ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Enhanced Multimedia Data Sharing for Privacy Preservation in Vehicular Ad Hoc Network using Authentication Group Key

[1]Ms. C. Navamani, MCA, MPhil., ME., Assisant Professor/MCA,
[2]Mr. P. Boopathi, Final MCA,
Department Of MCA, Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: navamanimca@gmail.com, boopathisanthamani@gmail.com

***Abstract*- Data sharing and low maintenance, provides a better computing, with the characteristics of intrinsic utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. In this project provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. The existing scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked.**

Index Terms- Attribute Key Generation, ECP And ABE Algorithms, Group Key Generation, Encryption, Decryption.

I. INTRODUCTION

Networks means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user it's just somewhere up in the nebulous "cloud" that the Internet represents.

Network is a buzzword that means different things to different people. For some, it's just another way of describing IT (information technology) "outsourcing"; others use it to mean any computing service provided over the Internet or a similar network; and some define it as any bought-in computer service you use that sits outside your firewall. However we define cloud computing, there's no doubt it makes most sense when we stop talking about abstract definitions and look at some simple, real examples-so let's do just that.

The goal of Networks is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games.

In Networks uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing tasks across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

A. *Attribute Access Control*

The proposed system needs to be implements all the existing system concepts in which the Ciphertext-Policy Attribute-Based Encryption with User Revocation. The proposed scheme also adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system.

Need a proposed system to allow a data owner to define the access control policy and enforce it on their outsourced data. It also enables more fine-grained access control with efficient attribute and user revocation capability. The different users are allowed to decrypt different pieces of data per the security policy.

Data outsourcing is becoming today a successful solution that allows users and organizations to exploit external servers for the distribution of resources. Some of the most challenging issues in such a scenario are the enforcement of authorization policies and the support of policy updates. Since a common approach for protecting the outsourced data consists in encrypting the data themselves, a promising approach for solving these issues is based on the combination of access control with cryptography. This idea is in itself not new, but the problem of applying it in an outsourced architecture introduces several challenges.

In this project, illustrating the basic principles on which architecture for combining access control and cryptography can be built. They then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Ciphertext-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data.

However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. The study proposes an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group.

II. RELATED WORK

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can b e selectively shared only at a coarse-grained level (i.e., giving another party your private key). Develop a new cryptosystem for fine-grained sharing of encrypted data that they call Key-Policy Attribute-Based Encryption (KP-ABE). In the cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Demonstrate the applicability of construction to sharing of audit-log information and broadcast encryption. Construction supports delegation of private keys which msubsumes Hierarchical Identity-Based Encryption (HIBE).

Dan Boneh, Matthew Franklin Identity-Based Encryption from the Weil Pairing proposed a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie Hellman problem. The system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. They give precise definitions for secure identity based encryption schemes and give several applications for such systems.

Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours.

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. They predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of the experimental file system demonstrate that proxy re-encryption can work effectively in practice.

III. SYSTEM METHODOLOGY

A. Trusted Key Pair

The trusted key pair created in the application for further process, following the key generation of the public key and the master key which are used for the purpose of encryption of the message. All such keys are created as group key. These details are generated by create command button event and showed in the multiline text mode. This key is saved in the application using save command button event.

B. Attribute Creation

This modules is used to create the attribute details in the application, It contains details such as attribute id, attribute names that are entered by user in the textbox controls, and saved by the save command button. The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

C. USER CREATION FORM

The user creation modules are to create the user details for accessing the attribute with privilege level. The user id, user name and passwords are entered by user in the textbox controls these details are saved by the save command button event. The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

D. ATTRIBUTE KEY GENERATION

Attribute key generation module is used to process the key generation process in the application. The access structure form is used to create the access specification for each and every user for specifying the details with the rights to select, insert, update and delete operation in those processes which are selected by the check box control. Attribute identity number and user identity numbers are selected by user from the ComboBox control. Given attribute name and user names are displayed in the textbox control. All these information are saved in the database using save command button event.

E. Attribute Group Key Generation

Attribute group key generation module is used to create group key in the application, attributes assigning with the group, identify each user belonging to the given group id. The attribute identity number is selected by the user in the checkbox control. Group identity number is inserted in the textbox control. All these details are saved in the specified table.

F. Group Key Generation For Users

This module is used to assign the user to group, for accessing the given process. The user identity number is selected by user in the check box control and group identity number is selected by the combo box control and all these details are saved in the specified table.

G. Key Encrypting Key Generation For Users

This module is used to encrypt the key value for corresponding username and user id. The id details are selected by user in the checkbox control and user key is generated using creating command button event. The corresponding username, user id and the given key encrypting values are inserted into the user details table.

H. Encryption Form

This module is used to encrypt the text using public key for the purpose of other users who do not know the given message. So, the public key is extracted using get key command button and displayed in the label control, the message is entered in the textbox control then the given encrypted message is displayed in the label control. The encrypted message is saved in the application using creates cipher text and save command button event.

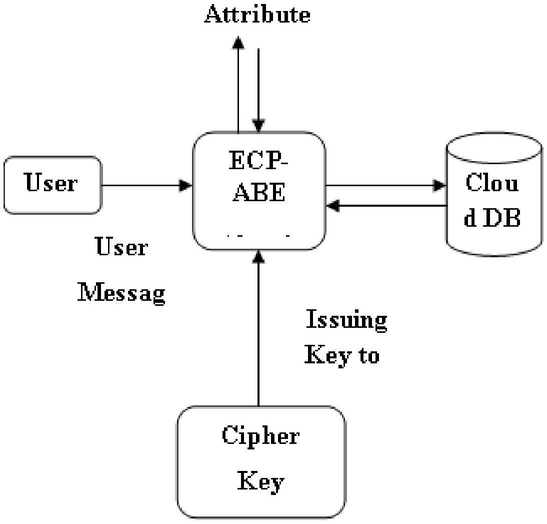

Fig. 1. Attribute Encryption Model

I. Re-Encrypt Form

This encrypted module is re-encrypting the encrypted data in the application based on the group key because the other user will not identify the same encrypted message. In this form, group identity number and cipher texts are selected from the combo box controls, and details are re-encrypted in the cipher text grid view control using re-encrypt command button event.

J. Elect Query Form

This module is used to check the user level access privileged rights in the application; query is inserted in the textbox control and processed by the check command button event.

K. Decrypt Cipher Text

Decrypt cipher text retrieves the plain data in the application. The given cipher text is entered the data is showed to the user. In this form user identity number and cipher texts are selected from the combo box control, group identity is displayed in the label controls. The message is decrypted in the cipher text grid view control using the decrypt command button event.

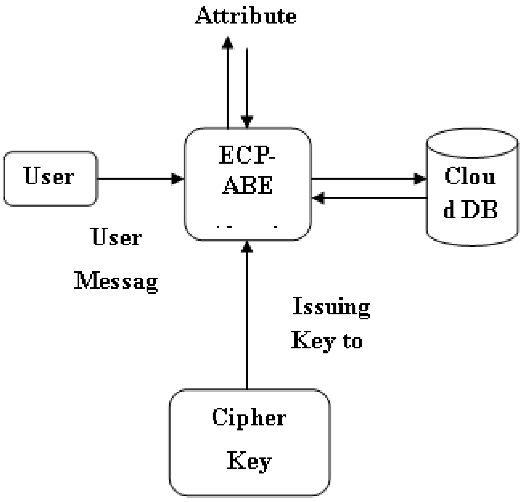

Fig. 2. Attribute Decryption Model

L. Encrypt Block Security Form

This module is used to create cipher text in this experimental system given database the user access the high privileged level or not. The field one , field two and field three data's are entered by user in the list box controls and privilege settings is selected by the check box control. The Advanced Encryption Key (AES) is entered in the textbox control and data is encrypted using the encrypt command button event.

M. Proposed Algorithm

*$KeyGen_{CE}(M)$:*K is the key generation algorithm that maps a data copy M to a convergent key K;

*$Encrypt_{CE}(K,M)$:*C is the symmetric encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a ciphertext C;

*$Decrypt_{CE}(K,C)$:*M is the decryption algorithm that takes both the ciphertext C and the convergent key K as inputs and then outputs the original data copy M

TagGenCE(M): T(M) is the tag generation algorithm that maps the original data copy M and outputs a tag T(M). We allow TagGenCE to generate a tag from the corresponding ciphertext, by using T(M)=TagGenCE(C), where C=EncryptCE(K,M).

N. Process

The project experimental system contains the following modules.

- Symmetric Encryption
- Add Users
- Convergent Encryption
- Proof of Ownership
- Prrof of Ownership Based On Session
- Revocation of Users

1. Symmetric Encryption

In this module, general symmetric encryption/decryption technique is implemented. Symmetric encryption uses a common secret key *K* to encrypt and decrypt information. A symmetric encryption scheme consists of three primitive functions:

KeyGenSE (1): K is the key generation algorithm that generates *K* using security parameter 1;
EncryptSE (K, M): C is the symmetric encryption algorithm that takes the secret *K* and message M and then outputs the ciphertext C;

DecryptSE (K, C): M is the symmetric decryption algorithm that takes the secret *K* and ciphertext C and then outputs the original message M.

2. Add Users

In this module, user id, username, mail id, password and random globally unique identifier is generated which will be used as the tag for further modules is added to 'Users' table.

3. Convergent Encryption

Convergent encryption provides data confidentiality in deduplication. A user (or data owner) derives a convergent key from each original data copy and encrypts the data copy with the convergent key. In addition, the user derives a tag for the data copy, such that the tag will be used to detect duplicates.

To detect duplicates, the user first sends the tag to the server side to check if the identical copy has been already stored. Note that both the convergent key and the tag are independently derived and the tag cannot be used to deduce the convergent key and compromise data confidentiality. Both the encrypted data copy and its corresponding tag will be stored on the server side.

In this module, four primitive functions are implemented to achieve the convergent encryption mechanism.

$KeyGen_{CE}$ (M): K is the key generation algorithm that maps a data copy M to a convergent key K;

$Encrypt_{CE}$(K, M): C is the symmetric encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a ciphertext C;

$Decrypt_{CE}$(K,C): M is the decryption algorithm that takes both the ciphertext C and the convergent key K as inputs and then outputs the original data copy M and

$TagGen_{CE}$(M): T(M) is the tag generation algorithm that maps the original data copy M and outputs a tag T(M). We allow TagGenCE to generate a tag from the corresponding ciphertext, by using $T(M)=TagGen_{CE}(C)$, where $C=Encrypt_{CE}(K,M)$.

4. Proof Of Ownership

The verifier derives a short value from a data copy M. To prove the ownership of the data copy M, the prover needs to send and run a proof algorithm with the verifier. It is passed if and only if and the proof is correct.

5. Prrof Of Ownership Based On Session

In this module, session based deduplication is considered. Here if the user provides the session duration i.e, front date and to date, then only with the data range, proof of ownership can be allowed in server on those dates. This increases the security if the outsourced data need to be safely accessed on the given duration.

6. *Revocation Of Users*

In this module, we consider the revocation of users in the given group. If the original (first) user of the group intimates the server with a user's revocation, then the server rejects the proof of ownership submitted by that user .

O. *Advantages Of Proposed System*

The following are the advantages of proposed system.

- Any service provider may revocate users if unauthorized user tries to access the data above a given count.
- Data servicing is maintained by more than one service provider, the authentication process is enhanced.
- All data service manager take charge of managing the attribute group keys per each attribute group.
- Keys are assigned based on a condition and unique among all users, so the key duplication is not occurred in the current system.
- Handling the outsource data copies in a secure manner is easy to compare proposed attribute access control model.
- To capability and capture a series of attribute queries option.
- User profile is group into same group with attribute in the tuples structure only.
- Past query based suggestion is given to user group.
- All the data is maintained by multiple service providers so the data privacy do not affected by the third party storage area.
- The single data service manager is in-charge of managing the different attribute group keys per each attribute group.

IV. CONCLUSION

The rapid development of versatile cloud services, a lot of new challenges have emerged. One of the most important problems is how to securely delete the outsourced data stored in the cloud severs. The proposed ciphertext-policy attribute-based encryption with user revocation scheme provides a big advantage by supporting user-defined time-specific authorization and fine-grained access control and data secure self-destruction.

The proposed scheme allows a data owner to define the access control policy and enforce it on his outsourced data. It also features a mechanism that enables more fine-grained access control with efficient attribute and user revocation capability. It is sent that the proposed scheme is efficient and scalable to securely manage the outsourced data.

The proposed ciphertext-policy attribute-based encryption model does includes the set of the attributes, tree access policy, and the definition of the time instant, because their costs are negligible if compared with the key generation.

Data deduplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. This project attempts to formally address the problem of achieving efficient and reliable key management in secure deduplication. It introduces a baseline approach in which each user holds an independent master key for encrypting the convergent keys and outsourcing them to the cloud.

V. FUTURE ENHANCEMENT

The proposed ciphertext-policy attribute-based encryption with user revocation supports the function of user-defined authorization period and ensures that the sensitive data cannot be read both before its desired release time and after its expiration. In future the authorization period can be incorporated with the user session of the cloud server to provide the improved security mechanism.

The data owner encrypts the data to share with users in the system, in which every user's key is associated with an access tree and each leaf node is associated with a time instant, for this in further it can be enhanced with the logic minimum spanning tree. Further for the purpose of encryption and decryption process for the user data, Triple DES algorithm can be implemented for providing the better security for the user confidential data.The following enhancements are should be in future.

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in multiple copies of same database is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real environment during the implementation.

- In future Minimum Spanning Tree logic may applied for the access control tree.

REFERENCES

[1] S.Vimercati, S.Foresti, S.Jajodia, S. Paraboschi, and P. Samarati, “A Data Outsourcing Architecture Combining Cryptography and Access Control,” Proc. ACM Workshop Computer Security Architec-ture (CSAW ’07), Nov. 2007.

[2] L.Ibraimi,M.Petkovic,S.Nikova, P. Hartel, and W. Jonker, “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. Int’l Workshop Information Security Applications (WISA ’09), pp. 309-323, 2009.

[3] R.Baden,A.Bender,N.Spring,B.Bhattacharjee, and D. Starin,“Persona: An Online Social Network with User-Defined Privacy,”Proc. ACM SIGCOMM ’09, Aug. 2009.

[4] A.Sahai and B.Waters,“Fuzzy Identity-Based Encryption,” Proc.Eurocrypt ’05, pp. 457-473, 2005.

[5] V.Goyal,O.Pandey,A.Sahai,and B.Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[6] J.Anderson. Computer security planning study.Technical Rep ort 73-51, Air Force Electronic System Division, 1972.

[7] J.Saltzer, M.Schroelder. The protection of information in computer systems. Communications of the ACM , 17(7), July 1974.

[8] N. Provos . Encrypting virtual memory. In Proc. of the 9th USENIX Security Symposium , Denver, Colorado, USA, August 2000.

[9] S.Akl , P.Taylor. Cryptographic solution to a problem of access control in a hierarchy.ACM TOCS,1(3):239 248, August 1983.Germany, September 2007.