ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Shamir's Secret Sharing Scheme to Ensure Privacy in Multicloud Database Model

S.Selvi,M.E.,(Ph.D), C.Kayathiri, P.Saranya, R.Sumithra, U.Mounika

Assistant Professor, Department of CSE, ACET, Tamilnadu, India

IV year, Department of CSE, ACET, Tamilnadu, India

IV year, Department of CSE, ACET, Tamilnadu, India

IV year, Department of CSE, ACET, Tamilnadu, India

IV year, Department of CSE, ACET, Tamilnadu, India

ABSTRACT: Clouds or Online database services grant data to be ingresses from virtually different location all over the world through the internet access . Cloud computing carries a competitive benefits to smaller business due to limited budget. All the cloud users do not want to rely on cloud providers that can't be trusted for a personal and important details like credit card and debit card or medical reports from malicious insiders and hacker's intrusion. Handling with "single cloud" providers is supposed to become less protected with users due to loss of service failure in a single cloud. The information should be preserved from suspicious cloud service . The main objective of this paper is to enhance the Shamir Secret Sharing Scheme(SSSS) in multi cloud database model. This will give a secure cloud database to avoid risk hence we apply multi cloud concept making use of Shamir secret sharing algorithm(SSSS) will minimize the risk of data intrusion and loss of service availability to ensure cloud. As the rapid development of block chain technology, the cloud storage method based on crypto currency will be widely used in near future so privacy in multi cloud should be enhanced.

KEYWORDS: MCDB ,Privacy in MCDB, Shamir's Secret Sharing Scheme(SSSS).

I. INTRODUCTION

THE need for Data outsourcing or database as a service (DaaS) is extremely important for any organization. In addition, data storage or data retrieval cost high specially for small companies . Economic computing resources and advanced network technology is referred to as cloud computing. The use of cloud computing has increased rapidly in many organizations. The fast access to applications or the decreasing of the infrastructure costs are provided by cloud computing services.

The security of Cloud computing is considered to be the most critical issue in cloud computing environment due to the valuable stored information for users in the cloud. Cloud providers should address privacy and security issues as a matter of high and urgent priority. As a result of the importance of data security in cloud computing, this paper focus more on the issues related to the data security aspect of cloud computing. It proposes a Multi-clouds Database Model (MCDB) which uses Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service [5]. The purpose of the proposed new model is to address the security and the privacy risks challenges in cloud computing environment. There are three security factors that will be examined in our proposed model, namely data integrity, data intrusion, and service availability.

In our proposed model we used Shamir's enhanced secret sharing algorithm in this the solution was to store the secret keys at several location as shares and when authorized number of users collaborate together, they can retrieve the secret. The schemes are (t, n) threshold schemes where ay t number of user can collaborate to recover the secret out of n users. This provides security, reliability and convenience. Shamir's scheme is simple and easy to implement and is based on polynomial interpolation.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

II. RELATED WORK

Cloud providers should address privacy and security issues as a matter of high and urgent priority.[2] Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud[1]. In reason years, there has been a move towards "multi cloud","inter cloud" or "cloud of cloud"[5].

A. THE CHINESE REMAINDER THEOREM[4]

Suppose $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and suppose $a_1, a_2, \ldots, a_r$ are integers. Then the system r congruence $x \equiv a_i \pmod{m_i} (1 \leq i \leq r)$ has a unique solution modulo $M = m_1 \times m_2 \ldots \times m_r$, which is given in equation(1)[3].

$$X = \sum_{i=1}^{r} a_i M_i \, y_i \bmod M$$

Where, $M_i = M_i = \frac{M}{m_i}$ and $y_i = M_i^{-1} \bmod m_i$, for $1 \leq i \leq r$

You submit your final version, after your paper has been accepted , prepare it in two coloumn format, including figures and tables[10].

B. RSA[3]

RSA is an asymmetric system which means that a key pair will be generated[6], a public key and private key, obviously you keep your private key secure and pass around the public one[2]. RSA is rather slow so it's hardly used to encrypt data, more frequently it is used to encrypt and pass around symmetric keys, which can actually deal with encryption at a faster speed[7].

C. ELGAMAL ENCRYPTION SYSTEM[8]

The Elgamal encryption system is a type of public key encryption algorithm[5]. Security fearures of this algorithm stem from the difficulty of computing discerte logarithms in the finite field[1]. The disadvantages of this algorithm is, doubling of the encrypted text length as compared with the initial one, causing longer computing times, and tougher requirements for communication channel security[9].

D. ROBIN'S IDA

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 (1) Each of the n rows of M represents a slice[9]. This modified data is stored at multiple data centers such that none of them have access to s < k-1 slices[7]. 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' (2) Even with the loss of (n-k) slices, the data can be reproduced thus ensuring availability [2]

B. PROPOSED SHAMIR SECRET SHARING SCHEME(SSSS)

This paper focuses on the issues related to the data security aspect of cloud computing. As 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-

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

clouds in cloud computing is surveyed.

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.

III. ALGORITHM'S USED

SHAMIR'S SECRET SHARING ALGORITHM(SSSS):

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

A. ARCHITECTURE DIAGRAM OF SHAMIR SECRET SHARING SCHEME IN MULTI-CLOUD

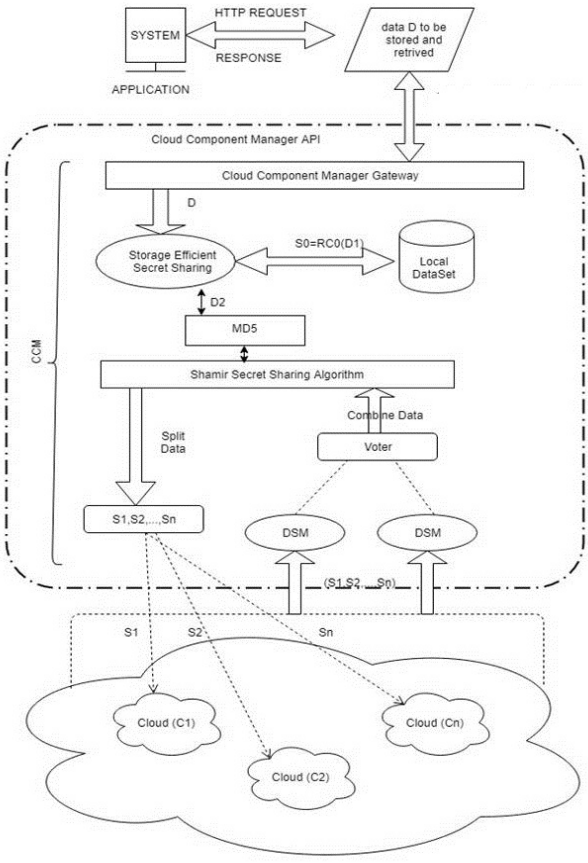

Fig 1.Proposed system architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

IV. SSSS ALGORITHM

1. MATHEMATICAL DEFINITIONS FOR SSSS

Shamir Secret Sharing Scheme (SSSS)enables to split a secret S in n parts such that with any k –out-of-n pieces you can reconstruct the original secret S, but with any k-1 pieces no information is exposed about S. That is conventionally called a (n, k) threshold scheme.

2. PROPERTIES

Some of the useful properties of Shamir's (k,n) threshold schemes are:

i. SECURE: information theoretic security
ii. MINIMAL: the size of each pieces does not exceed the size of the original data
iii. EXTENSIBLE: when k is kept fixed, D_i pieces can be dynamically added or deleted without affecting the other pieces.
iv. DYNAMIC: security can be easily enhanced without changing the secret, but by canging the polynomial occationally (keeping the same free term) and constructing new shares to the participants
v. FLEXIBLE: in organizations where hierarchy is important, we can supply each participant and different number of pieces according to his importance inside the organizations

3. ENCRYPTION OF SSSS

Our secret message is the text "SeCrEt" converting this to hex we have 0x536543724574 and continuously to decimal this is equivalent to 91694388364660. Thus S=91694388364660,also let N=5 and k=3. That is, we will split the text "SeCrEt" into 5 pieces and with any 3 of them we can reconstruct the text 3 of them we can reconstruct the text.

a_i < and a_0 =. Then those are used to generate theMpolynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 \dots a_{k-1} x^{k-1}$$

Back to our example we choose p=91994388364979.Then we generate random numbers:

a_1=5481390490034
a_2=4103884901909

And as a result the following polynomial is generated:

$$f(x) = 91694388364660 + 5481390490034\,x + 41038$$

The next step is to construct the N pieces that are distributed to the participants. Each piece is simply a point on the polynomial just defined. Each point D can be 527539161 calculated in an iterative manner:

$$DD_{x-1} = (x, f(x) mod\ p))$$

Where

$$x = 1,2, \dots, N)$$

In our case we need 5 points so we calculate them as follows:

$$D_0 = (1, f(1)\ mod\ p) = (1,928527539\,1624)$$
$$D_1 = (2, f(2)\ mod\ p) = (2,270783205\,87385)$$
$$D_2 = (3, f(3)\ mod\ p) = (3,530791355\,86964)$$
$$D_3 = (4, f(4)\ mod\ p) = (4,872877203\,90361)$$
$$D_4 = (5, f(5)\ mod\ p) = (5,377096866\,32597)$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

These are then distributed to the participants of the scheme.

2.DECRYPTION OF SSSS

In order to reconstruct the original secret from any k-out-of-n parts, we need to recreate the polynomial that we defined in the beginning. This can be achieved with the Lagrange polynomial Interpolation.. This is simply a formula named after the Italian mathematician Joseph Louis Lagrange For interpolating a polynomial of a degree less than n that passes through n points.
Initially, the Lagrange basis Polynomials need to be calculated. The formula for the basis polynomials is defined as follows:

$$l_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

Then, give n points, the interpolated polynomial is a linear combination of the above basis polynomial as a shown below:

$$f(x) = \sum_{j=0}^{n-1} y_j \, l_j(x)$$

Applying this our example we randomly select 3 out of the 5 points we derived above:
(x0, y0)=(1, 9285275391624*),*
(x1, y1)=(2, 27078320587385*),*
(x2, y2)=(4, 53079135586964*)*
Then the basis polynomials became:

$$l_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{1}{3}(x - 2)(x - 4)$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{1}{2}(x - 1)(x - 4)$$

$$l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{1}{6}(x - 1)(x - 2)$$

And the interpolated polynomial is derived form:

$$f(x) = \sum_{j=0}^{2} y_j \cdot l_j(x)$$

Therefore:

$$f(x) = \frac{9285275391624}{3}(x - 2)(x - 4) - \frac{27078320587385}{2}(x - 1)(x - 4) + \frac{87287720890861}{6}(x - 1)(x - 2)$$

$$f(x) = 410388490190 9x^2 + 5481390490034x - 300000000319 (mod\ p)$$

$$f(x) = 410388490190 9x^2 + 5481390490034x - 91694388364660 (mod\ p)$$

Note that since we are working over the Finite Field $Z_{91994388364979}$ the negative *-300000000319* can be changed to *+91694388364660.* And guess what… if this number looks familiar you are right! This is our **secret**.
We have just walked through the whole operation of the scheme manually and retrieved our secret back.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

V. MODULE DESCRIPTION

A. GLOBAL VARIABLE STRUCTURE

The global variables in the implementations are the user name and password implementation to access the different databases, a prime p, the number of shares K, and the database IP addresses. There also three array list structures:

1. A database address array list
2. Coefficient array list
3. Share array list

The prime number was implemented as a Big Integer, which allows the use of integers larger than 64 bit limitations of the long data type [20]. This large prime ensures that the coefficient generated are also very large, making it difficult for an attacker to recover the secret due to discrete logarithm problem.

B. RANDOM COEFFICENT GENERATOR

The coefficient generator is used to generate K-1 20147 bit cryptographic strength pseudo random numbers[22], and this process is repeated for every secret being split into shares. During the test smaller coefficient where used and we noticed that there where times where a zero was returned as a secure random number. this would have changed an entire term to zero during multiplication, so a check was added to add the value one to the secure random number when this was the case. The coefficients are stored in the coefficient array list and only accessed when generating shares

C. SECRET SHARE GENERATOR

The share generator produces shares corresponding to each x input. It uses a polynomial such as (1)using the generated coefficients mentioned earlier, and produces as many shares as indicated by the global variable k. in this implementation, the x values are generated incrementally with the loop. The resulting shares vary in size, depending on the number of shares being produced, but their size is increase as the number of shares increase. The shares where also implemented as a Big Integer, again due to the 64 bit limitations of the long data types[20].

D. DATABASE OPERATION

The operations are responsible for committing a record, fetching a record, deleting a record, and deleting all records.

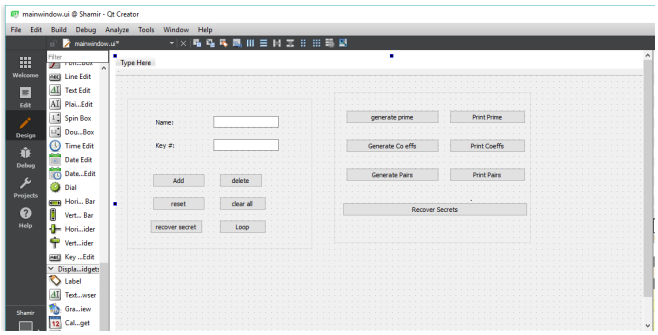

Fig. 2. Proof of concept Application depicting some of the control buttons. Add, Delete, Recover Secret, and Loop all operate on the databases, while the independent local controls do not interact with any database, and are used for debugging.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

The record commitment method stores the various shares in the different databases. First, an SQL command is built, and a hash along with the corresponding share are concatenated to the SQL command. This command is then executed within a loop, where a different database is accessed, on each iteration. If a duplicate name field is found in the database, then the error is caught and signaled as an output in the DB Operations output area whose tab is shown in figure 2.

VI. RESULT AND DISCUSSION

This SSS algorithm yields maximum security compared to the existing system.
There are two tests to analyze scheme's time for splitting and recovering, which are:
a. Test the effects of shares number (n) on the split and recovery time by testing varied number of shares.
b. Test the effects of threshold value on the split and recovery time by testing varied values of threshold.
Thus, the secret can be constructed with the trusted mathematically and shared among in the new trusted function and can be used to access and maintain confidentiality in cloud computing. Shamir secret sharing scheme can be used to improve security – an attacker cannot accumulate shares from multiple branches, because shares are valid in batches, and only the latest batch is the valid one that can be used for secret restoration. Migration to multi cloud is encouraged keeping in mind about its ability to minimize the breaches and other security problems.

VII. PERFORMANCE ANALYSIS

Robin's IDA scheme is less space-efficient than Shamir's and that they both work based on pretty different aspects (Shamir = polynomial-based; Robin IDA= hyperplane-based). The tests contacted to analyze the performance Shamir's scheme are as follows:

Flexibility analysis of Shamir's scheme:
The secret is recovered by combining shares in different order.
Storage requirement analysis for Shamir's scheme: Shamir's total storage requirements for data file of size |F| bytes and if the total number of shares is n then the total size is n ×|F| bytes. This means the storage requirement for each share (piece) is |F| bytes. Therefore the Shamir's scheme needs a high storage requirement.
Effects of number of shares on the split and recovery time:
the time increases with increasing in the number of shares n, as it is obvious that the time taken to split 450 KB into 10 shares is less than the time taken to split into 40 shares.

VIII. CONCLUSION

The purpose of this work is to survey the recent research on single clouds and multi-clouds using secret sharing algorithm and to address the security risks and solutions using Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves. The Shamir's secret sharing scheme has a good abstract foundation which provides an excellent framework for proofs and applications We are currently developing a secure computation platform based on a simple secret sharing scheme than Shamir's. the amount of protection needed to secure data is directly proportional to the value of the data. Security of the cloud relies on trusted computing and cryptography. Thus, in our proposed work only the authorized user can access the data. Even if some intruder gets the data accidently or intentionally the captures the data also, he can't decrypt it and get back the original data from it. Hence, forth, data security is provided by implementing Shamir's algorithm. We support the migration to multi clouds due to its ability to decrease security risks that is affect the cloud computing users.

IX. FUTURE WORK

The storage requirement can also be reduced if we use scheme where the share size is only half the size of the original secret. The schemes mentioned in this paper are simple and easy to implement when sharing data with third

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

party servers. We have used this schemes for efficient sharing of secret images also. The security can be enhanced if in future any other security algorithm is developed. As the rapid development of block chain technology, the cloud storage methods based on block chain will be widely used in the near future. Block chain uses distributed encryption format to store data and have a ordered chain path, in which every block has encrypted hash value of previous block.

REFERENCES

[1] Access, Identity and Secure Data Storage in Private Cloud using Digital Signature International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014.
[2] Mohammed A. AlZain , Eric Pardede, Ben Soh , James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds” IEEE Computer socity 45th Hawaii International Conference on System Sciences, 2012.
[3] Musthaler L (2009) Cost-effective data encryption in the cloud. Network World.
[4] Analysis of Security Algorithms in Cloud Computing International Journal of Application or Innovation in Engineering & Management (IJAIEM)Volume 3, Issue 3, March 2014.
[5] Pearson S (2009) Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD ’09.
[6] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.
[7] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: A research survey," in 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011, June 3, 2011 - June 5, 2011, Katra, Jammu, India, 2011, pp. 115-119.Zhijie Fan, Chunmei Wang, Bing Liu, Research on Access Control in Colud Storage System, Tongji university, china, vol-7,pp14, April 13,2018
[8] A.A Raipure, Secret Sharing Algorithm in Cloud Computing Cver Single to Multi Cloud, RMIT Universoty, June 3, 2016
[9] Vijaya Pinjarker,Neeraj Raja, Krunal Jha, Ankeet Dalvi, Single Cloud Security Enhancement using Key Sharing Algorithm, Mumbai, vol-4, Mar-7, 2013
[10] Binu VP, Sree kumar A, Simple and Efficient Secret Sharing Schemes for Sharing Data and Image, Cochin University of Science and Technology, Kerala,vol-6,pp-404, Feb 13,2015
[11] Siddharth Srivastava, Shashank axena, Rishabh Trikha, Polynomial based Database TransferTtechnique, Uttar Pradesh Technical University , Lucknow, U.P , vol-5, Feb 2, 2015
[12] Arun Singh, Darshan Jain, Paresh Chavan, Sweta Jain, Multi Cloud data security, Maharashtra, vol-3, Mar-3, 2016.
[13] Mohanned A.AIZain, Eric Pardede, Ben Soh, James A.Thom, cloud computing security from single to multi cloud, RMIT university, Melbourne, Australia, Dec 26, 2015.
[14] Rosemary Koikara, Kyung Seo, Anand Paul, Kee Young Yoo, Secret Sharing in Multi Clouds, Kyungpook National University,Daegu, South Korea, nov 14, 2017.
[15] Madhusekhar, Snehal P. Rokade, Ensuring Security in Multi Cloud Computing, india, 2014.