IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENHANCING PRIVACY USING COLLABORATIVE ATTRIBUTE ENCRYPTION TECHNIQUES

Ansari Tasin Habib Ahmad*, Dr. J. W. Bakal
[*] M.e Computer, New Panvel, Maharashtra, India
M. Tech, PhD (Computer Engineering.), New Panvel, Maharashtra, India

DOI: 10.5281/zenodo.164906

ABSTRACT

In the era where computers dominate the other facilities, it becomes even more productive once connected to the world with the help of internet. Although it possesses certain challenges to connect oneself to the world. The challenges of Authenticity, confidentiality, and anonymity and all of the notions of security with the concern aspects. Depending on the application the encryption techniques differs the most recent assortment that is the attribute based encryption, unlike traditional encryption technique this technique doesn't reveals its identity Security tends to be the most important aspect when it comes to enter in the visual world thus the cryptographic technique is very much essential to be optimally developed so the transactions made cannot be read or changed in the network that is the data have to be securely traverse via internet, Attribute based cryptography techniques are dominating the aspects of security. The innovative use of attributes can improve the traditional techniques of data sharing which was by using trusted mediated servers. These attributes have been exploited to generate the public key and have been used as user's access policy to restrict the user's access. It is attribute-based, as it allows encrypting under logical combinations of attributes, that is, properties that users satisfy. It is hybrid, as it combines ciphertext policy attribute-based encryption (CP-ABE) with location-based encryption (LBE) on the level of symmetric keys. It supports encryption under expressive policies, since it can efficiently handle dynamic attributes with continuous values, such as location. Public key encryption techniques provide authenticity through digital signature and confidentiality with the help of public key encryption technique. Security also overcomes the bottleneck of centralization since there is no central authority, it works as distributed attribute based encryption where the load is well distributed among every participating node.

KEYWORDS: Key-Policy, Cipher Text-Policy, Non Monotonic Framework, ABE and encryption, Location Based Encryption.

INTRODUCTION

In the recent years security became the essential factor in the field of data storage with the embarking ecommerce technologies a large population is getting dependent on web technologies; cloud computing, data processing etc. Recently developed Attribute based encryption techniques is emerging to be most favorable in the field of cryptography and security, Personalities like sahai, water, piretti, traynor, McDaniel, Bethencourt made a huge contribution to held up the concept attribute based encryption technique. ABE have the capability to provide decentralized security enforcement which allows us to provide security without any excessive dependency thus successfully emerging as an essential tool when it comes to ubiquitous computing applications. It is basically design to capture the distinctive feature of the user and bounding it around traditional private and public key cryptography. Precisely encryption technique is nothing but logical combination of attributes which are usually coined under the term 'Attribute policies' which in turn may allow making users addressable according to their properties. Attribute Encryption techniques have evolved all the way from the concept where the attribute was considered merely just as a string to the concept where it is considered as the descriptive attributes where certain threshold can only decrypt the enciphered message that is, A predefined value of threshold will the define the minimum number of common attribute required by the decrypter to the concept where the access policy is defined which is nothing but the set of rules which have to be followed in order to decrypt the encrypted message this policy is in the form of Boolean tree in the form of AND and OR condition to the concept where non-monotonic access structure also can be inculcated which includes NOT gates condition or negation conditioning, To the concept where a central authority control the various other entities or authorities so that multiple messages can simultaneously be encrypted and decrypted to finally a concept where the central authorities have been eliminated to avoid the bottle neck caused by the CA and various other technologies can be used to enhance the privacy of the vastly huge network.

Conceptually we proposed a system based on Distributed attributed based encryption (DABE) along with the location based encryption technique (LBE) developed by Scott & Denning, 2003 motivation behind developing this system is to restrict the possibility of the system being hacked by putting a an extra parameter to security which is location. The system will also include the online and offline encryption specification. The encryption and decryption process is much more independent as the D-ABE technique reduces the dependency over central Authority.

LITERATURE SURVEY

Data privacy in open cloud computing is one of the most challenging aspects in cloud computing to enhance data privacy in cloud environment these major problems have to be overcome

1. Common data privacy method" Throwing encryption at the problem" is not optimum for the cloud Computing and will require additional cryptographic coprocessors hardware
2. Traditional public and symmetric key encryption methods suffer from series of problem when handed over third party which is untrusted[1]
3. Cloud based applications which process and rely on the data may be vulnerable when run on hardware or virtual instances operated by an untrustworthy cloud provider.
4. Man-in-the-middle type attacks would be trivial for the cloud provider as they operate both the network, hardware and IP ranges for the virtualized services.

Identity based encryption technique: It is a public-key pairwise based encryption which uses attribute as a mere string to behave as identifier and a trusted third party as the private key generator For example, a PKG might be provided to delegating Secret keys corresponding to a public key consisting of a user's e-mail address upon request. Here the email address of each individual is considered as the specific attribute for that particular entity.

Fuzzy Identity-Based Encryption: authors [3] proposed that attribute cannot be just treated only as string Instead it has to be considered as a detailing package for every individual. Thus this concept induces attributes as characteristics of user which support in encrypting a message which can be only decrypted if a user processes certain predefined set of attributes so a threshold number of attribute value has to be set before encrypting the message to decrypt the message threshold value have to surpass at the receiver end. Although this theory led us the way to amplify the usage of rules along with attribute based encryption but also lacks in certain facts as Generation and distribution of a user's secret key and authentication of their identity is limited to a single trusted authority which imposes both scalability and trust issues. If the central authority or its private key should become compromised, the attacker would have the ability to decrypt any document in the system as well as create any identity for themselves (which could be problematic if the system is used for creating signatures or proving a user's identity).

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data: Key-Policy Attribute-Based Encryption (KP-ABE) (Goyal, Pandey, Sahai, & Waters, 2006) is an ABE scheme which embeds access control policies in the user's key rather than incorporating them into the ciphertext during encryption. KP-ABE builds upon the attribute encryption applications of FIBE and replaces the simple l of m attribute [7], threshold policy with a tree access structure consisting of AND and OR threshold gates as nodes, and leaves are associated with attributes.

Ciphertext-policy attribute-based encryption: It enables us to use a complex tree based access policy to be embedded in the ciphertext rather than the key as with KP-ABE. CP-ABE implemented the theory of "Variable Attributes" which use a set of traditional attributes to represent a value that can be evaluated with more complex operations [6].

Table: Summarize Literature Survey

Sahai and Waters in 2005	Attribute based encryption (ABE	ADVANTAGE: is a public-key based single to multiple encryption that allows users to encipher and decipher data based on user's attributes. In which the secret key of a user and the ciphertext are relied on attributes
		DISADVANTAGE: The application of this scheme is limited in the real environment because it use the access of monotonic attributes to monitor and allow changes to user's access in the system
R,Ostrosky A sahai And B water	Key Based Attribute based Encryption(KP-ABE)	ADVANTAGE: To reflect the access tree Structure the secret key of the user is defined. Ciphertexts are named with sets of attributes and private keys are bonded with monotonic access structure that monitors which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for single-to-multiple communications.
		DISADVANTAGES: KP-ABE scheme is the encryptor is compatible of deciding between which users can decrypt the encrypted data. It can only choose attributes for the data description; it is not suitable in some application because a data owner has to depend on the key issuer.
J.Bethencourt, Sahai, Waters	Ciphertext Based Attribute based Encryption	ADVANTAGE: In this scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is referred to a set of attributes. A user is able to decrypt a ciphertext only if those set of attributes linked with the user's private key reaches to the optimum access policy associated with the ciphertext
		DISADVANTAGES: Drawbacks of the most existing CP-ABE schemes are still not able to meet up the corporate requirements of access control which demands enormous flexibility and efficiency. CPABE has limitations in terms of declaring policies and managing user attributes
Multi-authority attribute based encryption	M. Chase and S. Chow.	ADVANTAGE: The system follows the working of the master and slave concept where a master called as central Authority (CA) and slaves as global identifiers (GI). The system also has M attribute authorities. Each attribute authority consists of certain values
		DISADVANTAGES: each authority's attribute set must be disjoint
Central Authority less multi-authority ABE	Chase M. and Chow S.S.M. proposed	ADVANTAGE: 1. No trusted central authority 2. User's privacy and secrecy 3.Decentralized i.e scattered pseudorandom operations are used in the system 4.Collusion avoidance for n numbers of colluding users
		DISADVANTAGES: The system does not support a tree access Structure

Data privacy is one of the major concerns in an open network where everything can be access by everyone, to grant security each data have to follow encryption and decryption process. The current system implements Attribute based encryption technique which doesn't successfully meet the growing challenges of worldwide environment so there is a need to develop a technique that will allow rapid encryption, less dependency, multiple encryption and decryption environment

PROBLEM DEFINITION

Data privacy is one of the major concerns in an open network where everything can be access by everyone, to grant security each data have to follow encryption and decryption process. The current system implements Attribute based encryption technique which doesn't successfully meet the growing challenges of worldwide environment so there is a need to develop a technique that will allow rapid encryption, less dependency, multiple encryption and decryption environment

ARCHITECTURE

The fig 4.1 depicts the block diagram of the proposed system which shows that it comprises of three different techniques which are

1. Location Tracking

2. Distributed Attribute based encryption
3. Linear secret sharing scheme

These when synchronized appropriately will generate a system that will help in enhancing privacy in cloud environment.

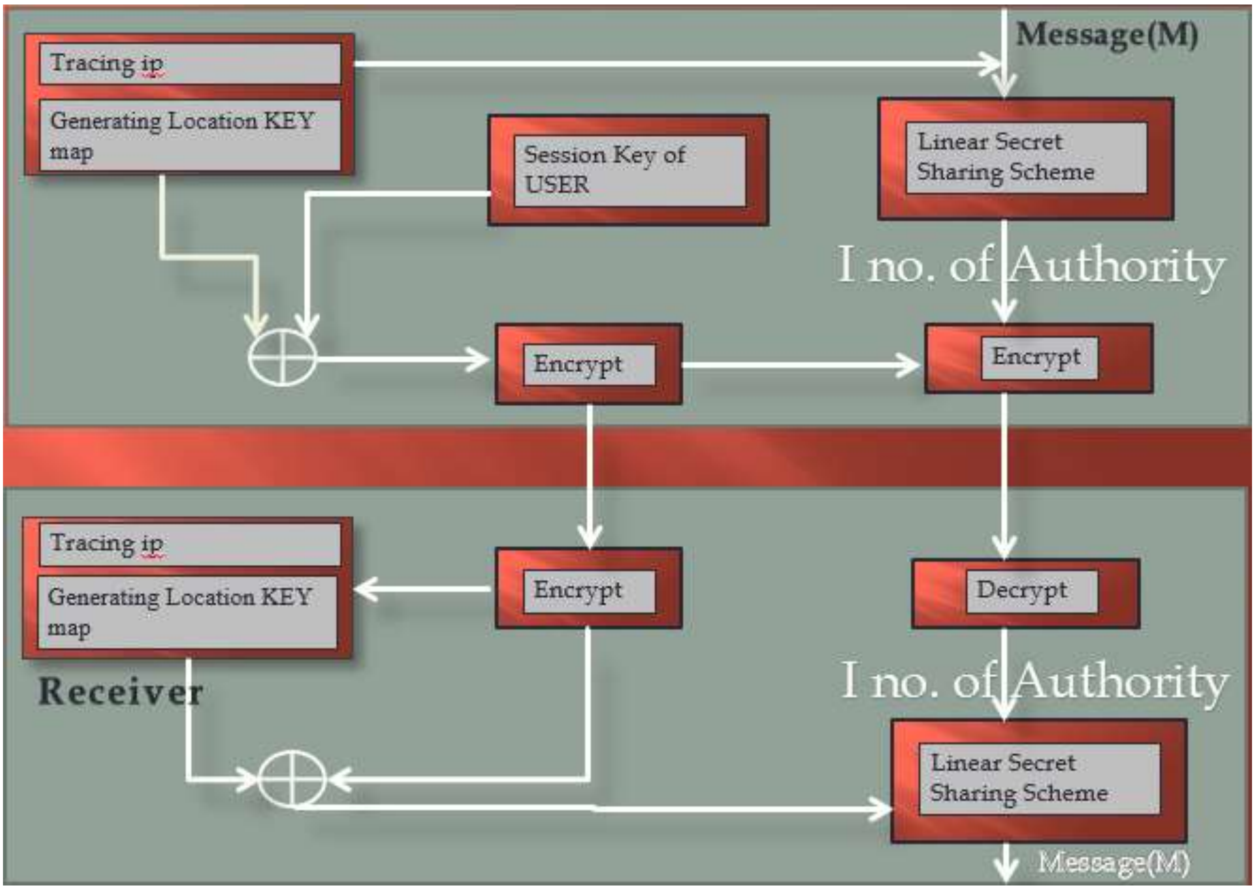

Figure 4.1: Block Diagram of the Proposed System

The block diagram of the below system that is being developed clearly depicts that it will be able to provide with the different level of encryption depending upon the user, tracing IP will generally be used to trace the location of the user, the working of each block will be discussed in the below points. The probable flow of the system would be as depicted in the figure below

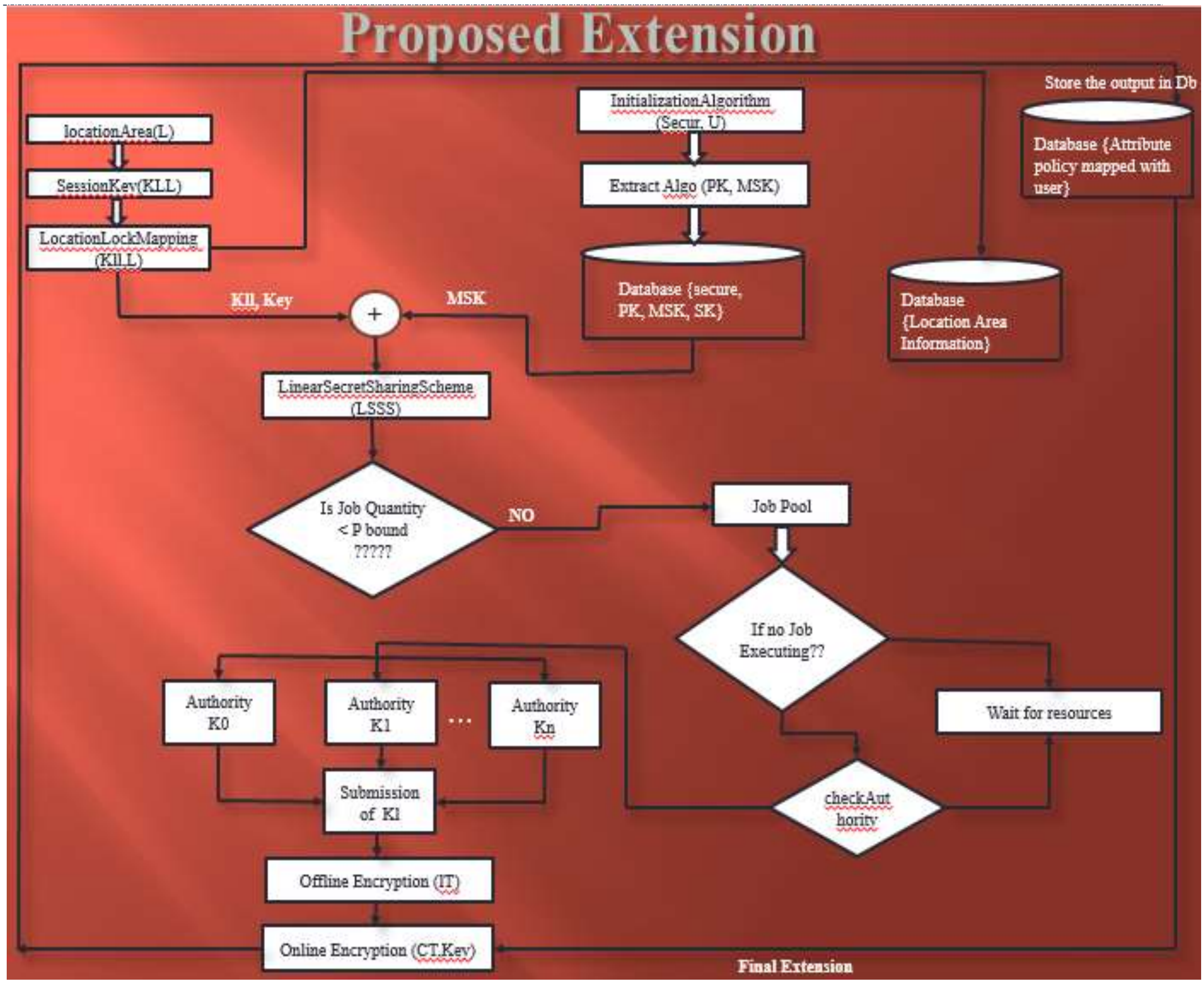

Figure 4.2: Flow of the system

Location Based Encryption: Location based encryption will basically accumulates the Tracing IP and location lock Mapping Blocks it generates the location lock key Kll, Key by following the series of steps

a. Transform latitude/longitude coordinate
b. Combine and hash
c. Generate final-key.

Use of location based encryption is to restrict the region up to which the message can be decrypted thus adding one more parameter to security .Thus reducing the probability of getting their privacy in to danger. A toleration distance (TolD) is designed to surpass the no accuracy and inconsistency problem of various GPS receiver. The process of LDE is shown in Figure 1. When the target coordinate and toleration distance that is submitted by an encryptor, an LDE-key is embarked from attitude/longitude coordinate and TolD. The random-key generator creates and assigns a session key, called R-key. Then, the secret-key for encrypting the message M is generated by exclusive-or R-key with LDE-key. The final-key can be used for the symmetric encrypt algorithm, such as DES, AES, triple-DES, etc.

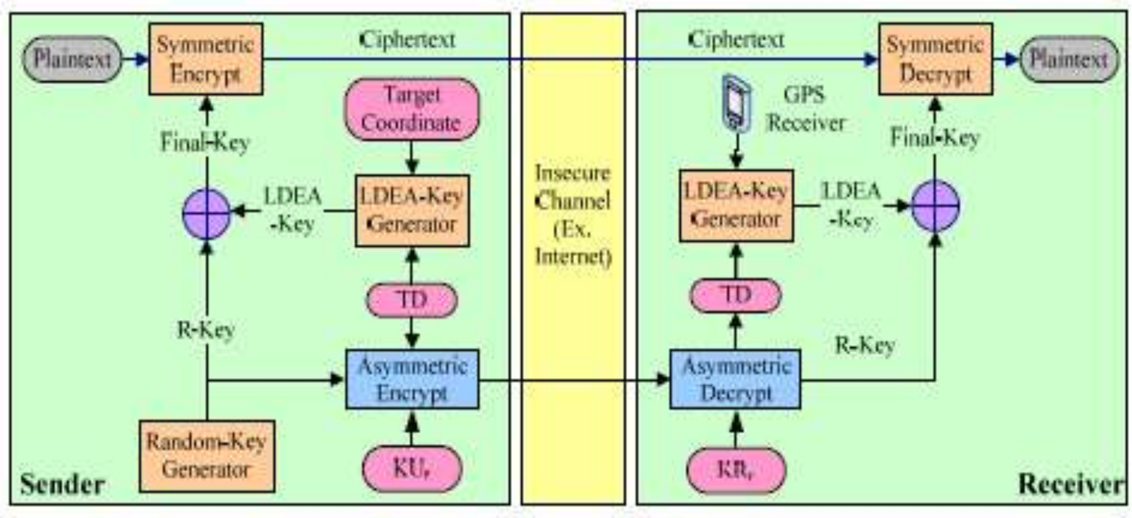

Figure 4.3: The LBE Process

Transform latitude/longitude coordinate: The very initial thing a system needs to do is to convert the longitude and latitude of the user been traced through IP via GPS system. According to NMEA a latitude and longitude can be converted as explained in an example “E 12231.5198” means 122 degrees and 31.5971 minutes east longitude. “N 5721.214” means 57 degrees and 21.214 minutes north latitude. The coordinates are multiplied 10000 to be an integer. Then, the integer is divided by a value corresponding to the Tolerance Distance in order to allow the coordinate inaccuracy. According to the estimation of CoordTrans tool of Franson Company, the values are 6 and 5.4 for longitude and latitude corresponding to one meter, respectively. **Combine and hash:** It is essential to secure the lock key since it will be the gate to access the sensitive information in order to make it more secure the results from the above step is the combine with the help of bitwise exclusive –OR operation. Then, various hashing algorithm is utilized and generates a 128-bit digest to complicate the result. Then, the digest is split into two 64-bit values, called LDE-keys. This step causes that the target coordinate is unable to be derived from the LDE-keys.

Generate final-key: A session R-key is generated of the same length randomly as that of LDE which is 64 bit. Two main keys are used as the secret key and initial value of DES symmetric encryption algorithm. Current design of LDE algorithm is based on the Hashing algorithm and DES algorithm. However, LDE is flexible and can be incorporated with other algorithms. The figure below will depict an example of LBE

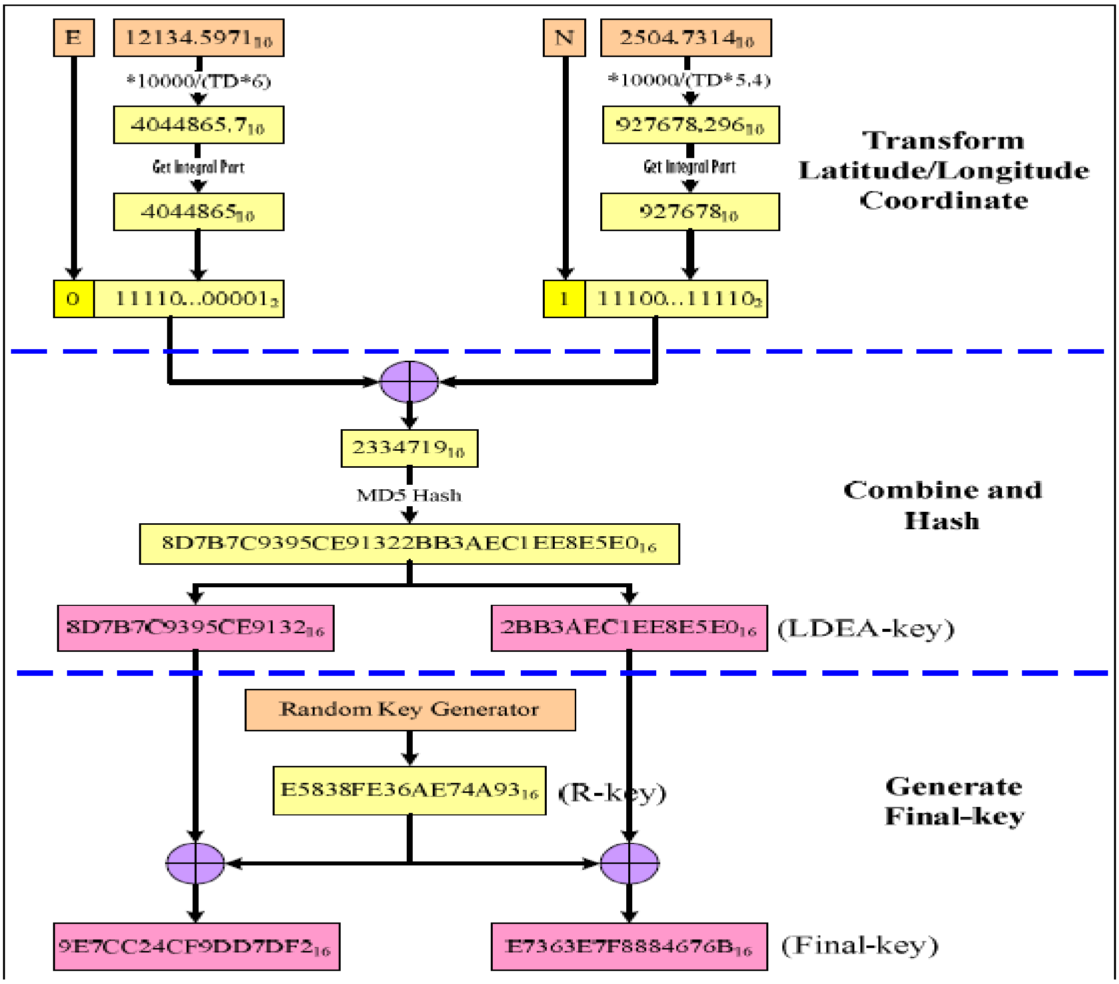

Figure4.4: An example of the final-key generation

The algorithm followed in implementing the proposed system will be the assimilation of location based encryption (LBE) and distributed authority based encryption (DABE)

Distributed Attribute based encryption: DABE allows an arbitrary number of authorities to independently manage their attributes. There are three different types of entities in a DABE scheme: a master, attribute authorities (AA) and users. The *master* is responsible for the distribution of secret user keys. The further task can independently be performed by the attribute authorities. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute. The Distributed attribute based Encryption (DABE) which is the Extended set of MABE. To encrypt a message, a user first formulates his access policy in the form of a Boolean formula over some attributes, which in our construction is assumed to be in Disjunctive Normal Form (DNF). The party finally uses the public keys corresponding to the attributes occurring in the policy to encrypt.
The algorithm followed in implementing the proposed system will be the assimilation of location based encryption (LBE) and distributed authority based encryption (DABE)

Encryption

1. A random session key KeySec is generated.
2. The message is symmetrically encrypted under KeySec, producing ciphertext CT1.
3. The location lock value is computed from the selected location area L and key KLL.
4. KeySec is XORed with the location lock value, generating a hybrid key KeyHyb.

5. *Setup:* The *Setup* algorithm chooses a bilinear group G of order *p* and a pairing *e* : G1 × G2 → G*T* . Next it chooses a generator $g \in$ G, a random point $P \in$ G and a random exponent $y \in Zp$. The public key of the system is PK = {G, G*T*, *e*, *g*, *P*, $e(g, g)^{y}$}, while the secret master key is given by MK = g^{y}
6. *CreateUser* (PK,MK, *u*)*:* The algorithm *CreateUser* chooses a secret mku $\in Zp$ and outputs the public key PK*u* := g^{mku} and the private key SK*u* := MK ･ P^{mku} = g^{y} . P^{mku} for user *u*.
7. *CreateAuthority* (PK, *a*). The algorithm *CreateAuthority* chooses uniformly and randomly a hash function *Hxa* : {0, 1}∗ → Z*p* from a finite family of hash functions, which we model as random oracles. It returns as secret key the index of the hash function SK*a* := *xa*.
8. *RequestAttributePK* (PK,*A*, SK*a*). If *A* is handled by the attribute authority *a* (i.e., *aA* = *a*), *RequestAttributePK* returns the public attribute key of *A*, which consists of two parts:PK*A*:= <PK*'A* := $G^{HSKa\ (A)}$, PK*''A* := $e(g, g)^{yHSKa\ (A)}$ >.This public key can be requested from the attribute authority by anyone, but *RequestAttributePK* can only be executed by the respective authority, because it requires the index of the hash function SK*a* as input.
9. *RequestAttributeSK*(PK,*A*, SK*a*, *u*,PK*u*). After determining that the attribute *A* is handled by *a* (i.e., a_A = *a*), the authority tests whether user *u* is eligible for the attribute *A*. If this is not the case, *RequestAttributeSK* returns NULL, else it outputs the secret attribute key SK*A*,*u* := $\mathrm{PK}u^{HSKa\ (A)}$ = $g^{\mathrm{mku}\ HSKa\ (A)}$.Note that the recipient *u* can check the validity of this secret key by testing if *e*(SK*u*,PK'*A*) = PK''*A* ･ *e*(*P*, SK*A*,,*u*) .
10. *Encrypt*(PK,*M*,A,PK*A*1, . . . ,PK*AN*). A policy in DNF can be written as: A=$\bigvee_{j=1}^{n}\left(\bigwedge_{A\epsilon s j} A\right)$ where *n* (not pairwise disjoint) sets *S*1, . . . , *Sn* denote attributes that occur in the *j*-th conjunction of A. The encryption algorithm gets repetitive over all *j* = 1, . . . , *n*,generates for each conjunction a random value $Rj \in Zp$ and constructs CT*j* as

$$\begin{aligned} \mathrm{CT}_j = < \mathrm{E}_{j\,:} &= \mathrm{M}.(\textstyle\prod_{A\in Sj} \mathrm{PK}''A\,)^{Rj}, \\ \mathrm{E}'_j &:= \mathrm{P}^{R,\,j}, \\ \mathrm{E}''_j &:= (\textstyle\prod_{A\in Sj} \mathrm{PK}'A)^{Rj} > \end{aligned}$$

11. KeyHyb is concatenated with an encoded location area L, producing the string L||KeyHyb. This string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT2. [12]

Decryption

1) After reception of CT = CT1||CT2, the recipient R tries to decipher CT2 using their private attribute set {A}R. On successful decryption, the location area L and KeyH are recovered.
2) *Decrypt*(PK,CT,A, SK*u*, SK*A*1,*u*, . . . , SK*AN*,*u*). To decrypt a ciphertext CT, *Decrypt* first checks whether any conjunction of A can be satisfied by the given attributes, i.e., whether the input SK*A*1,*u*, . . . , SK*AN*,*u* contains secret keys for all attributes occurring in a set *Sj* for some 1 ≤ *j* ≤ *n*. If this is not the case, the algorithm outputs NULL, otherwise

$$\mathbf{M} = \mathbf{E}_{j}\,.\,\frac{e(E'j,\prod_{i\in Sj} SKi,u)}{e(E''j,SKu)}$$

It is easy to see that the decryption is correct. Let *aj* := Σ *A*∈*Sj* $H_{\mathrm{SK}aA}$ (*A*).
Then $Ej = M\,.e(g, g)^{yajRj}$, *E''j* = *c* and

$$\mathbf{E}_{j}\,.\,\frac{e(E'j,\prod_{i\in Sj} SKi,u)}{e(E''j,SKu)} = \mathrm{M}.\ e(g,g)^{ya_j R_j}\,.\,\frac{e(P^{Rj},g^{mk_u\,aj})}{e(g^{ajRj},g^{y}.P^{mku})}$$

$$M.\ e(g,g)^{ya_j R_j}\,.\,\frac{e(g,P)^{Rj\ mku\ aj}}{e(g,P)^{Rj\ mku\ aj}.e(g,g)^{yajRj}} = M.$$

1. R's current GPS position PR is computed by means of a tamper-resistant GPS receiver and verified to be within the location area L. On success, the location lock value is computed, taking L and key KLL as input parameters.
2. The location lock value is then processed by exclusive OR with the recovered KeyHyb, in order to reconstruct KeySec.
3. KeySec is used to symmetrically decrypt CT1 to M

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption, in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321 V 334, 2007

[2] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 121–130.

[3] M. Chase, Multi-authority attribute based encryption," in *Proceedings of the Theory of Cryptography Conference*, pp. 515{534, 2007.

[4] Melissa Chase. Multi-authority Attribute Based Encryption. In *TCC*, volume 4392 of *LNCS*, pages 515–534. Springer, 2007.

[5] A. Sahai and B. Waters, \Fuzzy identity based encryption," *Advances in Cryptology V EUROCRYPT*, vol. 3494 of LNCS, pp. 457{473, 2005.

[6] B. Waters, \Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Public Key Cryptography V PKC*, vol. 6571 of LNCS, pp. 53-70, 2011.

[7] D. Boneh and M. Franklin. "Identity based encryption from the weil pairing". In *CRYPTO*,pages 213-229, 2001.

[8] A. Lewko and B.Waters. "New techniques for dual system encryption and fully secure hibe with short ciphertexts". In *TCC*, pages 455-579, 2010.

[9] Sascha Müller, Stefan Katzenbeisser, and Claudia Eckert, "On Multi-authority ciphertext-policy attribute-based encryption In:*Bulletin of the Korean Mathematical Society* 46,no.4 pages803-819, 2009

[10] Li, Keying, and Hua Ma. "Outsourcing Decryption of Multi-Authority ABE ciphertexts", In: *IJ Network Security* 16.4: 252-260, 2014

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute Based Encryption for Fine Grained Access Conrol of Encrypted Data". In *ACMconference on Computer and Communications Security*, pages 89-98, 2006.

[12] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. "Building efficient fully collusion resilient traitor tracing and revocation schemes". In *ACM Conference on Computer and Communications Security*, pages 121-130, 2010.

[13] Boneh, D.: A brief look at pairings based cryptography. In: FOCS, pp. 19–26. IEEE Computer Society, Los Alamitos (2007)

[14] A. Beimel, *Secure schemes for secret sharing and key distribution*, Ph. D. thesis, Dept. of Computer Science, Technion, 1996.

[15] R. Canetti, S. Halevi, and J. Katz. *A Forward-Secure Public-Key Encryption Scheme*. In Advances in Cryptology, Eurocrypt, volume 2656 of LNCS. Springer, 2003