International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Elliptic Curve based Collaborative Group Key Management for Cloud Data Sharing in Ciphertext Policy Attribute based Encryption

R. Mohan Naik, S.V. Sathyanarayana, T.K. Sowmya

Abstract--- Ciphertext policy attribute based encryption (CP-ABE) is one of cryptographic procedure that coordinates data information encryption with authenticated admission management for guaranteeing data information security in Cloud. The cloud computing where the application administrations using the Internet. In numerous applications, especially in Group Communication in cloud data information offering to various clients data information proprietors require to conceal undisclosed data information like encryption key. The effective key management system conventions are essential for giving security to this data information. Since, it is extremely difficult to provide security to group's secret data information particularly with various mechanisms of assurance. The effectiveness issue of CP-ABE is as yet accessible that corrupt the computation overhead on the grounds that bilinear pairing is exorbitant in such huge numbers of utilizations of ABE, so by supplanting the bilinear pairing utilized in the attribute coordinating with straightforward scalar multiplication on Elliptic Curves, accordingly diminishing the general computation just as communication overhead. And plan another key dispersion can considered in order to legitimately renounce a client or a characteristic without refreshing the other clients' keys during the property repudiation phase. By utilizing the Shamir's Threshold secret sharing designs access structure to develop the expressiveness of the entrance arrangement. Security and execution examination demonstrate that in this plan improving the general effectiveness just as guarantee the security of the cloud data information.

Index Terms--- Key Management, Access control, Elliptic Curve, CP-ABE.

1. INTRODUCTION

Cloud computing gives its buyers simplicity of utilizing the cloud based usages and stumpy hardware necessities at customer side. Data information possibly be put away or gotten to through client whenever, anyplace with the cloud utilizing internet. The cryptographic key gives the wellbeing yet it's difficult to open one without the correct blend. Additionally, in the event with correct key, it is extremrely simply to decrypt the encrypted data information; however decrypting it is contradictory without this key. Also, the keys that are used for the purpose of encrypting data information should be managed cautiously. The Efficient Key management gives all the computation and treatment of keys cautiously enough to guarantee that it ought not to get convinced. Cloud clients and suppliers need to secure the data information and just as secret keys against misfortune and theft [1].

Sahai and Waters [2] tackled the Key management issue by proposing another cryptographic procedure called attribute-based encryption (ABE). A data information proprietor can determine right of entry to the data information as a Boolean arrangement above numerous characteristics. Everybody in the ABE framework will be given a private key that speaks to his features from an expert. Nobody can easily decrypt the ciphertext except if the features related with his isolated key fulfill the Boolean equation described to the ciphertext. Bethencourt et al., then formulated another sort of ABE in which client private keys are determined with a lot of features and the data information proprietor can indicate a progressively sensitive access strategy over these characteristics, called CP-ABE.

For example client means to give access to his biomed-ical information and medical healing record with applicable physicians. (Chief Doctor ^ Internal Medicine)^ (Hospital P _ Hospital Q). In along these lines, the client could imply his protection of information have to just be comprehended by only concerned specialist of inner drug prescription from hospital X or in hospital Y. The Attribute Based Encryption splendidly consolidates information encryption process and access mechanism [3], however productivity issue is as still an issue restricting its advancement. In the bilinear pairing is viewed as the higher most costly task as well as time consuming task contrasted and scalar multiplication in pairing protocols approach [4]. Here in this paper the the process of mathematical calculation of bilinear combination is a few phases are more as compared to scalar multiplication in an equivalent Elliptic Curve. Henceforth, to diminish the process of mathematical calculation of bilinear pairing beyond what many would consider possible is an approach to basically improve the productivity of ABE. The principle commitment of the proposed strategy for improving the productivity is abridged as pursues:

1) For improving the effectiveness of ABE algorithms. In view of CP-ABE, an entrance control conspires for cloud data sharing which no longer needs any bilinear pairing which is entangled. The proposed plan can be progressively viable and realistic.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
R. Mohan Naik, Asst. Professor, Dept of ECE, SDMIT, Ujire (D.K). (e-mail: m.naik5785@gmail.com)
Dr.S.V. Sathyanarayana, Professor, Dept of ECE, JNNCE, Shimoga. (e-mail : svs@jnnce.ac.in)
T.K. Sowmya, Asst. Professor, Dept of ECE, SDMIT, Ujire (D.K). (e-mail: k.sowmya.02@gmail.com)

2) A better approach for key dissemination that every data client's secret keys are produced and it will be kept up by the property expert alongside a quality list. By along these lines legitimately renounce a client or a property without refreshing other clients' keys. It significantly diminishes the computation and correspondence overhead brought about by quality renouncement.

3) By utilizing SSS scheme access structural arrangement to improve the expressiveness of the entrance approach. Given a detailed security and execution examination of this plan and resultant demonstrate the effectiveness of this approach.

The paper organized as pursues: Related work is condensed in Section II, trailed by primers in Section III. The complte development of the proposed plan for Cloud framework is given in Section IV. Segment V and segment VI introduced the security and execution investigation individually. The paper closes with end in Section VII.

2. RELATED WORK

In 2007, Ling and Newport [5] displayed a CP-ABE approach supports AND entryway right of entry arrangement on mutually positive and negative characteristics. Lewko and Waters [6] elaborated a multi-specialist CP-ABE conspire without the requirement of the collabo-proportion among the attributes experts. In view of the tractability, Horvath [7] elaborated the multi expert CP-ABE plot, to understand identity dependence repudiation. Hur [8] elaborated a CP-ABE conspire which provides straight re-occupation on the characteristic arrangement of every user. Guofeng [9] solved the key escrow issue in CP-ABE schemes just as improved the quality expressiveness. Guo elaborated a CP-ABE conspire with consistent size keys, and the quantity of the decryption key is free of quality number. In any case, CP-ABE plans are computationally concentrated, which incorporate various pairing tasks and exponentiations. Secure Key Management (SKM) in the Cloud dependent on the secret sharing plan has been considered [11]. By presenting an innovative strategy for verifying cloud by giving multicast key to every client. It will provide dynamic session key where change over the period of time. At whatever point another client into the cloud, the new-fangled key will be created [12]. After the period the client will recharge the key for the following use of the cloud. Ensuring Data Privacy and Security by using Secret Sharing [13]. Here the real security difficulties is the cloud supplier required to guarantee that the framework is satisfactorily secure, and to avoid illicit record information gets to from outcasts, different customers, or may be the unapproved cloud representatives. Public Key Infrastructure dependent cryptography for secure cloud data storage by using the ECC [14] addresses the security related aspects and delicate data information and provides a PKI-based cryptography plot for cloud storage. Security in data forwarding using the Elliptic curve cryptography (ECC) in cloud [15]. A safe cloud storage framework that supports data information sending capacity utilizing ECC and it cautions to data information proprietor as a when assailant attempts to adjust the data information or any misbehavior and framework provides staggered security.

Two strategies ECDH key trade and symmetric key algorithm for encryption and decryption [16]. ECC and ECDH method gives similar dimension of security cryptosystems models with a smaller key size and reinforces the safety of the algorithm.

To streamline the ECC conventions, Freeman et al. [17] describes the pairing-friendly elliptic curves and presents the developments of them streamlining thought strategies.

In [18], Scott examined the methods of choosing the pairings and the curves for better effectiveness in productivity of ABE plans. Rivain additionally portrays regarding the procedure of executing scalar multiplication quicker in ECC conspires in depth. To basically streamline ABE algorithms, here is to supplant entangled bilinear pairings with other increasingly productive number-crunching tasks. Odelu and Das elobarates a CP-ABE conspire with consistent sized secret keys dependent on ECC, however it just backings AND entryway access structural arrangement, which restricts its adaptability. In this way, in light of RSA, they likewise formulated an innovative CP-ABE plot with steady size keys and ciphertexts. In spite of the fact the time intricacy of the encryption and decryption are both O (1), it just backings AND entryway access structural arrangement.

3. PRELIMINARY

Access Structure: Considering $\{A_1,A_2\ldots A_n\}$ be a set of properties. A accumulation $S \subseteq 2^{\{A_1.A_2..A_n\}}$ is monotone just on the off chance that $\forall$ B,C: in the event that B $\in$S and B $\subseteq$ C at that point C $\in$S. An entrance structural arrangement is a gathering S of nonempty subsets of $\{A_1,A_2\ldots A_n\}$i.e. S $\in^{\{A}1^{A}2^{\cdots A}n\}$ / $\{\phi\}$. The sets in S allude to the approved sets. Else, they are known as unapproved sets. In case of ABE framework, the entrance structural arrangement demands that a qualified client ought to have the relating characteristics in it. Consider a scenario, a Boolean equation A ^ B ^ (C _ D) speaks to that individual person who is capable of decrypting the ciphertext must have traits A, B, C or A, B, D. moreover, it can be communicated in an increasingly intelligible manner, similar to an entrance tree, as appeared in Fig.1. And [22] demonstrated that whichever monotonic right of entry structural arrangement can be changed over into a Linear Secret Sharing Scheme portrayal by standard techniques. There by utilizing the LSSS strategy so as to speak to regarding Shamirs mystery sharing plan technique for

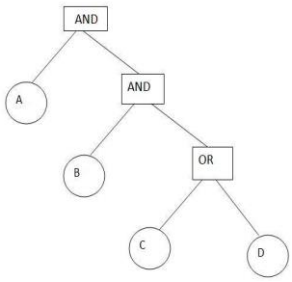


Fig. 1: Access structure

A. Shamir's secret sharing

Before going into the Shamir's Secret Sharing (SSS) let us know about the Linear SSS (LSSS).

LSSS

LSSS is intended for the purpose of relating exceptionally expressive monotone right of entry structures in CP-ABE schemes. A secret sharing plan over a lot of parties is called direct if.

1. A vector over Z_p is created by the shares for each party.
2. A matrix A with n lines and l sections is intended to produce the shares. For i ∈ {1….n} each column i is marked by the capacity to make it partner with one of the parties. Let s ∈ Z_p be the secret to be shared. A column vector v = (s,r_2…r_l) picks s as its first component, and randomly picks the rest r_2…r_l ∈ Z_p. Then A * v turns the vector of n shares of the secret s. The share (A * v) i has a place with the party ρ (i). If a direct secret sharing scheme is defined as above, it also satisfies the direct recreation property. To be explicit, let S ∈ A be any approved set, where A is the entrance access structure, and let L be the relating set of row number {i : ρ (i) ∈ S} Then, there must exist constants term is {c_i ∈ Z_p} i∈ I: with the end goal that if {λ_i} are the shares of the secret s, the secret can be recuperated by computing $\sum_{i\in L} c_i \lambda_i = s$.
3. Definition: Secret Sharing Scheme is a process that divides a given secret shares such that only specific subset of shares allow reconstruction of the original secret".

All the more for the most part, it is a couple of algorithm (Share, Rec), in which,

a) Share(S,n) is a kind of sharing scheme that on accepting secret S as input, and outputs a collection of n shares (s_1,s_2...s_n);
b) Rec(s_{i1},s_{i2}...s_{it}), t ≤ n is a reconstruction scheme that outputs a secret S in case if shares are approved other-wise stops..

The arrangement of shares associated with recreation is eluded as qualified shares. The arrangement of the complete certified set of shares will be tended to as Access Structure. The access structure will be called as monotone in case as set is additionally approved. In the event that a group of clients recuperate the mystery, at that point the all-inclusive group will likewise have the option to recoup the mystery.

In Secret sharing plan, believed seller parts and dis-tributes the offers to every one of the parties with the goal that solitary qualified parties can recoup the first mystery data information. The security of the plan is estimated dependent on how it offers it gives data about secret.

a) Completely secret sharing has three phases
b) Initialization Phase: During this time, condition of the plan and essentials like input and key space are characterized.
c) Share Generation and Distribution Phase: during this time, Key sharing scheme is characterized. Typically believed vendor performs share age process, at that point produced offers are circulated to each part through a verified channel.
d) Reconstruction Phase: At point of this stage characterizes key recovery formulas and methodology. Utilizing these characterized formulas, secret is restructured from an approved arrangement of offers.

Secret sharing plans are fundamentally partitioned into two classes dependent on access structure.

Standard Secret sharing Scheme: This plan, get to process includes every one of the offers. At this stage, it completely offers the required for secret reconstruction stage. Secret won't be retrieved when there is no collaboration from every one of the clients. This plan is meant as(n,n)- secret sharing plan. The common square graph is as appeared in Figure 2

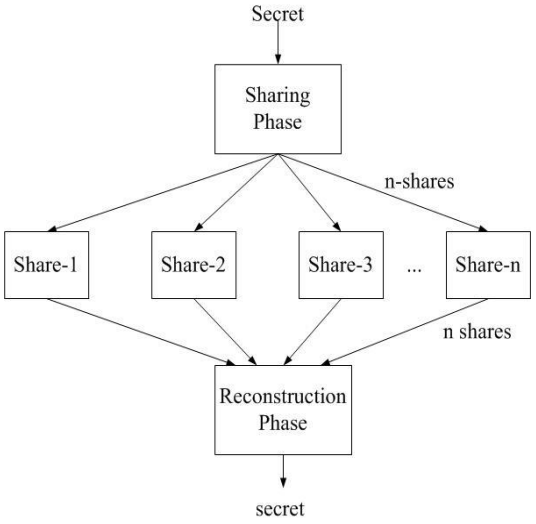


Fig. 2: Conventional secret sharing Scheme

b) Threshold Secret sharing Scheme: according to this scheme, get to structure includes the entire set with boundary in any event t, 2 t n. Also, any t or more offers are sufficient for the reason of reconstruction of the secret, inspite of reason that the shares with not as much as t won't uncover any secret. This plan is meant by (t,n) secret sharing plan. The general square chart is as appeared in Figure 9

Secret sharing Scheme is said to be a Homomorphic scheme on the off chance that it is conceivable to create new offers from existing shares. SSS scheme is an ideal secret sharing scheme in light of the fact that, unapproved subset of members gets no data about the secret information.

B. Mathematical Foundations

Polynomial Evaluations for share Generation. The idea of Shamir's scheme is conceptually simple. The secret data is expressed as constant term of random polynomial of degree (K-1). Then the polynomial is evaluated at 'n' distinct points. Polynomial evaluation starts with considering polynomial f(x) over commutative ring R.

$$f(x) = f_0 + f_1x + \ldots\ldots + f_{k-1}x^{k-1} \quad (1)$$

Polynomial f(x) is evaluated on a specified vector a = [a_1. a_2….a_n] 2 R^n. Polynomial evaluation mapping is defined as

$$eval(f) := R[x] \rightarrow R^n \quad (2)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

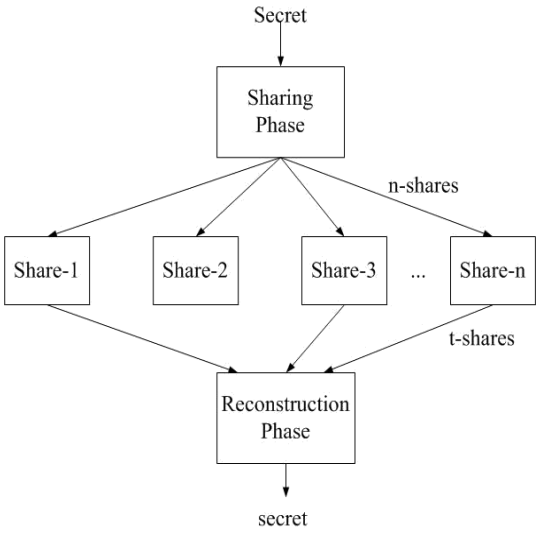


Fig. 3: Threshold Secret Sharing scheme

The result as a vector is provided as follows:

$$eval(f) := [f(a_0)\ldots.f(a_n)]^T \qquad (3)$$

Assessment of Polynomial over limited field has became consideration in numerous down to earth applications. Consider, provided enormous prime number P, it is obtained $F_P := [0, 1\ldots.P- 1]$ and regard activities like expansion and multi-plication over FP performed modulo P.

For the purpose of assessing polynomial coefficients for Polynomial and vector for polynomial assessment are considered from the field F_P. At that point the components of the subsequent vector are from field F_P. In case of Shamir's Scheme Polynomial assessment is done over huge prime field P.

Polynomial Reconstruction

Countless polynomial assessment and re-development plans might be utilized by any sift old individuals for the purpose of recovering the mutual secret information. Lagrange's introduction equation is an effective rebuilding technique. Lagrange's interpolation assumes a significant job covertly remaking period of (k,n) edge secret sharing plan. This formula was distributed by Lagrange in the year 1795. Interpolation Property: Given k sets of (i, f(i)), with i's everything unmistakable, there is novel polynomial f(X) of degree k-1, going through every one of the focuses.

The Lagrange interpolation procedure the equation utilized in polynomial development that goes with k focuses $(x_0; y_0),\ldots(x_{k-1}; y_{k-1})$. In order to develop a polynomial of degree n going with k focuses, a set of basis polynomial $L_j(x_i)$ are constructed.

$$L_j(x_i)= \prod_{J=1, j\neq 1}^{k} \frac{x-x_j}{x_i-x_j} \qquad (4)$$

where $L_j(x_i)=\{$ 1 when j = i and 0 when j≠I ….(5)

$(K-1)^{th}$ degree Lagrange's interpolation polynomial is given as

$$f(x)=\sum_{i=1}^{k} y_i \prod_{J=1, j\neq 1}^{k} \frac{x-x_j}{x_i-x_j} \ldots(6)$$

$$f(x)=\sum_{i=1}^{k} y_i L_j(x_i) \qquad \ldots\ldots. (7)$$

$$f(x)= \begin{aligned} &[\, y_1 \frac{(x-x_2)}{(x_1-x_2)} \frac{(x-x_2)}{(x_1-x_3)} \frac{(x-x_2)}{(x_1-x_k)} + \\ &y_2 \frac{(x-x_2)}{(x_2-x_1)} \frac{(x-x_2)}{(x_2-x_3)} \frac{(x-x_2)}{(x_2-x_k)} \ldots + \\ &y_2 \frac{(x-x_2)}{(x_k-x_2)} \frac{(x-x_2)}{(x_k-x_3)} \frac{(x-x_2)}{(x_k-x_{k-1})} \,] \end{aligned} \qquad (8)$$

When the premise capacities are built, at that point we obtain $(K-1)^{th}$ degree Lagrange's insertion polynomial x value represents customer and y value characterizes the relating share value.

C. Algorithm

Considering the SSS the Scheme having two stages, Share generation stage and Share reconstruction stage. Algorithm 1 portrays the procedure of first stage. Algorithm 2 depicts the procedure of reconstruction of secret utilizing Lagrange's Interpolation polynomial.

Algorithm 1: Share generation

Input: Prime field P, Secret data information S∈ P, Users n, Threshold k

Output: Allocated Shares $s_1.s_2..s_n$

Set c_0=S

Arbitrarily chooses polynomial constants $c_1, c_2\ldots c_{k-1} \in P$

Fabricates a secret polynomial $f(x)=c_0+c_1x+\ldots+c_{k-1}x^{k-1} \bmod P$

Compute shares with the assistance of constructed polynomial $s_i=f(i)$ for $1\leq i \leq n$.

s_i: Generated Shares

Algorithm 2: Secret Recontruction

Input: Prime field P, Shares $s_{t1}\ldots s_{tk}\in P$, where($t_j \in 1,\ldots n$)

Output: Secret data information S

Use Lagrange's Interpolation for the purpose fo discovering distinctive polynomial Reconstruct secret, S=f(0) mod P

Share generation and obscure reconstruction process by taking an example. Share generation is performed over a prime field P by using modular arithmetic operations. Let us consider the following inputs for Share Generation Phase.

Inputs

Prime Field, P=60077.

Secret, S=4834.

Number of Users, n=6.

Threshold, k=3.

Polynomial coefficients, a_0=S, a_1=157, a_2=203. Share Generation

Using coefficients, Trusted Dealer constructs a Polynomial f(x). Where,

$$f(x) = 4834 + 157x + 203x^2 \bmod P \quad (9)$$

On Substituting, x=1,2,...n., It generates Shares as fallows

$s_1 = f(1) = 5194$
$s_2 = f(2) = 5960$
$s_3 = f(3) = 7132$
$s_4 = f(4) = 8710$
$s_5 = f(5) = 10694$
$s_6 = f(6) = 13084$

Generated Shares are: (1, 5194), (2, 5960), (3, 7132), (4, 8710), (5, 10694), (6, 13084).

These shares are circulated to every one of the individuals through a verified communication channel.

Secret Reconstruction

Trusted Dealer reconstructs the Secret by using threshold shares.

Shares for reconstruction are: [s_1, s_3, s_4] Reconstruction is done using Lagrange's Interpolation formula given in Equation7. Inputs for interpolation is as fallows,

x=[1 3 4] (Indicates User).

y=[5194 7132 8710 (Indicates Share).

Expanding and solving Lagrange's Interpolation formula.

The framework is created by using the help of algorithm [23], here input is an admission tree representing the monotone Boolean approach. Where representing the non-leaf nodes on the tree are either AND OR door and the leaf nodes are denoting the attributes. Here by noticing that, the output is a LSSS matrix and the amount of rows of the matrix is accurately representing to the measure of leaf nodes on the input access tree. On the off chance that the parent node is named by OR entryway with a vector v, the algorithm labels both child nodes as v and keeps the counter c unaltered;

when parent node is represented by an AND door with a vector v, the algorithm cushions v with subsequent value at the end to change its length to c, then the algorithm labels its right child node with the vector v ovreall generated shares are assigned to values of the respective weighed attribute.

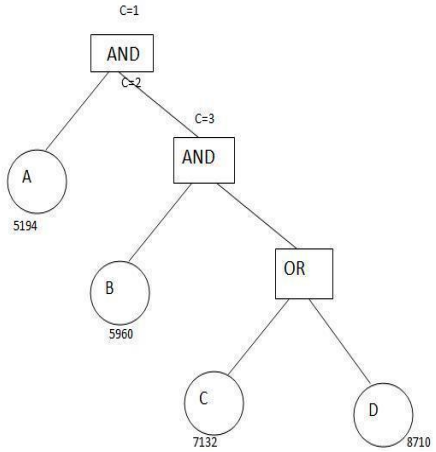


Fig. 4: Label of Access structure for generated share equivalent attributes

5194 = (1) = A
5960 = (2) = B
7132 = (3) = C
8710 = (4)= D

Maps every row of the matrix to attributes A, B, C and D individually. Given a characteristic set S, the LSSS is considered to be fulfilled by S just when the rows of the matrix tagged by the attributes in S integrate the vector in their limit.

D. Elliptic Curve Cryptography (ECC)

Elliptic Curve Systems which are connected in numerous Cryptographic applications were presented in 1985 individually by Neal Koblitz and Victor mill operator [22]. ECC is a difficult framework created to furnish extreme security with little key size. ECC is institutionalized by IEEE and detailed in IEEE P1363 std [23].

Elliptic Curves are simple capacities which can be framed as smooth circling lines in (x,y) plane. When all is said in done, cubic condition for this curve can be given by utilizing Generalized Weierstrass condition as provided in the following equation (10)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (10)$$

In which a_1; a_2; a_3; a_4; a_5; a_6 2 F_p and p is a prime number. Condition 10 of Elliptic Curve over F_q is a lot of arrangements (x; y) F_p together with exceptional point o, called point at infinity. In the event that normal for field is not one or the other '2' nor '3' at that point Equation 10 can be composed as

These curves are basic limits which can be drawn as smooth hovering lines in (x,y) plane. At the point when all is said in done, cubic condition for Elliptic Curve can be provided with the assistance of Generalized Weierstrass condition as provided in Equation (10)

$$E : y^2 = x^3 + Ax + B(11)$$

We by and large use Equation 11 for some applications, together with discriminant condition provided by Equation 12

$$4a^3 + 27b^2 \neq 0 \quad (12)$$

Elliptic Curves over prime field are exploited for the purpose of carrying out Secret Sharing.

E. Elliptic Curves over GF (P)

An elliptic curve characterized over Prime Field Z_P is acquired by choosing the factors a and b from the field Z_P. The elliptic curve includes the entire points (x,y) which accomplish the elliptic curve condition modulo p (in which x and y has a place with Z_P).

Elliptic curve over prime field is provided in the following Equation 13.

$$y^2 \bmod p = (x^3 + ax + b) \bmod p(13)$$

Addition and multiplication procedure in an elliptic curve group over Prime field is given as pursues. Give the focuses a chance to be P = (x_1; y_1) and Q = (x_2; y_2) in the elliptic group E_p(a; b) and O indicates the point at infinity. During the event that Q 6= P, their aggregate P + Q = (x_3; y_3) is provided in the following equation:

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$
$$y_3 = \lambda (x_1 - x_3) - y_1 \bmod p$$

Where $\lambda = \{y_2 - y_1/x_2 - x_1, 3x_1^2 + \alpha/2y_1$ if p=q and p.

The multiplication kP is acquired by reiterating the elliptic curve expansion job k times by a similar expansion equation. The scalar point multiplication over A can be described as kP = P + P +.... +P (k times).

During the case that P; Q 2 A, the expansion P + Q is a point R. The line going through P and Q catches the curve at a point known as R. The reflection of - R will be R about the x-axis[24]. This is indicated as point expansion as exposed in Figure 9.

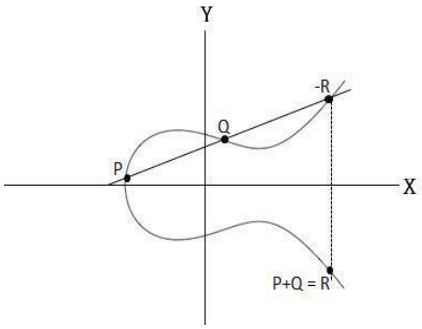


Fig. 5: Point Addition

F. Elliptic Curve Encryption/Decryption

Assume client A needs to send message P_m to client B then client an arbitrarily elects a positive number k, private key d_A. The open key of A is fabricated as $P_A = d_A G$ and the cipher text C_m is produced with consisting of pair of points.

$$C_m = (kG, P_m) + kP_B$$

Where G is the base point selected on the elliptic curve, $P_B = d_B G$ is the public key of B and d_B is the private key of B.

A will send the cipher text C_m as encrypted message to B. To decrypt the cipher text, B multiplies the first point in the pair by its private key d_B and subtracts the result from the second point to get the original message P_m [15].

$$P_m + kP_B - d_B(kG) = P_m + k(d_B G) - d_B(kG) = P_m$$

G. Actual Model and Security Model

1. Actual Model

Cipher text policy Attriute based encryption will be considered by using of five major steps u: System Setup, Authority Setup, Key Generation, Encryption and Decryption, as characterized beneath.

Framework Setup (k) → P. The framework setup algorithm takes a security parameter k as input and afterward outputs the majority of the essential public parameters (PP) for the framework.

Authority Setup (PP) → P K; SK. In light of the PP produced in the initial step, the attribute and gives the public keys (PK) and secret keys (SK).

The Key Generation (PP, i, ID, SK) →$SK_{i;ID}$ The key generation scheme make use of the public parameters, a attribute i, A temperament ID, and the SK of the distinctive expert as input. It provides an attribute secret key → $SK_{i;ID}$ in accordance with a ID and provides to clients.

Encryption (PP,M,(A, ρ),{pk_i} → CT Provided a message M, an entrance matrix (A,) and the public keys of the typical encryption method and gives ciphertext CT.

Decryption (PP, CT, {$SK_{i,GID}$ } → M Considering a gathering of secret keys controlled by an direct client accomplish the entrance matrix of the ciphertext, the decryption process will give prominently recover the message M.

Proposed strategy principally comprise of four substances: CSP, trait specialist, data information proprietor and data information user, as depicted in Fig.6

The Attribute Authority. The main confided in element in the framework other than data information client. It is having charge of issuing and denying clients' characteristics as per their jobs or personalities in the framework. The secret key of each attribute is created by it and the involving public key is distributed to the majority of the clients. Every client was bound with a Global Identity (ID), with which to enlist in the framework. An attribute rundown of every client is additionally kept up by the attribute authority. In the period of decryption, the attribute expert will tell the data information client with fragment of the decryption.

Cloud Service Provider. The CSP is a fair however curious element. As same as characterized in different plans, it will

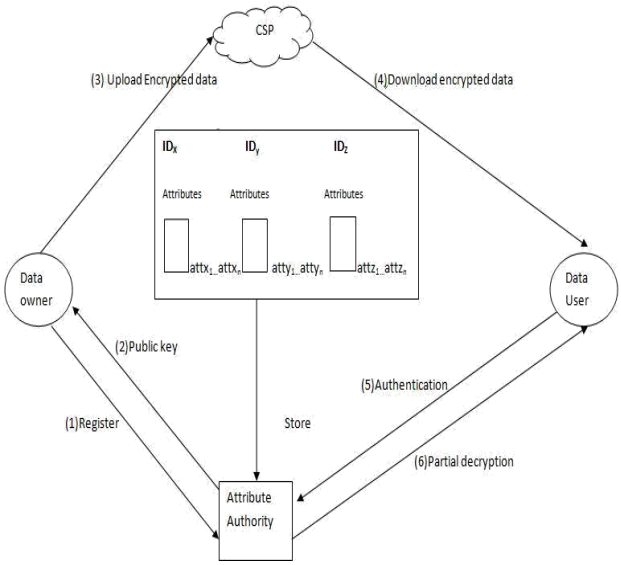


Fig. 6: System Model

Work in exacting understanding with the convention however might be interested to form ciphertexts. The CSP can collect the encrypted data information more willingly than the data information administrator and give data information right of entry administration later. They will characterizes the entrance control arrangement over attributes in the framework and under which completely encrypt before re-allocate it to the cloud.

Just the client, with enough attributes satisfying the entrance arrangement, can ready to completely decrypt the ciphertexts.

Data information User. The data information client can request the entrance to the encrypted data information put away in the CSP. Just if there is an arrangement of attribute similarity among the data information client and the entrance approach can the ciphertext will be effectively decrypted. The information client are not completely trusted as they may connive with one another, determined by interests, to completely decrypt the ciphertext which none of them can easily decrypt autonomously.

2. Security Model

The security model will prepare the access control policy. It is classified among challenger and a challenger Initialization.

The challenger initially picks a test access structure (A,) and later sends it to the challenger. In Setup process produces the essential public parameters compulsory for the framework just as the public and secret key pair for every attribute. The challenger imparts the public keys to the challenger.

Phase 1. The challenger cans follows inquiry for the attribute secret keys with the process of the keys cannot decrypt ciphertext.

Challenge Phase. The opponent chooses two equivalent length messages M_0, M_1 belongs to P and submits them to the challenger.

4. PROPOSED SCHEME

The proposed Elliptic cruve CP-ABE plot for efficient and secure data information sharing, For elobaration of the scheme by replacing bilinear pairing with the fundamental scalar increase on elliptic curves. Firstly encrypting the message M with sG, in which G is a generator of a cyclic subsection of an elliptic curve with request r, and s is an asymmetrically picked an incentive in Z_r Subsequently the encryption scheme parts the value s into offers $_x$ according to the LSSS matrix, and a value 0 is part into shares w_x similarly. In order to recover the message M, the data information consumer required to merge his attribute keys with the ciphertext to get the term sG. In request to counteract intrigue assaults, each attribute having a place with a specific client will be bound with a worldwide character. by along these lines, diverse client's attributes can't be effectively consolidated. This process gives the new content $H(ID)w_xnG$, where nG represents the public key of the attribute specialist. On the off chance that the data information client has a wonderful arrangement of keys with an equivalent character factor, these repetitive terms will be drop from the last results, as w_x are offers of 0. On the off chance that two clients with various characters mean to connive with one another, The structure $H(ID)w_xnG$ which is not be dispensed with. So, this will leads in a dissatisfaction of the recovery of sG, just as the message M. EC-CP-ABE will give the following stages :

Setup. Consider GF(q) represents a limited field of request q, E be an elliptic curve over GF(q) and G denoting a component of an prime request r in E. The point G generates a cyclic subgroup of E, here the elliptic curve discrete logarithm problem (EC-DLP) is determined. During extension, a hash work $H:\{(0, 1)\}^* \rightarrow Z_r^*$ is mapped ID to modules of Z_r..

The Authority Setup. The attribute expert picks an irregular number n Zr as its main secret key and dispenses nG exploited as its public key. Here in all the term of the process the attribute authority chooses arbitrary number $k_i \epsilon$ Z_r. All i in the framework, the attribute expert chooses randoml number $k_i \epsilon$ Z_r.

Key Generation. In order to generate a key of a attribute i for a particular consumer with ID, the attribute professional can figures Sk_i, $ID=k_i +H(ID)n$, and record this attribute i on its relating attribute list. The encryption algorithm comprising of the accompanying stages:

The plaintext message is right off the bat plotted against a point M on the elliptic curve E. It prefers an arbitrary $s \epsilon Z_r$ and figures $C_0 = M + sG$

The encryption scheme take in the entrance model provided by the data information proprietor and subsequent to the outputs an n×l acquire to matrix A with mapping its rows to features.

It prefers an arbitrary vector $v\epsilon Z_r^l$ with 0 as its initial segment is furthermore picked and let w_x means $A_x \times u$.

The ciphertext is computed as $C_{1;x}= \lambda_x G+w_x$

$$pK\ \rho_{(x)}, C_{2,x}= w_x G, \forall x$$

Decryption In order to decrypt the ciphertext, it is essential that the data information client primarily determine a fantastic prearrangement of rows A_x of attributes. By means of submitting ID with $(C_{2;x}, \rho(x))$ of each one such x.

The expert will checks its personality and whether it possesses these attributes as indicated by its attribute list. On the off chance that the solicitation is legitimate, for each $(C_{2;x}, (x))$, the authority calculates:

$= \sum C_{2;x}\ SK_{\rho(x)}, ID$

$= \sum (W_x G(K_{\rho(x)}+H(ID)n)$

$= \sum (W_x(K_{(x)}G+(w_xH(ID)nG).$

At that point the attribute expert transmits the results to the data information consumer in a safeguarded channel. Along with the assistance of the outcome, the data information consumer can figure out,

$= \sum c_{1,x}\text{-}c_{2,x}\ ^{SK}{}_{\rho(x)}, ID$

$= \sum (\lambda_X G - w_x H(ID)nG)$

$= \sum \lambda_X G + w_x P K_{\rho(X)} - \sum (W_x(K_{\rho(x)}G+(w_xH(ID)nG).$

for all such x. The data user then selects constants $c_x \in Z_r$ such that

$\sum c_x A_x=(1,0,..0)$ and computes

$\sum (c_x(\ \lambda_x G - w_x H(ID)nG)) = sG$

Finally, the data user can just compute $C_0 - sG = M$.

Attribute Revocation. It is of EC-CP-ABE plan gives the clients secrete key are produced and kept up by the attribute expert, which make it conceivable to legitimately denying a client or a attribute deprived of refreshing different clients keys during the attribute revocation stage. In order to revoke a client, the credit expert requires wiping away its attribute accessible i.e by means of associating to its specific ID. With the intention of revoking an attribute, the attribute expert requires wiping away the public key of this attribute. With the aim of revoking an attribute requested by a client, the attribute expert requires wiping away this attribute from its attribute list.

5. PERFORMANCE ANALYSIS

In this area examining the capacity overhead on the attribute specialist, every client and the cloud server independently in depth.

Attribute Authority.

It must be observed that the attribute authority is in charge of generating, distributing and revoking the attribute keys for the entire clients in its particular framework. All the same time, all the data regarding the attributes, the attribute authority requires to accumulate an attribute list for each client in the structure.

Every User. Here, there is no prerequisite for clients to accumulate their secret keys in neighboring as these keys are generated and kept up as attribute list by the attribute. Henceforth, every client needs just accumulate the public constraints in vicinity for any supplementary encryption.

Server. Every single ciphertext includes of three sections and is linear to the amount of the attributes exploited in the encryption from now on, the capacity overhead on the server is completely reduced.

Communication Overhead In this plan, the attribute authority possible would modify the attribute list of the one to be revoked for the purpose of finishing the attribute revocation without manipulating others in the framework. So decline the general communication overhead.

Computation Overhead

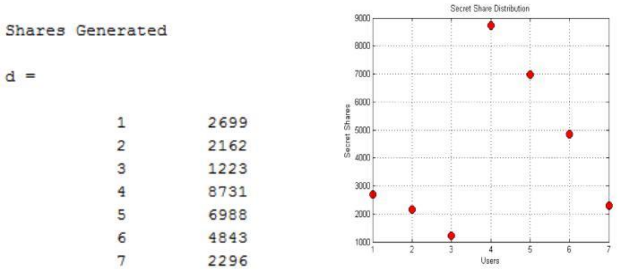
It appears that costs the slightest in encryption and decryption as its computation overhead is unrestricted of the quantity of attributes. In any case, the tradeoff is just backings AND door right of entry structure which is deficient to deal with the fine-grained right of entry control. Furthermore, it exploits RSA as its cryptography crude whose essential key length, in any event 2048 bits, is excessively long for skill obliged tools.

Shamir's SSS right of entry structure and the computation overhead is conforming to the amount of attributes employed in encryption which is the share value generated in this approach.

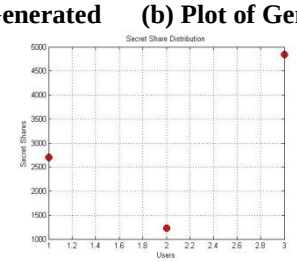
6. RESULTS AND ANALYSIS

According to discussed Algorithm1 and Algorithm2, Threshold based Shamir Secret Sharing scheme is implemented for different input key space. The coefficients for the share generating polynomial are randomly chosen from the given prime field. Following are the some of the results obtained using MATLAB 7.0 tool.

Figure7 shows the result of Shamir's scheme for a given input conditions. Users, n=7. Threshold, K=3. Prime field,P=8849. Secret, S=2834. Figure7(a) shows the generated shares for a given conditions. Figure7(b) shows the scattered plot of the generated shares. Figure7(c) shows the selected shares for reconstructing the shared secret using Lagrange's interpolation formula.



(a) Shares Generated **(b) Plot of Generated Shares**



(c) Shares for recovery

Fig. 7: Secret Sharing over Field GF (8849)

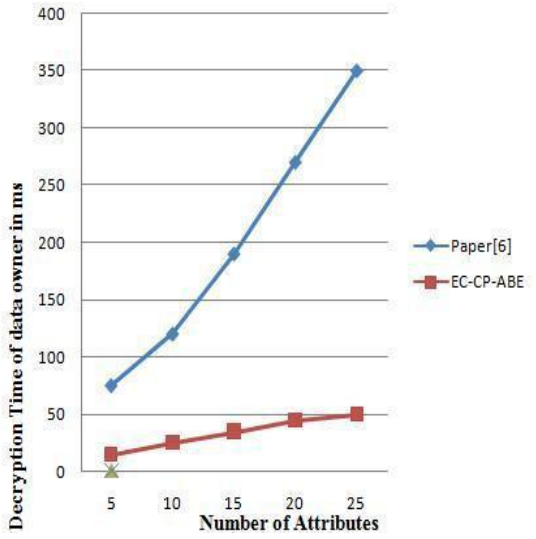


Fig. 8: Comparisons of Decryption time

Finally on observing the results, We can say that their is a linearity among the generated shares, Which proves that Shamir's Scheme is an linear approach.

For EC-CP-ABE choosing subgroup G_{p2}, G_{p3} in their convention are just used to apply the double framework encryption system for security proof. And executing EC-CP-ABE with Intel Processor at 2.60GHz and 2GB RAM. The scheme simulates in Ubuntu Linux 16.04LTS. Considering the pbc library (version 0.5.14), the execution uses a 160-bit elliptic curve group in accordance with the

Super singular curve $y^2 = (x^3 + x)$ over a 512-bit restricted field for the purpose of obtaining good security model.

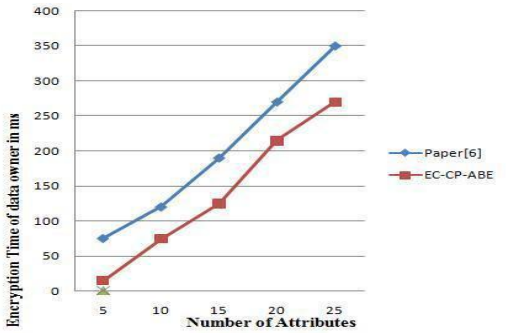


Fig. 9: Comparisons of Encryption time

7. CONCLUSION

Here, a novel effective CP-ABE access control scheme is formulated for the purpose of data information sharing in the environment of cloud data sharing, called EC-CP-ABE. It is to be noted that, by replacing bilinear pairing by means of fundamental scalar multiplication on elliptic curves, which effects in essentially diminishing the common overhead for users. Also, another method is designed for key conveyance, so the framework can legitimately revoke a client or an attribute without refreshing different client's keys. In this plan embraced expressive Shamir's SSS access structure for the purpose of fulfilling diverse access control requires in many applications.

REFERENCES

1. Mohan Naik R and Dr.S V Sathyanarayana, "Key management infrastructure in cloud computing environment-a survey" ACCENTS Transactions on Information Security, Vol 2(7) 2017, Page no 52-61.
2. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. 2005, pp. 457-473.
3. Shulan Wang and Kaitai Liang and Joseph K. Liu, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY VOL. 11, NO. 8, AUGUST 2016.
4. SHENG DING and CHEN LI and AND HUI LI," A Novel Efficient Pairing-Free CP-ABE Based on Elliptic Curve Cryptography for IoT " SPECIAL SECTION ON SECURITY AND TRUSTED COMPUTING FOR INDUSTRIAL INTERNET OF THINGS IEEE ACCESS, June 5, 2018.
5. C. Ling and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 456-465.
6. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol.-EUROCRYPT, Tallinn, Estonia, 2011, pp. 568-588.
7. M. Horvath, "Attribute-based encryption optimized for cloud computing," Infocommun. J., vol. 7, no. 2, pp. 1-9, 2015.
8. J. Hur, "Improving security and effciency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271-2282, Oct. 2013.
9. GUOFENG LIN and HANSHU HONG and ZHIXIN SUNF, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing," IEEE Access, June 28, 2017.
10. J. L. Beuchat, and S. Mitsunari, and E. Okamoto, and T. Teruya, "High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves," in Proc. Int. Conf. Pairing-Based Cryptogr., 2010, pp. 21-39.
11. Ivan Damgrd and Thomas P. Jakobsen, "Secure Key Management in the Cloud", 14th IMA International Conference on Cryptography and Coding, 2013,
12. K.Sriprasadh, Saicharansrinivasan, "A novel method to secure cloud computing through multicast key management", 2014.
13. Ching-Nung Yang and Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", International Symposium on Biometrics and Security Technologies, 2013, IEEE.
14. XiaoChun Yin and ZengGuang Liu, "PKI-Based Cryptography for Secure Cloud Data Storage Using ECC", ICTC 2014, 194-199, May, IEEE.
15. S.V.Divya and Dr.R.S.Shaji, "Security in Data Forwarding Through Elliptic Curve Cryptography in Cloud", International Conference on Con-trol, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, 1083-1088, feb, IEEE.
16. Shilpi Singh and Vinod Kumar, "Secured Users Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography", 2015,791-795,IEEE.
17. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," J.Cryptol., vol. 23, no. 2, pp. 224-280, 2010.
18. M. Scott, "On the efficient implementation of pairing-based protocols," in Proc. IMA Int. Conf. Cryptogr. Coding, 2011, pp. 296-308.
19. A. Beimel, "Secure schemes for secret sharing and key distribution," Fac. Comput. Sci., Technion-Israel Inst. Technol., Haifa, Israel, 1996.
20. A. Lewko and B. Waters, "Decentralizing attribute-based encryp-tion," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryp-tol.EUROCRYPT, Tallinn, Estonia, 2011, pp. 568-588.
21. Shalini I S, Mohan Naik R, and Dr.S V Sathyanarayana, "A Com-parative Analysis of Secret Sharing Schemes with Special Reference to Group Communication Applications", IEEE International Conference on Emerging Research in Electronics and computor sceince and Technology (ICERECT-2015). December 2015.
22. Koblitz N, "Elliptic Curve Cryptosystem", Journal of mathematics computation, Vol. 48, No. 177, pp203- 209, 1987.
23. Miller, V, "Use of elliptic curves in cryptography", Proc. of Advances in Cryptology-CRYPTO 85, LNCS, Vol. 218, pp. 417 426, 1985.