CLOUD COMPUTING SECURITY USING SHAMIR'S SECRET SHARING ALGORITHM FROM SINGLE CLOUD TO MULTI CLOUD.

Monica G. Charate[1], Dr. Savita R. Bhosale[2]

[1]PG Scholar, Department of Computer Engineering, MGMCET,Kamothe, New Mumbai (India)

[2]Professor, Department of Electronics & Telecommunication, MGMCET, Kamothe, New Mumbai (India)

ABSTRACT

Cloud Computing offers enormous benefits to its adopters, but it also comes with its set of problems and inefficiencies of which security is the biggest concern. In order to leverage a remote cloud based infrastructure, a company essentially gives away private data and information that might be sensitive and confidential. Secret sharing schemes are used to restrict access to such sensitive and confidential data. Threshold secret sharing schemes is a scheme in which the number of the participants in the reconstruction phase is important for recovering the secret. In this paper the performance of the Shamir's secret sharing scheme, is used in a multi cloud environment.

Keywords: Data Security, Cloud, Secret sharing, Information Dispersal

I. 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.

In order to protect data from hackers, 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.

II. LITERATURE SURVEY

In the past more research has been conducted into single clouds than into multi-clouds. Multi–clouds can address the security issues that relate to data integrity, data intrusion, and service availability in multi-clouds. In

addition, most of the research has focused on providing secure "cloud storage" such as in DepSky. Therefore, providing a cloud database system, instead of normal cloud storage, is a significant goal in order to run queries and deal with databases; in other words, to profit from a database-as-a-service facility in a cloud computing environment.

Rocha and Correia et al.(2010) determine possible attackers for IaaS cloud providers. For example, Grosse et al propose one solution is to prevent any physical access to the servers. However, Rocha and Correia argue that the attackers outlined in their work have remote access and do not need any physical access to the servers. Grosse et al. propose another solution is to monitor all access to the servers in a cloud where the user's data is stored. However, Rocha and Correia claim that this mechanism is beneficial for monitoring employee's behavior in terms of whether they are following the privacy policy of the company or not, but it is not effective because it detects the problem after it has happened.[1]

2.1 Shamir's Secret Sharing

Shamir's algorithm is implemented based on the secure order preserving technique discussed in Shamir's algorithm is applied to each field of the table. The n shares obtained are then distributed to different data centers out of which only k of the shares are required to achieve the International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.4, August 2012 ,67original values. It is possible to support structured querying of the data parsing the query, extracting the conditional values, transforming the values and appending them back to the original query before it is sent to the server. Inverse of Shamir's Secret sharing algorithm has to be applied to the received data set to get back the intended result. Assume that the table 'employees (emp_no, salary, empname)' is outsourced. The client should be able to execute the following type of queries without revealing the data to any of the Database service providers.

Exact match queries

Range queries

Aggregate queries such as MIN/MAX, MEDIAN, SUM and AVERAGE

2.2 Rabin's Information Dispersal Algorithm

Rabin's IDA is implemented using the technique discussed in. Considering k as the threshold value, n as the number of slices, and D as the Data Matrix of size k x t, The data to be stored is arranged in terms of the data matrix D and C as the secret Vander monde Matrix of size n x k. The matrix M of size n x t is computed as

$$M = C * D \quad (1)$$

Each of the n rows of M represents a slice. This modified data is stored at multiple data centers

such that none of them have access to s < k-1 slices. Data retrieval can be achieved by obtaining any k of the n slices and applying the reverse IDA. Consider M' to be the k x t matrix formed by obtaining the k slices of data stored in the cloud and C' to be the k x k matrix obtained by selecting the corresponding rows of C. Then the data matrix

D can be retrieved as:

$$D = C'^{-1} * M' \quad (2)$$

Even with the loss of (n-k) slices, the data can be reproduced thus ensuring availability. A Message authentication code can be applied to the test data before dispersal to achieve integrity [2].

2.3 Secret Sharing Strategy

Having multiple copies of data into different clouds it will just create multiple gates for intruders to hack in. Therefore, we need to make sure that the data shipped to multiple clouds is safer that it was on a single cloud. This is when we apply the secret sharing algorithm presented by Adi Shamir in [3] .Invented in 1979, the algorithm has occupied a huge place in the area of cryptography. The author discussed the issue of information distribution with the aim of showing that there is an orthogonal approach which is based on information distribution instead of encryption. The need of a secure communication between two endpoints challenged most of the work on data security. A similar approach was discovered by George Blakely [3], but the mathematical evolution behind the algorithm is more complicated, that's where the secret sharing algorithm of Shamir lies – in its simplicity of implementation. Shamir's secret sharing or secret splitting represents a way for distributing a secret among a group of n participants, eachof whom is allocated a part of the secret, in our case, a piece of data. The strong point of this method is that the secret can be reconstructed only when a predefined number of shares are combined together; individual shares are of no use on their own, so anyone with fewer than t out of n shares has no extra information about the secret than someone with 0 shares.

Sharmila Banu K. et al describes organized cloud computing security into three sections: security categories, security in service delivery models and security Hore et al.(2013) describes techniques for building privacy preserving indices on sensitive Attributes of a relational table, and provides an efficient solution for data bucketization. A scheme progressive elliptic curve encryption is presented in [4] that used multiple encryption keys to encrypt a part of data multiple time such that final cipher can be decrypted in one run using single key. This scheme is based on public/private key cryptography and consumers of application manage cryptographic private keys. Furthermore, N re-encryption will be required for N users in case of single data piece sharing.[4] dimensions. All relevant information are visualized into cloud computing security in a snapshot which is presented in **Figure.1** [5].

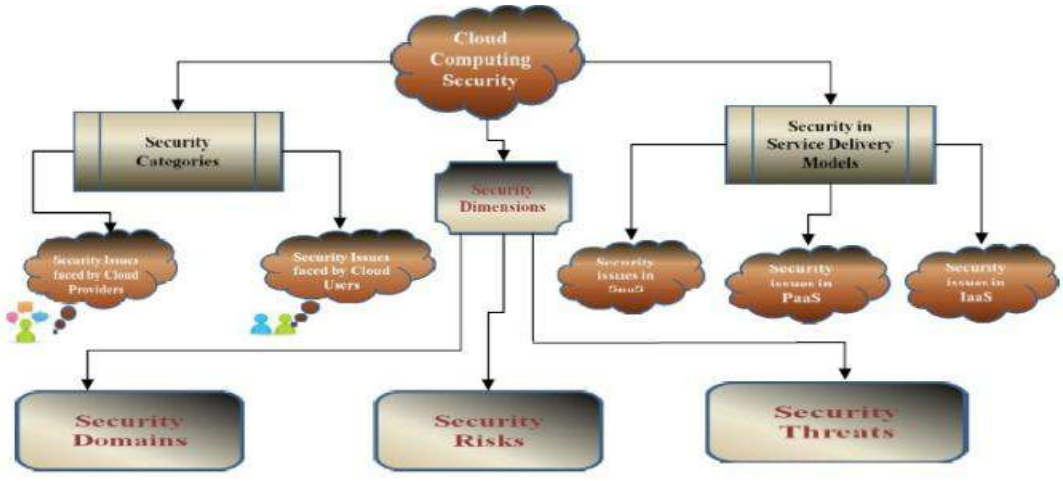

Figure 1: Graphical View of Cloud Computing Security [5]

Security in cloud services is based on the following:

1. Strong network security is possible around the service delivery platform
2. Data encryption: for data in transit (particularly over wide area networks), and sometimes stored data, but it cannot be applied to data in use.
3. Access controls to ensure that only authorized users gain access to applications, data and the processing environment and is the primary means of securing cloud security services.

The secret sharing algorithm possesses some dynamic properties that make it further more powerful, these properties, as described by Adi Shamir in [6] are as follows:

1. The size of each piece does not exceed the size of the original data.
2. When k is kept fixed, D pieces can be dynamically added or deleted without affecting the other Di pieces.
3. It is easy to change the Di pieces without changing the original data D - all we need is a new polynomial q(x) with the same free term. This can enhance security.
4. By using tuples of polynomial values as Di pieces, we can get a hierarchical scheme in which the number of pieces needed to determine D depends on their importance.[6]

Sonia Verma et al.(2014) describes that data and information will be shared with a third party, cloud computing users want to avoid an un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed [7].

2.3.1 Advantages

1. Data Integrity
2. Service Availability.
3. The user runs custom applications using the service provider's resources
4. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.[7]

Swapnila S Mirajkar et al.(2014) describes HAIL(High Availability and Integrity Layer) which is combination of Proofs and cryptography, presented in the year 2009 used to control multiple clouds. It ensures data integrity and service availability. But the limitation of HAIL is that it needs code execution in their servers and it does not deal with multiple versions of data. Moving from single clouds multi-clouds is sensible and significant for many reasons.

According to Cachin et al.(2014) , "Services of single clouds are still subject to outage". Vukolic accepts that the primary purpose of moving to inter-clouds is to amend what was offered in single clouds. DepSky presented by Bessani is virtual storage cloud system comprising of a combination of different clouds to build a cloud-of-clouds. None of above problems are found in DepSky as it combines Byzantine fault tolerance protocol, secrete sharing and cryptography [8].

K.Sai Sowmya et al.(2014) All Business organizations move their workload to cloud computing. Cloud clients are fear to lose the private information in single cloud. That's why present paper design to provide the integrity results with multi cloud architectures. We are making the strongest cryptographic technique named as a Shamir's secrete key algorithm. This algorithm provides the security results like integrity and aggregation. Integrity or aggregation results report is generate from k servers. Multi cloud architectures reduce the security issues. It's give final results like high availability. [9]

Gaidhankar Sushil, Kanase Amit et al.(2014) demonstrate following points:

1. A Practical Guide to cloud computing Security Giving risk and mitigation Points only the security of single cloud. [10]
2. Security Challenges for public cloud Outlining Challenges further investigation& motivate As maintaining security in public cloud, urgency of data not comes into picture.[10]

3. Foundations and Properties of Shamir's Secret Sharing Scheme Encryption & Decryption Properties related to Shamir's Secret Sharing.[10

III. PROPOSED SYSTEM

In this proposed system Shamir's secret sharing algorithm is extremely effective for storing the client data securely. It provides authentication to clients and also provide security by encryption and decryption using secret key.

Our proposed system can be enhanced by providing effective security by using stronger encryption algorithm. It also provides fast service to store data on server. It also giving proof of integrity of the data to client. This scheme reduce storage overhead of the customer by compressing the data and reduce computational overhead of the cloud storage server.

In the **Figure 2**, Architecture Design. In this, flow of system is shown. First admin login using username and password. After login confirmation, select data to be load on cloud..Upload data on cloud. Then place unique key with data on cloud. After that use Shamir's Secret sharing algorithm. Then specify threshold value. If the key is matched, then user can downloading data on cloud otherwise give Invalid key error.

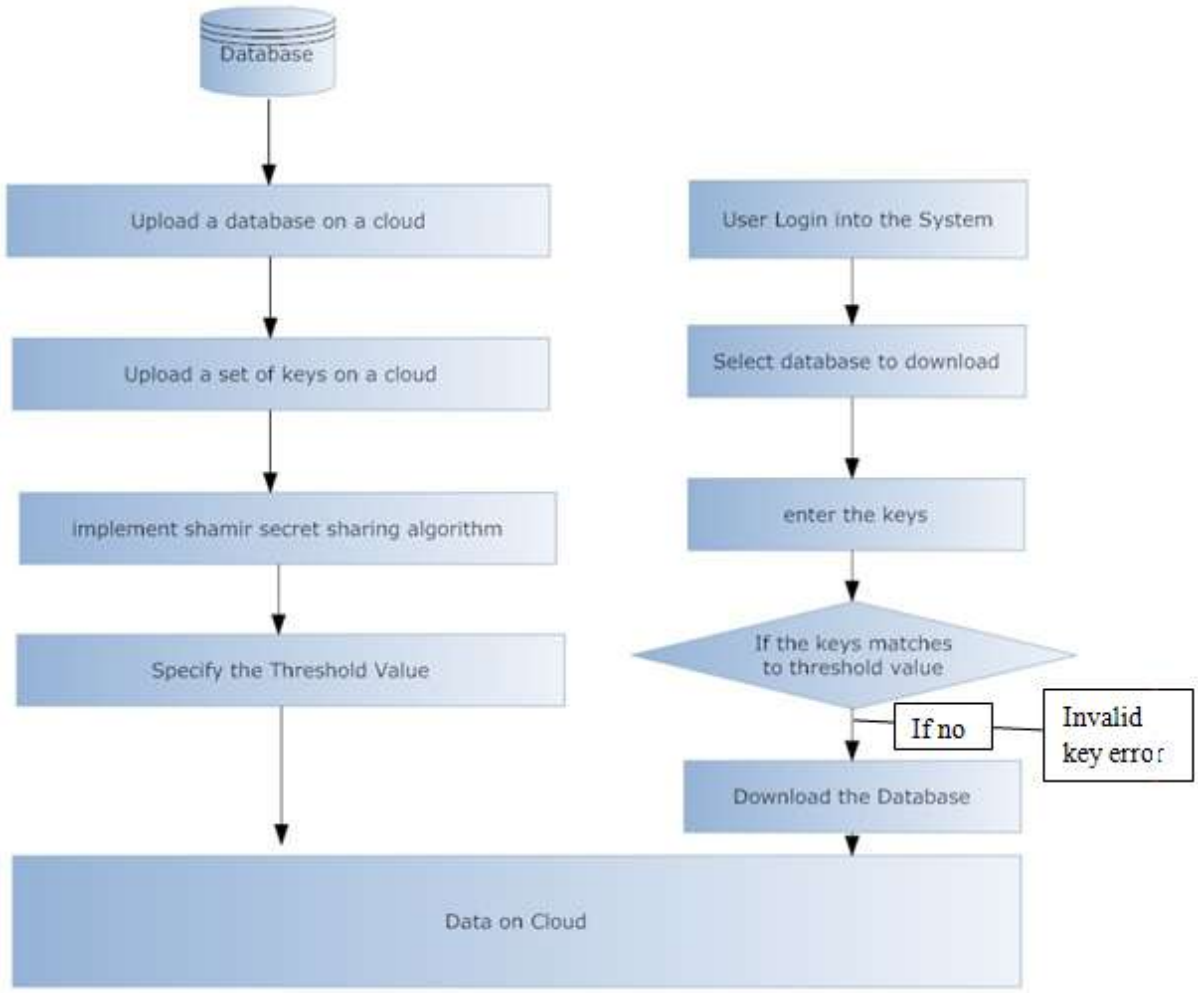

Figure 2: Architecture Design

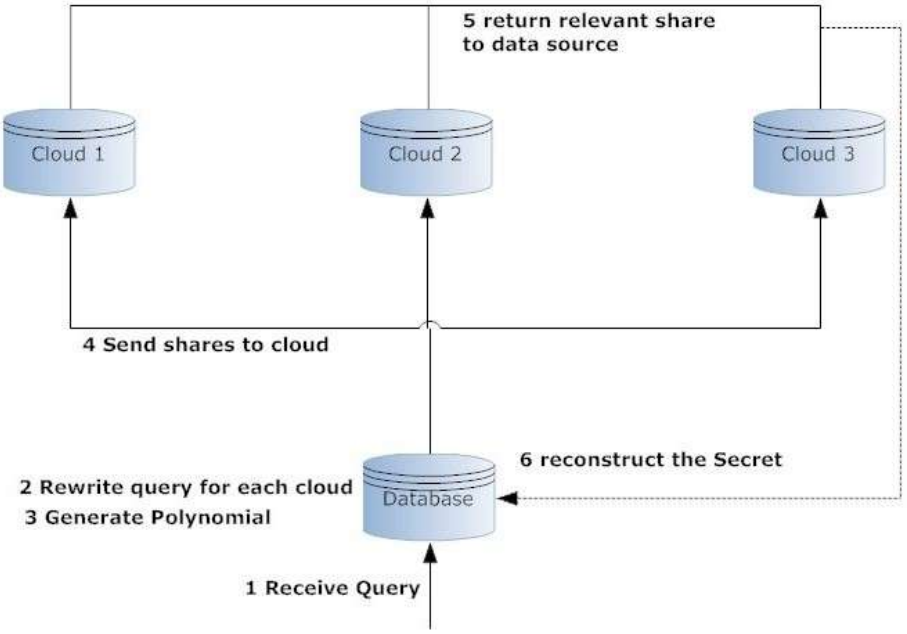

Figure 3: System Architecture

In the above **Figure 3**, System architecture is shown. In this figure, it describes simple execution of proposed system.

IV. RESULTS

On this form admin Login Into the Application.

Home page of Admin

On this form admin manages users.

Admin adds new User into the Application

On this form admin upload files on server.

Dropdown list contains the keys .admin select the 3 different keys to encrypt the file.

On this form admin share a file with user.

After sharing user get the mail which contains key for decryption and share keys for authentication.

This is to inform you that this organization share a file with you. Access details as Follows. Secrect Key is 'hmwhoNoffvOWNqqP' And Authentication keys are 'qlMckNy3 25DrYCKN D1SMq2Ie WAZBod2y cTDqzO5P rqPjyLUv GJMZNMNx MCpSX7OY deof8tmZ 5du9mzUk'.

This is the mail content.

The secret sharing schemes are perfect in the multi cloud environment to provide data security and authentication in cloud without the drawbacks of encrypting data and service availability failure due to single cloud providers.

V. CONCLUSION

This study is carried out to design single and multi-cloud using secret key sharing algorithm which will result in deduction of the cost for the physical infrastructure, reducing the cost entry and execution as well as the response time for various associated applications. It also aims at the issues for cloud security and solutions provided by Shamir's Secret Sharing algorithm. The algorithms used, use secure channel to distribute generated secret sharing scheme. and use secure channels to distribute shares among themselves. The Shamir's secret sharing scheme has enough strong features in addressing the problem of data integrity, confidentiality and availability which makes it a better approach to the single service cloud provider.

REFERENCES

[1]. M. AlZain, E. Pardede, B. Soh and J. Thom, Cloud Computing Security: From Single to Multi-clouds, Proceedings of (HICSS), IEEE, pp. 5490–5499, Hawaii, 2012

[2]. ..Jaya Nirmala , S.Mary Saira Bhanu , Ahtesham Akhtar Patel "A Comparative Study Of The Secret Sharing Algorithm For Secure Data In The Cloud". International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.No.4, August 2012 , DOI : 10.5121/ijccsa.2012.240663.

[3]. Ion Morozan, "Multi-Clouds Database: A New Model to Provide Security in Cloud Computing". 2012

[4]. D.Mounica, Mrs.Ch.Radhika Rani "Optimized Multi-Clouds using Shamir Shares" International Journal For Development Of Computer Science & Technology ISSN-2320-7884 ,VOLUME-1, ISSUE-III, Hore et al. (April-May 2013) .\

[5]. Md Kausar Alam, Sharmila Banu K. "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds". International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153.

[6]. Priyanka Pareek, "Cloud Computing Security from Single to Multi-clouds using Secret Sharing Algorithm**".** International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12, December 2013.

[7]. Sonia Verma1 and Amit Kumar Chaudhary, **"**Save And Secured Data On Clouds" Volume 5, No. 4, April 2014**,** Journal of Global Research in Computer Science.

[8]. Swapnila S Mirajkar, Santoshkumar Biradar,Cachin et al.(2014) ,"Secret Sharing Based Approach to Enhance Security in Cloud Computing", Mirajkar et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(6), June - 2014, pp. 53-57.

[9]. K.Sai Sowmya*1, M.KrishnaSiva Prasad, "Efficient and Secure Auditing To Cloud Storage in Cloud Computing. "International Journal of Computer Trends and Technology (IJCTT) – volume 16, number 3 – Oct 2014.

[10]. Gaidhankar Sushil, Kanase Amit, Lonkar Tushar, Patil Chetan, "Multi-Cloud Storage Using Shamir's Secret Sharing Algorithm". International Journal of advancement in Engineering Technology Management & Applied Science. Volume 1, Issue 7, December 2014.