ISSN: 2321-7782 (Online)
Volume 4, Issue 3, March 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Attribute based encryption of data storing in Clouds with key attribute cryptosystem

Abhijeet C. Ghabade[1]
Department of Computer Engineering
Sinhgad Institute of Technology
Lonavala, India

Prof. Manohar S. Chaudhari[2]
Department of Computer Engineering
Sinhgad Institute of Technology
Lonavala, India

Abstract: ***The major purpose of this study is to construct an optimal portfolio using Sharpe's single index model by using risk-return analysis of automobile and pharmaceutical sectors. This study includes ten stocks from automobile sector and ten stocks from pharmaceutical sector. Data for a period of five years (2010-2015) had been taken for the study. After analysing the collected data a "cut-off rate "can calculate. This cut–off rate is considered in the construction of optimal portfolio. Every investor prefers maximum return with a minimum risk. This study found out that Ashok Leyland having highest return and Hyundai having lowest return.This paper identifies an optimal portfolio from the selected companies which serves as a guide to function in maximising return.***

Keywords: Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

I. INTRODUCTION

Cloud storage is gaining in quality lately. Enterprise settings, we information outsourcing, within strategic management company that helps to increase demand to see a trend. It conjointly private applications for many on-line services as a core technology used in. Information sharing is very important in cloud storage practicality. For example, Bloggers are a set of your personal pictures of her friends will read; Associate degree may grant his staff access to venture a little sensitive to information. Hard to fault it effectively encrypted way of sharing information. In fact encrypted information transfer, storage users will they decode, then send them to distribute to others, Although it loses the value of cloud storage. Users will access these information from those servers directly access rights to others to be able to share information to be representative. Secret writing associated with 2 keys conjointly flavors symmetric key or asymmetric (public) key.

Writing, victimization symmetrical secret once Alice wishes to find a 3rd party originated from, she got him to offer encrypted secret key; Of course, it is often not always attractive. Against this, the secret key and explanations of key write entirely different are the key secret writing in public. Public key using secret writing, our offers additional flexibility for applications. For example, the encrypted data in enterprise settings, each worker not the master secret key while the company's cloud storage will be transferred to the server.

II. LITERATURE SURVEY

In S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, [1], Data sharing is an important functionality in cloud storage. In this paper, we define how to securely, efficiently, and flexibly share data with others in cloud storage. We describe latest public-key crypto systems that define constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all of the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the different encrypted files outside the set remain

confidential. This compact average key can be conveniently sent to others or be stored in a smart card with very limited secure storage.

In B. Wang, S.S.M. Chow, M. Li, and H. Li,[2], Nowadays, many organizations outsource data storage to the cloud such that a member of an organization (data owner) can easily share data with other members (users). Due to the existence of security concerns in the cloud, both owners and users are suggested to verify the integrity of cloud data with Provable Data Possession (PDP) before further utilization of data. However, previous methods either unnecessarily reveal the identity of a data owner to the untrusted cloud or any public verifiers, or introduce significant overheads on verification metadata for preserving anonymity. In this paper, we propose a simple, efficient, and publiclyverifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant overhead. Specifically, we introduce a security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners.

In S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, [3], Data sharing is an most important functionality in cloud storage. In this article, we define how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compress as a single key, but encompassing the power of all the keys being aggregated.

In J. Benaloh, M. Chase, E. Horvitz, and K. Lauter,[5], Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computers with internet access. Personal Health Record(PHR) is an emerging patient centric model of health information exchange, which is outsourced to be stored at a third party, such as cloud providers. Issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation have remained the most important challenges towards fine-grained, cryptographically enforced data access control. In the proposed work, a novel patient centric framework and a mechanism for data access control to PHRs stored in semi structured servers.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

Propose Work: Ciphertext-Policy Attribute-based Encryption (CP-ABE) is considered one amongst the foremost appropriate technologies for information access management in cloud storage, as a result of it provides data house owners a lot of direct management on access policies.

Mathematical Model:

Let S ={SP, KG, En, Ex, Dn }

1. **Setup ($1^{\lambda}, n$) :** Executed by the data owner to setup an account on an un trusted server

   Let g and

   Where bilinear group and p is is prime order

   Where 2^{λ}

   Compute = G

   Where i=1… n, n+2

   System parameter =(g, g1, ……., gn, gn+2)

2. **Key Gen()** : Executed by the data owner to randomly generate a public/master-secret key pair

   Select $\gamma \in_R \mathbb{Z}_p$

   Where $\mathbb{Z}_p$ is prime number

   Out put the public and private key

3. **Encrypt (pk, i, m) :** Executed by anyone who wants to encrypt data.

   Let m be the message and be the index i

   Where m ϵ G_T and i ϵ {1,2,….n}

   Let randomly select $t \in_R \mathbb{Z}_p$

   Where $\mathbb{Z}_p$ is prime number

   And compute the cipher text c as (g^t,$(vg_i)^t$, m,$e(g1, gn)^t$)

4. **Extract(msk = γ, s):** Executed by the data owner for delegating the decrypting power For the set s of indices j's aggregate key is

   Ks =

   Where S does not include 9, = always retrieve from param

5. **Decrypt: (Ks, S, I, C) :** Executed by a delegatee who received an aggregate key KS generated by Extract

   Check if $i \notin S$ the out put $\perp$.

   Otherwise,

   Return message m= c3.e(Ks.$\pi_{j\epsilon S, j\neq i} g^{c1}_{n+1-j+i}$,c1) /e($\pi_{j\epsilon S} g_{n+1-j}$, $c2$))

   Let γ *be the knowlede of data owner* , the term $e(g1, gn)^t$ can be recoverd by e.$(c1, gn)^\gamma$ =e $(g^t, gn)^\gamma$= e(g1, $gn)^t$

IV. CONCLUSION

The data privacy may be a central question of cloud storage. With additional mathematical tools, crypto graphical schemes have gotten additional versatile and infrequently involve multiple keys for one application. During this paper, we have a tendency to take into account a way to "compress" secret keys in public-key cryptosystems that support delegation of secret keys for various cipher text categories in cloud storage. Regardless of that one in all the ability set of categories, the delegate will forever get associate degree combination key of constant size. Our approach is additional versatile than hierarchical key assignment which may solely save areas if all key-holders share the same set of privileges. Though the parameter is downloaded with cipher texts, it might be higher if its size is freelance of the utmost range of cipher text categories. On the opposite hand, once one carries the delegated keys around in a very mobile device while not victimization special trustworthy hardware, the secret\'s prompt to escape, coming up with a leakage-resilient cryptosystem , nonetheless permits economical and versatile key

delegation is additionally a motivating direction. Outsourcing knowledge of knowledge of information} to server could cause leak the non-public data of user to everybody. Cryptography may be a one resolution that provides to share elect knowledge with desired candidate. Sharing of decipherment keys in secure method plays vital role. Public-key cryptosystems provides delegation of secret keys for various cipher text categories in cloud storage. The delegate gets firmly associate degree combination key of constant size.

ACKNOWLEDGEMENT

We would like to express our sincere thanks to our beloved Principle Dr. M.S. Gaikwad and project co_ordinator Prof. M.S. Chaudhari for facilities provided for preparing this project

References

1. S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment, "Proc. 10th Int'l Conf. Applied to Cryptography and Network Security (ACNS),vol. 7341, pp. 526-543, 2012.
2. B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS),2013
3. S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance,"Cryptography and Security,pp. 442-464, Springer, 2012.
4. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security(CCSW'09),pp.103-114,2009.

AUTHOR(S) PROFILE

Abhijeet Ghabade, received the B.E (Bachelor of Engineering) degree in Information Technology from Rajarshi Shahu College of Engg.(pune) in 2010. During 2012, 2016 He now research with sinhgad institute of technology Department of computer Engineering, Lonavala, India to study cloud computing and network security.

