTA SRIVANI, et al they used the pbc library to test the results of combined Multi-key Searchable Encryption Scheme with various elliptic curve parameters. In addition, their scheme is performed the encryption operations and decryption operations at the side of client, while the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

search operation on encrypted data can be done at the server side[7].

3. CLOUD STORAGE

Cloud storage can be defined as a delivering virtualized storage to the users on demand. Storage Networking Industry Association (SNIA) proposed Data Storage as a Service (DaaS) as depicted in Figure (1). DaaS is defined as "Delivery over a network of appropriately configured virtual storage and related data services, based on a request for a given service level"[8].

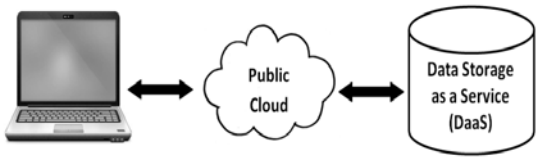

Figure 1: Data Storage as a Service (DaaS) according to SNAI definition (adapted from [8])

A cloud storage services provide transparency to the customers, which means the customers no need to know how the cloud service provider manages, implements, or operates their data within the cloud. Data resources must be available to access to the cloud at any time, and from any location in the world through networks. The main purpose from using cloud storage and other cloud services used to reduce the cost (i.e., "pay per use")[8]. The challenges that related to the cloud characteristics are:

- **Outsourcing:** Data and process security are the main reason behind the limitation of widespread use and development of cloud storage. When the customers outsourcing their data into cloud storage they will delegating the responsibility of business functions to a third party to perform the burden of maintaining data. On contrast, the customers will partially lose control on their data and tasks. Therefore, data owners must be aware of confidentiality, integrity and privacy challenges as well as business continuity, availability of services and data error recovery. Consequently, cloud service provider (CSP) must provide trust and access management to data storage[9].
- **Multi-tenancy:** Cloud service providers usually use virtual environment in cloud infrastructure to share multiple customers their resources, that means the data belonging to different customers may be put on the same physical machine. CSP use virtualization because its economic efficiency, so, malicious users may use this vulnerabilities on the cloud platform to perform flooding attacks[9].
- **Massive data:** Security of cloud computing is more difficult to control because the environment of it becomes dynamic and demanding. Moreover, data and applications scale grows such as data mining and image processing in the cloud. Therefore, traditional security mechanisms are not sufficient and efficient because the communication overhead and the heavy computations [2][9].

There are principal security properties are highly recommended with any remote storage system like cloud storage, namely, integrity, confidentiality and freshness. Data must protect from modified when it transferred and stored in cloud storage servers. As such, cloud service providers must provide to customers data availability claims and fine grained access as well as security requirements such as effective data and process isolation[9].

4. ADVANTAGES OF USING THE CLOUD

The most important advantages of using the cloud are hard to dispute but we will summarized it as follows[1][10]:

1. Saving the cost: for instance, the customers of cloud computing could rent a hardware space to use it in the peak time instead of buying server hardware to use it for a short time period (pay per use).
2. Reduce the costs of maintenance and implementation (IT departments of the organizations are focus on innovation rather than maintenance and implementation).
3. The infrastructures of cloud computing are scalable and Flexible.
4. Small/medium-sized organizations can be used the high-performance applications that available on the cloud computing to develop their businesses.
5. Reduced the effect of the environmental: sharing the hardware resources in the cloud computing will reduce the amounts of carbon footprint and saving the environment.

5. HOMOMORPHIC CRYPTOSYSTEMS

Homomorphic encryption means the ability to perform specific types of computations on ciphertext and generate an encrypted result, which matches the results of operations that performed on the plaintext after decrypted it. Cloud storage environments often used the homomorphic encryption therefore, the homomorphic encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

expected to play an important part in cloud computing because it allowing organizations to store encrypted data in a public cloud as well as allowing complex mathematical operations to perform on ciphertext without compromising the encryption[9][11][12].

A homomorphism in abstract algebra can be defined as a structure-preserving map between two algebraic structures, like groups. A group is a set G, jointly with an operation $\circ$ (denominate the group law of G) which combines any two elements (a and b) to compose another element, symbolized $a \circ b$. There are four requirements must be satisfied between the set and operation, $(G, \circ)$ to qualify as a group known as the group axioms[13]:

- **Associativity:** For all a, b, and c in G, $(a \circ b) \circ c = a \circ (b \circ c)$.
- **Closure:** For all a, b, and c in G, the result of the operation, $a \circ b$ is also in G.
- **Inverse element:** For each a in G, there exists an element b in G such that $a \circ b = b \circ a = e$, (where e is the identity element).
- **Identity element:** There is an element e in G, where for every element a in G, the equality $e \circ a = a \circ e = a$ holds. This element is unique, and thus one speaks of the identity element. The identity element of a group G is usually written as 1.

6. VIRTUALIZATION

Virtualization has evolved greatly since the 1960s, Figure (2) shows the evolution of the data center from the basic virtualization to a full Software-Platform-Infrastructure (SPI) model framework, thereby reducing the cost and increasing the flexibility.

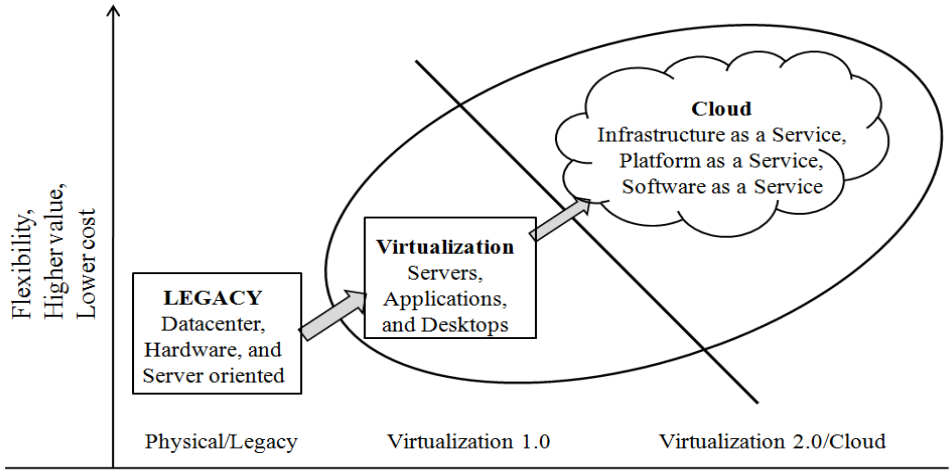

Figure 5: SPI evolution through virtualization (adapted from [14])

Also, the virtualization can be defined simply as an emulation of hardware in software platform in order to share the resources of one physical computer with a multitude of environments, so, the virtualization considered the essential technology of the cloud computing. Moreover, there are various types of virtualization for instance virtual memory (used to make the physical locations of the scattered data between the RAM and Hard Drive of the computer are worked and stored contiguously and in order), Redundant Array of Independent Disks (used with disk partitioning), processor virtualization, networks virtualization, and many of the other virtualization technologies like[15][16]:

- **Server virtualization**: it is the ability to partition one physical server into multiple virtual servers.
- **Application virtualization**: it is software that used to allow multiple operating systems to run on and separate from underlying operating system, hence, the applications believe it is working directly with the original operating system.
- **Presentation virtualization**: it is a way to isolate the processing from the input/output and graphics, in such a way, the client could run and control on an

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

application (store in the server in any location in the world) from his location.

In general, cloud computing used a large pool of servers called datacenter that may be located on any location of the world and it can be access via the Internet, In such a way, virtualizing servers is used in order to allows multiple virtual servers to run on one physical server [16].

Virtualization is used for many purposes and the most important of them are[16][14]:

- Allow multiple users to share computer system resources.
- Isolating the users from each other as well as from the control program.
- Emulating the hardware that found on another machine.
- The used of hardware resources will increase.
- The resource costs and the management will reduce.
- Enhanced business flexibility.
- Reduced downtime and enhanced security.
- Could deployment of additional servers rapidly.

Anyway, a hypervisor is usually software virtualization that used to monitor and control on virtual machines and also used to allow multiple virtual machines to share a single physical machine resources as well as it allows multiple guests operating systems to run on one computer hardware[15]. Therefore, the hypervisor considered the important part when using the virtualization, because the attacker if succeeds to attack the hypervisor he will be succeed to access to all the system resources.

In addition, the denial of service attacks are increased in virtualized systems because the virtualized systems share the same resources for instance processor, I/O devices, disk, memory, and so on. So, the protection techniques against denial of service attacks are more complex than traditional systems[14]. The basic types of the Denial-of-service attack are[15]:

- Consuming of Computational resources for instance processor time, bandwidth, disk space, and so on.
- Obstruction of configuration information for instance the information of routing
- Obstruction of state information for instance unsolicited resetting of TCP sessions
- Disruption the components of physical network.
- Crippling the communication media between the victim and the intended users therefore they cannot be communicate adequately between them.

7. GENERAL DESCRIPTION OF PROPOSED SYSTEM ARCHITECTURE:

We present, in this section, a typical technique for key aggregate searchable encryption (KASE) for group data sharing via cloud data storage based on Identity-Based Cryptography (IBC) and partition the private key into multi portions. In addition, in this proposal we used two techniques (symmetric cryptography and asymmetric cryptography) to take advantage of the advantages of each technique. This proposal is aimed to: (1) Reduce the complexity of the keys management and reduce the number of keys that distributed; (2) The users could search over any numbers of encrypted shared files depending on their file properties (name, size in bit, created date, modified date, etc.) and their private keys; (3) Protect the security of data that are shared in the cloud from the cloud provider and other malicious users by encrypt the data before storing into the DaaS; and finally (4) Easy to add users to the group or revocation the users from the group.

Figure (3) illustrates a descriptive the structure for the proposed system, which consists of four main parts. It relies on the following entities, permitting a user to share, store and retrieve data as well as search on encrypted data with multiple users:

- **Data owner:** Each Data Owner must have a unique and authentic identity, denoted by IBC and it can be either an individual or an enterprise. Moreover, the Data Owner used Data Storage as a Service (DaaS) to share, store and retrieve data as well as search on encrypted data with multiple users.
- **Semi-Trusted Third Party (STTP):** Provide an access control of all users of proposed system as well as enable the users to search on encrypted documents.
- **Data Storage as a Service (DaaS):** A DaaS provides virtual infrastructure to host application services, in addition, it has significant resources to manage distributed cloud storage servers. Data Owner can use the virtual applications to manage his/her data stored in the cloud servers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- **Users:** The users have the ability to access and decrypt the documents stored in the cloud depending on the access rights that are authorizations granted by the Data Owner. Moreover, the Data Owner must classify the users depending on their access rights into several groups and characterized each groups by a identifier with their a set of access rights.

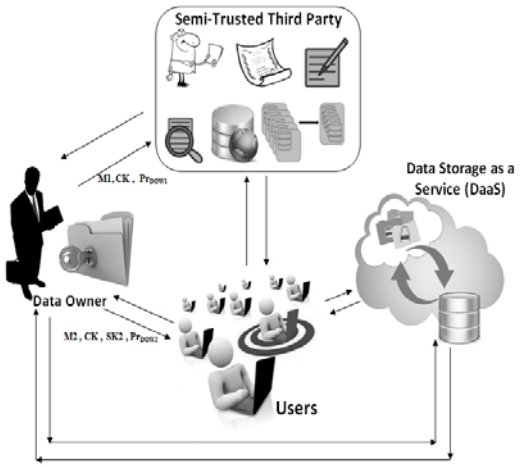

Figure 3: The general proposed system structure

8. SYSTEM OPERATIONS

8.1 Data Owner Operations

Firstly, Data Owner generate private key (Pr_{DOW}) depending on his identity and dividing the private key (Pr_{DOW}) into two parts giving one half (Pr_{DOW1}) to the Semi Trusted Third Party (STTP) and send the other part (Pr_{DOW2}) to all authorized users, There are many algorithms used to split the private key of user. Therefore, we will use the threshold to splitting the private key, whereas, Data Owner will make the "master" public key (the identity of the Data Owner (Pu_{DOW})) public for all the interested users. The users used the identity of the Data Owner in order to verify him.

Secondly, Data Owner also chooses secret key (SK) and dividing it into two parts sends one part (SK1) to all authorized users by secure e-mails and sends the other part (SK2) to STTP. The secret key (SK) is used to encrypt the documents of the Data Owner locally before uploading to the un-trusted cloud because the symmetric cryptography (block ciphers) is much faster than asymmetric cryptography in such applications (clouding applications).

After that, Data Owner must classify his documents into multi groups depending on users' authorizations, and then encrypt his documents (P) by using the secret key (SK) and the properties of the documents or folders (dp), and upload the results to un-trusted cloud (data owner may store each documents that have the same authorized access into one folder). We use the AES algorithm for the encryption and decryption of documents:

$$F = H(SK + (dp));$$

$$C = E(P, F);$$

In addition, Data Owner encrypts the keywords and documents properties (dp) by using his public key (Pu_{DOW}):

$$CK = E(keywords, dp)^{(PuDOW)} \bmod n$$

The Data Owner should attach the index of the encrypted keywords with the encrypted documents and uploading it to un-trusted cloud. Hence, the data owner matches the index of the decrypted documents with the index of the encrypted documents by using integer numbers that used by the users after decrypted the keywords. Thereafter, the Data Owner decrypts the keywords and documents properties (CK) by using the two halves of his private key ((Pr_{DOW1}) and (Pr_{DOW2})):

$$M1 = D(CK)^{(PrDOW1)} \bmod n$$

$$M2 = D(CK)^{(PrDOW2)} \bmod n$$

M1, CK and tables (contain the information about all users and documents) send to Semi Trusted Third Party (STTP), while M2 and CK send to the authorized users. In this way, neither the user could complete the search to obtain the decrypted keywords without getting help from the STTP nor the STTP could decrypt the encryption keywords and obtain the secret keywords due to he does not have the other part of the data owner private key (Pr_{DOW2}) and the secret key (SK_2).

Finally, in this proposal, we used the properties of the documents (dp) as a part of the secret key in order to reduce the complex of the keys distribution, and ease revoke any user from the group without change the master secret key. Anyway, any member within the group must be able to gain access to the documents anytime, anywhere without the data owner's intervention. Moreover, this system allows the data owner to add new users to the group or revoke access rights against any user of the group over his shared documents. As well as, this system, provides gain access to the documents, to all authorized users and data owner, and prevent un-trusted cloud service provider and unauthorized users to view the documents of the data owner.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

8.2 Semi Trusted Third Party Operations

STTP is the second part of the system which will have the half of the user's private key (Pr_{DOW2}), STTP also provides an access control of all cloud computing users. STTP takes all the halves of the users' private keys for each organization from Data Owners and stores it in the database with decrypted keywords and decrypted documents properties as well as other information of the users. STTP has many advantages such as:

i. The full operations of search to get the documents properties cannot be accomplish without acceptance of STTP because it has the halves of users private key.

ii. STTP manages the activities of users for instance (authorization, checks expire of key, etc.).

iii. It manages the revocation of the users. When the data owner revokes a user, he sends the users' identity to the STTP to add the user to the "revocations user's database". Therefore, the STTP should check the recipient of the users' request in the "revocations user's database" if the user is not revoke STTP sends to the user all data that help him to search, download, and decrypt his documents or files.

8.3 Users Operations

The third part of the proposed system is the users. The users use inquiry privacy when they need to search about the documents, that means the attaches cannot determine the keyword used in an inquiry. However, the users could be staffs of an organization in the same group or department, which permits them to search, download, and decrypt documents or files from the cloud.

The user should send request to STTP to take the permission from it. So, the STTP checks the user' request in the "revocations user's database" if the user is not revoke and he has the authorization to access to the documents, the STTP return to the user token ($M1= D (CK)^{(PrDOW1)}$ and SK2). Thus, the user multiplies M1 by M2 in order to get the decryption keyword and the documents properties.

$$M = M1 * M2 \bmod n$$

The STTP could not decrypt the encrypted documents because he does not have the M2 and the SK1. However, the user matches the index of the decrypted documents with the index of the encrypted documents to know the encrypted keywords. After that the user send the encrypted keywords to the cloud storage to download the encrypted documents then the user takes hash function to the documents properties (dp) and adds the result with the hash function of (SK2 + SK1) to obtain the F.

$$SK = SK1 + SK2;$$

$$F = H (SK + (dp));$$

$$P = D (C, F);$$

8.4 Data Storage as a Service (DaaS) Operations

The final part of the system is DaaS, A DaaS used to provide space storage (virtual infrastructure) to store and retrieve the encrypted documents of the data owner. In addition, Data Owner can use the virtual applications to manage his/her data stored in the cloud servers. Moreover, DaaS has an algorithm used to search within encrypted documents by using the encrypted keywords and return the result to all users, therefore, any user could search and download the encrypted documents if he has the properties of documents (dp) and the secret key (SK). In such way, we reduce the searching time and then retrieve the documents.

9. SYSTEM REQUIREMENTS AND RESULTS

9.1 System Requirements

We implemented the proposed system by using computer simulation as a first step for experimentation it. Moreover, we used Microsoft Visual Studio 2010 (visual C# language); due to it provide a great support of GUI to computing environments as well as it present to the data owner and the users a possibility to change or modify the content of the cloud services depending on their demands.

However, to implement the system we use the operating system Windows 7 (32-bit), and Microsoft SQL Server 2008 database as well as Microsoft Visual Studio 2010 (visual C#). While the hardware was, PCs of Intel Celeron Pentium 4 with CPU speed 1.50 GHz. In addition, RAM 2 GB and 40 GB free on hard disk.

Moreover, the system provides simple GUI for both the data owner and the users to simplify the use of the system. A sample data owner and user interfaces windows for the simulation software are illustrated in Figure (4).

Journal of Theoretical and Applied Information Technology
30th June 2018. Vol.96. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

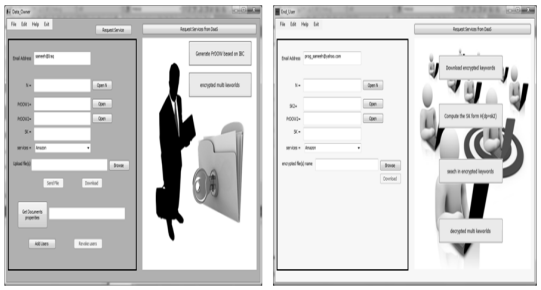

Figure 4: Typical interfaces windows for data owner and users

9.2 The Results and Discussion

There are many operations such as; cryptography, store, retrieve data, and search in encrypted documents were implemented in the proposed system. Furthermore, we use different types of hash functions (MD5 with output 16 bytes, SHA1 with output 20 bytes, SHA256 with output 32 bytes, SHA384 with output 48 bytes, SHA512 with output 64 bytes, and RIPEMD with output 20 bytes) with many system operations and compare the results and the execution time in millisecond with each others. The Table (1) provides details on the execution time taken for generate **data owner** private key (Pr_{DOW}) based on IBC and split it into two parts by using different types of hash functions.

Table 1: Time in milliseconds for generate data owner private key (Pr_{DOW}) based on his IBC

Types of hash function					
sha1	**md5**	**sha256**	**sha384**	**sha512**	**RIPEMD**
2 ms	3 ms	36 ms	2 ms	2 ms	18 ms

Table (2) shows the execution times that are required from the data owner to completing the operations of search about folders names in the database (as shown in Figure 5) and then taken hash function to the properties of files inside it by using different types of hash function. After that, the data owner encrypts the result based on his IBC in order to generate the encrypted keywords (CK). The data owner should not use SHA512 to do the mentioned operations because SHA512 was the slower than the other types of hash function.

Table 2: Time in milliseconds for search about folders names and taken hash function to the properties of files, subsequently encrypts the result based on data owner identity

The length	**Types of hash function**					
	sha1	**md5**	**sha256**	**sha384**	**sha512**	**RIPEMD**
One file inside one folder	158	199	210	171	195	190
100 folders each folder contain 10 files	36228	36393	37907	41286	44148	36035
1000 folders each folder contain 10 files	57426	55261	71257	103126	122051	60793
2000 folders each folder contain 10 files	118368	116287	146474	214525	250998	121624

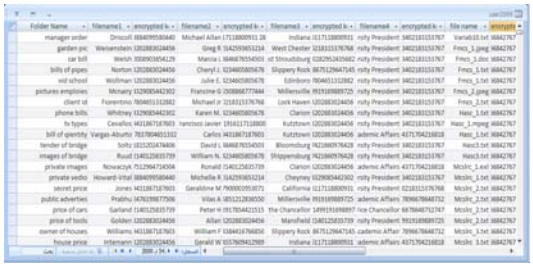

Figure 5: Database for folders names and the files which inside it

When **the user** wants a service, he should send request to STTP to take the permission from it. And the STTP return to the user token $(M1=D(CK)^{(PrDOW1)}$ and SK2), if the user has authorization access. Subsequently, the user multiplies M1 by M2 in order to get the decryption keyword and the documents properties. Hence, the user must used encrypted keyword to search in the database of DaaS and then download encrypted files or documents. So, the encrypted keywords and the decrypted keywords store in the user database at same table and same index, therefore when the user requests service from DaaS he uses the decrypted keywords in the GUI of the system and the program searches invisibly in the user database and send the encrypted keywords to the DaaS. Table (3) illustrates the average of implements time to search in encrypted database using encrypted keywords and return the results as a decrypted keywords by using different types of hash function.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Time in milliseconds to search in encrypted database using encrypted keywords and return the results as a decrypted keywords

The length	Types of hash function					
	sha1	md5	sha256	sha384	sha512	RIPEMD
500 encrypted keywords	2931	2999	2914	2925	2934	2952
5000 encrypted keywords	2943	3051	3076	2984	2970	2771
10000 encrypted keywords	3108	3109	3052	2945	2931	2946

In addition, **the user** must extract the properties of documents (dp) (size in bit, name, type) and add the result with the SK then compute different types of hash function on the result to get final secret key that used with the AES algorithm for the decryption of documents. The execution time to get the final secret key is shows in table (4). It's tested with three files different in size (1MB, 10 MB, 100MB). The data owner could use RIPEMD hash function to generate his private key based on his IBC because RIPEMD was the slowest than the other and it immune from collision attacks and brute-force attack.

Table 4: Time in milliseconds to get final secret key (SK)

Size of files	Types of hash function					
	sha1	md5	sha256	sha384	sha512	RIPEMD
1 MB	1704	1447	2086	2194	2485	6460
10 MB	1870	1923	1809	2110	2954	11257
100 MB	1984	2120	2047	2589	2468	15549

10. CONCLUSION

We studied in this paper the problem of searching over encrypted shared data in the cloud computing, and proposed some possible solutions. The aim from proposed system is to achieve privacy to the data owners' files those are stored on the public cloud. Furthermore, enhance the keys management as well as the system provides to data owner the ability to revoke or add any user without change the master secret key. In addition, we used the asymmetric cryptography to exchange the keys while a symmetric cryptography used to encrypt and decrypt the big files. We applied six types of hash function (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD) on different cryptography operations to compare the results and to compute the implementation time for each type.

The future works that could be done, by designing and implementing other types of asymmetric cryptography for exchanging and splitting the private key (such as Diffie–Hellman problem) and then compare the advantages and disadvantages of the results with our proposal.

REFRENCES:

[1] Mohammed M. Alani, "Elements of Cloud Computing Security", A Survey of Key Practicalities , ISSN 2191-5768 ISSN 2191-5776 (electronic), SpringerBriefs in Computer Science, ISBN 978-3-319-41410-2 ISBN 978-3-319-41411-9 (eBook), DOI 10.1007/978-3-319-41411-9, 2016, pp.1-16.

[2] Wakchaure Sonali Pandharinath and Sonkar Shrinivas K., " Group Data Searching And Sharing Using Key Aggregate Cryptosystem", IJARIIE-ISSN(O)-2395-4396, Vol-2 Issue-1 2016, pp.674-677.

[3] D. Boneh, Giovanni Di Crescenzo, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, LNCS 3027, 2004, pp. 506-522.

[4] K.Manohar,2R. Anil Kumar and N.Parashuram, "Key Aggregate Searchable Encryption for Group Data Sharing Via Cloud Data Storage", International Journal of Computer Engineering In Research Trends, ISSN (O): 2349-7084, Volume 2, Issue 12, December-2015, pp. 1132-1136.

[5] K. Rajasrika and P.S. Smitha, "Achieving Cloud Data Sharing Using Key Aggregate

Searchable Encryption", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, (An ISO 3297: 2007 Certified Organization), DOI: 10.15680/IJIRCCE.2015. 0312154, Vol. 3, Issue 12, December 2015, pp. 12773 - 12778

[6] Nikesh Pansare, Akash Somkuwar , Adil Shaikh and Satyam Shrestha, "Key-Aggregate Searchable Encryption (KASE) for User Revocation in Cloud Storage", International Journal of Engineering and Techniques - Volume 2 Issue 1, ISSN: 2395-1303, Jan - Feb 2016, pp.68-70.

[7] PUTTA SRIVANI, SIRANDAS RAMACHANDRAM and RANGU SRIDEVI, "EXPERIMENTAL RESULTS ON MULTI-KEY SEARCHABLE ENCRYPTION TECHNIQUE WITH DIFFERENT ELLIPTIC CURVES AND APP DESIGNING", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195, 15th November 2017. Vol.95. No 21, pp. 5787-5794.

[8] SNIA, Advanced Storage and Information Technology, "Implementing, Serving, and Using Cloud Storage". Cloud Storage Initiative. October 2010, http://www.snia.org/sites/default/files/2010-10-WP-ImplementingServingandUsingTheCloud.pdf , pp.1-15.

[9] Nesrine Kaaniche, "Cloud data storage security based on cryptographic mechanisms", TELECOM SudParis, PHD THESIS, Thesis No: 2014TELE0033, HAL Id: tel-01146029, Submitted on 27 Apr 2015, pp.11-13.

[10] John W. Rittinghouse and James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742, © 2010 by Taylor and Francis Group, LLC, International Standard Book Number: 978-1-4398-0680-7 (Hardback), 2010, pp. xxxiv-53.

[11] IBTIHAL MOUHIB and EL OUADGHIRI DRISS, "ENHANCED DATA SECURITY APPROACH FOR CLOUD ENVIRONMENT BASED ON VARIOUS ENCRYPTION TECHNIQUES", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195, 31st October 2015. Vol.80. No.3, pp. 439-446.

[12] OUADIA ZIBOUH, ANOUAR DALLI and HILAL DRISSI, "CLOUD COMPUTING SECURITY THROUGH PARALLELIZING FULLY HOMOMORPHIC ENCRYPTION APPLIED TO MULTI-CLOUD APPROACH", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195, 20th May 2016. Vol.87. No.2, pp. 300-307.

[13] Xun Yi, Russell Paulet, Elisa Bertino (auth.), "Homomorphic Encryption and Applications", SpringerBriefs in Computer Science, ISSN 2191-5768 ISSN 2191-5776 (electronic), ISBN 978-3-319-12228-1 ISBN 978-3-319-12229-8 (eBook), DOI 10.1007/978-3-319-12229-8, Springer Cham Heidelberg New York Dordrecht London, Library of Congress Control Number: 2014953221, 2014, pp.1-126.

[14] Ronald L. Krutz and Russell Dean Vines, "Cloud Security, A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., ISBN: 978-0-470-58987-8, 2010, pp. 23-159.

[15] David E. Y. Sarna, "Implementing and Developing Cloud Computing Applications", Auerbach Publications, Taylor and Francis Group, LLC, ISBN 978-1-4398-3082-6 (hardback), 2011, pp.10-176.

[16] Toby Velte, Anthony Velte and Robert Elsenpeter, "Cloud Computing, A Practical Approach, McGraw-Hill Osborne Media, ISBN: 978-0-07-162695-8, MHID: 0-07-162695-6, 2010, pp. 7-98.