ISBN: 978-1-948012-16-4

Contemporary Issues in Computing (CIC)

DOI: <http://doi.org/10.26480/cic.01.2020.33.38>

SECURITY OF DATA` IN CLOUD COMPUTING BASED ON ADVANCED SECRET SHARING KEY MANAGEMENT SCHEME

Shipra Yadav^a Keshao D. Kalaskar^b and Pankaj Dhumane^c^aResearch Scholar, IICC, RTM Nagpur University Nagpur, (MH), India^bAssociate Professor, Dr. Ambedkar College, Chandrapur, (MH), India^cAssistant Professor, Sardar Patel College, Chandrapur, (MH), India^{*}Corresponding Author e-mail: pdhumane@rediffmail.com

This is an open access article distributed under the Creative Commons Attribution License CC BY 4.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 26 October 2020

Accepted 27 November 2020

Available online 03 December 2020

ABSTRACT

Cloud Computing (CC) is a worldwide concept and there are no boundaries define with in the cloud computer which is used to access and store user data can be located anywhere on the global network, depending on where the capacities that are required are available in the global computer networks used for cloud computing. Because of the efficient features of (CC) many Organization are using cloud storage for storing their essential information. The data can be stored remotely in the cloud computing environment by the user and can be retrieved by the client at the time of need. Data security is the major concern in cloud computing. Data Storage is risky because of use of internet by cloud based services which means less control over the store data. Essential elements of cloud is how do we grab all the benefit of the cloud while maintain security controls over the organization assets. Our aim is to propose a more reliable, decentralized light weight key-management scheme (KMS) techniques for cloud system which provide more efficient data security.

KEYWORDS

CC, Data Security, Advanced Secret Sharing, KMS, Byzantine failure.

1. INTRODUCTION

One of the most testing issues of cloud administration sales is to convince clients to confide in the security of cloud administration and transfer their touchy information. Al-however cloud specialist co-ops can guarantee that their administrations are well-ensured by expand encryption instruments, customary cloud frameworks still can't persuade the clients that regardless of whether cloud servers are undermined, information are still safely secured. Key organization consider as hardest area to regulate in cryptosystems. In a request to manage safely the encryption keys, attempts must use in cloud encryption, further managing secure storage of the on-site encryption keys. Keys should never be stored as mixed data in a comparable location. Keys used to scramble inconsistent customer data should be guided by sparse key turn and new keys to re-encrypt data. Employees should not be given more access than they can rely on to accomplish their task.

Morsy et al, 2010 analyzed the problems of cloud computing using the cloud architecture, cloud computing define the characteristics features, Drivers of cloud computing, and cloud computing service and delivery models perspectives.

The component of paper is organized as follows: The key management challenges in cloud. Mentioned the types of KMS and issues in cloud computing. Solution to these security issues is discussed. The need of secret sharing schemes and die rent types of secret sharing schemes respectively. Background concepts are discussed. The problems with

existing key management secret sharing and finally comes to the conclusion.

1.2 Cryptographic Key Management Challenges in the Cloud (Cryptographic Key Management Issues, 2014)

Essential component of distributed computing is the protected administration of the assets that are related with cloud administrations. The fundamental assignments of secure administration is cryptographic activities. Henceforth self configurable assets, flexible capabilities and universal registering is sanctioned by cloud administrations at a less cost, they likewise involve playing out a few cryptographic tasks for the accompanying:

For give secure capacity of information that is handled by those administrations.

By give secure association of the cloud shopper with different administrations.

Above limits can grow the multifaceted key organization system required to help cryptographic undertakings capacities the contrasts in control and obligation regarding structures on which the advantages and Key organization system are found.

1.3 Types of key management scheme (A Survey of Key Management, 2003)

Particular dissemination keys and encryption is used for security of basic

Quick Response Code	This paper was presented at	Access this article online	
	International Conference on Contemporary Issues in Computing (ICIC-2020) - Virtual IETE Sector V, Salt Lake, Kolkata From 25th-26th July 2020	Website: www.intelcomp-design.com	DOI: 10.26480/cic.01.2020.33.38

data is a basic framework for limiting access to information. Information data is given to encryption calculation and a couple of changes are performed on it using a cryptographic key. A gured substance is delivered in this method. There is no straightforward way to deal with recuperate the first message from the gured content by some other means than realizing the correct decoding key.

There are a couple of differing strategies to gathering key administration could be categorized into three key classes:

Key Centralized Plans: assembling key organization shows: In this show single substance controls the whole assembling, in this manner this show restrains the information move limit utilize computational power, amassing necessities, of both client and Server sides.

Key Decentralized plans: In decentralized structures, a tremendous social affair is disconnected into little subgroups and these subgroups are directed separate subgroup officials which point of confinement the issue of concentrating the exceptional job that needs to be done solitary spot.

Distributed Key organization shows: In this designing, the key organization errand is performed by the people themselves and no unequivocal KDC is required (Introduction to Combinatorial Mathematics, 1968).

1.4 Problems with key management in cloud Systems

Key organization is the hardest component to control in cryptosystems Problems are associated with the encryption key organization of Cloud Computing (Cloud Security).

- CC Organization, the insider likely to ambush. Employees can gain or steal the keys without having to learn the end customers.
- Records Keys for all records must be appropriately assigned. Verification is the ability to quickly and accurately record real records using their individual keys.
- Another problem for the main organization is availability. If a structure goes on the web, then how do you get the keys? Regardless of whether a system goes to the web, there must be a key save to retrieve the keys.
- Byzantine failure is a major blemish on cloud servers (The Byzantine, 2010). In the event of this kind of inadequacy, a limit can fall on the server's self-assured ways.
- Server plotting in the fog and the ambush that changes the data are common, in that the range servers can undermine the competitor, so little can be changed.

1.5 Security issues Solution

The above features is used in order to request securely manage encryption keys, adventurers must use encryption cloud state, as to manage secure on-site storage of encryption keys. Encryption keys cannot be stored as mixed data a comparable location. keys used to encrypt weak user data guided precisely random key turn and by re-encrypting the data with new keys. Do not give employees more access than they need to make mistakes.

Byzantine failure is a frequent drawback on servers of Cloud, due to which a capacity of server can fail in subjective ways. When Byzantine despair, the framework responds in a brisk way. Exactly when a Byzantine disappointment has occurred, the system may respond in any whimsical manner, except if it is proposed to have Byzantine adaptation to internal failure. The cloud is deployed for information modification and server gyrating intrusion attacks, in which capacity servers can undermine the enemy because they can modify data as long as they are persistent. The forgiving security capability of the information on the distributed storage server requires that the information be encoded.

1.6 Necessities associated with Secret Sharing schemes

In 1968, Liu pondered the problem with this: eleven researchers are taking a shot at a niche venture. If at least six researchers are available, they would like to secure a bureau of archives with the aim of opening the bureau. Most affordable number of locks required? What are the most modest number of keys to the locks each scientist must carry? On the off chance that we researchers are viewed as combined of which they can't open the specific lock. In the event that we think about a specific researcher, he should have the keys of those.

Locks that can not be opened through any of the other ten researchers. Of the 11 researchers, five researchers are associated with $11C5 = 462$ methods, and among the ten researchers, researchers can be selected by $10C5 = 252$ in various ways. With these lines, for the negligible arrangement, 14 researchers require 252 keys and 462lock. This is clearly inexcusable, and if the number of researchers is formed then it should move towards becoming faster and more terrible.

1.7 Key Management Secret Sharing Schemes

Di event secret sharing schemes are discussed below:

Simple secret sharing

1.7.1 Additive Secret Sharing

In additive secret sharing for a given secret S , n random integers $R = r_1, r_2, \dots, r_n$ are selected by the dealer uniformly from F . X then computes

$$S_n = S \oplus_{i=1}^n r_i \text{ mod } F$$

Element X sends the share $s_i = r_i$ to each player P_j , $1 \leq j \leq n$, and the share s_n is sent to P_m . The secret S reconstruction is trivial and it can be generated simply by adding all the shares together.

$S = \oplus_{i=1}^n s_i \text{ mod } F$ In this plan commitment of offers from every one of the members is required so as to reproduce mystery. The first offer can't be recouped on the off chance that on the off chance that at least one of the members are feeling loss of, A plan wherein commitment of considerable number of members are assigned an ideal mystery sharing plan.

2. THRESHOLD SECRET SHARING SCHEME

In 1979, a group of researchers presented together the idea as it generate message faster safe (Adi, 1979; Blakley, 1899). In this scheme, the message MG is separated into n pieces; $M G_1; M G_2; M G_3; \dots$; With the without transformation of $M-GN$, or the message, in this way, for a specified $K, 1 \leq K \leq n$. Learning any k or more pieces makes MG countable; 2. Information of any K or more pieces leave MG completely suspicious. This plan is called (k, n) -threshold plan. The parameter k in (k, n) is called the threshold value.

The Asmuth and Bloom Secret Sharing Scheme Asmuth & Bloom proposed a scheme in which particular number juggling is utilized to share mystery among gatherings and Chinese leftover portion hypothesis issued for reproduction of first mystery (A modular approach, 1983). Keys are otherwise called shadows.

(Le) Background concepts

2.1 Lagrange (Le) polynomial

Numerical Analysis is used for polynomial interpolation (Le) lagrange polynomials. Two odd distinct points x_i and numbers y_i are mentioned, the Lagrange poly-nomial (Le) is the least degree of the polynomial where each point x_i assumes the corresponding value y_i .

When a set of $p+1$ data points are given

$(x_0, y_0), (x_1, y_1), \dots, (x_p, y_p)$ where no two x_i are the same, the interpolation polynomial in the Lagrange form is a linear combination

$$L(x) = \sum_{i=0}^p y_i l_i(x) \text{ of Lagrange basis polynomials}$$

$$X := \sum_{j=0}^p y_j l_j(x) \text{ where } l_j(x) = \prod_{i \neq j} \frac{(x - x_i)}{(x_j - x_i)}$$

where $0 \leq j \leq p$.

2.2 Sharing Scheme of Shamir Secret

Shamir's Edge-Sharing Plan depends on plan that a line 2 points for me as D is enough, so according to De Ne, a parabola three are sufficient, 4 to de cubic curves are thus ahead. Therefore, in the form of degree $K-1$ polynomial, D concentrated enough.

Suppose we want to use a (k, n) threshold scheme to share our secret S , without loss of generality assumed to be an element in a finite field F of size P . Positive integers a_1 select at random $k-1$; a_k with a_0 , and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{k-1}x^{k-1}$. Let us construct any n

points out of it, for instance set $i = 1; n$ to retrieve $(i, f(i))$. Each member is given a point (Contributing a number to the polynomial, and the related whole number yield). Looking at any sub-group of k of these sets, we can use the polynomial and can use objection. The secret is a stable word a_0 .

2.3 Existing Problem with secret sharing scheme

Blakeley and Shamir[6] introduced the concept of Mystery Secret Sharing so that they remain e-mails in a prudent and secure way. Laranzes putting polynomial is the basis of the Shamir secrets, while the Blakely[7] in 1979 mystery sharing depends on linear projective geometry. In both of these mystery sharing plans, a part of the loss is mentioned below:

A fake shadow might be distributed to a specific member thru a deceptive vendor also afterward genuine mystery could never be acquired by that member.

A fake share might be offer by a vindictive member to different members, thus the true mystery must be reproduced by malevolent member.

2.4 Remark

On the off chance that a solitary KDC is utilized it might turn into a point of disappointment. Notwithstanding it in view of huge number of clients it progresses toward becoming di religion to keep up a solitary key circulation focus .so, proposed work, we try to pronounce on the decentralized method in the Mistake key, while the secret key also gives credit to customers.

2.5 Proposed Technique Model

This concept is organized as follows: proposed model and main entities are introduced. The cloud manager and the sub modules in it. Phase of Share renewal is discussed. Explained the voting technique used to ensure integrity of the shares. Proposed model process is described in detail. The essential features of proposed system over existing systems is described. Finally provide the conclusion.

2.6 Main entities in proposed model

The principle elements in the proposed calculation are Cloud Client, Distributed Storage Server, Cloud Chief, Keysplitter Server, Investor Server, Security Server, Log Manager, which are detailed in detail:

Share User: The user can create, update and delete his/her profile, store and retrieve the data.

FileInfo	Users Share(xu)	Users Share(f(xu))
----------	-----------------	--------------------

Loud Storage Server: This is a repository of information on a virtualized stockpiling pool or a remote server. Distributed data by the customer to store their information. Clients can purchase stockpiling limits from cloud facility organizations. Principle obligations of distributed storage servers are removed from the encoded reports, with the final goal of key administration to remove the split encryption key properties.

2.7 Key Management Server

The key splitter enters the server parts di erent offers split into store key encryption and di erent investor server..

FileInfo	Users Share(xu)	Users Share(f(xu))
----------	-----------------	--------------------

2.8 Key Share Holder Server

These servers stores offers for different keys for different clients. Investors can be of two sorts. Essential investor straightforwardly get the offers from the cloud administrator. Optional investors are the investors at leaf level and these investors get their offers through essential investors..

CloudUser Id	File Info	xi	f(xi)
--------------	-----------	----	-------

2.9 Log editor

It checks investor servers opportune to check whether offers are provide modification.

ShareHldserver Id	CloudUser Id	Value (t-60)	Value (t)	Value Status
-------------------	--------------	--------------	-----------	--------------

2.10 Security server

It has the encryption decryption algorithm.

Encryption process:

Step 1- Split the letter of modified plaintext.

Step 2- Assign the position(i) of the letter.

Step 3- Generate the ASCII value of plaintext letter.

Step 4- $E = (p + k + i)p$ -plaintext, k-shared key, i-position

Step 5- Generate the ASCII character of the corresponding decimal value in the result from the above given formula.

This would be the cipher text. Decryption process:

Step 1- Generate the ASCII value of the cipher text character.

Step 2- Same encryption key is used.

Step 3- Assign the position i of the cipher text.

Step 4- $D = ((c - k - i) + 256)p$ -plaintext, k-shared key, i-position.

Step 5 Generate the ASCII character of the corresponding decimal value in the result from the above given formula. This would be the original plain text.

Log editorial manager checks in time of 60 sec if any offer gets refreshed. In the event that no key updates are played out the essential investors are utilized in unscrambling process. On the off chance that an essential investor gets refreshed other essential investors are additionally checked. On the off chance that the greater part are unaltered the unaltered qualities are utilized. Table 1 demonstrates the activities that ought to be performed for different estimations of essential and auxiliary investors.

Table 1: Actions to be performed for different values of primary and secondary share holders.		
PrimaryShareHolder	SecondaryShareHolder	Action
Unchanged	Unchanged	Trusted
Changed	Changed	Use another share holder
Unchanged	Changed	Trusted
Changed	Unchanged	Regenerate primary from secondary

2.11 Cloud Manager

It comprises of a security server module & a voter module. Security server has encryption unscrambling figuring & throwing a tally module in cloud boss per-structures throwing a tally to check whether offer keyholder is real or not. Structure trustworthiness is extended by using throwing a vote framework. The normal correspondence channel b/w client & cloud chief is secure. Figure 1 shows the diferent modules in cloud chief.proposed method is recommended for cloud frameworks utilizing symmetric encryption.

Figure 1: Cloud Manager

2.12 Share Renewal Phase

The keys are thought to be put away in a various leveled way. The optional key director disseminates the offers to the essential key holders. Essential key holders thus appropriate mystery auxiliary key holders. The mutual keys will have a crypto period. At the point when this period is going to terminate every one of the offers will be reestablished. The estimations of

offers that investors are having ought to likewise be checked now and again there might be a probability of a portion of the offers being modified by the assailants. Figure 2 shows how the essential and auxiliary investors are checked by the log proofreader.

2.13 Overview of voting technique

Security and protection of clients information is safeguarded in the proposed strategy by the replication of key offer among a few mists, but the utilization of the mystery sharing methodology, and utilizing a casting a ballot technique offers. Figure 3 shows how the casting a ballot is performed by the voter module in cloud administrator.

Figure 2: Proposed Key Management Scheme in Cloud

2.14 Working of proposed system

2.14.1 File Upload

Exactly when the cloud customer needs to exhibit a le to a cloud first the le is sent to the cloud executive. Security module in cloud boss makes key and scrambles the le using encryption count as showed up and a while later advances the best approach to key organization module. Mixed le is sent to cloud data accumulating center. Key organization module segments key into various offers. Pro key to cloud customer and disperses all remaining keys to ShareHolderServers. Every basic financial specialist and helper speculators are checked time to time to ensure that their characteristics are not changed by an assailant.

Figure 3: Voter in the Cloud Manager Module

Share Holder Servers. All the primary share holders and secondary share holders are monitored from time to time to ensure that their values are not modified by attacker.

Figure 4 shows the data communication in le upload process. The le upload consists of following communications:

User requests to upload ale in cloud system.

- (a) Encrypts the le. Forwards the shares to the secondary key manager
- (b) Forwards the master key to the cloud user
- (c) Forwards the encrypted le to the data storage server

Key manager distributes the shares among the share key holders.

File Download

Exactly when cloud customer needs to download a le that is secured in cloud le name and shared expert key is entered by cloud customer. Download sales is sent to key organization server. Key organization server requests all ShareHolderServers to propel their bit of keys that identify with le. Key the official's server joins all of ideas to make the subsequent

level keys and advances route to security server merges the expert key with another master keys to create guideline key. le is unscrambled additionally is sent to cloud customer

Figure 4: Communication in le Upload

Figure 5 shows the process of le downloading. It consists of the following data communication:

(a). Request to cloud customer to give an ace key that was given in encryption technique

(b) Request to safety server for le downloading

(c) Master Key given by cloud customer

(a) Data stockpiling server sends encoded le to distributed storage server

(b) Request to data storing server to send mixed le as referenced by the customer

(a) . Data accumulating server sends encoded le to dispersed capacity server.

Figure 5: Communication in le download

3. ADVANTAGES OF THE PROPOSED TECHNIQUES OVER EXISTING TECHNIQUES

(a) Shareholder servers forward their offers identifying with customer to a key boss

(b). Key Manager requests offer from different financial specialists

Key boss unites all of offers secure server

Security server joins an expert key given by customer and discretionary key given by key organization server and makes a certified key. At that point, it unscrambles customer le set away in cloud and send it to the customer.

Our method gives adaptation to internal failure to byzantine assaults, information modification and server conspiring assaults.

Existing strategies are brought together in nature. We attempt to give unappropriated way to deal with key administration

3.1 Remark

In this segment we have proposed a structure which ousts drawbacks of a part of current cloud systems. New modules are added to current structure to in-exhibit unfaltering quality likewise security of current cloud structures that usage key encryption symmetric techniques to ensure data security

4. IMPLEMENTATION AND RESULTS

Simulation Environment

The implementation is done using the following tool and techniques:

- CloudSim
- Amazon Web Services
- Jswings
- Cloud Sim
- CloudSim is a web app that runs in a virtual machine on the Amazon Web Services (AWS) cloud.
- It enables clients to dispatch, end & screen (VM) in AWS cloud.
- Different configurations must be propelled, contingent upon necessities, & accessible components on cloud
- Each CloudSim configuration maps to a group of stars, which are accumulations of numerous virtual machines running together.

4.1 Results

Proposed technique is implemented with different l_e size ranges from 100KB to 50MB and we try to find out performance comparison between a existing and proposed technique. The key provided from AWS is the token that allow CloudSim to access AWS on behalf of the AWS user. Figure 6 and Figure 7 shows the snapshots of how the key is divided into several shares and is again combined to generate the original key. For our implementation 128 bit key is used and $n=128$.

Figure 6: Snapshot of Key Generation

Table 2 and Figure 8 represents the time taken to split a 128 bit key into 10 pieces for different threshold values.

Threshold(k)	Time(ms)
5	4.56
6	4.08
7	3.39
8	2.50
9	3.41
10	2.26

Table 3 and Figure 7 represents the time taken to combine the shares for different threshold values

Figure 7: Key Splitting Snap Shot

Figure 8: Key Dispersal for 128bit key with $n=10$

File Upload Time-It incorporates an opportunity via scramble l_e which mentioned through customer, It time between the focuses when client demand cloud framework to transfer l_e and when errands of encryption also producing key offer really niches and encoded l_e is really put away in the cloud information stockpiling demonstrates the times taken for l_e transferring different l_e sizes file down time it incorporate time to gather produce the optional key, Consolidate master key also secondary key to period to decode information l_e . It is time between 2 solicitation to download a l_e also client really get his l_e duration for downloading different size.

Threshold(k)	Time(ms)
5	.79
6	.75
7	.76
8	.073
9	.74
10	.77

Figure 9: Key recovery from shares for a 128 bit key with $n=10$

Figure 10: Time vs Size for l_e uploading

Figure 11: Size vs Time for l_e downloading

5. CONCLUSION

Key management is the toughest part to manage in cryptosystems. In the cloud platform, there is always a possibility of insider attack or outsider attack. Keys can be accessed or stolen by employees without the knowledge of end users. Our aim is to provide security to the data as well as keys that are stored in cloud systems. Our proposed technique provides better data security and key management in cloud systems. This technique also provides better security against byzantine failure, server clouding and data modification attacks. Further in the survey of this writing, we have deliberately investigated CC security so as to recognize key innovation issues today. Using 52 Using criteria to figure out which writing to be incorporated to incorporate different articles in the audit. These 52 were assessed and 26 articles were viewed as pertinent for investigate query. Utilizing these 26 articles, the writers of this survey could recognize distributed computing security just as key issues and arrangements in territories where further research ought to be finished

5.1 Recommendation

In future, this work can be extended to use some other secret sharing schemes which are more efficient so that the performance of proposed system can be further improved. In addition to this, the proposed technique can be extended to work with asymmetric encryption algorithms.

REFERENCES

- A modular approach to key safeguarding. 1983. IEEE transactions on information theory, 30(2), 208-210.
- A survey of key management for secure group communication. 2003. ACM Computing Surveys (CSUR), 35(3), 309-329, 78-79.
- Adi. 1979. How to share a secret. Communications of the ACM, 22(11), 612-613, 81.
- Blakley, G.R. 1979. Safeguarding cryptographic keys. Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, 81.
- Cloud Security: Efficient and Reliable Encryption Key Management Crucial for Data Protection. <https://spideroak.com/privacypost/cloud-security/secure-encryption-key-management-in-the-cloud/> p79
- Cryptographic Key Management Issues and Challenges in Cloud Services. 2014. Springer New York. 78.
- Introduction to Combinatorial Mathematics. 1968. McGraw- Hill, New York, 79.
- The Byzantine empire in the intercloud. 2010. ACM SIGACT News, 41(3), 105-111.