Provide Privacy of Shared Data and Calculate Performance of Data Management System in Multiple Clouds

Konna Sirisha [1], E. Deepthi[2]
Final M.Sc. Student[1], Lecturer [2]
[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, Old Gajuwaka, Visakhapatnam
Andhra Pradesh

Abstract*:*

In Computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. We do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed. The idea behind cloud computing is similar, the user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. The cloud is internet based on how the internet is described in computer network diagrams, which means it is an abstraction hiding the complex infrastructure of the internet. Could technology-enabled services from the Internet without knowledge of, or control over the technologies behind these servers. Now way days cloud computing having the advantages in initial cost and availability for all users, whatever the shared information is fastly spreading all over the networks so fast and easily. Now concern is always problem all about security and memory management of the servers effectively changing the future values. In this paper we are calculate performance evaluation of data management for multiple clouds by implementing cryptography techniques.

Keywords: *Multi Cloud, Secret Shares, Cryptography, Encryption and Decryption .*

I. Introduction

The cloud computing is a cost-effective, service availability, flexible and on demand service delivery platform for providing business through the internet . Cloud computing resources can be quickly extracted and effortlessly scaled with all the processes, services and applications provisioned on demand service despite the consequences of the user location or device. Hence, the opportunity for an organization to enhance their service deliverance efficiencies is achieved through cloud computing. The issues in cloud security series from substantial security of the cloud fixing and hardware infrastructure, through the architectural security of function and data deployments, to the actual security of the cloud framework in the presence of peripheral attacks and the mechanisms accessible to respond to and recuperate from these attacks . The use of cloud computing Subashini and Kavitha argue services for many reasons including because this service provide fast access the applications and reduce service costs . Cloud computing providers should address privacy and security as matter for higher and urgent priorities. The dealing with 'single cloud' providers is becoming less popular service with customers due to potential problems such as service availability failure for some time and malicious insider's attacks in the single cloud. So now single cloud move towards 'multi clouds', 'interclouds', or 'cloud of clouds'.

Cloud computing concept is relatively new concept but it is based on not so many new technologies. Many of the features that makes cloud computing attractive, however has to meet certain basic security criteria. In our paper, we have briefed on various measure ion cloud computing security challenges from single to multi clouds. While making a cloud secure, the following objectives are to be met:

- Understanding the cloud computing environment provided by the cloud service provider.
- The cloud computing solution should meet the basic security and privacy requirements of any firm deploying it.
- Maintain an account of the privacy of the cloud and data security and applications that are deployed in cloud computing environment.
- Data Integrity

. • Service Availability.

- The user runs customer applications using the service provider's resources

Cloud computing is defined as a service model that enables convenient, on-demand network access to a large shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction . This innovative information system architecture, which is fundamentally changing the way that computing, storage and networking resources are allocated and managed, brings numerous advantages to users, including but not limited to reduced capital costs, easy access to information, improved flexibility, automatic service integration, and quick deployment . In spite of these advantages, as an emerging technology, cloud computing also faces tremendous security and privacy challenges which hinder its rapid adoption. Security has been recognized as the top barrier for users to move to cloud computing. The reason is multifaceted. First, in the cloud environment, users outsourcing their data and applications can only rely on the Cloud Service Provider (CSP) to protect their security. Many concerns are raised due to the fear of the unknown. Second, the unique characteristics of cloud computing introduce various new security challenges. Third, the immaturity of security technologies and lack of security governance in the cloud are obstacles to satisfy users' security needs. Frequent security outages in the cloud have undermined users' confidence in adopting this new technology. The development of advanced research on cloud security challenges and solutions is urgent. On the other hand, cloud computing presents some serious challenges to privacy. This is partly due to the fact that a person may easily lose control of his or her personal information under the terms and conditions of the CSP storing the person's information. In fact, many cloud-based social media rely on their leverage on an individual's private information to make profits. Therefore, it is highly probable for these companies to have clashes with their customers regarding their privacy policies. In this paper, we do not have separate sections that address privacy concerns in cloud computing. Rather, we discuss privacy in an opportunistic manner in various sections of our paper whenever the discussion is relevant

II. RELATED WORK

Cloud computing represents one of the most currently emerging technologies, in which a cloud service provider (CSP) offers efficient data computing and storage to a global client base. Storing data into the cloud offers great convenience in the sense that users do not need care about the direct deployment and management of hardware infrastructure. As promising as it is, cloud computing is much more powerful than personal computing, but it brings new security challenges to users' data. Since users no longer have physical possession of their outsourced data, data outsourcing is relinquishing users' control over their data. As a result, the privacy of users and the security of data face various threats. Therefore, the data owner requires high security and confidentiality of the data when outsourcing it in the cloud. However, traditional cryptographic primitives cannot be directly employed to achieve data security. Recently, there has been a plethora of work on privacy and security in the content of ensuring sharing of remotely stored data under different systems and security models. Those works mainly focus on how to preserve the user's privacy and realize the desired security goal without bringing a high complexity on the user decrypted stage. To solve this issue, researchers either utilize key-policy attribute-based encryption (KP-ABE) for secure access control, or employ hierarchical identity based encryption (HIBE) for data security. The KP-ABE-based schemes , however, reveal some users access attributes to the cloud, and then these cannot fully preserve the user's privacy and are also not fully collusion resistant. On the other hand, the HIBE-based schemes, introduce too many keys (each user has a mass of keys) and cannot manage efficiently. Therefore, the challenge to achieve goals of both privacy preserving and effective cloud data sharing service still remains open. To realize an effective and privacy-preserving data sharing service in cloud computing, the following requirements should be achieved. Firstly, the data owner should be able to decide whether a user can access to his cloud data or not. Secondly, the privacy of users should be protected against the cloud. Finally, the accessing users may access the sharing data using connected terminals with low computing ability, such as smartphone and tablet. To date, these important fields in cloud sharing remains elusive.

Newly, multi-cloud data hosting has received wide notice from researchers, customers, and start-ups. The fundamental principle of multi-cloud (data hosting) is to allocate data across multiple clouds to gain improved redundancy and avoid the vendor lock-in risks. Cloud storage services such as Microsoft One Drive ,Google Drive and Drop boxes provide users with a convenient and reliable way to share and store data from anywhere, on any device, and at any time. The users' data stored in cloud storage are mechanically synchronized across all the designated devices connected to the cloud in a well-timed manner. With multiplicity of devices – particularly mobile devices – that users possess today, such "anywhere, anytime" features significantly simplify consistency maintenance and data management, thus provide an ideal tool for data sharing and association. File operation includes file creation, file deletion, file modification, and frequent file modifications. Data update rate denotes how often a file operation happens. Sync deferment. When frequent file modifications happen, some cloud storage services intentionally reschedule the sync process for a certain period of time for batching file updates. Data sync granularity. A file operation is synchronized to the cloud either in a full-file granularity or in an incremental, chunk stage granularity. When the former is adopted, the whole updated file is delivered to the cloud; when the latter is adopted, only those file chunks that contain altered bits (relative to the file stored in the cloud) are delivered.

III.PROPOSED SYSTEM

In the proposed system we are implementing an efficient Tiny Encryption authority identity based technique for authentication of data consumers. Before performing authentication of users or data consumers each user will register into cloud. After completion of user registration the cloud server will performing authentication process. The completion of authentication process the cloud server will generate master key for all users. The master key is used for encryption and re encryption of shared data in cloud. After successful authentication of each user the cloud server will send the master key to all users in the cloud. The cloud server will also send the master key to data owner. The cloud server will send mater key to respected users mail ids. After completion of key generation process the data owner will encrypt the data and stored into cloud. The data consumer or user will retrieve required file and re encrypt that file. After completion of re encryption process the user will get original plain format data. The implementation procedure of multi authority identity based technique is as follows.

Authentication of Users:

In this module each user will be identify by the cloud server by performing multi authority identity based technique. Before performing authentication process each user will login into cloud server. After completion of log in process each user will perform the following steps for performing authentication process.

Each user or data consumer randomly choose the random nonce Ri and send that value to cloud server.

The cloud server will retrieve all users random once and generate universal key to all users. After generating that key the cloud server will send universal key (U) to all users in the cloud.

Each user will retrieve universal key and generate shared point (xi, yi). the user will take shared point and perform xor operation between universal key and shared point is

$(xi,yi\circledR\ U)$. Take the xor shared point and send to cloud server.

The cloud server will retrieve all users xor shared points and get original share points (xi,yi) by performing xor operation. The cloud server takes those shared points of all users and generates unique identity of each user by using following equation.

$$(uid)I = Ri \circledR U \circledR (xi, yi)$$

After generating unique identity of each user the cloud server will send those ids to individual users.

Each user will retrieve the unique identity and generate signature by using following equation.

$$sigi= H\ (id \circledR Ri\circledR U \circledR (xi, yi) \circledR (uid)i)$$

After generating signature each user will send those signatures to cloud server. The cloud server will retrieve all users signature and again generate signature by using those values.

The cloud server will take both signature and compare it. If the both signatures are equal those users are authenticated users else those users are not authenticated users.

After completion of authentication process the cloud server will sending authentication status of individual users. Before sending authentication status of users the cloud server will generate master key for encryption and decryption process. After generating master key the cloud server will send that key to all users mail id. The implementation procedure of master key is as follows.

Generation of Master key:

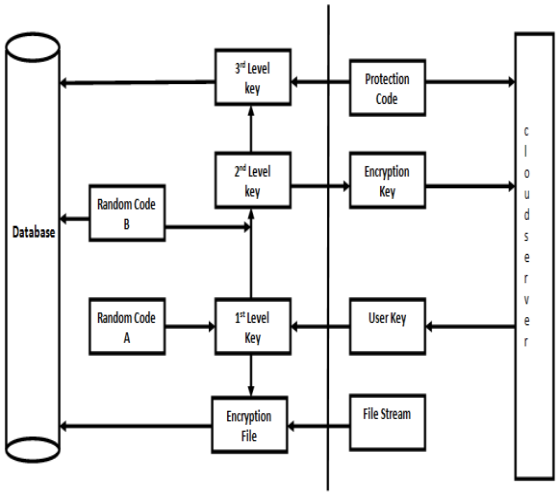
In this module the cloud server will generate master key and send that key all users in the cloud. The sending of master key can be done only the authenticated users in cloud. The master key can be send through respect user's mail ids. The cloud server will also send master key to data owner. The data owner will use master key for encryption of uploaded documents. The generation of master key is as follows.

In the key generation process the cloud server will randomly generate code A and the string in request stream is encoded with code A to generate the first level encryption key. The first level encryption key is also known as master key.

In the second level, the cloud server randomly generates code B and the first level encryption key is encoded with code B to generate the second level encryption key.

The code B is stored in the database, and the new file of second level encryption key is generated and sent to the each user by using the mail which is developed by using the smtp protocol.

In case of losing the second level encryption key, the cloud server generates the third level encryption key based on the second level encryption key and a protection code which is randomly generated by the system. The third level encryption key is stored in the database.



The completion of key generation process the data owner will retrieve first level encryption key and encrypt the uploaded file. After completion of encryption process the data owner will store the cipher format document into cloud server. The cloud server will contain all cipher formatted documents. So that nobody could not get plain format documents. So that we can provide privacy of uploaded documents in the cloud. The implementation process of data encryption is as follows.

Encryption Process:

In this module the data owner will choose upload document and perform the encryption process. In this paper we are using extended tiny encryption algorithm. The implementation procedure of extended tiny encryption algorithm of encryption process is as follows

```
        private final static int SUGAR = 0x9E3779B9;
          private final static int CUPS  = 32;
          void brew(int[] buf) {
                   assert buf.length % 2 == 1;
                   int i, v0, v1, sum, n;
                   i = 1;
          while (i<buf.length)
          {
                   n = CUPS;
                  v0 = buf[i];
                   v1 = buf [i+1];
                   sum = 0;
            While (n-->0)
           {

v0  += (((v1 << 4 ) ^ (v1>>5)) + v1) ^ (sum +S[sum
& 3]);
sum += SUGAR;
v1   += (((v0 << 4 ) ^ (v0 >> 5))+ v0) ^ (sum
+S[(sum>>11) & 3]);
          }
buf[i] = v0;
buf[i+1] = v1;
i+=2;
}
         }
```

The completion of encryption process the data owner will stored cipher format into cloud server. After completion storing process each user will get all cipher format document and select required document. Take that document and perform the decryption process of extended tiny encryption algorithm. Before performing decryption process each user will be authenticated by cloud server. After successful authentication of users each user will get second level and get the first level encryption key or master key. Before getting master key each user will enter the second level key and get first level key or master key. Take that key and perform the decryption process.

Decryption Process:

In this module each user will retrieve the first level encryption key and perform the decryption process. In this module the user will take second level and using that key user will get first level encryption key. After getting first level encryption key the user will choose required document and perform the decryption process. The implementation procedure of decryption process is as follows.

```
private final static int SUGAR = 0x9E3779B9;
         Private final static int CUPS  = 32;
         Private   final   static   int   UNSUGAR   =
0xC6EF3720;

       void unbrew (int[] buf)
      {
                  assert buf.length % 2 == 1;
                  int i, v0, v1, sum, n;
                  i = 1;
         while (i<buf.length)
          {
            n = CUPS;
            v0 = buf[i];
            v1 = buf[i+1];
            sum = UNSUGAR;
            while (n--> 0)\
            {
v1   -= (((v0 << 4 ) ^ (v0 >> 5))+ v0) ^ (sum
+S[(sum>>11) & 3]);
         sum -= SUGAR;
v0  -= (((v1 << 4 ) ^ (v1>>5)) + v1) ^ (sum +S[sum
& 3]);

                           }
                           buf[i] = v0;
                           buf[i+1] = v1;
                           i+=2;
                  }
         }
```

After completion of decryption process each user will get original plain format documents. In this paper we are also implementation of AES algorithm for performing encryption and decryption process. After completion of encryption and decryption process we can calculate time for both algorithms. Take that time of both algorithms and evaluate performance of both algorithm. By evaluate performance the proposed system will get better performance compared to AES algorithm.

IV. Conclusions

So in this paper we are proposed a novel multi authority and efficient cryptography techniques for authentication in the cloud. Before stored data into cloud server each user will be identify by the cloud server. After completion of authentication process the cloud server will generate master key or first level encryption key for data encryption and decryption. Before performing encryption and decryption process the cloud server will send second level key all user mail ids. By using second level each user will get first level encryption key. The cloud server also sends first level encryption key or master key to data owner. The data owner will take first level encryption key and perform the encryption process. In this paper we are using extended tiny encryption algorithm for performing encryption process. After completion of encryption process the cloud server will stored cipher formatted data into cloud server. The authenticated user will take second level key and get the first level encryption key. By using first level encryption key or master will perform the decryption process of extended tiny encryption algorithm. After completion of decryption process each user will get plain format data. In this paper we can also implement AES algorithm for doing encryption and decryption of data. After completion of encryption and decryption process we can calculate time of those algorithms. Taking that time we can evaluate performance of those algorithms. After completion of performance evaluation process the proposed algorithm give the better performance other the AES algorithm. By performing those operations we can improve privacy in the shared data and provide more efficiency in the authentication, key generation process.

References

[1] N Cao, C. Wang, M. Li,K.Ren, and W. Lou, “Privacy preserving keyword ranked search over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol, 25, no. 1, pp. 222-223, Jan. 2014.

[2] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou,”secure ranked keyword search over encrypted cloud data,” in Proc. IEEE 30th Int. Conf. Distrib. Compute. Syst. (ICDCS), jun.2010, pp. 253-262.

[3] B. Wang, S. Yu, W.Lou, and Y.T.Hou, “privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2112- 2120.

[4] C.Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” IEEE Trans.Parallel Distrib. Syst., vol.23, no.8, pp. 1467- 1479, Aug. 2012.

[5] K. Srinivasa Reddy and S. Ramachandram “A New Randomized Order Preserving Encryption Scheme” In International Journal of Computer Applications (0975 – 8887) Volume 108 – No 12, December 2014.

[6] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” In Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[7] A. Boldyreva, N. Chenette, Y. Lee, and A. O‟ Neill, “Order preserving symmetric encryption,” In Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2009, pp. 224– 241.

[8] Raluca Ada Popa , Frank H. Li , Nickolai Zeldovich “An Ideal-Security Protocol for Order Preserving Encoding” In Proc. of the 34th IEEE Symposium on Security and Privacy.

[9] K. Srinivasa Reddy and S. Ramachandram “A novel Dynamic Order-Preserving Encryption Scheme” In Networks & Soft Computing (ICNSC), 2014 First International Conference on 19- 0 Aug. 2014.

[10] R. Agrawal, J. Kiernan and R. Srikant, “Order preserving encryption for numeric data,” *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*. ACM, pp. 563-574, 2004.