An Efficient Technique for Security of the Data in Cloud Computing through Key Management

Kruti Patel¹ Vijaykumar Gadhavi² Kaushal Jani³

¹M.E Student ^{2,3}Assistant Professor ^{1,2,3}Department of Computer Engineering ^{1,2,3}Gujarat Technological University, Gujarat, India

Abstract— Cloud computing has opened up a new frontier of challenges by introducing a different type of trust scenario. Computers are used to process and store user data can be located anywhere on the globe, depending on where the capacities that are required are available in the global computer networks used for cloud computing. Security has remained a constant issue for Open Systems and internet. Cloud really suffers at security. Security in cloud is consistently increasing when the applications and data are moving to the cloud because the individual loss of control over their data. The storage of data in cloud is very risky due to less control over stored data .One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets. Attacks. In this paper, I a more reliable, decentralized key management technique for cloud systems. It will provide more efficient data security and key management in cloud systems.

Keywords—Cloud Computing, Data Security, Key Splitting Method, Key Management, Server Colluding Attacks, Group Key Management, Secret Sharing, Shamir's Secret Sharing

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [5]. The cloud computing is a new computing model that provides the uniform access to wide area distributed resources on demand. Cloud computing is a way of leveraging the Internet to consume software or other IT services on demand. There are no shrink wrapped boxes containing discs or hardware for you to buy and set up yourself. Cloud providers typically charge monthly recurring fees based on your usage [1]. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm [2].

However, there still exist many problems in cloud computing today. A recent survey by Cloud Security Alliance (CSA) shows that security have become the primary concern for people to shift to cloud computing.

In this paper, we survey the security concerns of current Cloud Computing systems. As Cloud Computing referred to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centers) that provide those services [4], we present the security concerns in terms of the diverse applications and infrastructures. More concerns on security issues, such as availability, confidentiality, integrity control, authorization and so on, should be taken into account.

It can divide them into three main classes[13]:

II. APPROACHES TO GROUP KEY MANAGEMENT

A. Centralized Group Key Management Protocols:

A single entity is employed for controlling the whole group, hence a group key management protocol seeks to minimize storage requirements, computational power on both client and server sides, and bandwidth utilization.

B. Decentralized Group Key Management Protocols:

The management of a large group is divided among subgroup managers, trying to minimize the problem of concentrating the work in a single place.

C. Distributed Group Key Management Protocols:

There is no explicit KDC, and the members themselves do the key generation. All members can perform access control and the generation of the key can be either contributory, meaning that all members contribute some information to generate the group key, or done by one of the members.

III. RELATED WORK

The concept of secret sharing scheme was developed by Shamir [11] and Blakely [16] in 1979 in order to keep the secret efficiently and safely. Lagrange interpolating polynomial is the basis of Shamir secret sharing, while Blakely secret sharing is based on the linear projective geometry. Some of the drawbacks in both these secret sharing schemes [11] and [12] are as follows:

- 1) A fake shadow may be distributed to a certain participant by a dishonest dealer and then the true secret would never be obtained by that participant.
- 2) A fake share may be provided by a malicious participant to other participants, and so the secret can only be reconstructed by the malicious participant.

IV. MAIN ENTITIES IN PROPOSED MODEL

The main entities in the proposed method are cloud users, cloud storage server, cloud manager, key splitter servers, share holder servers, security servers, log editor which are defined in detail as follows:

- 1) User: The user can create, update and delete his/her pro le, store and retrieve the data.
- Cloud Storage Server: It is a model of data storage on virtualized storage pools or servers located remotely. Cloud storage can be used by users to store their data. Users can buy storage capacity from the cloud hosting

companies. The main responsibilities of cloud storage server are storing the encrypted document, storing the splitted encryption key values for the purpose of key management.

- 3) Key Management Server: Key splitter server splits the encryption keys into different shares and store the splitted keys in different share holder servers.
- 4) Share Holder Server: These servers store the shares for the different keys for different users.
- 5) Log editor: It checks the share holder servers timely to see if the shares are getting modified.
- 6) Security server: It has the encryption decryption algorithm.

V. STEPS OF PROPOSED METHOD

A. Share Construction

To share the secret among shareholder such that k shareholder are required to reconstruct the secret.

- Dealer D generates a polynomials f(x) of degree k-1 by taking the pixel values of secret as as d0, d1, d2 dk-1. f(x) = d0+ d1x + d2x2 + .. + dk-1xk-1 (mod p)
- 2) The shares are constructed by using the value of f(x) generated for all pixel values of original secret image
- 3) Dealer destroys secret and generated f(x) functions.
- 4) Each i'th shareholder will get a share.

B. Share Reconstruction

To reconstruct the secret image pixel from any k image shares out of n image shares

- Dealer asks shareholders to submit their image shares.

 Dealer uses Shamir's Lagrange interpolation formula to get the original secret images.

VI. RENEWAL OF SHARES

The purpose here is to renew the shares periodically. We assume an initial stage where a secret s is encoded into n shares using Shamir's secret sharing scheme. After some specific time period Dealer will generate and distribute new shares by taking old shares from participants.

- Dealer will generate a polynomial Pi(X) of degree k-1.
- Dealer will ask to share existing shares f(i) from all shareholders.
- Dealer computes new image share by adding old sharef(i) to the sum of the new n shares.

$$h(i) = f(i) + \sum_{c=1}^{n} p c(i)$$

Dealer distributes new image share h(i) to each shareholder i

VII. DETECTION OF CORRUPTED SHARE

- Dealer will ask all shareholders to share their image shares.
- Dealer will make all combinations of k groups of received shares.
- Dealer will compute secret from those groups.
- After analyzing wrong secret generated groups dealer will come to know about corrupted share.

VIII. PROPOSED METHOD FLOW CHART



Fig. 1: Diagram of Proposed algorithm

IX. SIMULATION ENVIRONMENT AND RESULTS

The implementation is done using the following tool and techniques:

- Cloud Sim
- Amazon Web Services
- Netbeans

A. Construction of Shares

Create Share	Generated Shares Datacenter_0 Share 1	
ihare secret Key		
121	97	
lumber of Share(N)	Datacenter_1 Share 2	
5	73	
Threshold(K)	Datacenter_2 Share 3	
2	49	
CRYPTO_PERIOD (In Seconds)	Datacenter_3 Share 4	
30	25	
Generate Share Renew Share	Datacenter_4 Share 5	
-1000	1	

Fig. 2: Construction of shares

B. Reconstruction of Secret

Cloud Manager Share Management Cloud Uker Page 2 Page 3		
Create Share share secret Key	Generated Shares Datacenter_0 Share 1	Combine Shares Provide 2 Share Number [Comma Seperated]
121	12	1,4
Number of Share(N)	Datacenter_1 Share 2	Combine Share
5	66	Share 1
hreshold(K)	Datacenter_2 Share 3	12
2	120	Share 2
RYPTO_PERIOD (in Seconds)	Datacenter_3 Share 4	11
30	11	
Generate Share Renew Share	Datacenter_4 Share 5	Combine Share Validate Share
	65	The Original Share SecretKey is::> 121

Fig. 3: Reconstruction of shares

C. Renewal of Share

Create Share	Generated Shares	
Share secret Key	Datacenter_0 Share 1	
121	59	
lumber of Share(N)	Datacenter_1 Share 2	
5	238	
Fhreshold(K)	Datacenter_2 Share 3	
2	176	
CRYPTO_PERIOD (In Seconds)	Datacenter_3 Share 4	
30	114	
Generate Share Renew Share	Datacenter_4 Share 5	
	52	

Fig. 4: Renewal of shares

D. Detection of Corrupted Share

reate Share	Generated Shares	Combine Shares
hare secret Key	Datacenter_0 Share 1	Provide 2 Share Number [Comma Seperated]
121	12	1,4
umber of Share(N)	Datacenter_1 Share 2	Combine Share
5	66	Share 1
'hreshold(K)	Datacenter_2 Share 3	50
2	120	Share 2
RYPTO_PERIOD (In Seconds)	Datacenter_3 Share 4	11
30	11	
Generate Share Renew Share	Datacenter_4 Share 5	Combine Share Validate Share
	65	The Original Share SecretKey is::> 121



X. ADVANTAGES OF PROPOSED TECHNIQUE OVER EXISTING TECHNIQUES

- 1) Existing techniques are centralized in nature. We try to provide to provide a distributed approach for key management. The proposed system stores share in different data center.
- 2) Reliably of the system is increased by using the Validating technique to ensure that the share does not get modified by the attacker.
- After a pre decided crypto time, the shares are renewed in order to ensure the security of user data if in case some of the shares get compromised.

Threshold(k)	Time(ms)	Time(ms)
	Proposed	Existing
	System	Shamir's System
5	4.56	5.02
6	4.08	4.15
7	3.39	3.45
8	2.50	2.56
9	2.26	2.30

XI. COMPARISON RESULTS







XII. CONCLUSION AND FUTURE WORK

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. The proposed technique provides more security through validating shares provided by participants. It solves data modification attack and share holder's server crash problem.

The scheme can be modified for better time complexity without dealers interference and to handle active attacks in near future. One can also try to built this system using asymmetric key management system.

REFERENCES

- [1] P. Mell and T. Grance. The nist definition of cloud computing (draft). National Institute of Standards and Technology, 53:7, 2010.
- [2] I. Foster, Y Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360
- [3] Vukolic, Marko. "The Byzantine empire in the intercloud." ACM SIGACT News 41.3 (2010): 105-111.

- [4] http://south.cattelecom.com/rtso/Technologies/CloudCo mputing/0071626948_chap01.pdf
- [5] Almorsy, Mohamed, John Grundy, and Ingo Mller. "An analysis of the cloud computing security problem." the proc. of the 2010 Asia Paci c Cloud Work-shop, Colocated with APSEC2010, Australia. 2010.
- [6] The Future of Cloud computing, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-reportfinal.pdf.
- [7] Chandramouli, Ramaswamy, Michaela Iorga, and Santosh Chokhani. Cryp-tographic Key Management Issues and Challenges in Cloud Services. Springer New York, 2014
- [8] Rafaeli, Sandro, and David Hutchison. "A survey of key management for secure group communication." ACM Computing Surveys (CSUR) 35.3 (2003): 309-329.
- [9] Cloud computing layer, https://developers.google.com/appengine/training/intro/ whatiscc.
- [10] Liu, C.L. Introduction to Combinatorial Mathematics. McGraw- Hill, New York, 1968.
- [11] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613
- [12] Blakley, George Robert. "Safeguarding cryptographic keys." Managing Re-quirements Knowledge, International Workshop on. IEEE Computer Society, 1899.
- [13] Kalyani M. "Cloud Security: E cient and Reliable Encryption Key Manage-ment Crucial for Data Protection". https://spideroak.com/privacypost/cloudsecurity/secure-encryption-key-management-in-thecloud/
- [14] Agbaria, Adnan, and Roy Friedman. "Overcoming Byzantine Failures Using Checkpointing." University of Illinois at Urbana-Champaign Coordinated Sci-ence Laboratory technical report no. UILU-ENG-03-2228 (CRHC-03-14) (2003).
- [15] A Versatile and Ubiquitous Secret Sharing, Muhammad Adeka, Simon Shepherd, Nuredin A. S Ahmed, IEEE, March 2015
- [16] Performance Evaluation on Data Management Approach for Multiple Clouds Using Secret Sharing Scheme, Atsushi KANAI, Shigeaki TANIMOTO, Hiroyuki SATO, IEEE, January 2016
- [17] Space-efficient Verifiable Secret Sharing Using Polynomial Interpolation, Massimo Cafaro, Piergiuseppe Pell, IEEE FEB 2015