ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

Customer Survey Associated With Characteristic Dependent Encryption Approaches

Ansari Tasin Habib Ahmad[1], Koul Rahul[2], Kunal Waghela[3]

M.e Computer, New Panvel, Maharashtra, India[1,2,3]

ABSTRACT— Inside cryptography, attributes is commonly very helpful to be able to successfully and firmly encrypt the data. This modern by using attributes enables you to improve the classic techniques associated with info revealing that is by making use of honest mediated computers. Most of these attributes have been exploited to get the general public important and possess already been utilised while user's admittance plan to be able to minimize the actual user's admittance. Access plan can be even more inlayed directly into devices through two various strategies. (1) This Key-Policy. (2) This Cipher Text-Policy. This Key-policy can be admittance framework on the user's personal important as well as the cipher text-policy will be the admittance framework on the cipher wording. Every single plan need certain admittance framework exactly where framework itself can be even more grouped while Monotonic Framework (Only binary 'AND 'and 'OR' binary gates can be employed) and Non Monotonic Framework (includes all popular features of monotonic constructions properties along with privilege pertaining to the employment of DEFINITELY NOT gates). Applying ABE strategies offers the huge benefits: (1) lessening associated with Verbal exchanges over head on the web. (2)Providing the actual Great Access Management. Within this document we tried to do the actual study associated with ABE that features Characteristic based encryption, key-policy, Cipher Text-Policy, Numerous Specialist ABE, hierarchical ABE. Featuring some interesting features. Various Evaluation variables are viewed to be able to map this specific techniques in line with their features.

KEYWORDS- Key-Policy, Cipher Text-Policy, Non Monotonic Framework, ABE and encryption.

I. INTRODUCTION

Web technology keeps growing everyday and people need to store, talk about in addition to process their own info through the use of their own ability. So quite a bit regarding storage space center is important, leading to be able to just about the most trending techniques for useful storage space in addition to collection regarding info we. age Foriegn Storage (Cloud Computing) later got Large Facts, Hadoop and many others. Such storage space support application men and women can purchase this providers on the cloud manager and may along personal this storage space support as a result this tends to reduce the price in addition to will need regarding big storage space Equipment. It also possesses certain troubles that your Foriegn Owner must face plus it must be resolved. The dog owner should provide

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

certain common accessibility coverage that may let users to be able to monotonically accessibility this kept info, these kind of accessibility plans must be versatile, in addition to scalable so that only authorized consumer can accessibility the precise necessary info. Other than privacy the info must be encrypted just before storing about like storage space providers therefore involves a variety of encrypting strategies in addition to the variety of tactics get their own root base in public important encryption. With traditional Public-key encryption strategies, public-key is employed to be able to encrypt, this simply wording whereas non-public important needs to decrypt this cipher-text but so as to encrypt this meaning, this sender should accessibility the general public important certificate. Expressing strategies just a party overburden this calculation in the server given that we will need to encrypt exactly the same meaning for every single person person. Shamir throughout 1979 demonstrated the thinking behind solution sharing when a solution Debbie is divided in to okay portions (known while (k, n) tolerance scheme) in ways that understanding of almost any okay and up portions can simply restore solution Debbie; but understanding of almost any k-1 or even a lesser number of portions will always make renovation infeasible. With 1984, Shamir introduced a story cryptographic plan termed Identity-Based Encryption (IBE), [5] allowing almost any pair of users to be able to converse safely and securely without exchanging general public important or even non-public important. Alternatively, this meaning is encrypted in line with the recipient's one of a kind identity, like a IP address. At this point, only the user while using the corresponding identity can decrypt this meaning. With not a important change, the chance regarding important direct exposure is reduced. With subsequent work, Goyal, Pandey, Sahai, in addition to Waters further cleared up the idea of Attribute-Based Encryption. For example, they will proposed a pair of supporting sorts of ABE. Within the 1st, Key-Policy ABE, capabilities are utilized to be able to annotate this cipher scrolls in addition to formulations of these capabilities usually are related to be able to users' solution recommendations. The 2nd sort, Cipher text-Policy ABE, is supporting as capabilities are utilized to describe this user's experience as well as the formulations of these experience usually are attached with this cipher wording because of the encrypting bash. Also, Goyal et 's. provided a development for Key-Policy ABE which was really expressive as it authorized this plans (attached to be able to keys) to become expressed by simply almost any monotonic formulation over encrypted info. The device has been shown selectively protected under the Bilinear Diffie-Hellman supposition. Even so, they will remaining generating expressive Cipher wording Insurance policy ABE strategies being an open dilemma. To fulfil the requirements regarding much larger level corporations which might be that will outsource info storage space, CP-ABE still requirements further refinement.

II. LITERATURE SURVEY

Within this chapter all of us illustrate the applicable novels questionnaire that utilizes various procedures for distinct cryptographic Programs. Recommender programs or perhaps professional recommendation programs really are a subclass connected with data selection method that seek out in order to predict the 'rating' or perhaps 'preference' that a person would certainly share with something. Recommender programs are usually resources for hinting that items to customers. They often possess some form of customization, attempting to find things that the actual person will like.

1. Attribute based encryption (ABE):

A characteristic primarily based encryption scheme presented through Sahai, and Rich waters throughout 2005 plus the objective is to provide stability and access handle. Attribute-based encryption (ABE) is usually a public-key primarily

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

based anyone to many encryptions that enables customers in order to encrypt and decrypt information based on person qualities. That secret-key of any person plus the ciphertext are usually structured on qualities (e. h. the country your lover lifestyles, or perhaps the kind of registration your lover has). Ordinary method, the decryption of any ciphertext can be performed as long as the number of qualities from the person crucial suits the qualities from the ciphertext. Decryption is only achievable when the amount of related is in minimum a new threshold worth d. Collusion-resistance is important stability characteristic connected with Attribute-Based Encryption. A foe that keeps several important factors ought to just have the capacity to access information if a minimum of one individual crucial scholarships access.

2. Key Policy Attribute Based Encryption (KP-ABE):

It does not take revised type of established type of ABE. Consumers are usually assigned with the access shrub framework over the information qualities. Tolerance entrances would be the nodes from the access shrub, the qualities are usually associated through leaf nodes in order to echo the access shrub Framework the key crucial from the person will be described. Cipher texts are usually labelled having models connected with qualities and private important factors are usually related to monotonic access set ups that handle that cipher texts a new person will be able to decrypt.

3. Cipher Text Policy Attribute Based Encryption (CP-ABE)

Inside a CP-ABE scheme, each and every cipher text will be related to an access insurance plan with qualities, and each and every user's private crucial will be associated with a number of qualities. A new person will be able to decrypt a new cipher text as long as the number of qualities from the user's private crucial complies with the access insurance plan from the cipher text. CP-ABE operates from the opposite way of KP-ABE. Your access framework with this scheme or perhaps formula, it inherits the identical technique which has been utilized in KP-ABE to develop [1]. And the access framework internal the encrypted information can allow encrypted information opt for that crucial can recuperate your data, it means the wearer's crucial having qualities simply complies with the access framework from the encrypted information.

4. Multi-Authority attribute-based Encryption

Sahai and water's process cantered mostly within the one characteristic encryption for encryption and decryption. Therefore negatives throughout one specialist scheme

1)All the qualities from the method will be maintained by the one specialist; Failing or perhaps file corruption connected with one Expert may freeze lower the full method thus creating one specialist additional liable to the harmful customers.

2) One more issue would be the "key Escrow" Problem. Important escrow (also known as a new "fair" cryptosystem) is definitely an arrangement when the important factors necessary to decrypt encrypted information are usually used throughout escrow making sure that, beneath specific circumstances, an authorized vacation may obtain people important factors. These types of next functions might include companies, who might wish use of employees' private devices, or perhaps health systems, who might want in order to watch the material connected with encrypted devices

5. Hierarchical attribute-based Encryption (HABE)

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

This particular scheme Hierarchical attribute-based encryption (HABE) is derived through Wang et 's Your HABE type (Fig 1. HABE) consists of a main get good at (RM) that corresponds towards the next honest get together (TTP), several area experts (DMs) when the top-level DMs correspond to several venture customers, and many customers that correspond to many staff within an venture. This particular scheme utilised the house connected with hierarchical creation connected with important factors throughout HIBE scheme to come up with important factors.

III. PROBLEM DEFINITION

The main limitations associated with credit dependent encryption process may be the complexities interested in working out if your adjustable associated with polynomial exceeds to the higher range. This specific cryptographic approaches adjustments the entire strategy associated with encryption as well as decryption. This method by itself has the modern cold start out issue, overspecialization as well as serendipity. These are get over by means of applying hierarchical credit. Although important escrow is still this issue for your research workers and also the approaches to take on this kind of problems inspires in order to develop brand new approaches in the field of cryptography.

The intention of this survey is really as practices:

1. To analyse this encryption approaches which often provide this Individuality in the individual as well as determine his or her limitations that might help in order to advise a lot better strategy which may overcomes this cons present approaches.
2. To recognise approach to element extraction intended for encrypting process to help keep this safety associated with hard drive App as well as collaborative blocking that might help individual in order to strongly keep this reliable home elevators machines.
3. To recognize examination stage would be to advise this relative review of each one approaches determined by personality dependent encryption as well as offered this opinionated the best possible answer.

IV. PROPOSED WORK

1 Attribute Based Encryption

In Attribute based encryption access Policy of algorithm is associated with Private Key of user where leaf nodes are attributes coming from fuzzy identity. The attribute based key policy encryption setup algorithm generates Alice's master key. Alice's identity is being decided by key policy which in turn is being decided from identity. Key Policy algorithm generates private key for Alice. Charisma encrypt message M with set of attributes k. Priyanka can decrypt M if her key policy is satisfied with K. Alice can decrypt M if her key policy is satisfied with k. For Example Alice can decrypt the file encrypted with set of attributes {"Information Technology", "Admission Committee"}.But Alice cannot decrypt the cipher text associated with attributes {"Information technology", "Program"} .The difference between key policy and cipher text policy attribute based encryption is, in key policy attribute based encryption access policy depends on private key and in cipher text policy attribute based encryption access policy depends on cipher text. The Hierarchical attribute based encryption is a combination of hierarchical identity based encryption and cipher text policy attributes based encryption. The Hierarchical attribute based encryption is classified into trees according to their relationship defined in the access control system. For example employee database access control depends on

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

hierarchical attribute based encryption. According to concept of hierarchical attribute based encryption manager has privilege to access the entire data in the company. Team leader has privilege to access the employee's details and his own data in the company. Employee has privilege to access his own data in the company.

Notation	Signification
G_x	The bilinear group of prime order p, $x = 1, 2$
g	A generator of G_1
A_U	Attributes of data user U in private key
A_{CT}	Attributes with the encrypted data CT
A_{U-KP}	The access structure in user's private key
A_{CT-CP}	The access structure in the encrypted data
A_{CT-HA}	The DNF access control policy in the encrypted data
$\widetilde{A_U}$	The non-monotonic access structure in user's private key
D	User's private key
M	The message

Tab: 4. 1 Implementation Notations

2. Key-Policy Attribute Based Encryption KP_ABE

If attributes of the encrypted data can satisfy the access structure in user's private key *D*, an user can obtain the message through decrypt algorithm. In addition, the KeyGen() algorithm is different from the attribute-based encryption. The user's private key is according to the access structure to generate. In this algorithm, it adopts secret sharing and chooses a polynomial *qx* such that *qx*(0) = *qparent*(*x*)(*index*(*x*)), (Note that *parent*(*x*) is *x*'s parent node, and *index*(*x*) is the number associated with node *x* that is given by *x*'s parent node.) in a top-down manner which is to start from the root node *r* for each node *x* in the access structure. So *qr*(0) is equal to the master key *y*, and the master key *y* is distributed among the user's private key component *Di* which is corresponding to the leaf node (Note that the leaf node represents attribute).

Since the KeyGen() algorithm is different, the Decrypt() algorithm also be different. It use attributes of encrypted data to run decrypt node function in the decryption algorithm. And it can input encrypted data, user's private key, and nodes of the access structure in user's private key; it adopts bottom-up manner in the access structure and recursive manner to decrypt the encrypted data. Beside, this scheme divides nodes of the access structure into the equal the leaf nodes. Finally, it will get a bilinear formula and use polynomial interpolation to get the message. For example, the encrypted data with attributes are {MIS Λ student} and user's private key with access structure is an user's private key, and then user can get the message. In this scheme, there are four algorithms to be executed: Setup, KeyGen, Encrypt, and Decrypt. And the parameters described in this scheme and parameters of the ABE scheme are the same. It will be depicted as follows.

1) Setup(*d*): The authority chooses several uniform and random numbers *t*1, ..., *tn*, *y* from *Zq*, and makes public the public key, $PK = (T1 = gt1 \ldots\ldots, Tn = g^{tn}; Y = e(g, g)^{y})$. And keeps the master key, $MK = (t1, \ldots, tn; y)$ be secret.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

2) KeyGen (*AU-KP; PK; MK*): The authority generates private key components for each leaf node *x* in the access structure. The private key components are *Dx* = , where *i* is equal to a leaf node in the access structure. These components will be merged into the user's private key, and be sent to an user.

Encrypt (*M, A_{CT}, PK*): Data owner chooses a random number *s* from *Zq* and encrypts a message *M* ϵ *G*2 with a set of attributes A_{CT}, and then he generates the encrypted data as

$CT = (A_{CT}, E = MY^{s} = e(g; g)^{ys}; Ei = g^{tis} g \ \forall \ I \in A_{CT})$.

Decrypt (*CT; D*): This algorithm can be executed by a recursive algorithm, It inputs the encrypted data, user's private key, and nodes of the access structure in user's private key. If *i* is equal to the leaf node, and *i* is in the access structure of user's private key, it will call the decrypt node function, $e(Dx; Ei) = e(g; g)^{s.qx(0)}$. If *i* is not in the access structure of an user's private key, it will call the decrypt node function; and it outputs invalid. If *i* is not equal to the leaf node, it will call decrypt node function and input all children nodes of node *x*, *z*, and use Lagrange coefficient to compute to obtain $e(g; g)^{s.qx(0)}$. Finally, the decryption algorithm call the decrypt node function on the root of the access structure and compute $e(g; g)^{ys} = Y^{s}$, if and only if the encrypted data satisfies the access structure of private key. And the message $M = \frac{E}{y^{s}}$ can be obtained.

3. Ciphertext-Policy Attribute-based Encryption Scheme

The access control method of this scheme is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access policy is in user's private key, but the access policy is switched to the encrypted data in ciphertext policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message. For example, the access structure in the encrypted data is

1) Setup: The authority chooses two random numbers α, β from *Zq* as exponents, and generates the public key, PK=(G_0,g,h=g^{β},$F = g^{\frac{1}{\beta}}$,e(g,g)$^{\alpha}$) The master key is $MK = (\beta, g^{\alpha})$

2) KeyGen (*Mk,AU*): The authority chooses a random number *s* from *Zq*, and random *sj* for each attribute *j* in a set of attributes in user's private key. The user's private key $D = (Dk = \frac{(\alpha+s)}{\beta}, \forall j \in Au : D_j = g^{s}.H(j)^{sj}, D_j^{*} = g_j^{s})$ is output.

3) Encrypt(*PK,M,ACT-CP*): Data owner executes this algorithm to encrypt the message *M* with the access structure *ACT-CP* . Choose a random number *y* ϵ *Zq*, set *qr*(0) = *y*, where *r* is the root node, and let *I* be the set of leaf nodes in *ACT-CP* . The message is encrypted with access structure $A_{CT\text{-}CP}$, and then outputs the encrypted data,

$CT = A_{CT-CP}, \check{C} = Me(g,g)^{\alpha y})$, C=$h^{y}$, $\forall I : C_i = g^{q i(0)}, C_i^{*} = H(att(i))^{q i(0)}$

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

4) Delegate(*D; ÃU*): This algorithm takes the user's private key *D* and a set of attributes whose each attribute is in *AU* to create a new user's private key Ď.

5) Decrypt(*CT;D*): When data user receives the encrypted data, he can execute this algorithm. The user's private key *D* and the encrypted data are input in this algorithm and the recursive function, and decrypt node is called.

4. MULTI Authority-ABE

As a first thought, we might simply have many copies of SW, one for each authority. We want to require that a user be able to decrypt a ciphertext only if he has at least d of the specified attributes from each of the K authorities. Recall that the SW scheme centers around finding enough polynomial shares $e(g, g)^{p(i)s}$ to reconstruct the secret $e(g, g)^{p(0)s} = e(g, g)^{ys}$ which has been used to blind the message. (Recall that the encryption includes $E = e(g, g)^{ys}m$). Now, if we want each authority to give out its own polynomials, one simple solution might be to do an additive secret sharing to form the SW secrets (i.e. the values y such that every random polynomial p is chosen with p(0) = y). Thus, we pick a random value for the master secret y0 and for each authority k = 1 . . .K, yk is a share of y0 so Σyk = y0.We can output $e(g, g)^{y0}$ as the entire system's public key. Then to encrypt message m, a user gives $E = e(g, g)^{y0s}m$ and $Ek,i = T^{s}_{k,i}$ for all i, k where they wish to allow a decryptor to use attribute i from authority k. To decypt, the user has to perform SW decryption for each authority and find $Y_k^s = e(g,g)^{Yk,s}$, then multiply the results together to get $\Pi_{k=1}^{K} Y_k^s = \Pi_{k=1}^{K} e(g,g)^{Yk,s} = e(g,g)^{s\Sigma_{k=1}^{K} Yk} = e(g,g)^{Y_0 S}$ and thus obtain m. However, if a user does not have enough of the required attributes from one Authority Ќ, then the SW secret for that authority: $Y_{\acute{K}} = e(g,g)^{Y_{\acute{K}} s}$ will remain indistinguishable from random and thus so will $e (g, g)^{y0s}$ and m. Multi Authority Scheme is as follows:

System

Init First fix y1 . . . yk, {tk,i}i=1...n,k=1...K ← Zq. Let $Y_0=\sum_{k=1}^{K} Yk$.

System Public Key $Y0 = e(g, g)^{y0}$.

Attribute Authority k

Authority Secret Key The SW secret key: yk, tk,1 . . . tk,n.

Authority Public Key Tk,i from the SW public key: Tk,1 . . . Tk,n where $Tk,i = g^{tk,i}$

Secret Key for User *u* from authority *k* Choose random d − 1 degree polynomial p with p(0) = yk.

Secret Key: $\{ Dk,i = g^{p(i)/t_{k,i}} \}$I ϵ A_u

Encryption for attribute set AC Choose random s ← Zq. Encryption: $E = Y_0^s m, \{E_{k,i} = T_{k,i}^s\} i \in A_c^k, \forall k.$

Decryption: For each authority k, for d attributes $i \in A_C^k \cap A_u$ compute $e(Ek,i,Dk,i) = e(g, g)^{p(i)s}$.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

Interpolate to find $Y_s^k = e(g,g)^{p(0)s} = e(g,g)^{Y_k s}$. Combine these values to obtain $\prod_{k=1}^{K} Y_K^s = Y_0^s$ Then $m = {}^{Y}/_{Y_0^s}$

There is a problem with the scheme as described above: Suppose an encryptor encrypts a message to the attribute set A_C which includes attributes A_C^k for each authority k. Now suppose we have a set of K users where each user k has attribute set $A_u = A_C^k$ from authority k, but no attributes from any other authority. Recall that we want to allow decryption only if the decryptor has enough of the required attributes from every one of the authorities. However, if the scheme is as described above, this set of users will be able to collude: Each user k will use his attribute set to find the SW secret for authority k: $Y_k^s = e(g,g)^{yk^s}$ Then the users combine these values to obtain $\prod_{k=1}^{K} Y_K^s = \prod_{k=1}^{K} e(g,g)^{yk^s} = e(g,g)^{Y0^s} = Y_0^s$ and thus m.

5. Hybrid ABE:

HABE is the novel combination of CABE and LBE where LBE is the location Based encryption the hybrid encryption scheme are derived from the underlying CP-ABE and LBE concepts. For brevity of presentation, we only consider the following two authorities and entities explicitly in our setting:

1) *Attribute authority AA*: the AA is responsible for creating the private credentials (attributes) used for decryption. Especially, it issues a private attribute set $\{A\}_R$ to every possible recipient.

2) Recipient R: this entity receives encrypted messages on her communication device. The device is initialized for decryption with the recipient's private attribute set $\{A\}_R$ and KLL, the key for the location lock function. Also, the device has a tamper-resistant GPS receiver that is leveraged in the following schemes.

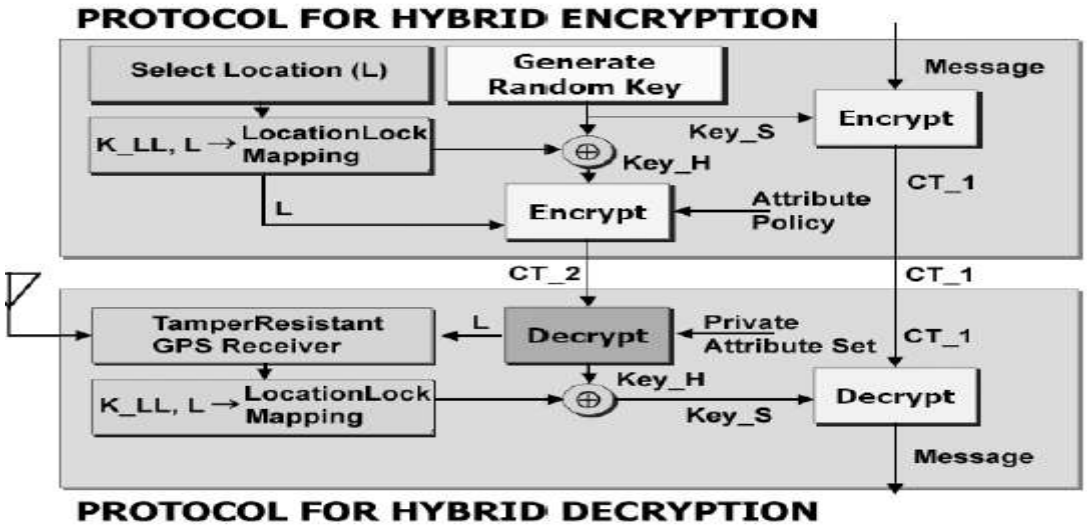

Fig 4.5 overview of hybrid ABE

1. A random session key Keys is generated.

2. The message is symmetrically encrypted under Keys, producing ciphertext CT1.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

3. The location lock value is computed from the selected location area L and key K_{LL}.

4. Keys is XORed with the location lock value, generating a hybrid key Key_H.

5. Key_H is concatenated with an encoding of the location area L, producing the String L || Key_H. This string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT2

6. CT1 concatenated with CT2 represent the ciphertext CT. CT is transferred to a receiver R.

Protocol for Hybrid Decryption: The protocol for hybrid decryption works as follows

1. After reception of CT = CT1 || CT2, receiver R tries to decrypt CT2, using his private attribute set $\{A\}_R$. On successful decryption, the location area L and KeyH are recovered.

2. R's current GPS position PR is computed by means of a tamper-resistant GPS receiver and verified to be inside the location area L. On success, the location lock value is computed, taking L and key KLL as input parameters.

3. The location lock value is then XORed with the recovered KeyH, in order to reconstruct KeyS.

4. KeyS is used to symmetrically decrypt CT1 to M.

V.CONCLUSION

In this Papers, the research associated with distinct Cryptographic approaches according to identity primarily based encryption is actually shown. The various approaches for example critical plan credit primarily based encryption, cipher text-policy primarily based ABE, Multi-Authority Centered ABE, and a mix of both Centered ABE, we can end which utilizing a mix of both technique which usually also affords the revocation plan together with scalable encryption strategy would likely give greater exactness, effectiveness which usually reduce the overhead encrypting and decrypting occasion effects.. The relative examine of various approaches stated earlier is actually shown on this record. Diverse evaluate boundaries such as Effectiveness, Scalability, Collusion Resistance and Great grained Entry handle are explained. The research shows that many enhancement can be done with processes for obtaining greater effects.

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] G.Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.