Cloud Computing Security in Multi-Clouds using Shamir's Secret Sharing Scheme

Naveena R. Kannan
Bachelor of Technology
Usha Mittal Institute of Technology

Nikhita Salian
Bachelor of Technology
Usha Mittal Institute of Technology

ABSTRACT
In order to leverage a remote cloud based infrastructure, a company essentially gives away private data and information that might be sensitive and confidential to the service provider. Data Integrity and Confidentiality can be protected by using secret sharing schemes. To prevent service availability failure, multi-cloud data storage system can be implemented. In this paper, multimedia is protected using the Shamir's Secret Sharing in Multi-cloud Databases.

General Terms
Secret Sharing, Algorithm, Cloud Security

Keywords
Data Security, Cloud, Secret sharing, Information Dispersal

1. INTRODUCTION
In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored in the cloud. The data can be confidential and extremely sensitive. Hence, the data management should be completely reliable. It is necessary that the information in the cloud is protected from malicious attacks. Security brings in concerns for confidentiality, integrity and availability of data. Unauthorised access to information results in loss of data confidentiality. Data integrity and availability suffers due to failure of cloud services. Security has the characteristics of a complement to reliability.

In addition, doing business with single cloud providers is becoming less popular due to potential problems that can affect our data, such as service availability failure (e.g. some catastrophe befalling the cloud service provider and disruption of services) and the possibility that there are malicious insiders in the single cloud (e.g. stolen data by an attacker who found a vulnerability). To this end the use of multi-clouds instead of single cloud service provider to protect data is an optimal solution [1] .

In order to protect data from attackers, we can encrypt it. But in order to protect the encryption key, we need a different method which increases the complexity of the intended solution. Another drawback of this approach is that the entire process of encryption and decryption process is time consuming.

The secret sharing schemes are a perfect fit in the multi cloud environment to provide data security in cloud without the drawbacks of encrypting data and service availability failure due to single cloud providers. In this paper, the Shamir's Secret Sharing Algorithm has been used for the implementation of security of multimedia such as video and images in the multi-cloud environment.

2. LITERATURE REVIEW
Compared to the other schemes, Shamir's secret sharing scheme is a perfect secret sharing scheme as the secret cannot be rebuilt using less than the required threshold. Also, it is ideal and extendable as the value of n can be increased without changing the threshold. The more the number of shares, the harder it is to find the threshold value. It also has a homomorphic property due to which changes made to the shares cascades to the reconstructed data. The disadvantage of Shamir's scheme is that it is complex when compared to the Blakley's scheme. Moreover, as the choices offered by the Blakley scheme in the selection of co-efficient vector is 28k as compared to 256 choices provided by the Shamir's scheme [2], the former is more flexible and scalable. On the contrary, it is less space efficient as the size of each share is three times more than the file size and as the number of shares increase, the chances of finding the threshold point increases. The Rabin's IDA is the strongest scheme in terms of space efficiency as the share size is less than the actual file size. This leads to optimal efficiency in data overhead. However, it is not a perfect secret sharing scheme, unlike the Shamir's scheme, due to its weaker confidentiality. The Threshold secret sharing scheme using the Chinese remainder theorem that include the schemes such as Mignotte's and Asmuth-Bloom is the strongest

in terms of security. The Mignotte's scheme has shares that are small in size and therefore, can be used in applications that need to be space efficient. The Asmuth-bloom scheme is perfect as it uses a constant that is completely independent of the secret. Conversely, the Mignotte's scheme is complex to implement. Both the schemes are also prone to information leakage which makes the schemes vulnerable to confidentiality problems.

Table 1 Comparison of Secret Sharing Schemes

Scheme	Advantages	Disadvantages
Shamir	Perfect security, ideal, extendable, homomorphic property.	It is complex.
Blakley	Flexible, scalable and less complex compared to Shamir.	It is less space efficient.
IDA	Optimal efficiency in data overhead.	Weaker Confidentiality.
CRT	Strongest in terms of security.	Information leak.

3. SHAMIR'S SECRET SHARING SCHEME
Adi Shamir, one of the researchers who invented the RSA cryptosystem, designed the first secret sharing scheme in 1979. He published this scheme, based on polynomial interpolation. His goal with the scheme was to take k points on the Cartesian plane, and with those k points, a unique

polynomial $q(x)$ is guaranteed to exist such that $q(x) = y$ for each of the points given.

The system relies on the idea that you can fit a unique polynomial of degree *(k-1)* to any set of *k* points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic curve, and so on [3].

Shamir's secret sharing represents a way for distributing a secret among a group of n participants, each of whom is allocated a part of the secret. The strong point of this method is that the secret can be reconstructed only when a predefined number of k shares are combined together; individual shares are of no use on their own, so anyone with fewer than k out of n shares has no extra information about the secret than someone with 0 shares.

Lagrange's polynomial is used to reconstruct the secret [4]. The size of each share does not exceed the size of the secret. Keeping *k* fixed, shares can be easily added or removed, without affecting other shares. It is easy to change the shares, keeping the same secret, Shamir's scheme is a perfect secret sharing scheme, as k-1 shares are just as useless as no shares. Each share is p-bits long. The value of p should not be too small or it could be susceptible to brute-force attack. If the value of p is 128 bits then this provides 2^{128} possible values, which is a range too large for brute force to ever attempt [2].

4. EXPERIMENT AND ANALYSIS

4.1. Experiment Environment Setup

In this system, we design and implement prototype system of UMIT Momento application with PHP in Xamp. In this prototype, we have implemented Shamir's Secret Sharing Scheme in MCDB for images and video files. The UMIT Momento application website is a portal for the UMIT students to share pictures and videos of various events that occur in the college campus which includes seminars, competitions, festivals etc. A student can view and download the pictures and videos, add events and upload content. We have used Google Drive, OwnCloud and Dropdox as Multi Cloud Databases.

4.2.Experimental Result Analysis

A client request includes query request to update the databases (such as adding an event, image/video or deleting event, image or video) or query request for retrieval of data from database (such as viewing log files, displaying the events, event images or videos). Shamir's Secert Sharing Algorithm is implemented on client's service request. The query request sent by the client to the cloud manager is parsed by the cloud manager and a random degree polynomial is generated. Query is rewritten for each cloud. Shares are created and sent to the respective cloud. When the client sends request that involves retrieval of data, the cloud manager will check if all the cloud servers are functioning properly or not, will make a note of this in the log file and will obtain the minimum required shares from the relevant servers that reduce the response time. The cloud

manager will check if all the cloud servers are functioning properly or not, will make a note of this in the log file and will obtain the minimum required shares from the relevant servers that reduce the response time. The cloud manager joins the shares and decrypts its value to obtain the original secret. The requested information is then displayed to the client. The image/video file is split and stored separately in Google Drive, Dropbox and OwnCloud. Let us consider for video files. Since three different clouds are used, we are following the (2,3) threshold scheme, which means out of the three shares generated, deletion of one share from one cloud should not affect the display result in the event video page (the page has videos of particular event), whereas deletion of two or three shares should result in the particular video not being displayed in event video page. On deleting a share of a video file from OwnCloud did not change the result in the event video page. But when shares of that video is deleted from OwnCloud and Dropbox, the event video page did not display that particular video, a note is made in the error log file and the remaining share present in Google Drive is moved to error file folder.

5. CONCLUSION

This paper proposes the use of Shamir's Secret Sharing Scheme in MCDB for images and videos. Multi-cloud systems decrease the security risk considerably compared to the security of single cloud and cloud storage. Scalability and performance is optimized. By using Shamir's Secret Sharing Scheme in Multi-cloud systems, availability, confidentiality and integrity of data is further improved.

6. ACKNOWLEDGEMENT

We would like to thank our Alma Mater, Usha Mittal Institute of Technology, for supporting us in realising this project. Also, we would like to acknowledge the Head of Computer Science Department, Mr. Sumedh Pundkar for his guidance.

7. REFERENCES

[1] I. MOROZAN, "Multi-clouds database: A new model to provide security in cloud computing," CNS, 2014.

[2] M. Li, "On the confidentiality of information dispersal algorithms and their erasure," in ArXiv, 2013.

[3] S.-J. L. a. W.-H. Chung, "An Efficient (n,k) Information Dispersal Algorithm Based on Fermat Number," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 8, no. August, 2013.

[4] S. S. B. ,. A. A. P. S.Jaya Nirmala, "A COMPARATIVE STUDY OF THE SECRET SHARING ALGORITHMS FOR SECURE DATA IN THE CLOUD," International Journal on Cloud Computing: Services and Architecture(IJCCSA), vol. 2, no. August, 2012.

[5] E. E. a. A. B. Hamza, "SECRET SHARING OF 3D MODELS USING BLAKELY SCHEME," in 25th Biennial Symposium on Communications.

[6] Y. C. H. J. L. T. Y. K.-C. L. Su Chen, "A Secure Distributed File System Based on Revised Blakley's Secret Sharing Scheme," in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[7] B. S. a. E. P. Mohammed A. AlZain, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds," JOURNAL OF SOFTWARE, vol. 8, no. MAY, 2013.

[8] S. B. K. M. K. Alam, "An approach to secret sharing algorithm in cloud computing security over single to multi clouds," International Journal of Scientific and, 2013.

[9] V. A. S. I. Daniel Pasail˘a, "Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes".