International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 05 | August-2015 www.irjet.net p-ISSN: 2395-0072

Secure System for data sharing using Cipher-Text Policy Attribute Based encryption with Message Authentication Codes for Data Integrity

Ashwini Ahire, Prof. P. Jawalkar.

[1 2] *Department of Computer Engineering , JSPMS B.S.I.O.T.R. (W), Pune, India.*

Abstract: - Attribute based encryption (ABE) techniques to encrypt each message. Different from previous works in secure data outsourcing, it focuses on the multiple data owner scenario, and divides the users in the KGC system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of user privacy is guaranteed simultaneously by exploiting multi-authority ABE public keys. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. In the existing approaches they fully deal with the data security. Key escrow problem is resolved by a key issuing protocol. Second problem is that user revocation problem. The user revocation problem is solved by; if a user is revoked from some other attribute groups he/she can able to decrypt the information as long as his access policy is satisfied by the cipher text. Finally the solutions to the problems are only focused on data security during data sharing. But the highlighted problem is data integrity. In the existing approaches it doesn't deal any solutions or approaches to provide data integrity. Here proposed a new secure system which supports both data security and data integrity. For data security here use Cipher Text Policy-Attribute Based Encryption for secure data sharing. The data integrity problem is solved by the MAC mechanism. Message Authentication Code (MAC) Message Authentication Codes (MAC) is a method in which the integrity of data is checked using secret key that is shared between a sender and a recipient. Finally our proposed approach gives solution for the data security and data integrity.

Keywords: - *Message Authentication Code, Cipher Text Policy-Attribute Based Encryption, Attribute based encryption.*

I. INTRODUCTION

In most secure communication, the following two security functions are commonly considered: Message confidentiality: Message confidentiality ensures the sender that the message can be read only by an intended receiver. Message authentication: Message authentication ensures the receiver that the message was sent by a specified sender and the message was not altered en route. To provide these two functions, one-time session keys need to be shared among communication entities to encrypt and authenticate messages. Thus, before exchanging communication messages, a key establishment protocol needs to distribute one-time secret session keys to all participating entities. The key establishment protocol also needs to provide confidentiality and authentication for session keys.

There are two types of key establishment protocols: key transfer protocols and key agreement protocols. Key transfer protocols rely on a mutually trusted key generation center (KGC) to select session keys and then transport session keys to all communication entities secretly. Most often, KGC encrypts session keys under another secret key shared with each entity during registration. In key agreement protocols, all communication entities are involved to determine session keys. The most commonly used key agreement protocol is Diffie-Hellman (DH) key agreement protocol. In DH protocol, the session key is determined by exchanging public keys of two communication entities. Since the public key itself does not provide any authentication, a digital signature can be attached to the public key to provide authentication.

Distributed group key management protocols: there is no explicit group key distribution center, and each group member can contribute to the key generation and distribution. The class of centralized group key management protocols is the most widely used group key management protocols. Proposed a group key management protocol that requires, where n is the size of group, encryptions to update a group key when a user is evicted or added if backward and forward secrecy are required. A set of scalable hierarchical structure-based group key protocols have been proposed. Proposed a protocol based on Exclusion Basis Systems (EBS), a combinatorial formulation of the group key management

problem, which allows protocol user to trade-off between the number of keys needed to be stored and the number of messages needed to be transmitted for each key update with no counter collusion solution provided.

II. RELATED WORK

Rolf Blom, consider that user pairs in a network share secret information to be used for mutual identification or as a key in a cipher system. If the network is large it becomes impractical or even impossible to store all keys securely at the users. A natural solution then is to supply each user with a relatively small amount of secret data from which he can derive all his keys. A scheme for this purpose will be presented and we call such a scheme a symmetric key generation system (SKGS). However, as all keys will be generated from a small amount of data, dependencies between keys will exist. Therefore by cooperation, users in the system might be able to decrease their uncertainty about keys they should not have access to[1].

A disseminated KP-ABE plot that tackles the key escrow problem in a multi power framework. In this approach, all (disjoint) attribute powers are taking an interest in the key generation convention in an appropriated manner such that they can't pool their information and connection various attribute sets having a place with the same client [5].

Chow proposed an unacknowledged private key generation convention in character based writing such that the KGC can issue a private key to a confirmed client without knowing the rundown of clients' characters. It appears that this unknown private key generation convention lives up to expectations legitimately in ABE frameworks when treat an attribute as a character in this development [6].

Attrapadung and Imai [3] recommended an alternate user-revocable ABE plans tending to this problem by joining show encryption plans with ABE plans. In any case, in this plan, the information holder ought to take full charge of keeping up all the participation records for each one attribute gathering to empower the immediate user denial.

A. Existing System

A Cipher text Policy attribute-set-based encryption (CP-ABE) scheme for access control in Data sharing. CP-ABE extends the cipher text-policy attribute- set-based encryption with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. In this process, the cipher text is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text. Through CP-ABE, have achieved fine grained access control and secured data in a multiuser environment categorized in a Data sharing Environment. Key generation center responsible for generation of group keys for data sharing clients with the policy of attribute based encryption. A high degree of user privacy is guaranteed simultaneously by exploiting multi-authority ABE public keys. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

In the existing approaches it doesn't deal any solutions or approaches to provide data integrity. Here proposed a new secure system which supports both data security and data integrity. For data security here use Cipher Text Policy-Attribute Based Encryption for secure data sharing. Attribute based encryption (ABE) techniques are used to encrypt each message. Different from previous works in secure data outsourcing, it focuses on the multiple data owner scenario, and divides the users in the KGC system into multiple security domains that greatly reduces the key management complexity for owners and users. Following section (section III)shows the actual system workflow of proposed system.

III. SYSTEM WORKFLOW

Different from previous works in secure data outsourcing, it focuses on the multiple data owner scenario, and divides the users in the KGC system into multiple security domains that greatly reduces the key management complexity for owners and users. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. In the existing approaches they fully deal with the data security. Key escrow problem is resolved by a key issuing protocol. Second problem is that user revocation problem. The user revocation problem is solved by; if a user is revoked from some other attribute groups he/she can able to decrypt the information as long as his access policy is satisfied by the cipher text. Finally the solutions to the problems are only focused on data security during data sharing. But the highlighted problem is data integrity. The data integrity problem is solved by the MAC mechanism.

Message Authentication Codes (MAC) is a method in which the integrity of data is checked using secret key that is shared between a sender and a recipient. Finally proposed approach gives solution for the data security and data integrity. The message authentication codes are used between senders and recipients that share a secret key to validate the information being transmitted. For MAC mechanism here are going to implement HMAC algorithm. Keyed Hash Message Authentication Codes (HMAC) is a method that uses the same concept as MAC by means of a secret shared key, but also uses other cryptographic hash functions.

First module name as Data Owner Credentials Module create each Data owner needs to register at KGC to subscribe the group key transfer service and to establish a secret with KGC. KGC can send the group key and interact with all group members in a broadcast channel. In this module data owner should register in the Key Generation Center (KGC).After registration only the KGC activate the group key transfer service to the corresponding data owner. After that a secure path is established between the data owner and key generation center to transfer the secret key. Authentication for data owner also takes place based on the data owner credentials or attributes.

Second module is Manipulation of KGC Module KGC is responsible for the generation of group keys which is used for the communication between the data owners and the users. Key Generation Center mainly duty is to authenticate both the data owner and end user to store and retrieve the data from the storage node. It generates the key for both data owner and end user. It provides differential access to the individual users based on the attributes.

The third module of system is Group Key Generation module after receiving a group key generation request from any user, KGC needs to randomly selects a group key and contact all shared secrets with group members. KGC needs to distribute this group key to all group members in a secure and authenticated manner. All communication between KGC and group members is in a broadcast channel. In this module the key generation process takes place.

Fourth module named as Attribute based data key generation attribute based encryption is proceeded by bilinear mapping of attribute information of data owner and the data to be stored in the data storing center. Bilinear mapping process achieved by multiplicative factors of both Logical AND, XOR operations. It is the process of pairing up the attribute information and thus cipher text policy ABE is processed. Master key is generated by doing the Logical AND operations of given attributes of data owner. Using the master key, public key is generated and secret key is generated by doing the logical XOR operations. Ciphering algorithms are applied using the secret key, thus secured secret key is generated by Attribute based encryption.

Fifth module is Data Integrity checking. In this module the Data owner's files have been applied security. These files are stored in the Data storage servers. Before the data owner store his files in the storage node the MAC codes is generated for that data. This MAC code is for sender information. In Data storage servers client files are stored as secured files so the crypto process has applied. For crypto process use AES algorithm for the encryption and decryption process. Data retrieval process not only consists of retrieval of encrypted files from the Data storage server and decrypted using respected private keys. Before retrieving the information from the storage node after authentication should generated the MAC code for that data. Then verification process takes place whether there is a change in the MAC code, it shows that there is a change in the information during data sharing.

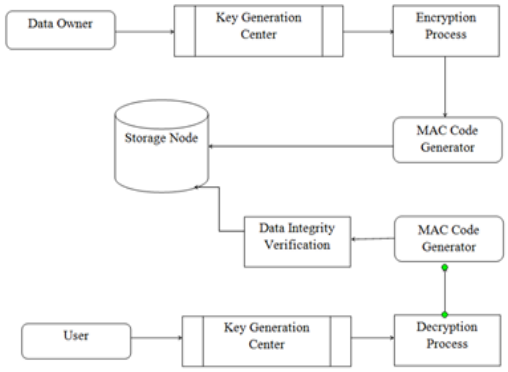

Fig 1. System architecture.

IV. MATHEMATICAL MODEL

Input : Consider `n` number of user who are data owner, user

C=ABE_Encrypt (MSG, χ)

CodeSend=HMAC (MSG)

Process: Process (Sharing, cipher text gen, MAC gen)

- Sharing and accessing the data with secure manner.

- Given plaintext are converted into cipher text which is encrypted form of data
- Generate the MAC code for message.

Output : privacy provided to data and securing the process and verify the data integrity.

C=ABE._Decrypt (MSG, χ)

CodeRec=HMAC (MSG)

Result=Authenticate (CodeSend, CodeRec)

WHERE,

C=Cipher text,

ABE=Attribute Based Encryption

MSG=message (data)

X=access structure

HMAC=Mechanism

CodeSend=Sender data's Hash based Message Authentication Codes

CodeRec=Receiver data's Hash based Message Authentication Codes

Steps

1. Derive the set of round keys from the cipher key.

2. Initialize the state array with the block data (plaintext).

3. Add the initial round key to the starting state array.

4. Perform nine rounds of state manipulation.

5. Perform the tenth and final round of state manipulation.

6. Copy the final state array out as the encrypted data (cipher text).

7. Generate the MAC code for data which is send by data owner to the storage node.

8. Generate the MAC code for data which is received by the user

9. Validation of MAC code of sender side and receiver side.

V. IMPLIMENTATION

1. Initially create new user1 login by using personal information like user name, IP address, ID etc. and store the user information. Same like as user1 create another user i.e. user2. After completing registration login by using username and ID then connected to KGC. As shown in figure 2.

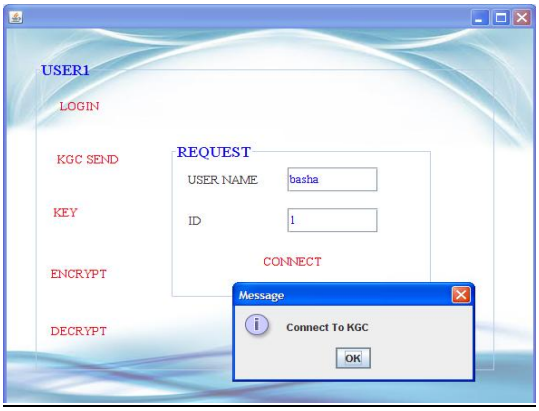

Figure2. User Registration.

2. Click on user record and select user in combo box and click on random button and then click encrypt and initiator command. As shown in figure 3, 4.

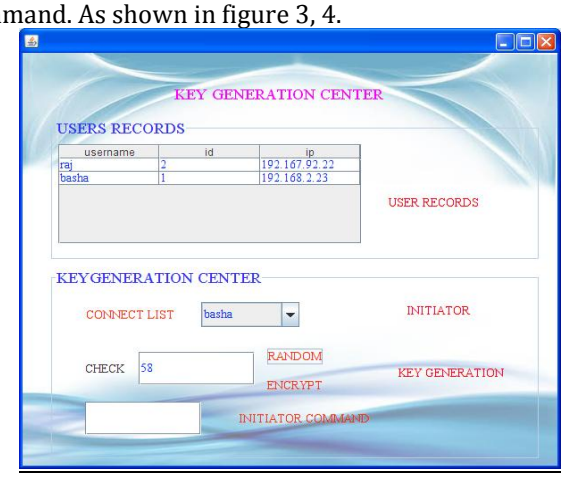

Figure3. Key Generation Center

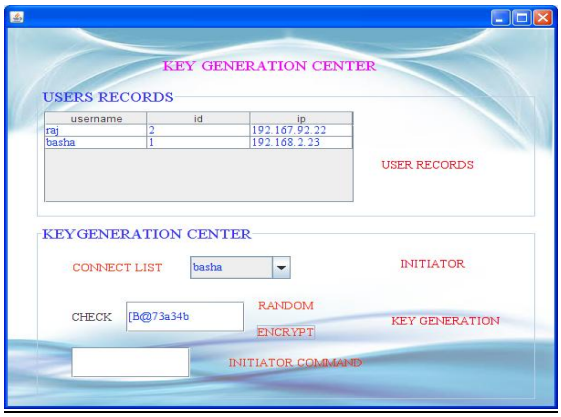

Figure 4. Encryption

3. After that click on KGC send then click decrypt and in the textbox give some request and click request button. In user1 form click on KGC send. As shown in figure 5, 6.

Figure 5: Key Generation Center after decrypt

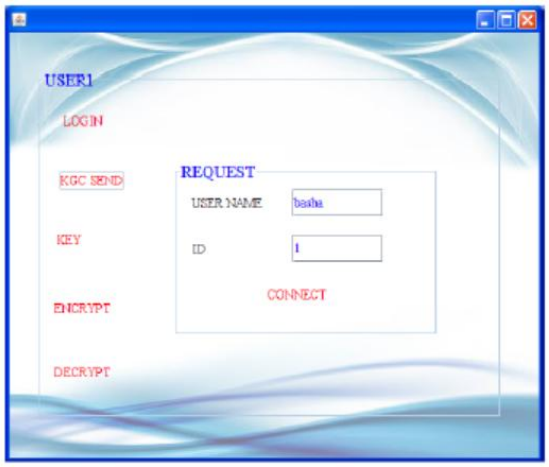

Figure 6: User1 form after sending KGC

4. In initiator form, click on User1 sent then click on User1 in the initiator report panel after that click Initiator command button and then key Generation button. As shown in figure 7, 8.

Figure 7: Initiator form.

Figure 8: User Records.

5. Click Random Button and then click Distribute key button. Select Respective user1 or 2(logged n) click Distribute button and at last click Send button. Click Key button in user1 then click on Encrypt. As shown in figure 9. Then request send to user1 then received group key and then click on decrypt .As shown in figure 10.

Figure 9 : Encrypt group key.

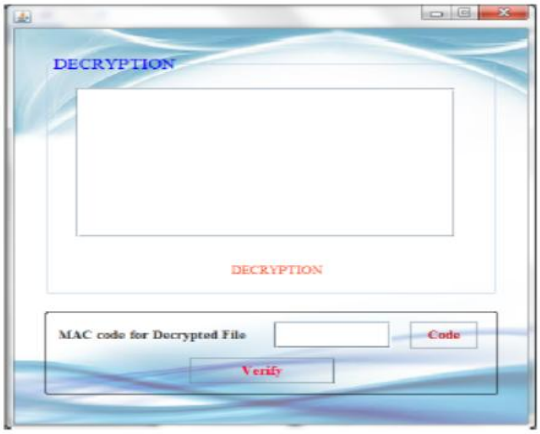

Figure 10: Decrypt MAC code.

VI. RESULT

As shown in Table 1, the proposed scheme requires ciphertext size of (2t + 1) $C_0 + C_1 + C_T$, which is the same as that of BSW. The proposed scheme requires rekeying message (Hdr) size of (m +2) $C_0$to realize the user revocation for each attribute in the system. In the proposed scheme, each user stores one more private KEK for decrypting the rekeying messages and obtaining attribute group keys than the basic BSW scheme.

Table 1. Efficiency Comparison

System	Cipher Text Size	Private key size	Public key size
BSW	(2t + 1) $C_0 + C_1 + C_T$	(2k+1) C_0	$C_0 + C_1$
Proposed	(2t + 1) $C_0 + C_1 + C_T$	(2k+2) C_0	$C_0 + C_1$

Fig. 11 represents the number of users in a single attribute group during 100 hours. The solid line and dotted line represent the number of current valid users and accumulated revoked users in an attribute group, respectively.

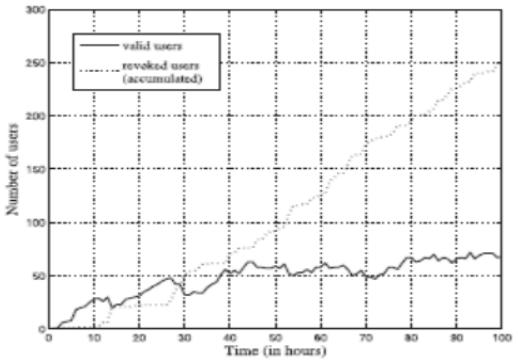

Fig. 11. The number of users in an attribute group.

Fig. 12 shows the total communication costs in log scale that the data owner or the data-storing center needs to send on a membership change in the network system. It includes the ciphertext and rekeying messages for nonrevoked users. It is measured in bits.

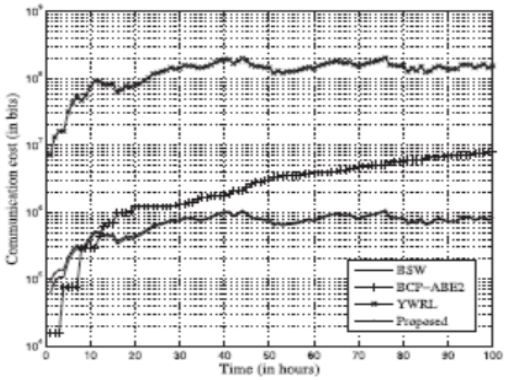

Fig. 12. Communication cost in the system.

VII. CONCLUSIONS

To exploit a novel PKC Attribute-Based Encryption (ABE) to provide cryptographically enforced data access control. With ABE, are able to enjoy fine-grained access control. However, there are still several open security issues in state-of-the-art constructions of ABE. Toward providing a full-fledged cryptographic basis for secure data sharing on untrusted storage, proposed three security enhancing solutions for ABE: The first enhancement made is to provide efficient user revocation in ABE. Proposed an efficient group key transfer protocol based on secret sharing. Every user needs to register at a trusted KGC initially and pre share a secret with KGC. KGC broadcasts

group key information to all group members at once. The confidentiality of our group key distribution is information theoretically secure. Here provide group key authentication. Security analysis for possible attacks is included. In proposed protocol, only focus on protecting group key information broadcasted from KGC to all group members. Here, briefly explain how to provide user authentication and authenticate messages transmitted from group members to KGC. In model, assume that the KGC is a mutually trusted entity and each registered user, needs to share a secret, with KGC during registration. User authentication can be achieved based on the knowledge of the shared secret between each user and KGC. In addition to the data security also provide the data integrity. In system achieve both data security and data integrity using ABE based method and MAC technology. To achieve data integrity use HMAC mechanism of MAC technology and achieve a good result of data integrity.

ACKNOWLEDGMENT

I would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. I am thankful to the authorities of Savitribai Phule conference, organized by, for their constant guidance's and support. I am also thankful to the reviewer for valuable suggestion. I am also thank the collage authorities for providing the required infrastructure and support. Finally, I would like to extend a heartfelt gratitude to friends and family member.

REFERENCES

[1] Rolf Blom, An optimal class of symmetric key generation systems, in Proc. 13th ACM SIGKDD Int. Conf. KDD, San Jose, CA, USA 2012, pp. 95104.

[2] T.Purusothaman, Dr. S. Annadurai, An Efficient and Secured Conference Key Agreement Protocol, in Proc. NIPS, 2011.

[3] Xukai Zou, A novel Conference Key Management solution for Secure Dynamic Conferencing, in Proc. 18th ACM SIGKDD Int. Conf. KDD, New York, NY, USA, 2008.

[4] Junbeom Hur, Improving Security and Efficiency in Attribute-Based Data Sharing,IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013

[5] A. Boldyreva, V. Goyal, and V. Kumar, Identity-Based Encryption with Efficient Revocation, Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[6] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, A Content- Driven Access Control System, Proc. Symp. Identity and Trust on the Internet, pp. 26-35, 2008.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, Attribute Based Data Sharing with Attribute Revocation, Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS 10), 2010.

[8] S.D.C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, Over- Encryption: Management of Access Control Evolution on Outsourced Data, Proc. Intl Conf. Very Large Data Bases (VLDB 07), 2007.

[9] A. Kate, G. Zaverucha, and I. Goldberg, Pairing-Based Onion Routing, Proc. Privacy Enhancing Technologies Symp., pp. 95-112, 2007.

[10] L. Cheung and C. Newport, Provably Secure Ciphertext Policy ABE, Proc. ACM Conf. Computer and Comm. Security, pp. 456-465, 2007.

[11] X. Liang, Z. Cao, H. Lin, and D. Xing, Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption, Proc. Intl Symp. Information, Computer, and Comm. Security(ASIACCS), pp. 343-352, 2009.