IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Maintaining Data Confidentiality Using Attribute Based Secret Sharing

Rohit Dokhe[1], Pooja Bathe[2], Apurv Kolte[3]

UG Student, Department of Computer Engineering, SSBT's College Of Engineering and Technology, North Maharashtra University, Jalgaon, Maharashtra, India[1,2,3]

Abstract: Despite that existing data sharing systems in untrusted storage propose to encrypt data before sharing, the multiparty access control of encrypted data has become a challenging issue. In this, a secure data sharing based on cipher text-policy attribute-based proxy re-encryption and secret sharing. In order to protect user's sensitive data, this allows users to customize access policies of their data and then outsource encrypted data to the service provider. In this a multiparty access control model, which enables the disseminator to update the access policy of cipher text if their attributes satisfy the existing access policy. Further, a partial decryption construction in which the computation overhead of user is largely reduced by delegating most of the decryption operations to the service provider. It's also provide check ability on the results returned from the service provider to guarantee the correctness of partial decrypted cipher text. Moreover, in this presents an efficient attribute revocation method that achieves both forward and backward secrecy. The security and performance analysis results indicate that is secure and efficient in untrusted storage.

Keywords: Encrypt, Cipher text, Policy, Re-encryption, Secret sharing.

I. INTRODUCTION

In this system maintaining data confidentiality using attribute based encryption. Service provider provide services that enable users to interact with their friends and other users, and Also, to upload their data (e.g. news stories, blog posts, photos) in their personal spaces. Despite the network should be secure but it's not possible due to hackers. Network security is one of the important issue addressed and solved by using many algorithm but still there is a chance of hacking of message by unauthorized users because of only single encryption at sender side. So, to minimize drawback of current security system attribute based secret sharing algorithm going to implement. There is attribute authority it can take attribute of user and generate two keys one is public key and another is attribute secret key. Owner take that public key, define the access policy and outsource the encrypted data to store in service provider .Service provider manages the user and stored encrypted data and policies from owner .It is also update the policy and re-encryption the cipher-text with the re-encryption key. If the disseminator customize the new access policy. Moreover, the service provider partially decrypts the cipher-text for the accessor if accessory attribute satisfy the access policy in the cipher-text. Disseminator enjoy the owner's data and set policy then accessory take the attribute secret key and decrypt the data.

Main Objective Of this Project is to develop keeping in the view the current requirement of sending data securely at any authorized user keeping in view these objectives:-

- To develop an application that deals with the day to day requirement of any user.
- To enable the end-user come out with as easy to handle application of the secure data sharing.

The Attribute Based Encryption Algorithm has been proposed in this paper with its algorithm, result, technical discussion and conclusion.

II. LITERATURE SURVEY

Web-based applications are web sites with user interactivity. The key advantage of the web-based application is its availability, as it can be accessed by anyone connected to the Internet and multiple users can access it at the same time. The web-application can be designed as a three-tier architecture, which includes a web client, network servers, and a back-end information system supported by a suite of databases [3].

The goal of this project is to develop a user-friendly web-based application that automates the routine activities for an IT consulting firm. Maintaining data confidentiality avoid to the data access to unauthorized user. Save our time. Owner upload encrypted data on service provider, service provider re-encrypt that data.

The accessor after Logging can search the uploaded les to select and send request for attribute secrete key and decrypt the data. The advantage is that the file is encrypted. If the accessor wishes to download the file he can do so by clicking at the download button should enter the ASK key given by attribute authority, in order to segregate the unauthorized users. In which the file is downloaded and to be stored thus can be decrypted by the accessor and can be viewed by him.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

ABE was proposed by Sahai and Waters [5]. In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In Key-policy ABE or KPABE (Goyal et al. [6]), the sender has an access policy to encrypt data.

A. Motivation

- Improve the security for data sharing.
- Get access only authorized users.
- To decrease the Problem of data access from unauthorized user.

III. PROPOSED SYSTEM

The proposed system is a solution for unauthorized users access the data on untrusted storage. Proposed system provide the re-encryption on untrusted storage and generate attribute base key to decrypt the data when full feel the policy.

A. Problem Definition

Now a days data security and access control are very important issues .we have tried to solve problem of data confidentiality and access control.

Despite the network should be secure but it's not possible due to hackers. Network security is one of the important issue addressed and solved by using many algorithm but still there is a chance of hacking of message by unauthorized users because of only single encryption at sender side. So, to minimize drawback of current security system attribute based secret sharing algorithm going to implement.

There is a attribute authority it can take attribute of user and generate two keys one is public key and another is attribute secret key. Owner take that public key dene the access policy and outsource the encrypted data to store in service provider .Service provider manages the user and stored encrypted data and policies from owner .It is also update the policy and re-encryption the cipher-text with the re-encryption key .If the disseminator customize the new access policy. Moreover, the service provider partially decrypt the cipher-text for the accessor if accessor attribute satisfy the access policy in the cipher-text. Disseminator enjoy the owner's data and set policy then accessor take the attribute secret key and decrypt the data.

B. Architecture

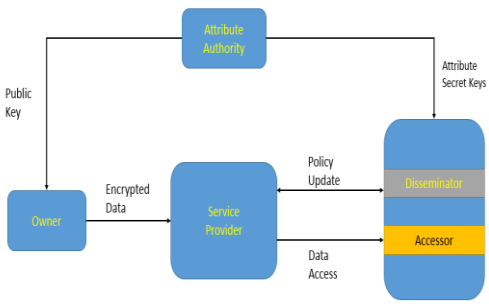

Figure: 1 Proposed System Architecture

IV. IMPLEMENTATION

Implementation of the proposed system involves the environment in which the system is implemented and the overall system development. The overall development of the proposed system requires suitable environment and proper resources for its successful completion. The proposed system is developed for a owner-accessor communication. At the owner, the data is re-encrypted and distributer set the police. At the accessor, decrypted when police full feel.

The ABE algorithm will encrypt and decrypt the text to provide security. The existing algorithm is having complex design and can be easily hacked. To overcome this issue the ABE algorithm is proposed. By implementing this algorithm, users achieve better performance, accuracy over the channel.

A. Flow of system development

The attribute authority generate the two public key PKand secret key ASK. Public provide to the data owner. The owner takes as input the public key PK, and a message M,an access policy T, outputs the ciphertext CT. Re-encryption key generation algorithm takes as input the PK, an original access policy T, and the attribute secret key ASK. The algorithm outputs a re-encryption key, as in [1].
In Re-encryption takes as input a ciphertext CT associated with the T and a re-encryption key, and outputs a new ciphertext. Thus only the user whose attributes satisfy the T can decrypt the cipher text. The accessor takes as input a ciphertext CT and the attribute secret key of user ASK, and outputs the message M if the attribute secret key ASK satisfies access policy in the ciphertext [1].

Table I Notations

PK	Public Key
ASK	Attribute Secret Key
M	Message
T	Policy

V. RESULT

At the data owner end, the owner is the user who defines the access policy and outsources the encrypted data to the service provider.

Table II Result for Data for Owner

NAME	DATA
PK(8683)	MAINTAINING DATA CONFIDENTIALITY USING ATTRIBUTE BASED SECRET SHARING, SSBT's COET
Encrypted Data	¼Ï-ó¯ÍÝ?æ¤Û3]Ï?ÒÆ-Ì8?=ZCËG¯¬?cjT 9ák?õi} Ì{ÍBB'?Ò□±Ï¶?cQËQ|è¦,»û?0¶"F]ñk□□Þüi©c□□?ãX□Q¾b/¬¡?ã
Secret key(ap211112)	¼Ï-ó¯ÍÝ?æ¤Û3]Ï?ÒÆ-Ì8?=ZCËG¯¬?cjT 9ák?õi} Ì{ÍBB'?Ò□±Ï¶?cQËQ|è¦,»û?0¶"F]ñk□□Þüi©c□□?ãX□Q¾b/¬¡?ã
Re-encrypted Data	[B@43840f

DOI 10.17148/IJARCCE.2016.5514

At the disseminator end, the disseminator is the user who enjoys the owner's data and wants to share the data with his friends in the by customizing the new access policy.

Table III Result for Disseminator

User Name	Nilesh
File Name	pp.text
Access Policy	View/Download/Denied

At the accessor end, the accessor is the user who has sufficient attributes satisfying the access policy of encrypted data and can recover the plaintext in the OSNs.

Table IV Result for Accessor

Nilesh	pooja	ppt.tex	View/Download/ Denied

The proposed system provides better reliability, integrity and security as compared to the existing system.

VI. CONCLUSION

Concluded that, Maintaining Data Confidentiality Using Attribute Based Secret Sharing (MDCABSS) is plays very important role in our Data security system. Compared aspects are data security, multiparty access control, partial decryption, and attribute revocation. In this MDCABSS design the more security while data sharing systems in untrusted storage propose to encrypt data before sharing. The main data leakage drawback is removed by using MDCABSS and system will be more secure in our online Data sharing. It is helps to avoid the data leakage on untrusted storage and save time. The system can be further extended for the secure transmission of image, audio and video data through various image processing techniques.

- Decentralized Access Control
- Extensibility
- Reusability
- Understandability

REFERENCES

[1]. HUANG Qinlong, MA Zhaofeng, YANG Yixian, NIU Xinxin, FU Jingyi. “Improving Security and Efficiency for Encrypted Data Sharing in Online Social Networks”. “Information Security Centre, Beijing University of Posts and Telecommunications”, Beijing 100876, China, March 2014

[2]. J. M. RAJI F, MIRI A, “”cryptographic privacy protection framework for online social networks[j]”,” Computers and Electrical Engineering, vol. 3, no. 7, July 2013

[3]. S. J. Bethencourt and B. Waters, “ciphertext-policy attribute-based encryption”,” In Proc. of SPT07, Washington, DC, USA, vol. 4, no. 6, sept 2007

[4]. S. J. Bethencourt and B. Waters, “ciphertext-policy attribute-based encryption”,” In Proc. of SPT07, Washington, DC, USA, vol. 4, no. 6, sept 2007

[5]. A. Sahai and B. Waters, “Fuzzy identity-based encryption” in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473, 2005

[6]. Yang, Chou-Chen, Ting-Yi Chang, and Min-Shiang Hwang. "A (t, n) multi-secret sharing scheme." Applied Mathematics and Computation 151.2(2004):483-490.

DOI 10.17148/IJARCCE.2016.5514