International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 9 5592 - 5595

Security Enhancement on Cloud to multi Cloud using Audio Cryptography

Anuja Phapale
AISSMS IOIT,
Pune, India
anuja.phapale@gmail.com

***Abstract*—** Nowadays, cloud computing is most popular and modern technology of storing the large amount of information on the internet and accessing it from anywhere. Costs reduction, universal access, availability of number of applications and flexibility is a number of reasons for popularity of cloud computing. Users store sensitive information on cloud, providing security becomes important aspect as these cloud service providers cannot be trusted one. As the cloud computing assures user to provide the data, the cloud computing environment failure may result in loss or unavailability of data so the concept of Multi-Clouds is introduces. Dealing with single cloud" service providers are anticipated to become infamous with customers due to scare of service availability failure and the possibility of malicious intruders in the individual cloud. Multi-clouds guarantee to provide service at any cost if there is any failure at any cloud due to any reason. The use of multi-clouds as it can tackle the security and mainly availability issues much effectively than single cloud that affects cloud computing user.

The proposed work surveys recent research related to single and multi cloud security and addresses possible solutions. This work aims to promote the use of multi clouds to solve problem of data availability due to failure in individual cloud. To provide data confidentiality as well as data integrity, security mechanism which uses an image audio secret sharing scheme(ASS) cryptography instead of visual secret sharing scheme(VSS)**.**

Keywords*- Multi-cloud, Cloud, Security, Audio Secret sharing scheme, Confidentiality, Integrity*.

*****

I. INTRODUCTION

In the current world, many organizations work on big data which may require huge storage. But these organizations cannot afford to create their own storage servers as it will be too expensive. The cloud computing provides services to such organization which are really fast and at low and affordable cost. Thus, cloud computing is a way to increase the capacity or add capabilities dynamically without investing cost on new infrastructure, for training new personnel, or licensing new software. Thus cloud computing extends Information Technology's existing capabilities. But as more and more information of individuals and organizations are placed on the cloud, concerns are beginning to grow about security and privacy of stored information.

As the use of cloud computing is increasing rapidly, because these services provide fast access to applications and reduce infrastructure costs. Cloud computing provides many benefits in terms of low cost and accessibility of data. Security is major aspect which needs to consider in cloud computing environment as user often use cloud facility store sensitive information with cloud storage providers but these providers may not be authenticate. Single cloud providers are predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud leads to movement towards multi-clouds has emerged recently [1]. With advantages of cloud computing like high speed and low cost, the problems as data integrity, data confidentiality, data availability becomes important aspect to consider. So to provide security the concept of secret sharing scheme to used before uploading data on cloud. In 1979, Shamir [2] and Blakley [3] firstly developed the concept of the secret sharing. The secret sharing technology is an efficient method to keep the secret data safe, which plays an important role in protecting important information from getting lost, destroyed, or into wrong hands. In cryptography, a Secret Sharing Scheme (SSS) is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. This is based on audio shares which uses cover sound to create each share. If an eavesdropper plays one share in a media player, he or she will only hear as original sound, but when shares are mixed together, secret data is recovered. Thus only the user with valid share is able to download data from cloud.

II. RELATED WORK

Many organizations have been increasingly outsourcing services and computation jobs to the cloud. A client that outsources a computation job must verify the correctness of the result returned from the cloud, without incurring any significant overhead as it being to execute the job locally, which would nullify the benefit of outsourced job execution. Such verifiability is important to achieving cloud service trustworthiness [4]. One of the most important issues related to cloud security is the risk of data integrity. The data stored in the cloud may get damage during transition operations from or to the cloud storage provider. Data stored on cloud needs to be saved from cloud owners as well as external hackers. The cloud owner may try to access or modify data stored on the cloud. Hence the integrity of the user's data may lose.

To protect user data in the cloud, a key challenge is to guarantee the confidentiality of sensitive data while it is stored and processed in the cloud. The cloud is not fully trusted because of operator errors or software vulnerabilities. As a result, the cloud provider shouldn't be able to see unencrypted or decrypted sensitive data during the data's residence in the cloud. (In other words, sensitive data should remain encrypted while in the cloud.) However, such a requirement can limit the usability of (encrypted) data when a cloud application processes it [4].

As sensitive data will be shared with a third party, cloud computing users want to maintain it confidential. The data stored will be important to the user, hence if third person gains

access to the sensitive data, it will not possible to maintain data confidential. Protecting private and important data from attackers or malicious insiders is of critical importance.

Multi-cloud strategy is the use of two or more cloud services to minimize the risk of data loss or downtime due to a localized component failure in a cloud computing environment. The basic idea behind the use multi-cloud at the same time to mitigate the risks of malicious data manipulation, disclosure and process tampering. By integrating multi-cloud, the trust assumption can be lowered to an assumption of no collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data applications of a specific cloud user. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti [5,6] their previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios [7]. Another major concern in cloud services is data availability. In the single cloud environment it is possible that the service might be unavailable from time to time. Though the cloud computing has multiple servers but what if some important node fails and user is unable to access the data. By using multi-cloud it is possible for private or important data will be available for user all the time.

A major concern of cloud users is the potential for losing data privacy once the data has moved to the cloud. Customers need assurance that their data is well protected by cloud service providers. Encryption can alleviate this fear, but it also has drawbacks as it is time-consuming process for downloading and uploading of data for customers, the cloud provider can perform operations in the cloud. However, to manipulate encrypted data in the cloud, users must share their encryption/decryption keys with the cloud provider, effectively allowing them access to the data. One of the top threats to cloud computing is malicious insiders. An insider can be an administrator employed by a cloud service provider, an employee of the victim organization who exploits vulnerabilities to gain unauthorized access, or an attacker who uses cloud resources to launch attacks. Thus the cloud computing environment makes it difficult to detect and prevent insider attacks.

A. Data Integrity

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption. Data stored on cloud needs to be saved from cloud owners as well as external hackers.

The cloud owner may try to access or modify data stored on the cloud. Hence the integrity of the user's data may lose.

B. Data confidentiality

Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the data stored on the cloud for the stolen user account or modify it.

As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. The data stored will be important to the user, hence if third person gains access to the client files, it will be fatal. Protecting private and important information and files from attackers or malicious insiders is of critical importance.

C. Data availability

Another major concern in cloud services is data availability. In the single cloud environment it is possible that the service might be unavailable from time to time. Though the cloud computing has multiple servers but what if some important node fails and user is unable to access the data. User wants the data available all the time as it's his private data and can be of utmost importance at any time.

Confirming the security of cloud computing is a major factor, as users often store sensitive information with cloud storage providers, but these providers may be untrusted. Dealing with single cloud service providers is anticipated to become infamous with customers due to scare of service availability failure and the possibility of malicious intruders in the individual cloud. An action towards this issues solve with using multi cloud concept. To provide data confidentiality and data integrity the concept of audio secret sharing scheme which is very similar to visual secret sharing scheme in which instead of image as a cover data audio data is used.

III. EXISTING AUDIO SECRET SHARING SCHEME

Basically, secret sharing scheme proposed by Shamir [2] is a threshold scheme based on polynomial interpolation. It allows a dealer D to distribute a secret value s to n players, such that at least $t < n$ players are required to reconstruct the secret. The audio secret sharing scheme uses same technique as like Shamir with using audio instead of image data.

A. DHQ Audio Cryptography Scheme

An Audio Secret Sharing (ASS) scheme is a special type of secret sharing scheme [8], in which the shares of embedded messages use music as cover sound. Desmedt, Hou, and Quisquater first proposed the (2, 2) audio secret sharing (ASS) scheme. This scheme is abbreviate it as the DHQ (2, 2) ASS scheme. The goal of the DHQ ASS scheme is to embed a binary secret message by cover sound. In the DHQ (2, 2) ASS scheme, the human "ears" can decode the concealed message if one plays two shares simultaneously.

Desmedt, Hou, Quisquater also proposed the generalized DHQ (2,n) ASS scheme based on their (2, 2) ASS scheme using (log2n) different cover sounds. More cover sounds are needed when the number of participants n increases, this will overburden the human hearing system and may also become difficult for people to distinguish the secret bit correctly. Thus, their scheme is not practical when n is large.

B. (2, n) Audio Cryptography Scheme

(2, n) Audio Cryptography Scheme proposed [9], in which shares are created by combining secret text data and audio

data. For audio signal samples are created in order to combine with secret data. Secret data is converted into binary which is combined with audio samples. Algorithm for (2,n) Audio Cryptography Scheme:

1. Let the sample in the cover sound be digitized to m bits, and its binary form be $(b_m, b_{m-1} \ldots b_1)$.
2. Use any s bits $i_1, i_2 \ldots i_s$ (from *LSB to MSB*) of each sound sample. In order to represent *(2, 2)* with one cover sound, where $n=2^2$ i.e. $s=1$. Then, a *(2, n)* scheme with one cover sound, where $n = 2^s$, has high matrices M_H and low matrices M_L.
3. One constructs n participants according the matrices in M_H and M_L which will cause the high and low volume, respectively. The minimum difference between high and low volume when "adding" any two shares is 2^{i_1-1} and the maximum difference is $2^{i_1-1} + 2^{i_2-1} + \ldots + 2^{i_s-1}$.
4. Construction of high matrices M_H and low matrices M_L.

   M_H = { all the matrices obtained by permuting the rows of $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ } , and

   $M_L = \{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \}$ for s = 1, i.e., the (2,*2) scheme*.

   M_H = {all the matrices obtained by permuting the rows of $\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$}, and

   $M_L = \{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \}$

   for *s = 2*, i.e., the (2,4) scheme.

M_H and M_L for $s \geq 3$ can be produced using the same procedure as (2,2) and (2, 4). With the same procedure (k, n) scheme is implemented.

In order to reconstruct original secret data, any 2 shares from n created shares are selected. In order to recover original secret data the minimum difference between high and low volume when "adding" any two shares is 2^{i_1-1} and the maximum difference is $2^{i_1-1} + 2^{i_2-1} + \ldots + 2^{i_s-1}$.

IV. PROPOSED WORK

As data and information will be shared with a third party i.e. cloud, users want to avoid an untrusted cloud provider for protecting private and important information. This system focuses on the issues related to the data security and availability aspect of cloud computing.

While uploading file, file is divided into n shares using (k, n) audio secret sharing algorithm proposed by Ching Nung Yang [9] and each share is uploaded to each cloud. Before dividing the file hash value of file is generated using MD5 so after downloading of file hash value of original uploaded file is compared with downloaded file. If this value is similar then we conclude that file is not corrupted. In download phase, any (k, n) authenticated shareholder submits their shares, and then only uploaded file is reconstructed. So in this way user can reconstruct the file and stored into local desktop system to maintain confidentiality property of security.

While creating shares the secret text is converted into binary format and embedded in cover audio file which is also consider in binary format. The size of each share is equal to the size of cover audio file. When an eavesdropper tried to play individual share in a media player, it will sound exactly same as original sound like cover sound as there minor change in cover audio file and share audio file. Thus, audio shares do not leave any suspicious property as visual share. Also, audio share does not leak any information about uploaded secret data.

V. CONCLUSION

Due to the accelerating integration of computer and communication technology, internet has been established worldwide, and thus brings about various commercial services. Thereby, to transmit secret commercial data is a great security concern. So, Cloud computing security is one of the major issues in the cloud computing environment as user does not want to lose their private/sensitive data stored on the cloud. The important problems like unavailability of service and data intrusion attacks lose the privacy of user's data. This system provides availability of the data using multi-cloud with security while sharing the confidential data with another user. To maintain confidentiality audio secret sharing scheme using binary data formats which is proposed by Ching Nung Yang is applied before uploading sensitive information on cloud. While downloading uploaded file there is need to submit share by authenticated users then only it is possible to download file. Also integrity of uploaded and downloaded file is checked by comparing their hash value before and after downloading file.

Thus, framework will apply multi-clouds and the audio secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

REFERENCES

[1] Mohammed A. AlZain , Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences 2012.
[2] Adi Shamir , "How to Share a Secret," Communication of ACM,1979.
[3] M. Naor, Adi Shamir, "Visual Cryptography," Advances in Cryptology: Eupocrypt' 94, Springer –Verlag, Berlin , pp.1-12,1995.
[4] Zahir Tari, " Security and Privacy in Cloud Computing", IEEE Cpmputer Society,(54-57) 2014.
[5] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.
[6] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation," Proc.

IEEE Third Int'l Conf. Cloud Computing (CLOUD), pp. 337-345, 2010

[7] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy- Enhancing Multicloud Architecture", IEEE Transactions on Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[8] Yvo Desmedt, Shuang Hou, Jean-Jacques Quisquater, "Audio and Optical Cryptography", Advances in Cryptology ASIACRYPT '98, October 18-22, 1998, Proceedings.

[9] Ching Nung Yang, " Improvements on Audio and Optical Cryptography", Journal of Information Science And Engineering 18, 381-391, 2002.

[10] Chen Chi Lin, Chi-Sung Laih And Ching-Nung Yang, "New Audio Secret Sharing Schemes With Time Division Technique," Journal of Information Science And Engineering 19, 605-614 2003.

[11] Yusuf Adriansyah, "Simple Audio Cryptography".

[12] Tanvi Sharma, Dr.Deepti Sharma,"Security Architecture of MultiCloud", IJARCSSE, 2014.

[13] Zahir Tari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, and Ibrahim Khalil," Security and Privacy in Cloud Computing: Vision,Trends and Challenges", IEEE Cpmputer Society,(30-38) 2015.

[14] R.L. Rivest, A. Shamir, and L. Adleman ,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"

[15] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers," Twenty security considerations for cloud-supported Internet of Things", IEEE Internet of Things Journal,2015.

[16] S. Subashini , V.Kavitha," A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (2011) 1–11.