ISSN 2395-1621

Secure Key Management Using Session Based Encryption and Re-Encryption System

[#1]Shraddha Banne, [#2]Maitreyee Shende, [#3]Sneha Gade, [#4]Shravani Varute

[1]svbanne123@gmail.com
[2]maitreyeeshende@gmail.com
[3]snehagade45@gmail.com
[4]shravanivarute@gmail.com

[#1234]Computer Department
NBN Sinhgad School Of Engineering, Pune
Pune University

ABSTRACT

To the cloud, outsourcing data is the most beneficial for the reasons of economy, scalability, reliability and accessibility. but still there remain some significant technical challenges. Sensitive data that is stored into the cloud must be protected by a cloud provider. As the mobile devices are having resource limitations as well as the need of reducing cost of processing and communication, cloud based data access is the need of the hour. Fresh modifications to attribute-based encryption are proposed to allow the users an authorized access to cloud data such that it will satisfy required attributes. One of the feature to minimize the total communication cost to the mobile user is achieved by assigning cloud provider the major computational activity of cryptographic operations . Furthermore, data re-encryption may be an optional part performed by the cloud provider to reduce expense of user abrogation in a mobile user environment preserving the privacy of user data stored in cloud. The proposed protocol has been realized on commercially popular mobile and cloud platforms to demonstrate real-world benchmarks that show the potency of the scheme. A simulation calibrated with the benchmark results shows the scalability potential of the scheme in the context of a realistic workload in a mobile cloud computing system.

Keywords— **Encryption, Decryption, Re-Encryption, Security.**

ARTICLE INFO

Article History

Received:28th September 2015

Received in revised form :

1st October 2015

Accepted:5th October, 2015

Published online :

8th October 2015

I INTRODUCTION

Cloud computing is the model which enables convenient, on-demand access to the shared pool of configurable computing resources. Also it focuses on increasing the effectiveness of the shared resources. Cloud computing is one of the evolutionary model for distributed computing which has centralized data centres providing the resources for massively scalable units of computing. However, Internet is that insecure medium over which these computational facilities are delivered in the form of a service. A client sending request to access the data in the cloud can address various changes for its processing needs with the help of a cloud provider which creates replicas of the applications. Clients that access the data from cloud pays only for the storage amount, amount of network communication and related computation but not for maintenance and capital cost of an in-house solution. Along with the various facilities provided by the cloud provider like safety, longevity and high accessibility there is still a limitation that, the data stored in cloud may be accessed and

read by cloud administrator without the knowledge of the client. An additional risk is that sensitive data carries persistent risk of being manipulated or intercepted by an unauthorized party despite safeguards promised by the provider. Therefore, it can be helpful to apply some software techniques, such as encryption keys, to ensure the privacy and confidentiality of the cloud data is preserved at all times also increases the safety. Our system utilizes five entities namely "The data owner, Cloud Service Provider (CSP), User, Controller, and the Manager". Data owner encrypts the data items using symmetric encryption algorithm. Then, data owner uploads encrypted data items and data to the network. The cloud provider i.e. Cloud Service Provider unit provides the cloud service. The role of the CSP is acquiring and managing the infrastructure needed to provide the services and operate the cloud software providing those services along with delivering the cloud services via network access. User or client is an entity subscribing to a service provided by a cloud provider.. A controller administrates access through external client interfaces. Manager is a trusted authority within the system and is completely independent of the CSP. It is sufficiently trusted to authorize access to the cloud and to contain key material as necessary; however , to minimize the risk of it being compromised, a user will only share as much of its own key material with the manager as is necessary in the security scheme utilized. Furthermore, the manager will not be as economical as a cloud provider due to its more limited computational resources.

The main contributions of the proposed work are as follows:

1. A protocol for outsourcing data storage to a cloud provider in secure fashion is provided.
2. Re-encryption permits efficient revocation of users; it does not require removal of attributes and subsequent key regeneration, and may be administered by a trusted authority without involvement of the data owner.

In Section 2, related work on key management to secure cloud data storage is presented, with a focus on attribute-based schemes in the context of applications accessed by mobile devices. In Section 3, an existing system of key store management is presented. In Section 4, the proposed algorithm for attribute based encryption and re-encryption for the users of the cloud is presented. In Section 5, complete system architecture is presented. In Section 6, conclusion is provided. Finally section 7 provides references.

II.RELATED WORK

Numerous solutions may be forecast to exchange encrypted data with a cloud provider in a secure manner, such that the cloud provider is not directly invest with key material, but naïve schemes often prove difficult to scale. For instance, the main drawback of a scheme based on the use of a public key management system which works on the complexity level of factoring large integers, such as RSA (stands for the authors Rivest, Shamir, and Adleman) is that, it requires the data owner to provide an encrypted version of data for each recipient that may access it. If single key encrypted user data is used, then that key is required to be shared with all registered users, resulting in a high traffic cost. This is more impacting if this responsibility rests on a mobile data owner. Users may log 'in and out' frequently of the authorized user set and it will lead to constant key re-generation and redistribution through additional communication sessions to handle user annulations. In a high traffic system, such events may occur at relatively high frequency. Other communication method like wireless for transmitting the data, is expensive and demands high power consumption rapidly draining the battery. Hence data should be encrypted and ideally be stored in the cloud so the cloud provider cannot access it. This notion is dependent on the keys being securely managed by an entity outside of the provider's domain. The problem faced in this system, is when new users join, and existing ones leave the system, demanding generation of new keys. The process of data re-encryptions is required here. In this process encrypted data should ideally get transformed such that it may be unlocked with new keys, without an intermediate decryption step hence not allowing the cloud provider to read the plaintext. Although it appears to be a promising technique in managing encrypted data as access rights evolve over time, current solutions mentioned here neither address the issue of higher magnitude services in efficient manner. nor do they necessarily strive to lessen the computational and communication burden on users connecting to the cloud from mobile devices having limited resources. With this context, the technique of cipher text-policy attribute-based en-cryption (CP-ABE) [4] offers multiple advantages. It allows a user to obtain access to encrypted data in the cloud based on the possession of certain attributes that satisfy an access structure defined in the cloud, rather than the possession of a key that must be disseminated to all interested parties in advance. The requisite attributes may be determined by a data owner in advance; this owner is responsible for generating the user data to be shared, encrypting it, and uploading it to the cloud. The owner may not necessarily be required in every read transaction. Normally, a scheme based on CP-ABE relies upon the data owner granting access permission through an access tree, which requires his or her constant availability. In some transactions , key material is distributed among multiple parties; for instance, a data owner and a trusted authorizer may function in concert to grant access permission to other users [5];This method/ solution, however, is not adapted for a mobile environment due to its computational demands, the required constant availability of the data owner, and time- based expiration of access leading to frequent key retrieval.

Another related approach combines Hierarchical Identity- Based Encryption (HIBE) and CP-ABE [23], using hierarchical domain masters to distribute user keys; this is done at the cost of increased storage requirements for key material held by users and a greater amount of processing when generating cip-her-text.

A method relied on a writer uploading encrypted

data to the cloud, then distributing credentials to the cloud to perform re-encryption, and also to the reader on each data access attempt of trusted data sharing has been proposed. It uses a progressive elliptic curve encryption scheme [8]. But this solution does not really works in environment having device and network limitations. To handle annulations in a highly scalable system, alternative approach is suggested but with the limitation of requirement of granting access solely based on user identity. It uses the cloud provider for distributing portions of key material and for automatic and blind data re-encryption [9.

Various other proxy re-encryption schemes have been applied to secure distributed storage. One method is to re- encrypt the stored content during retrieval. Such a technique has been applied to an encrypted file storage system where a content owner encrypts blocks of content with unique, symmetric content keys, and these keys are then further encrypted to form a lockbox [10]; users communicate with an access control server to decrypt them. Disadvantage: requires dynamic re-encryption of the same data whenever multiple users access it and the content owner is under greater burden to manages access control for all other users, In the model herein, one-time re- encryption only occurs whenever membership changes, presumably a less frequent occurrence than that of data access. Other approaches require a trusted proxy for each decryption [11], which increases the communication cost.

III.EXISTING SYSTEM

Clients that engage a cloud provider typically only pay for the amount of storage, related computation, and amount of network communication actually consumed; they do not incur the capital and maintenance costs of an in-house solution.

Data outsourcing to a cloud is appropriate for any class of applications that requires data to be kept in storage and disseminated to many users.

The cloud provider also offers the additional features of automatic backup and replication to ensure the safety, longevity, and high accessibility of the user data. A risk that is not efficiently addressed in this practice, is that data, by default,

is stored in the clear and can be accessed and read by a cloud administrator without knowledge of the client.

Therefore, it is advised to apply software techniques, such as encryption key management, to ensure that the confidentiality

of cloud data is preserved at all times, It is especially crucial to safeguard sensitive user data such as e-mails, personal customer

It is very much useful specially when a cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. An additional risk is that sensitive data carry the persistent risk of being intercepted by an unauthorized party despite safeguards promised by the provider.

IV. PROPOSED METHODOLOG

Data outsourcing to a cloud is appropriate for any class of applications that requires data to be kept in storage and disseminated to many users. Clients that engage a cloud provider typically only pay for the amount of storage, related computation, and amount of network communication actually consumed; they do not incur the capital and maintenance costs

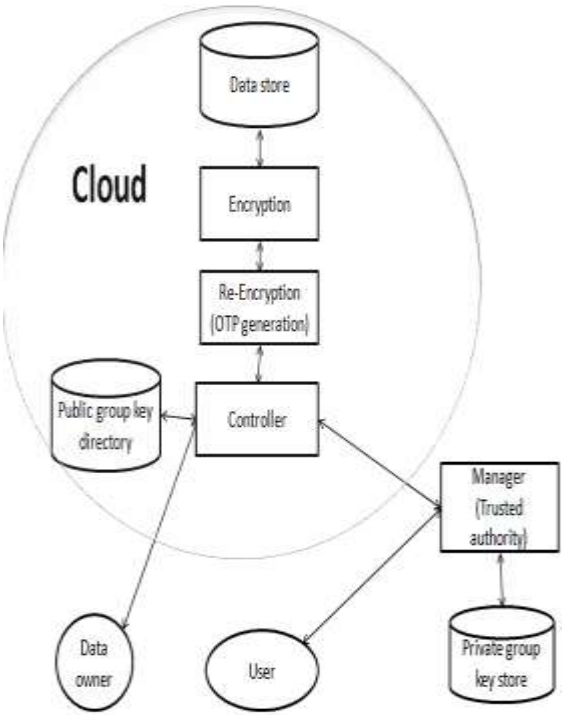
of an in-house solution.

In addition, the cloud provider offers the advantages of automatic backup and replication to ensure the safety, longevity, and high accessibility of the user data. A major concern that is typically not sufficiently addressed in practice, however, is that data, by default, are stored in the clear; it may be accessed and read by a cloud administrator without knowledge of the client.

A cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. An additional risk is that sensitive data carry the persistent risk of being intercepted by an unauthorized party despite safeguards promised by the provider. Therefore, it is useful to apply software techniques, such as encryption key management, to ensure that the confidentiality

of cloud data is preserved at all times, It is especially crucial to safeguard sensitive user data such as e-mails, personal data.

V.SYSTEM ARCHITECTURE



VI. IMPLEMENTATION

Initially for the implementation of proposed methodology we are going to use algorithms like ABE, RSA and Cipher text policy etc. The entire process of the data as input and as output will be as follows:

1) Input function:

a) Initially we will need to create a login credentials to enter into the cloud domain to access the data stored in it. This login details will be available and created with the permission of cloud service provider.
b) The user who wants to access any particular data in the cloud will have to login using login details with the cloud service provider.
c) Once a user is registered that is he/she successfully logins, then it can request the cloud manager or service provider for the data he needs to access.

2) Request to send the data

Now the user will send a request to the cloud service provider for the necessary data. Then the CSP will process the same request to the data owner who has stored the particular data in the cloud. Once a confirmation is received from the data owner to access his/her data the CSP acknowledges the requesting user.

3) Data accessibility procedure

1) The data stored in the cloud is in the encrypted form. When the CSP requests data from the data store then with the help of controller and Manager the "ONE TIME PASSWORD" i.e. key is generated which is available with CSP and is given to the user who as requested for the data. Using this key the user de-crypts the data i.e. converts it into user understandable language which is initially in the cipher text format.

2) After the user finishes the use of the accessed data and gets out of that session then the validity of the key expires. This key cannot be used again by any user to access any data.

3) After session is expired the data again gets en-cryption and gets back into the cloud.

4) Advantage

1) As the key is one time password chances of it getting leaked and data getting hacked reduces to a considerable extent.
2) This can also be applied in BYOD in the industry sectors.

VII.CONCLUSION

In this paper we have proposed secure key management using session based encryption and re-encryption scheme. A protocol for outsourcing data storage to a cloud provider in secure fashion has been provided. However, some additional security mechanisms such as re-encryption will be added to provide formal security and also to reduce increasing data theft. Our improved approach performs double encryption to generate an OTP(One Time Password).

VIII.REFRENCES

[1] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds," Technical Report 13, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2013.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 26, no. 1, pp. 96-99, Jan. 1983.

[3] N. Balasubramanian, A. Balasubramanian, and A. Venkataramani, "Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications," Proc. Ninth ACM SIGCOMM Conf. Internet Measurement Conf. (IMC '09), pp. 280-293, 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[5] A. Tassanaviboon and G. Gong, "OAuth and ABE Based Authorization in Semi-Trusted Cloud Computing: Aauth," Proc. Second Int'l Workshop Data Intensive Computing in the Clouds