Enhanced Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks

S. Kalpana[1] MCA., Part –time M.Phil Scholar, Department of Computer Science, Navarasam Arts & Science College for Women, Arachalur.

Mrs. C.Premavathi[2] M.Sc., M.Phil., Asst.Professor, Department of Computer Science, Navarasam Arts & Science College for Women, Arachalur.

Abstract--- **Data Outsourcing issues were monitored, where a trusted server is in charge of defining and enforcing access control policies. The main scope of the thesis is used to deliver the necessary data for the third party based on demand access. The user access the details on privilege level based on access control. The dual encryption is processed in the cloud environment which is varied from one group to another for secure data transmission process. The thesis summarizes an algorithm namely Enhanced cipher text-policy attribute to enforce access control policies with user revocation capability. This algorithm executed in the basis of setup process to create the master key and public key, key encrypting key generation process, attribute key generation process based on access control, encrypt the data using public key, re-encrypt process using group key and decryption of data. Dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. Thus, different users are allowed to decrypt different pieces of data as per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. This paper proposes a novel Sybil attack detection mechanism, footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU. A location-hidden authorized message generation scheme is designed for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification.**

Keyword: **Cloud Computing, Secure Data Sharing Scheme, Certificate Authorities, Encrypted text-policy Attribute Based Encryption, Sybil Attack Detection.**

I. INTRODUCTION

A novel Sybil attack detection scheme Footprint, using the trajectories of vehicles for identification while still preserving the anonymity and location privacy of vehicles. Specifically, in Footprint, when a vehicle encounters an RSU, upon request, the RSU issues an authorized message for this vehicle as the proof of its presence at this RSU and time. Intuitively, authorized messages can be utilized to identify vehicles since vehicles located at different areas can get different authorized messages.

However, directly using authorized messages will leak location privacy of vehicles because knowing an authorized message of a vehicle signed by a particular RSU is equivalent to knowing the fact that the vehicle has showed up near that RSU at that time. In Footprint, to design a location-hidden authorized message generation scheme for two purposes. First, RSU signatures on messages are signer-ambiguous which means an RSU is anonymous when signing a message.

In this way, the RSU location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same RSU are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the link ability of two authorized messages, authorized messages used for long term identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harm anonymity of vehicles.

II. RELATED WORKS

U. Jyothi K et al., [1] summarizes for which resources of the computing infrastructure are provided as services over the Internet. This paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. The aim to keep the data confidential against untrusted servers cryptographic methods may be applied by disclosing data decryption keys only to authorized users. However, these solutions inevitably introduce a heavy computation overhead

on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well.

Brent Waters et al., [2] describes a public- key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share a targeted user or device. While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials. In the techniques provide a framework for directly realizing provably secure CP-ABE systems. The encrypted text distributes shares of a secret encryption exponent s across different attributes according to the access control LSSS matrix M. A user's private key is associated with a set S of attributes and he will be able to decrypt an encrypted text if his attributes "satisfy" the access matrix associated with the encrypted text. During decryption, the different shares that the algorithm combines are multiplied by a factor of the ultimately these randomized shares are only useful to that one particular key. To construct a structures and high level intuition for security is similar to the BSW construction. The main novelty in the paper is provided a method for proving security of such a construction.

Dan Boneh et al., [3] describe Identity Based Encryption (IBE) system where the public key can be an arbitrary string such as an email address. A central authority uses a master key to issue private keys to identities that request them. The first construction for HIBE is due to where security is based on the Bilinear Diffie-Hellman (BDH) assumption in the random oracle model. A subsequent construction due to Boneh and Boyen gives an efficient (selective-ID secure) HIBE based on BDH without random oracles. The length of cipher-text and private keys grows linearly in the depth of the hierarchy. There are currently two principal applications for HIBE.

Vipul Goyal et al., [4] describe a 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 issues handled in this paper is encrypting the data that would be selectively shared only at a coarse-grained level (i.e., giving another party 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, encrypted text are labeled with sets of attributes and private keys are associated with access structures that control which encrypted text a user is able to decrypt. Demonstrate the applicability of construction to sharing of audit-log information and broadcast encryption.

Michael Armbrust et al., [5] concentrates the illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning. The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs. The cloud users need to pay for use of computing resources on a short term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

III. CP-ABE MODEL

The working algorithm logic in encryption is ABE comes in two flavors called Key-Policy ABE (KP-ABE) and cipher text-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to describe a user's credential, and an encryptor determines a policy on who can decrypt the data's-ABE is more appropriate to the data outsourcing architecture than KP-ABE because it enables data owners to choose an access structure on attributes and to encrypt data to be outsourced under the access structure via encrypting with the corresponding public attributes.

While encrypting the confidential data, there may introduce several challenges with regard to the attribute and user revocation. The revocation issue is even more difficult especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, it refer to such a collection of users as an attribute group). It also defines the affect due to the revocation of users from the group. It may result in bottleneck during re-keying procedure or security degradation in the system.

The existing system depending full of manual process, manual system maintains the limited number of process. The existing system includes an attribute-based access control scheme using CP-ABE with efficient attribute and user revocation capability for data outsourcing systems. The existing system consists of the following entities:

The authorized person will generates public and secret parameters for issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on the attributes. It is the only party that is fully trusted by all entities participating in the data outsourcing system.

Server who outsources data to the external data server provided by the service provider is termed as data owner. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before outsourcing it.

\ The one who access the outsourced data will be known as user. If user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then the user will be able to decrypt the encrypted text and obtain the data.

Service Provider consists of data servers and a data service manager. The cloud service provider is in charge of controlling the accesses from outside users to the outsourced data in servers and providing corresponding contents services.

The following are the drawbacks of E-CP-ABE system:

- Handling the outsource data copies in a secure manner is difficult.
- Storing and retrieving of data from cloud server takes more time and effort.
- The data owner need to take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation.
- All the data is maintained by single service provider so the data privacy may be affected by the third party storage area.
- Keys are assigned randomly and independently from each other, so the user can access the data of another user group by the system.
- No capability to capture a series of attribute queries option.
- User profile is group into single group attribute in the tuples structure only.
- Past query based suggestion is not given to user group.

Below mentioned are the main objectives of the proposed system:

- User can be revocated from particular group. After revocation, key assigned to the revocated user will be redefined and reused for another new user.
- To maintain data servicing by more than one service provider.
- To make all data service managers take charge of managing the attribute group keys per each attribute group.
- To assign keys based on uniqueness among all users.

IV. ENHANCED CP-ABE- METHODOLOGY

In proposed Secure-ECP-ABE system, first, enabling user access control enhances the backward/forward secrecy of outsourced data on any membership changes in attribute groups compared to the attribute revocation schemes.

Second, the user access control can be done on each attribute level rather than on system level, so that more fine-grained user access control can be possible. In practical scenarios, users may miss many key update messages so that it cannot sometimes keep the key states up-to-date. This is called stateless receiver problem. In the proposed scheme, rekeying in the attribute group is done with a stateless group key distribution mechanism using a binary tree. This alleviates the scalability problem and resolves the stateless receiver issue.

Third, data owners need not be concerned about any access policy for users, but just need to define only the access control policy for attributes as in the previous EABE system. The main objective of the proposed system is to reduce the time consuming and make the system more user friendly, efficient, accurate and fast process. The primary objective of the proposed system:

- To relocate users by any service provider may if unauthorized user tries to access the data above a given count.
- To maintain data servicing by more than one service provider.
- To make all data service managers take charge of managing the attribute group keys per each attribute group.

The proposed system implements all the existing system concepts in which the encrypted text-Policy Attribute-Based Encryption with User Revocation is carried out. Like existing system, the proposed scheme also adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system. In addition, multiple service providers are included and data is distributed among them. User privileges may be varying for data maintained by different service providers. This requires different kind of encryption mechanisms in data maintained by different service providers. The following are the advantages of proposed system:

- Any cloud service provider may revocate users if unauthorized user tries to access the data above a given count.
- Data service is maintained by more than one cloud service provider, the authentication process is enhanced.
- 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

In the first phase, 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.

The attribute creation is done in second phase. 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 to delete the specified record and close command button is user to terminate the current form.

The user creation form is 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.

Attribute key generation form 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 database 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.

Attribute group key generation form 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.

- This first phase 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.
- This next phase 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 create command button event. The corresponding username, user id and the given key encrypting values are inserted into the user details table.
- This next phase 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.
- This next phase, re-encrypt 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.
- 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. This next phase 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.
- This last phase 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.

V. CONCLUSION

The proposed encrypted-text 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. This thesis proposes a cryptographic approach to enforce a fine-grained access control on the outsourced data that is dual encryption protocol exploiting the combined features of the encrypted text policy attribute-based encryption and group key management algorithm. The proposed encryption scheme allows a data owner to define the access control policy and enforce it on his outsourced data to protect confidential data from unauthorized access.

It also employs 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 encrypted text -policy attribute-based encryption model does includes the set of the attributes, tree access policy, and the definition of the time instant, because the costs are negligible if compared with the key generation.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4,pp. 50–58, Apr. 2010.
2. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
3. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted

storage,"in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

4. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. etw. Distrib. Syst. SecuritySymp., 2003, pp. 131–145.
5. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improvedproxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.
6. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-basedencryption for fine-grained access control of encrypted data,"in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
8. 8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: Theessential of bread and butter of data forensics in cloudcomputing," in Proc. ACM Symp. Inf., Comput. Commun. Security,2010, pp. 282–292.
9. [9] B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
10. X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
11. D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf.Theory Appl. Cryptographic Techn., 2005, pp. 440–456.
12. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusionsecure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.
13. Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: ecure multiowner data sharing for dynamic groups in the cloud," in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.
14. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
15. X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible keymanagement mechanism for trusted collaborative computing,"in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.