Multi Attribute Based Technique in Key Generation System

Aparna.V, Jabisha Arul, Nandhini. S, Vishnu Kumar. A

Abstract: ***The main objective of this paper is to improve the security and the efficiency while sharing the data between data owner and the users. Based upon the attributes of the users we are going to share the data. One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the support of policies updates. Cipher text policy attribute based encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of problem. It enables data owners to define their own access policies over their user attributes and enforce the policies on the data to be distributed. However, the advantage of the system comes with a major drawback which is known as a key escrow problem. The key generation center might decrypt any kind of messages addressed to specific users by generating their private keys. This is not suitable for data sharing typical scenarios where the data owner would like to make their private data only accessible to designated users. In addition, applying CP-ABE in data sharing system introduces another challenge with regard to the user revocation. From this study, we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. The performance and security analysis indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.***

Index Term: ***Attribute Based Encryption, Escrow Free Key Issuing Protocol, Ant Colony Algorithm, Revocation.***

I. INTRODUCTION

In the prevailing system, a user's identity must be validated by the authority, in distributed system; it is a complex task to manage numerous user identities. Also, all users must trust the central authority, if the authority is malicious; he can impersonate any user without being detected. Hence we are facing a major issue with Key-Escrow problem .The secret key is generated in a single space. In turn, the system can be easily attacked by attacking the single space. Keys were generated randomly and it is decided by the key generation center and the user doesn't have any control/preferences or specification of deciding the key based on user centric purpose. The key generation center (KGC) can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential risk to the data confidentiality or privacy in the data sharing systems. The revocation of any attribute or any single user in an attribute group would affect all users in the group.

Manuscript received on April, 2013.

Aparna.V, Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India.
Jabisha Arul Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India.
Nandhini. S , Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India.

Most of the existing ABE (Attribute-based encryption) schemes are constructed on the architecture where a single trusted authority or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. The major drawbacks of the prevailing system is that the data sharing is not much secure and any other user can easily access the data in data store. In addition to it, the system won't distribute the data based on the attributes of the user. Hence in the proposed system, the key issuing protocol generates and issues user secret keys by using the multiple attributes obtained from the user. The proposed scheme delegates most laborious tasks of membership management to the data center. The major advantage of the proposed system is that the data is shared between the data owner and the users based on the attributes.

II. SYSTEM MODEL

The user will be allowed to specify their details in which the keys will be generated using the multiple attributes of the user(Fig 1). Now the key generation system will generate the keys and provide them to the user. Key is used to access the application center and for accessing the confidential data. After the user makes a successful validation to the system, user will get access with their confidential data from the data center. The accessing of the data is done. The user will be allowed to define their attributes in which the user's key will be generated. After the key generation, the user will be provided with keys. When the user's key matches, then the data will get decrypted and the user can view their confidential data. The user's parameters params and a security parameter l are taken as input during the process of new user creation. Based on the parameters obtained from the user, an unique key is generated. The keys are generated using the multiple attributes of the user and are stored in a data center. The Keys that are generated are distributed to the user. The corresponding keys of the user are used to perform encryption before it is stored in the database. During the process of verifying crendentials or process of login, the security parameter l and the input parameter params is authenticated. If the result of authentication is 1, the user can make use of corresponding key to view the original data.

III. ALGORITHM FOR PROPOSED SYSTEM

A. Ciphertext Policy Attribute-Based Encryption (CB-ABE):

In a ciphertext policy attribute-based encryption scheme[11], each user's key is related with a set of attributes representing their capabilities, and a ciphertext is encrypted .

B. MD 5:

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Takes as input a message of arbitrary length and produces as output a 128 bit "message digest" of the input. MD5 has been employed in a wide variety of security applications, commonly used to check data integrity.

C. Triple DES Algorithm:

Triple DES Algorithm is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

D. Ant Colony Optimization Algorithm:

The basic philosophy of the algorithm involves the movement of a colony of ants through the different states of the problem influenced by two local decision policies. In our project, we are trying to identify/predict and assign the possible access to be provided to the particular user based on user details.

E. Multi Attribute Based Technique In Key Generation System :

Commitment: (1^l) The Commitment scheme consists of the following three algorithms C=(Setup,Commit,Decommit). output params as the systems output parameter.

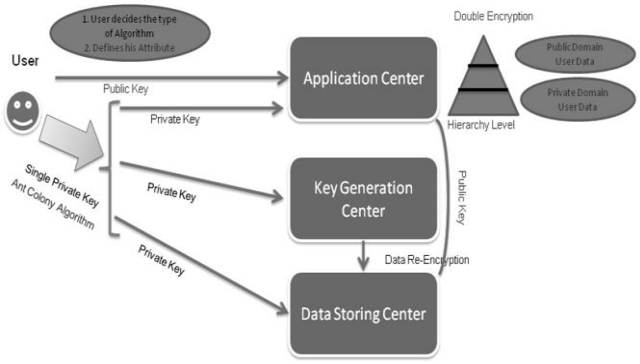

Fig 1. Architecture Diagram

Commit: This algorithm takes parameters and a message M as input parameters and an commitment comm is obtained as output. The decommitment decomm is used to decommit the commitment comm.

Decommit: This algorithm takes as input the parameters param, a message M and a commitment comm. The decommitment decomm is used to decommit the commit. If the decomm decommits the comm to the message M, then output 1 is obtained. Otherwise the algorithm outputs 0.

The KP-ABE consists of a set of parties $\{P_1,P_2,\ldots,P_N\}$. An access structure (resp., monotonic access structure) is a collection (resp., monotonic collection) A of non-empty subsets of $\{P_1, P_2, \cdots, P_N\}$, namely $A \subseteq 2^{\{P1,P2,\cdots,PN\}} \setminus \{\varphi\}$. The sets in A are called the authorized sets, and the sets outside of A are called the unauthorized sets.

Following are the five algorithms which a KP-ABE scheme consists:

Global Setup $(1^l) \rightarrow$ params. A security parameter l is taken as an input and the parameters params is obtained as the output of the system.

Authority Setup $(1^l) \rightarrow (SK_i, PK_i, A_i)$. Each authority Ai generates his secret-public key pair $KG(1)^l \rightarrow (SK_i, PK_i)$ and an access structure Ai, for i =1, 2, · · · , N.

We have used the keyGen algorithm .The algorithm is defined as follows:

Key generation(KeyGen) (U(params, PKi, decom) ↔ Ai (params, SKi, PKi, Ai, com)) → (SKiU , empty). In this algorithm, the user U runs the commitment algorithm Commit(params,) → (com, decom) and sends com to the authority Ai. Then, the user U and the authority Ai consider input as (params, PKi, decom) and (params, SKi, PKi, Ai, com), respectively. If Decommit(params, com, decom) → 1, this algorithm gives the outputs of a secret key Ski U for U and empty for Ai. Otherwise it outputs in error messages for both user and authority.

with the trusted authorities. Selective-failure needs that the identifier of the users are not known by the unauthenticated or the malicious authorities and they cannot cause the algorithm KeyGen to fail based on the choice of the identifier of the user.To define the above stated properties we use the following.

Leak-freeness. The user's confidential information is secured by the Setup$(1^l) \rightarrow$ params and Authority Setup$(1^l) \rightarrow$ (SKi, PKi, Ai) by executing the Key Generation algorithm with the authority.Due to this the identifier cannot be tracked by the malicious authority or by the unauthenticated one and also cannot know about the user identity.

Selective-failure. The adversary A_i submits .The public key PK_i, and two identifiers u_0 and u_1.Then, a bit $b \in \{0,1\}$ is randomly selected.A_i can have a black-box access to U(params,PK_i,u_b) and U(params,PK_i,u_{1-b}).Then,U executes keyGen protocol with A_i. U outputs secret keys SK^b_U and SK_U^{1-b} for identifiers u_b and u_{1-b},respectively.If $SK^b_U \neq \perp$ and $SK_U^{1-b} \neq \perp$,A_i is given(SK^b_U,SK_U^{1-b}). If $SK^b_U \neq \perp$ and $SK_U^{1-b} \neq \perp$,A_i is given ($\in$, $\perp$).If $SK^b_U = \perp$and $SK_U^{1-b} \neq \perp$,A_i is given($\perp$,$\in$).If $SK^b_U = \perp$ and $SK_U^{1-b} = \perp$,A_i is given($\perp$,$\perp$).At the end ,A_i outputs his prediction b'on b.

Encryption : The algorithm takes as input the system parameters param, a message M and a set of attributes A_C and outputs a cipher text CT, where $A_C=\{A^1_C,A^2_C,\ldots,A^N_C\}$.

Decryption :($\{SK^i_U\}_i \in I_C$, CT). This algorithm takes as input the identifier ID, the keys $\{SK^i_U\}_i \in I_C$ and the ciphertext CT , and outputs the message M, where I_C is the index set of the authorities A_i.The concepts used in this paper are inference from the following:

III. MEDIATED CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION AND ITS APPLICATION

In Cipher text-Policy Attribute-Based Encryption (CP-ABE)[7], the cipher text is associated with an access policy over attributes and the user secret key is associated with a set of attributes.The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. Several CP-ABE schemes have been intended, however, some practical problems, such as revocation, still need to be addressed. In

this paper, we propose a mediated Cipher text-Policy Attribute-Based Encryption (mCP-ABE)[6] which extends CP-ABE. Furthermore, we instruct how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs). The scheme allows the encrypt or to encrypt a message according to an access policy over a set of attributes.A possible extension to this work would be to provide a scheme which would have a security proof under standard complexity assumptions.

IV. IDENTITY-BASED ENCRYPTION WITH EFFICIENT REVOCATION

Identity-based encryption (IBE) is an exciting alternative to public-key encryption. The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, the identities (e.g. emails or IP addresses) of the latter are alone enough to encrypt. Any setting, PKI- or identity-based, must provide a means that the users must be revoked from the system.The efficient revocation is a studied problem in the traditional PKI setting. However in the setting of IBE, there is a need for the study of revocation mechanisms. The most important practical solution requires the senders to also use time periods while encrypting, and all the receivers (regardless of whether their keys have been compromised or not)need to update their private keys regularly by contacting the trusted authority. We note that this solution does not scale well as the number of users in the system increases, the work on key updates becomes a bottleneck. Any setting, PKI- or identity-based, must provide the means for revocation of the users from the system.
IBE scheme that significantly improves key-update efficiency on the side of the trusted party (from linear to logarithmic in the number of users), while staying efficient for the users.Our schemes should be particularly useful in the settings where a large number of users is involved and here scalability is an issue.

V. IMPROVING PRIVACY AND SECURITY IN MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. The attribute based encryption scheme, verify and manage the different sets of attributes and provide corresponding keys to users. The encryptors require that a user obtain keys for their corresponding attributes from each authority before decrypting system was more complex and the confidentiality depends critically on the security of the central authority. The methods and techniques used in this project does not contain all the security for the database.

VI. A CONTENT-DRIVEN ACCESS CONTROL SYSTEM

Protecting identity in the Internet age requires the ability to go beyond the identification of explicitly identifying information like social security numbers, to find the broadly held attributes, when taken together, are identifying. We present a system that work in conjunction with natural language processing algorithms or user-generated tags, to protect identifying attributes in content.. attributes are encrypted with an encryption.This paper didn't explain about the about the type of hacking and the relationship between the attributes and the prevention technique.

VIII. ANALYSIS OF OUR ALGORITHM

In Mediated Cipher Text-Policy Attribute-Based Encryption[10] we referred the concept of Instantaneous Attribute revocation with this concept duplication can be avoided. In Improving Privacy and Security in Multi –Authority attribute based encryption[6] we referred the concept of Global Identifiers. It removes the trusted central authority.
In Identity based encryption with efficient revocation[16] we referred the concept of Public key Infrastructure .It improves key update efficiency.

IX. EXPERIMENTAL WORK AND RESULT

Protecting privacy is an alarming issue in the distributed systems. Henceforth, our multi-attribute based technique in key generation concept can be used as a sound solution to construct privacy preserved data transfer and access control concepts in distributed systems. Users can obtain keys from authorities. As a result, our scheme can provide the following important properties: 1. access tree; 2) Users cannot be impersonated as they can obtain keys.

X. SUMMARIES AND FURTHER EXTENSION

Biometrics such as iris scanners would provide provably very high security by making it ideal for biometric identification.

XI. CONCLUSION

The performance and security analyses was made efficient to securely manage the data distributed in the data sharing system. Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the cipher text encrypted under the CP-ABE algorithm. The escrow problem was solved.

REFERENCES

[1] A.LewkoandB.Waters,"DecentralizingAttribute-based encryption, "in Proceedings:AdvancesinCryptologyEUROCRYPT"11(K.G.Paterson .ed),vol.6632ofLectureNotesInComputerScience,(Tallinn,Estonia),pp.568-588,Springer,May 15-19 2011.

[2] Lewko,A.Sahai,B.Waters,"RevocationSystems with very small private keys,"Proc.IEEE Symposium on security and privacy 2010, pp.273-285,2010.

[3] M.Chase,"Multi-authorityattributebased encryption,"inProceedings:TheoryofCryptographyConferenceTCC'07(S.P.Vadhan,ed.),vol.4392ofLectureNotesinComputerScience,(Amsterdam,TheNetherlands),pp.515-534,Springer,February 21-24 2007.

[4] M.ChaseandS.S.Chow,"ImprovingPrivacyandsecurityinmultiauthority Attributebasedencryption",Proc.ACMConference on Computer and communicationsSecurity-CCS'09,pp.121-130.

[5] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in Proceedings: ACM Conference on Computer and Communications Security - CCS'07 (P. Ning, S.D.C.di Vimercati, and P. F.Syverson, eds.), (Alexandria, Virginia, USA), pp. 456–465, ACM,October 28-31 2007

[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. WISA 2009, LNCS 5932, pp. 309–323, 2009.

[7] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symposium on Security and Privacy 2007, pp. 321–334, 2007

[8] R.Gennaro,S.Jarecki,H.Krawczyk,andT.Rabin,"Robust threshold signatures," Information and Computation,pp.54-84,2001.

[9] M. Green and S. Hohenberger, "Blind identity based encryption and simulatable oblivious transfer," in Proceedings: Advances in Cryptology-ASIACRYPT'07(K. Kurosawa, ed.), Lecture Notes in Computer Science, (Kuching, Malaysia), pp. 265–282,Springer, December 2-6 2007.

[10] D.Chaum,"Security withoutidentification: Transaction systems to make big brother obsolete," Communication of ACM, vol. 28,no. 10, pp. 1030–1044, 1985.

Ms. Aparna.V Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Ms. Jabisha Arul Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Ms. Nandhini S Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Mr. A.VishnuKumar received her B.E., Degree from IFET college Engineering, which is affiliated to Anna University in 2007. he received his M.E., Degree from Govt. College of Engineering - Anna University in 2009. At present working as Assistant Professor in Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Avadi from 2009 to tilldate. He doing his Ph.D. in Anna University and his research work is progressively going on in the area of Cloud Computing