www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Novel Sybil Attack Detection in VANETusing CP-ABE Delegation

[1]Mr. C.Mani, M.C.A., M.Phil., M.E., Associate Professor,
[2]Ms. P.Aarthi, FinalMCA.,
Department of MCA, Nandha Engineering College(Autonomous), Erode-52.
E-Mail ID: cmanimca@gmail.com, aarthipalanisamy611@gmail.com

***Abstract*—In this paper, Ciphertext-policy attribute-based encryption (CP-ABE) delegation scheme is proposed, which allows road side units (RSUs) to perform most of the computation for the purpose of improving the decryption efficiency of the vehicles. In addition to that, proposed 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.**

***Keywords*—VANET, CP-ABE delegation, novel Sybil attack, footprint.**

I. INTRODUCTION

THIS document is a 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.

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 ciphertext-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.

ARCHITECTURE DIAGRAM

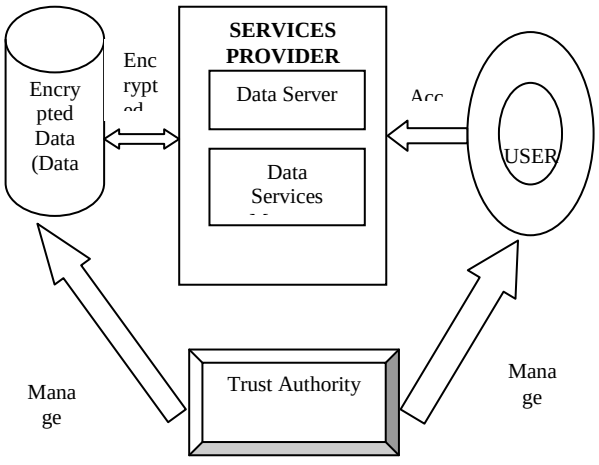

Fig 1.1 Attribute Architecture Diagram

II. RELATED WORKS

"Persona: An Online Social Network with User-Defined Privacy" [3] the authors R. Baden, A.

Bender, N. Spring, B. Bhattacharjee, and D. Starin described that, Online social networks (OSNs) have become a de fact oportal for Internet access for millions of users. These net-works help users share information with their friends.

However, users entrust the social network provider with such personal information as sexual preferences, political and religious views, phone numbers, occupations, identities of friends, and photographs. Although sites over privacy controls that let users restrict how their data is viewed by other users, sites provide insufficient controls to restrict data sharing with corporate affiants or application developers. Not only are there few controls to limit information disclosure, acceptable use policies require both that users provide accurate information and that users grant the provider the right to sell that information to others.

Facebook is a representative example of a social network provider. The Facebook \Statement of Rights and Responsibilities" re-quires that users \not provide any false personal information on Facebook" and \keep [their] contact information accurate and up to date." Further, it states that users \grant [Face-book] a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP [Intellectual Property] content that [they] post on or in connection with Facebook."

A. Fuzzy Identity-Based Encryption [4]

Identity- Based Encryption(I BE) allows for a sender to encrypt a message to an identity without access s to a public key certificate . T he ability to do public key encryption without certificates has many practical applications. For example, a user can send an encrypted mail to a recipient, without the requiring either the existence of a Public- Key Infrastructure or that the recipient b e on-line at the time of creation. One common feature of all previous Identity- Base d Encryption system s is that they view identities as a string of characters.

B. Attribute-Based Encryption

For Fine-Grained Access Control of Encrypted Data" [5], the authors V. Goyal, O. Pandey, A. Sahai, and B. Waters described that, There is a trend for sensitive user data to b e stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Go ogle and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion rep orts individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that pemrsonal data will b e compromised.

III. MULTIMEDIA CONTENT SHARING METHODOLOGY

The data outsourcing scenario challenges the approaches of traditional access control architectures such as reference monitor, where a trusted server is in charge of defining and enforcing access control policies. This assumption no longer holds in modern data outsourcing systems, because users want to be able to share private contents with a group of people they selected and to define some access policy and enforce it on the contents. Thus, it is desirable to put the access policy decisions in the hands of the data owners.

Recently proposed access control models, such as attribute-based access control, define access control policies based on different attributes of the requester, environment, for the data object. In addition, the current trend of storage outsourcing requires increased protection of data including access control methods that are cryptographically enforced. The concept of attribute-based encryption is a promising approach that fulfills these requirements. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts.

Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. However, the problem of applying the ABE to the data outsourcing architecture introduces 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 is referred to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. It may result in bottleneck during rekeying procedure or security degradation in the system.

This research attempts to solve these problems in attribute-based data access control using CP-ABE for data outsourcing systems. Recently, several attribute revocable ABE schemes have been

proposed. They realize revocation by revoking attribute itself using timed rekeying mechanism, which is implemented by setting expiration time on each attribute. A coarse-grained revocation is called because the immediate rekeying on any member change could not be possible. In particular, Dekey remains secure even the adversary controls a limited number of key servers. They implement Dekey using the Ramp secret sharing scheme that enables the key management to adapt to different reliability and confidentiality levels.

The evaluation demonstrates that Dekey incurs limited overhead in normal upload/download operations in realistic cloud environments. This thesis study makes new construction Dekey to provide efficient and reliable convergent key management through convergent key deduplication and secret sharing. Dekey supports both file-level and block-level deduplications. Security analysis is demonstrates that Dekey is secure in terms of the definitions specified in the proposed security model. Symmetric encryption uses a common secret key to encrypt and decrypt information. Since the key used for this experimental work are very weak, the existing system is less secure. User revocation management is not implemented. The key can be management only within the group members.

A. Authentication Model

A hashing function can be used to return a unique key for a block of data, based only on the contents of the data; if two people have the same data, the hashing function will return the same key. If this key is used as the index for storing the data block, then any attempt to store multiple copies of the same block will be detected immediately. In some circumstances, it may be necessary store additional metadata, or a reference count to keep track of the multiple "owners", but it is not necessary to store multiple copies of the data itself.

Encrypting data invalidates the de-duplication; two identical data blocks, encrypted with different keys, will yield different encrypted data blocks which can no longer be shared. Typical implementations involve complex schemes for storing and managing these keys as part of the block meta-data. This can be a reasonable approach when the de-duplication is part of a local file system.

But there is considerable overhead in interrogating and maintaining this meta-data, which can be significant when the de-duplication and encryption is being performed remotely and this is necessary in this case to preserve the privacy of the data. Securing outsourced data for multi-user accesses can be achieved through encrypted file systems.

De-duplication systems decrease storage consumption by identifying distinct chunks of data with identical content. They then store a single copy of the chunk along with metadata about how to reconstruct the original files from the chunks. The proposed methodology is used to provide a provably secure design of a cryptographic le system along with rigorous security definition.

B. Cipher Text-Policy Attribute-Based Encryption With User Revocation

Step 1:

The setup algorithm is executed which is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key PK and a master key MK.

Step 2:

The attribute key generation algorithm is executed which takes input the master key MK, a set of attributes □□□L,, and a set of user indices U □□u as parameters. It outputs a set of private attribute keys SK for each user in U that identifies with the attributes set.

Step 3:

The key encrypting key (KEK) generation algorithm is executed in this module, which takes a set of user indices U □□u as input, and outputs KEKs for each user in U, which will be used to encrypt attribute group keys $K_{□i}$ for each Gi□□□G.

Step 4:

An encryption algorithm (which is a randomized algorithm) that takes as input the public parameter PK, a message M, and an access structure 'A' over the universe of attributes. It outputs a cipher text CT such that only a user who possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

Step 5:

The re-encryption algorithm is a randomized algorithm that takes as input the cipher text CT including an access structure 'A', and a set of attribute groups G.

If the attribute groups appear in 'A', it re-encrypts CT for the attributes; else, returns □. Specifically, it outputs a re-encrypted cipher text CT' such that only a user who possesses a set of attributes that satisfies the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

Step 6:

The decryption algorithm is executed which takes as input the cipher text CT' which contains an access structure 'A', a private key SK, and a set of attribute group keys $K_{\square\square}$ for a set of attributes □. The decryption can be done if □□satisfies 'A' and $K_{\square}$□ is not revoked for any □□□□□□

Step 7:

If the data contains most important information and in order to protect the data security, more privileged service providers view most of the data and less privileged service providers view limited data.

C. 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;

Algorithm Steps:

Ciphertext = $E_{K3}(D_{K2}(E_{K1}(plaintext)))$
Create 16 subkeys, each of which is 48-bits long.
Encode each 64-bit block of data.
C[0]D[0] = PC1(key)
for 1 <= i<= 16
C[i] = LS[i](C[i-1])
D[i] = LS[i](D[i-1])
K[i] = PC2(C[i]D[i])
Encipherment:
L[0]R[0] = IP(plain block)
for 1 <= i<= 16
L[i] = R[i-1]
R[i] = L[i-1] xor f(R[i-1], K[i])
Cipher block = FP(R[16]L[16])
Decipherment:
R[16]L[16] = IP(cipher block)
For 1 <= i<= 16
R[i-1] = L[i]
L[i-1] = R[i] xor f(L[i], K[i])
Plain block = FP(L[0]R[0])

$Decrypt_{CE}$(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

Algorithm Steps

Input:
CC: 64 bits of cipher text
k16, k15, ..., k1: 16 round keys
IP: Initial Permutation
FP: Final Permutation
f (): Round Function
Output:
TT: 64 bits of clear text

Process:
CC' = IP(CC), applying initial permutation
(LL0, RR0) = CC', dividing CC' into two 32-bit parts
(LL1, RR1) = (RR0, LL0 ^ f(RR0, k16))
(LL2, RR2) = (RR1, LL1 ^ f(RR1, k15))
.....
TT' = (RR16, LL16), swapping the two parts
TT = FP(TT'), applying final permutation

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

IV. EXISTING METHODOLOGY

The existing system maintained by the cloud service providers, provides storage space for hosting data files in a pay-asyou-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager takes charge of system parameters generation, user registration, and user revocation.

The group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In this scheme, the group membership is dynamically changed, due to the new user registration and user revocation. It includes an attribute-based access control scheme usingCP-ABE with efficient nnattribute and user revocation capability for data outsourcing systems. The proposed scheme has following advantages with regard to the security and

scalability compared to the previous revocable CP-ABE schemes.

In existing 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.

- The data owner need to take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation.
- Keys are assigned randomly and independently from each other.
- All the data is maintained by single service provider.
- The single data service manager is in charge of managing the attribute group keys per each attribute group.
- All the nodes are treated equally and weak capable nodes also require huge computations.
- All the mirror nodes store the file with same encryption mechanism.
- Unauthorized data leakage still remains a problem due to the potential exposure of decryption keys.
- Only single cloud provider environment is considered.

V. PROPOSED METHODOLOGY

The proposed system implements all the existing system concepts in which the Cipher 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 and so computation overhead is reduced.

- 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.
- 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.
- Partial data of files are taken from multiple mirror locations and send to selected client.
- Suitable for very large size files.
- Irrelevant size blocks of data are handled among the multiple cloud service providers based on their computational capabilities.
- Different trust level is set to different cloud providers and encryption or decryption is varied based on the clouds computational capability.

VI. CONCLUSION

Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. This project 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 ciphertext-policy attribute-based encryption and group key management algorithm.

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.

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.