International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Enhanced SEaaS to Provide Better Security for Data in Cloud Computing Environment

Rachitha M.V
Assistant Professor, Department of Computer Science & Engineering
Vemana Institute of Technology, Bengaluru, India

Abstract: ***Cloud computing is evolving very fast with the passage of time. Many users are storing their data on cloud. Security for the cloud is important because of its outsourced nature of computing. There are many issues related to the safety of data in cloud storage, so users are stepping back to store their data in the cloud. Hence, it is required a robust security technique to enhance the data security which gives better data storage, searching and retrieving data from cloud and also secures from various vulnerable attacks by users. Cloud provides anything as a Service, Security as a service (SEaaS) is one of the services provided by the cloud service provider (CSP).In this paper algorithms are used to address the security issue in cloud storage in order to safe guard the data stored in the cloud and for better searching and retrieving data from cloud.***

Keywords: ***Cloud computing, Security, SEaaS ,CSP.***

I. INTRODUCTION

Cloud computing, often specified as the cloud, is the conveyance of on-demand computing resource everything from applications to data center over the internet on a pay for use basis. cloud computing is the distribution of computing services servers, storage, databases, networking, software and more over the Internet ("the cloud"). The Companies which contributes these computing services are called cloud providers. Benefits of cloud are: Less expense, speed, performance, productivity, reliability.

The things that we can do with the cloud are:

1. *Create new apps and services*
2. *Store, back up and recover data*
3. *Host websites and blogs*
4. *Stream audio and video*
5. *Deliver software on demand*
6. *Analyze data for patterns and make prediction*

A. TYPES OF CLOUD SERVICES:

Cloud computing services classified into three categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another.

Infrastructure-as-a-service (IaaS): It is the basic category of cloud computing services, with IaaS, you rent IT infrastructure: servers and virtual machines (VMs), storage, networks, operating systems from a cloud provider on a pay as you go basis.

Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications.

Software as a service (SaaS): Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and handle the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their mobile phone, tablet or Personal Computers.

B. CLOUD DEPLOYMENTS:

There are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud. Public cloud: Public clouds are maintained and run by a third-party cloud service provider, which deliver their computing resources like servers, storage over the Internet.

Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is maintained and handled by the cloud provider. You access these services and manage your account using a web browser.

Private cloud: A private cloud refers to cloud computing resources used completely by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud: Hybrid clouds combine public clouds and private clouds, enslaved organized by technology that allows sharing of data and applications between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

II. CLOUD SECURITY

Cloud computing is the conveyance of computing services over the Internet. Due to massive growth of data, the Data owners tend to outsource their data in the cloud with the advantage of reducing cost and assuring availability. The cloud computing model allows access to data and computer resources from anywhere that a network connection is available. It is a model for enabling suitable, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services can be quickly provisioned and released with minimal management effort or service provider communication. 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 like Google drive, social networking sites like Facebook, twitter, LinkedIn etc., webmail, and online business applications. Because of these benefits each and every organizations are moving their data to the cloud. Security is a major challenge [1] in cloud system due to its nature of outsourced computing. The problems to be considered for cloud data outsourcing are:

1) Data sent to the cloud is warehoused in public cloud storage and cloud storage is controlled and maintained by cloud service providers (CSP).2) Users do not have the rights to control and monitor the data in the cloud storage and do not even know where the data is kept. 3) Data may be mixed with other user's data in storage of cloud, because outsourced data is stored as plaintext in cloud storage like Amazon S3.4) Improper use of database information may be done by the provider itself. Another concern in cloud is useful data retrieval, to overcome this problem several solutions have been proposed to allow the search of keywords over encrypted data which are not efficient. Cloud systems are vulnerable to various attacks and susceptible by the users unless robust security scheme is implemented. So there is a need to protect that data against unauthorized access, modification or denial of services etc. Cloud security includes storage (databases hosted by the Cloud provider) and securing the treatments (calculations). Security goals of data include three points, they are: Availability Confidentiality and Integrity. Mostly, confidentiality, integrity and authentication are the critical areas. Confidentiality of data in the cloud is accomplished by cryptography and integrity of data is ensured by hashing algorithms.

III. LITRETURE REVIEW

There are number of works or research has been conducted to achieve the security for the data or the information in the cloud mainly by using different cryptographic techniques. To give importance about the performance of the encryption algorithms, this section describes and examines previous work done in field of data encryption.

Sunitha rani et al. [1] proposed an encryption algorithm to provide security in the cloud. The proposed method uses three encryption algorithms sequentially to encrypt a message. First, plaintext is encrypted by the ceaser cipher. Then the encrypted result from ceaser cipher is again encrypted via using RSA substitution algorithm and finally the result from RSA is once again encrypted by the mono alphabetic substitution method. This technique has taken more time to encrypt the text by three algorithms one by one.

Subhasri P. et al. [2] proposed a Multi-level Encryption algorithm to secure the data in the cloud. The proposed algorithm uses rail fence and ceaser cipher algorithm. Initially, plaintext is encrypted using rail fence technique. Assign the position value i to each letter in the encrypted text. Generate the ASCII values of each character. Assign a key and apply it on the text using the formula: $E = (p + k + i) \% 256$, where p denotes Plaintext, k denotes key and i denotes Position. Algorithm produces the ASCII character of the equivalent decimal value. Key used for encryption is not generated. Maintain the position of each character in the text requiring additional storage. Here, Author has not mentioned where the characters position details are maintained.

Manpreet K et al. [3] presented a Cipher Cloud framework. It helps users to keep their data confidential on public cloud. To achieve this, the framework uses a two-step encryption process, by which all the data sent from the client to cloud and cloud to client is retained completely encrypted. A thorough security control is needed to protect the most sensitive data that may not be guaranteed in the public cloud computing architectures.

Anshu P et al. [4] proposed encryption algorithm to make cloud data secure and vulnerable. Author discusses security issues, challenges of cloud and compares the existing algorithms like AES, DES, BLOWFISH and RSA Algorithms. Comparison shows that DES algorithm consumes less encryption time. RSA takes larger memory usage and encryption time. AES algorithm takes less time to execute cloud data. Blowfish algorithm consumes minimum memory.

Seth et al. [5] have done the comparative analysis of three algorithms; RSA, DES and AES while considering certain parameters such as computation time, memory usage and output byte. These parameters are the major issue of concern in any Encryption Algorithm. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

IV. METHODOLOGY

Data security is a precarious issue in cloud computing environment. Cloud has no border, and the data can be located anywhere in any data centers across the geographically distributed network, because of this many organization are ready to adopt the cloud storage by outsourcing their IT requisite. As the nature of cloud computing gives raises to serious issues concerning user data confidentiality. However, due to the issues related to security of data in the cloud storage, the organizations are stepping back to store their information or data on to the cloud storage. Hence, it is desired to propose and implement novel security technique to enhance the data security which gives better data storage, searching and retrieving data from cloud. Security is achieved by confidentiality parameter. By concentrating on this confidentiality parameter the flowing goals can be achieved.

1) *To ensure that stored information in the cloud is only accessed by the data owner.*
2) *To prevent the unauthorized access (outsider or CSP itself) by encrypting data before they are uploaded to cloud storage.*
3) *To efficiently search and retrieve the data.*

Cloud provides anything as a Service, cloud has mainly 3 services: SaaS (Software As a Service), PaaS (Platform As a Service), and IaaS (Infrastructure As a Service). Recently two more services have been provided by the Cloud Service Provider, they are:SEaaS(Security As a Service)[10] and NEaaS(Network As a Service). SEaaS provides different security service algorithms for safeguarding the data in the cloud. Figure 1 shows the cloud environment with CSP, which has SEaaS as one of its services. In figure 1, CSP1 provides services like SaaS, PaaS, IaaS, NEaaS, and SEaaS. Here, CSP1 is used only for security service, and not for storing the data. Users could store their data with other CSP's who provide storage as a service.

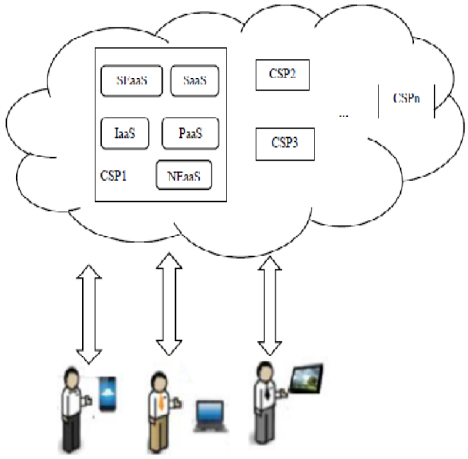

Figure 1. Cloud provider Architecture with SEaaS

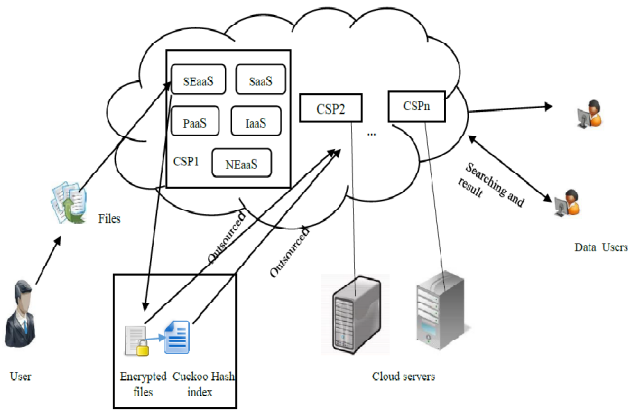

Figure 2. Architecture of encrypted files stored on Cloud using Cuckoo hashing

Figure 2 shows the proposed system architecture, SEaaS uses encryption algorithms to encrypt data (either plain text, audio, video). Encryption of plain text is achieved by combining substitution and transposition cipher techniques [10]. Encryption of audio, video [12] is done by dividing into frames then shuffling the frames and encrypting the shuffled frames by using AES(Advanced Encryption Standard).This encryption technique takes place at client's side before outsourcing data onto the cloud, after encryption the data owner outsources the encrypted data with cuckoo hash index to the cloud server. Cuckoo hashing and Latent Semantic search techniques help in efficient search & retrieval of data in the cloud.

V. ALGORITHM

DES algorithm and RSA algorithm for providing security to cloud storage. Cyber criminals can easily cracked single level encryption. Hence proposed system uses multilevel encryption and decryption to provide more security and Cuckoo hashing and Latent Semantic search techniques help in efficient search & retrieval of data in the Cloud Storage.
Key Generation Procedure:

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculate: $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1<e<\phi(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \phi(n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d).

Keep all the values d, p, q and ϕ secret.

ENCRYPTION

SENDER DOES THE FOLLOWING:-

1. *Obtains the recipient B's public key (n,e).*
2. *Represents the plaintext message as a positive integer m*
3. *Computes the cipher text $c = m^e \bmod n$.*
4. *Sends the cipher text c to B*

DECRYPTION

Receiver does the following:-

1. *Uses his private key (n, d) to compute $m = C^d \bmod n$.*
2. *Extracts the plaintext from the message representative m.*

DES ALGORITHM:

1. *Fractioning of the text into 64-bit (8 octet) blocks.*
2. *Initial permutation of blocks.*
3. *Breakdown of the blocks into two parts: left and right, named L and R.*
4. *Permutation and substitution steps repeated 16 times called rounds.*
5. *Re-joining of the left and right parts then inverse initial permutation.*

CUCKOO HASHING ALGORITHM STEPS TO INSERT DATA:

1. *Put in first location and displace residing element if needed*
2. *Put displaced element in its other location*
3. *Until finding a free spot*

ALGORITHM FOR LATENT SEMANTIC INDEXING:

To perform Latent Semantic Indexing on a group of documents, you perform the following steps:

Step 1: convert each document in your index into a vector of word occurrences. The number of dimensions your vector exists in is equal to the number of unique words in the entire document set. It is recommended that common words (e.g., "this", "him", "that", "the") are removed.
Step 2: Scale each vector so that every term gives the frequency of its occurrence in context
Step3: Combine these column vectors into a large term-document matrix. Rows represent terms, columns represent documents.
Step4: Perform Singular Value Decomposition on the term-document matrix. This will result in three matrices commonly called U, S and V. S is of particular interest, it is a diagonal matrix of singular values for your document system.
Step5:Set all but the k highest singular values to 0. k is a parameter that needs to be tuned based on your space. Very low values of k are very lossy, and net poor results. But very high values of k do not change the results much from simple vector search. This makes a new matrix, S'.
*Step6:Recombine the terms to form the original matrix (i.e., U * S' * V(t) = M' where (t) signifies transpose).*
Step7:Break this reduced rank term-document matrix back into column vectors. Associate these with their corresponding documents. Now you have a Latent Semantic Index.

VI. CONCLUSION

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations; there is a need to protect that data against unauthorized access, modification or denial of services etc. The security level of the proposed technique is high as compared to other existing because of multilevel encryption, integration of substitution, transposition cipher encryption and cuckoo hash index. Latent Semantic search techniques, performance (searching and retrieving time) of the proposed technique consumes less time than compared to other existing techniques but because of multilevel encryption and decryption it takes time.

REFERENCES

[1]. Sunita Rani, AmbrishGangal "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", International Journal of Computer Science and Information Technologies, Vol.3, pp.4302-4304, 2012.
[2]. Subhasri P., Padmapriya A., "Multilevel Encryption for Ensuring Security in Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, pp. 527-532,2013.
[3]. ManpreetKaur and Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Vol. 70, pp. 16-21,2013.
[4]. AnshuParashar and RachnaArora, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications, Vol. 3, pp. 1922-1926, 2013.Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", Worldof Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012
[5]. Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.
[6]. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.
[7]. S. Pavithra and Mrs. E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, pp. 43-45, August 2012.
[8]. Dr. L. Arockiam, S. Monikandan " A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 12,pp 1053-1058, December-2014
[9]. Dr. L. Arockiam, S. Monikandan " A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 12,pp 1053-1058, December-2014
[10]. Ashok George,A. Sumathi " Efficient Data Storage and Retrieval in Cloud Environment Using Cuckoo Hashing and Latent Semantic Search" Middle-East Journal of Scientific Research 23 (6): 1053-1058, 2015
[11]. Ashok George,A. Sumathi " Efficient Data Storage and Retrieval in Cloud Environment Using Cuckoo Hashing and Latent Semantic Search" Middle-East Journal of Scientific Research 23 (6): 1053-1058, 2015
[12]. Ajay Kulkarni Saurabh Kulkarni Ketki Haridas Aniket More "Proposed Video Encryption Algorithm v/s Other ExistingEngineering Research and Applications, Vol. 3, pp. 1922-1926, 2013
[13]. Michael T. Goodrich "Using Data-Oblivious Algorithms for Private Cloud Storage Access"Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh "Data Security Algorithms for Cloud Storage System using Cryptographic Method" International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March -2014
[14]. Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh "Data Security Algorithms for Cloud Storage System using Cryptographic Method" International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March -2014.

