International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

REVIEW ON CLOUD COMPUTING

A.R.RahimaYasmin
III B.sc(CS)
Madurai SivakasiNadars Pioneer Meenakshi Women's College-Poovanthi
reshrahim6@gmail.com

Abstract - Cloud Computing is very flexible in nature that helps to quickly access the resources efficiently from the third party service provider to expand the business with low capitalization cost.A cloud storage system stores large number of data in its storage server. Since the data is stored for a long term over the internet it does not provide the data confidentiality and make the hackers to steal the data provided in the storage system and even when data forwarded to cloud environment, it lacks data integrity and makes the cloud user unsatisfied. In this paper, we study about different encryption technique to protect the cloud storage environment. This paper concisely covers some of the existing cryptographic approaches that can be used to improve the security in cloud environment.

Keywords: Cloud computing, security threat, multitenantbehaveour,standards,cryptographictecniques,Cloud storage system,Encryption technique and policies.

The concept of cloud is not new. Network based computing is evolving for more than 50 years. But the term 'cloud' originated in 1990s. Many believe the first use of "cloud computing" in its modern context occurred in 2006, when then Google CEO Eric Schmidt introduced the term to an industry conference. It is a virtual environment that provides resources to users and charges only for services they consumed. Most of the things we see and use on internet are cloud, for example email services, google map, online file viewers, online file converter. In brief 'Cloud is metaphor for internet'. Its use is spreading rapidly because it captures a historic shift in the IT industry as more computer memory, processing power, and apps are hosted in remote data centers, or the "cloud." NIST (National Institute of Standards and Technology) has given official definition for cloud computing according to which a cloud should have these characteristics:

a)Resource Pooling
b)Self Service and on Demand Service
c)Broad Network Access
d)Rapid Elasticity
e)Measured Service

ADVANTAGES

First, expenses are lowered too much for companies. Now companies don't need to purchase computers or hire personnel for maintenance. Every computing facility (softwares), platforms, even whole infrastructure is provided as service virtually. This is especially useful for small startups which don't have much capital to invest.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

Second, cloud architecture is very scalable. For example cloud storages can easily manage thousands of GBs of data due to its distributed architecture whereas this task is problematic locally. Finally, there is cloud for everything, storage cloud for storage services, data cloud for data management services and compute cloud for computational services.

DISADVANTAGES

First, Cloud faces latency and bandwidth related issues because of being remotely hosted. Denial of service is also a threat to cloud computing. DOS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DOS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed.

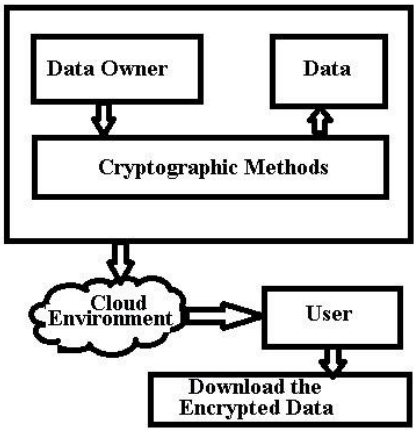
Then comes the problem of interoperability among cloud services.

Finally security issues are there such as data being accessible to third parties. Possibility of security leakage due to multi-tenancy nature.

CRYPTOGRAPHIC TECHNIQUES

The main components of a cryptographic storage service which can be implemented by using a different techniques, out of which, some were designed specifically for cloud storage. In the beginning of the Cloud Computing, common encryption Technique like Public Key Encryption was applied. This traditional technique does not provide expected result as it support one to one encryption type communication. Public Key Encryption is not highly scalable. This gave rise to move forward to some advanced encryption methods. The advanced cryptographic methods includes the below encryption methods.

- Searchable Encryption
- Symmetric searchable encryption
- Asymmetric Searchable Encryption (ASE).
- Homomorphic Encryption
- Identity Based Encryption
- Attribute-based Encryption
- KP-ABE
- CP-ABE
- MA-ABE
- Cloud DES Algorithm



CLOUD STRATEGY

SEARCHABLE ENCRYPTION

A searchable encryption scheme is applied at high level inoder to encrypt the content that is available in search index so that it can hidden from others except the party that provide the authorised tokens A collection of files which consists of full-text

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

index otherwise keyword It provides the authorisedtokens A collection of files which consists of full-text index otherwise keyword index considered to generate a search index. The index is encrypted based on searchable encryption scheme in such a way (i) The pointers to the encrypted files can be retrieved based on the tokens given for the keyword. (ii) if the token is not provided then the contents are hidden for the index. However, with the complete understanding of secret key, the tokens are generated. The retrieval procedure does not reveal the content of the files or the keywords apart from the files that comprise the keyword in common.

SYMMETRIC-SEARCHABLE ENCRYPTION

It is suitable for the environment where the client that searches the data and also he is responsible for generates it. A Single Writer/Single Reader (SWSR) is derived from cloud storage terminology. SSE schemes were presented in4 and enhanced constructions and security terms were specified in5-7. SSE has two major advantages they are efficiency and security. It also has disadvantages such as functionality and tradeoff efficiency. SSE schemes are suitable for the entity who perform the encryption and also for the entity who searches with a keyword from the cloud storage system. Most SSE schemes are efficient because they use the concept of pseudo-random functions and also block ciphers for encryption purpose. In7, Search technique can be efficient since SSE allows to pre-processed the data and efficiently represent in data structures. SSE provides security guarantees which are discussed as (i) the information about the data are hidden until the tokens are revealed. Since token is not revealed, the server learns only the length information. (ii) when the token is provided for a keyword, the server absorbs the document containing the keyword without knowing the keyword. When comparing with asymmetric and searchable encryption, it is found that security guarantees is much stronger without any limitations. Based on the various issues which is discussed above, every construction contains deterministic tokens. These deterministic tokens help the service provider to identify the repeated queries without knowing the query. It explained the duration of search time is optimal for the server but the index are inefficient during updates. On the other hand Goh5 proposed the index can be updated efficiently in the server but the search time is not optimal. The above mentioned scheme don't not focus on the search based on conjunctions or disjunction of terms. SSE scheme alone handles the concept of conjunction8 by pairing with the help of elliptic curves but it is inefficient when applying Asymmetric Searchable Encryption schemes (ASE). Another constraint of some searchable encryption is that they are only secure in a some situation where the queries are produced non-adaptively (ie, Without looking at the answer of the previous queries)., some queries which need the answer for the previous query can also bereffered and this is known as adaptive setting in a secure environment.

ASYMMETRICSEARCHABLE ENCRYPTION (ASE)

This scheme is suitable for the environment where the client that searches the data is different from

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

the one who generates it. This scenarios is referred as Many Writer/Single Reader application of ASE has been surveyed. In17, the complete privacy of queries is guarantee in ASE. The main disadvantage of ASE is weaker security and it is not efficient while the major advantage is its functionality. Compared to SSE scheme, The ASE is suitable for enormous amount of setting due to the multiple writer and reader. ASE is inefficient because it make use of the concept of pairings on elliptic curves. This concept will make the operation slow when compared to hash functions or block ciphers. ASE allows to pre-processed the data and inefficiently represents in data structures. ASE provides security guarantees which are discussed as (i) the information about the data are hidden until the tokens are revealed. Since token is not revealed, the server learns only the length information. (ii) when the token is provided for a keyword, the server absorbs the document containing the keyword without knowing the keyword which is inefficient when compared to SSE setting. In depicts the server can introduced a dictionary attack for a token and identify the proper keyword the client is looking for. It can also identify the token and perform a suitable search to find out which documents comprise the (known) keyword.

HOMOMORPHIC ENCRYPTION

Ronald Rivest explain the Homomorphic encryption concepts. This scheme is applied in the cloud environment to protect the data. This Homomorphic encryption scheme allows executing computations on the encrypted data. It is only of the advanced cryptographic technique. In20 the major drawback of homomorphic encryption is explained. It has a slow processing time during computation

IDENTITY BASED ENCRYPTION

Identity Based Encryption cryptographic scheme has been developed by Shamir21 in 1984. Major issue is the inability to build Identity Based Encryption system which is based on RSA. Later in 2001 an efficient Identity Based Encryption has been developed by Boneh and Franklin19. In Identity Based Encryption, an identity of the user plays a vital role. The sender who sends the message only needs to know the receiver's identity attribute in order to send the encrypted messages. Email Encryption is one of the major applications for Identity Based Encryption. However, key revocation is not achieved in Identity Based Encryption. (MWSR). The basic concept of ASE schemes were discussed and the enhanced definitions were explained in10. Numerous works have been performed to show how to achieve more difficult queries in public-key setting like conjunctive searches and range In different issues that arise in various

ATTRIBUTE BASED ENCRYPTION

It is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). A user can encrypt a message under a public key and a policy. Decryption will only work if the attributes

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

associated with the decryption key match the policy used to encrypt the message.

FULLY-HOMOMORPHIC-ENCRYPTION

Homomorphic encryption ensures privacy of data in communication, storage or in use with tools similar to conventional cryptography, but with extra features of computing over encrypted data, searching an encrypted data, etc. Search and manipulation of cipher text was difficult with traditional encryption techniques.

INTELLIGENT ENCRYPTION

Conventional public-key and shared-key encryption systems rely on standard protocols and a pre-established public key certification infrastructure (public key infrastructure), allowing people all over the world to use encryption according to standard methods. But in conventional cryptographic methods only one person, i.e., owner of the key can view original data. This creates problem in case of cloud where number of users are there to access same data. Intelligent encryption works on basis of various conditions. It allows various users to view encrypted data based on certain conditions rather than only single authorized user. It is similar to attribute based encryption but conditions are extended for multiple users.

Consider a situation where access to confidential information is managed within a company. Conditions for viewing the information are incorporated into the cipher text, and attribute information is applied to the decryption key so that decryption is possible only with a key that matches these conditions. If the data is encrypted with embedded conditions such as "[Director] OR [Personnel department AND Section manager]", then it can be decrypted with a key containing the attributes [Personnel department, Section manager], but not by a key containing the attributes [Personnel department, Section #1, Employee]. In this way number of users satisfying condition can get view original text.

SECURITY ALGORITHMS

Example

- DES
- BLOWFISH
- RC5
- 3DES
- AES
- RSA etc..

ALGORITHM

DATAENCRYPTIONSTANDARD(DES)
Function DES ENCRYPT(M,K) where M=(L,R)
M*IP(M)
For round *1 to 16 do
Ki
*SK(K,round)
L*L xor F(R,Ki)
Swap(L,R)
END
Swap(L,R)
M*IP-1
(M)
Return(M)
END

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 21, 2017 ISSN: 2348-6600
Reference ID: IJCS-258 PAGE NO: 1647-1652
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

CONCLUSION

Privacy and security in cloud can be said to be achieved when users have control over information they want to reveal to cloud and who can access their information. Without guarantee of security and privacy users can't make shift to cloud only on the basis of lower cost and faster computing. Certain cloud related standards and cryptographic methods for security are coming to existence, still there is long way to go for public cloud to become a trustworthy computing environment.

REFERENCES

1. https://en.wikipedia.org/wiki/ID-based_encryption
2. Goh E-J. Technical Report 2003/216, IACR ePrint Cryptography Archive, 2003. Available from: http://eprint.iacr.org/2003/216.
3. http://www.ijcsit.com/docs/Volume%206/vol6issue02/ijcsit2015060233.pdf
4. https://en.wikipedia.org/wiki/Attribute-based_encryption
5. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. Proceedings of Cryptography 2001, LNCS, Springer-Verlag. 2001; 2139:213–29.
6. Fontaine C, Galand F. A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security 2007. 2007 Jan; 1–15.
7. Shamir A. Identity-Based Cryptosystems and Signature Schemes. In Proceedings of Cryptography 1984, LNCS. Springer-Verlag. 1985; 196:47–53.