International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : 10.32628/CSEIT1952252

Attribute-Based Encryption with Equality Test in Cloud Computing Using Key-Policy

Dr. Gopal Sakarkar[1], Mrunal Prabhakar Rohad[2], Rahul Ashwani Gupta[3]

[1]Assistant Professor, Department of Master of Computer Applications, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India

[23]PG Scholar, Department of Master of Computer Applications, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

The privacy of users should be thought of because the utmost priority in distributed networks. To protect the identities of users, attribute-based encoding (ABE) was presented by Sahai et al. ABE has been wide utilized in several situations, significantly in cloud computing. During this paper, public key encoding with equality check is concatenated with key-policy ABE (KP-ABE) to present KP-ABE with equality test (KP-ABEwET). The projected theme not solely offers ne-grained authorization of cipher texts however additionally protects the identities of users. In contrast to ABE with keyword search, KP-ABEwET will take a look at whether or not the cipher texts encrypted by completely different public keys contain constant data. Moreover, the authorization process of the conferred theme is additional edible than that of Ma et al.'s scheme. Moreover, the projected scheme achieves one-way against chosen-cipher text attack supported the additive Dife Hellman (BDH) assumption. Additionally, a brand new procedure drawback referred to as the twin-decision BDH downside (tDBDH) is proposed during this paper. tDBDH is established to be as laborious because the decisional BDH downside. Finally, for the rest time, the protection model of authorization is provided, and also the security of authorization supported the tDBDH assumption is proved within the random oracle model.

Keywords : Cloud Service, Attribute-Based Encryption, Public Key Encryption, Equality Test, Keyword Search

I. INTRODUCTION

In the current network era, cloud service suppliers provide in - nite space for storing and computing power for users to manage their information. To fancy these services, people and organizations store their non-public information on cloud servers. However, within the case of security breaches, users' non-public information hold on within the cloud is not any longer safe. once users source their information to cloud servers, they expect complete privacy of their information hold on within the cloud. Protective the privacy and information of users has remained a awfully crucial drawback for cloud servers. To avoid any inconvenience, users store their non-public information in encrypted kind.

For ne-grained sharing of encrypted information, Sahai and Waters conferred attribute-based cryptography (ABE) [2]. ABE may be a public key cryptosystem variant that enables users to access secret information supported their attributes. This cryptosystem enriches the property of the cryptography policy and therefore the description of users' rights and it changes from a one-one to one-many situation throughout the encryption and decoding phases. Moreover, it hides the identities of the users in acceptable terms. During a resultant work, Goyal et al. projected key-policy attribute-based cryptography (KP-ABE) in 2006 [18]. The underlying cryptonyms-tem combines the key key and therefore the access structure. Bettencourt et al. projected cipher text-policy attribute-based cryptography (CP-ABE) in 2007 which mixes the cipher text and therefore the access structure. Thereafter, various cryptographers conferred several analyses works supported ABE shortly once its conceptualization, ABE reached prime importance in our existence (for example, in tv payment systems, personal health record sys-teams and then on). Moreover, ABE is additionally being wide incorporate-rated in cloud computing. However, if one needs to check plaintexts adore 2 cipher texts, the key should be wont to decipher the 2 cipher texts. To overcome this drawback, Yang et al. conferred a replacement cryptosystem referred to as public key cryptography with equality take a look at (PKEwET) in 2010. His planned system will take a look at whether or not 2 cipher texts contain constant plaintexts with-out secret writing. However, this theme permits anyone to perform such a check. to beat this defect, Tang created some enhancements to the theme (e.g., PKEET with ne-grained authorization (FGwPKEET), all-or-nothing PKEET (AoNwPKEET) [28] associate degree an extension of FG-PKEwET). In 2015, Ma et al. projected a replacement primitive referred to as PKEwET supporting edible authorization (PKEwET-FA). There area unit four forms of edible authorizations in their theme. To change the certificate management of PKEwET, Ma combined the ideas of PKEwET and identity-based cryptography to gift identity-based cryptography with equality check (IBEET). Recently, in 2017, Wu et al. improved Ma et al.'s theme by reducing the machine time value. To offer additional ne-grained authorization, we have a tendency to propose a replacement primitive known as key-policy attribute-based encoding with equality check (KP-ABEwET). we tend to mix the ideas of PKEwET and KP-ABE. As conferred in suppose that there area unit four users. S and S0 area unit the sets of attributes for encoding, and T and T0 check with the access structures utilized by the coding secret key. S00 denotes the set of attributes of the tester, and T0A is that the access structure used for the authorization of the attribute set of SA0. T0B is that the access structure used for the authorization of the attribute set of SB0. We tend to describe the underlying situation as follows: User one will store his personal information within the cloud and might decode the cipher texts that area unit encrypted by a group of attributes S with T(S) D one. User a pair of will store his personal information within the cloud, however he cannot decode the cipher texts that area unit encrypted by a group of attributes S with T(S) 6D1. User three has the attribute S00, wherever T0A(S00) D one and T0B(S00) D one, and he will perform the check over 2 completely different cipher texts encrypted by attribute SA0 and attribute SB0. User four doesn't have the attribute S00 satisfying T0A(S00) D one and T0B(S00) D one, and he cannot perform the check over 2 completely different cipher texts encrypted by attribute SA0 and attribute SB0.

A. Contribution

This paper presents a replacement primitive known as key-policy attribute-based encoding with equality take a look at (KP-ABEwET). Our objective is to realize a ne-grained authorization of cipher texts. the most technologies in our theme embrace key-policy attribute-based encoding (KP-ABE) [18] and public key encoding with equality check (PKEwET) the most contributions will be summarized as follows:

1) First, we tend to style a replacement theme by combining KP-ABE with PKEwET. Compared with the present PKEwET schemes, our projected theme supports activity the ne-grained take a look at of cipher texts and changes from one-one to one-many for users within the testing algorithmic rule.

2) Our theme will be viewed as associate degree extension of attribute-based encoding with keyword search (ABEwKS). at the side of different aspects, the planned theme permits testing whether or not the cipher texts contain identical data that square measure encrypted by completely different public keys.
3) The projected theme achieves unidirectional against chosen-cipher text attack (OW-CCA) supported the additive Dif e-Hellman (BDH) assumption within the random oracle model.
4) A new process drawback known as the twin-decision additive Dif e-Hellman drawback (tDBDH) is additionally conferred and is established to be as laborious because the DBDH drawback.
5) We give the protection model of authorization and prove the protection of authorization supported the tDBDH assumption within the random oracle model. To the most effective of our data, this work is that the rst to prove the protection of authorization in such a way.

B. Related Work

Deterministic encoding, planned by Bellare et al. [8], is another primitive that supports the equality take a look at on cipher-texts. This primitive was completely studied in several subsequent works [1], [7] however all of them square measure settled algorithms. Conversely, PKEwET could be a probabilistic algorithmic rule that supports the equality take a look at on cipher texts.

PKEwET may be viewed as associate extension of public key encoding with keyword search (PEKS). The construct of PEKS was projected by Boneh et al. [4]. It will perform keyword searches over cipher texts while not decrypting them. Later, many modi male erectile dysfunction schemes of PEKS were projected [6], [9], [11], [12]. to resolve the matter of access management in a very multi-user setting, PEKS was combined with ABE for achieving the applied perspective in cloud computing. In [5], [10], [13], [15], [17], the authors com-binned PKES with KP-ABE. In another works, including [3], [14], [16], the authors combined PKES with CP-ABE whereas incorporating the access structure with the cipher text of the keyword search. Though the results were slightly completely different, none of the works conferred a mechanism to see whether or not 2 {different totally different completely different} cipher texts encrypted by different public keys contain a similar data. to beat this limitation, we tend to gift a good KP-ABEwET mechanism.

C. Organization

The remainder of this paper is organized as follows. In Section two, we have a tendency to introduce connected preliminaries. Section three describes the system and also the security model. Our theme is conferred in Section four. Section five provides the protection proof of our theme and of authorization. In Section half-dozen, the performance evaluations area unit cheese y mentioned. Finally, Section seven presents the final remarks.

II. PRELIMINARIES

In this half, we tend to introduce some basic data, as well as cryptographically assumptions, Shamir's secret sharing theme and access tree, that's utilized during this paper

A. Cryptographic Assumptions

The following section presents the Diamond State nations of linear maps and also the drawback formulation.

De nation 1: linear Maps: Let G1 and G2 be multiplicative teams of prime order letter, e V G1 G1 ! G2 be a linear map, and g be a generator of G1.

linear maps West African ll the subsequent conditions:

(1) Bilinearity: 8g1; g2 a pair of G1 and 8a; b a pair of Zq, we've got e(ga1; gb2) D e(g1; g2)ab.

(2) Non-degeneracy: e(g; g) 6D1.

(3) Computability: 8g1; g2 a pair of G1, we are able to cipher e(g1; g2).

De nation 2: linear Dif e-Hellman (BDH) problem: Let G1 and G2 be increasing teams of prime order letter, e V G1 G1 ! G2 be a linear map, and g be a generator of G1. The BDH drawback is that given a 4-tuple (g; ga; gb; gc), the aim is to cipher e(g; g) abc, wherever a; b; c a pair of Zq.

De nation 3: Diamond Statecisional linear Dif e-Hellman (DBDH) problem: Let G1 and G2 be increasing teams of prime order letter, e V G1 G1 ! G2 be a linear map, and *g* be a generator of G_1. The DBDH problem is to distinguish between the distributions of 5-tuples

$(g; g^a; g^b; g^c; e(g; g)^{abc})$ and $(g; g^a; g^b; g^c; e(g; g)^d)$, where $a; b; c; d 2 Z_q$.

De nation 4: Twin-Decision Bilinear Dif e-Hellman (tDBDH) problem: Let G_1 and G_2 be multiplicative groups of prime order *q*, *e* V G_1 G_1 ! G_2 be a bilinear map, and *g* be a generator of G_1. The tDBDH problem is to In general, the tDBDH problem appears to be weaker than the DBDH problem. However, this problem is in fact as hard as the DBDH problem. (The tDBDH problem is different from the twin bilinear Dif e-Hellman inversion problem that proposed by Chen et al.)

***Theorem 1:** The tDBDH problem is as hard as the DBDH problem. Proof:* It is quite clear that tDBDH DBDH. Next, we present the proof of DBDH tDBDH. To prove DBDH tDBDH, we suppose that there is an algorithm A that can solve the tDBDH problem in polynomial time. We construct an algorithm B as follows. B takes a 4-tuple $(g^a; g^b; g^c; e(g; g)^d)$ as input, and its objective is to determine whether $e(g; g)^d$ D $e(g; g)^{abc}$ holds.

B chooses a random range x and constructs a 7-tuple (ga; gb; gc; e(g; g)d ; gbx ; gcx ; e(g; g)dx2). Then, it calls the algorithm A. The rule A checks whether or not e(g; g)d D e(g; g)abc and e(g; g)dx2 D e(g; g)abcx2 hold.

If A outputs affirmative, then it implies that e(g; g)d D e(g; g) abc and e(g; g)dx2 D e(g; g)abcx2 . Apparently, it's doubly con-riming that the input could be a affirmative DBDH instance. Thus, B replies "yes".

If A outputs no, then it implies that either e(g; g)d 6D e(g; g)abc or e(g; g)dx2 6De(g; g)abcx2 . no matter that is true, will quickly deduce that the input could be a no DBDH instance. Thus, B replies "no".

B. SHAMIR'S SECRET SHARING SCHEME

Shamir's (t; n)-threshold secret sharing theme is predicated on the Lagrange interpolation polynomial. an in depth introduction is delineated as follows:

Given t distinct points (xi; f (xi)), wherever f (x) may be a polynomial of degree but t, f (x) is set as follows: Shamir's theme is Delaware need for a secret s a pair of Zp by setting a0 D s and selecting a1; a2; ; at one a pair of Zq. For all one xi q; one i n, the trustworthy party computes f (xi), wherever f (x) D noble metal one a xk . The shares (x ; f (x)) ar distributed to n distinct parties. Since the key may be a constant term s D a0 D f (0), the key will be recovered from any t shares (xi; f (xi)) as follows:

C. ACCESS TREE

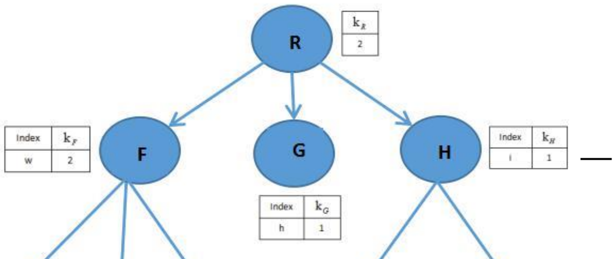

Figure 1. Access Tree

We suppose that T is AN access tree composed of leaf nodes and non-leaf nodes (e.g., Fig. 2). every leaf node represents AN attribute, and every non-leaf node represents a logic element. every logic element is drawn by its youngsters and also the threshold price. Let numb be the quantity of kids of a node x and kx be the brink price of the node x; we've got zero kx numb . Then, every leaf node includes a threshold price kx D one.

We suppose that the kids of each node do have orders from one to num. Next, we tend to First State ne some new functions. The perform parent(x) represents the parent of node x. The function att(x) is First State need as AN attribute related to the leaf node. The perform index(x) returns the quantity related to node x.

Let r be the basis of AN access tree T, expressed as Tr . Lone-Star State refers to the sub tree of T unmoving at node x. Lone-Star State (S) D one means the set of attributes S sates atomic number 99 the tree Lone-Star State . Here, we tend to use a algorithmic rule to reckon Lone-Star State (S).

If x may be a non-leaf node, we tend to reckon Tx0 (S) for all children x0 of x. If a minimum of youngsters come one, then Lone-Star State (S) returns one.

If x may be a leaf node, then Lone-Star State (S) returns one if att(x) a pair of S.

III. PROBLEM FORMULATION

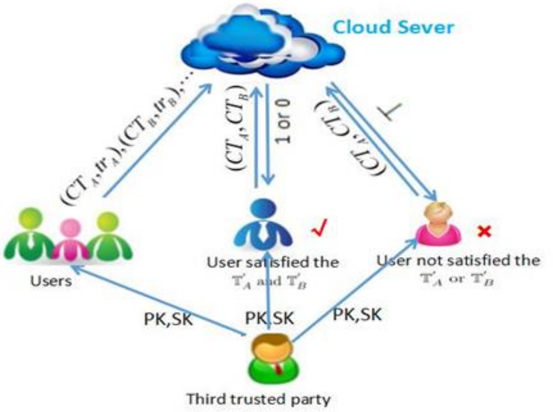
Cloud Sever
$(CT_A,tr_A),(CT_B,tr_B),\ldots$
(CT_A,CT_B)
1 or 0
(CT_A,CT_B)
$\perp$
Users
User satisfied the T'_A and T'_B
User not satisfied the T'_A or T'_B
PK,SK
PK,SK
PK,SK
Third trusted party

FIGURE 2. System model for KP-ABEwET.

A. System Model

Fig. 3 illustrates the system model of KP-ABEwET. The sys-tem has 3 taking part entities: the cloud server, the users and a sure third party. The trusty third party generates public key pk and personal key sk for users. The users code and send their non-public information to the cloud server. If a user needs the cloud server to check the cipher text, then the cloud server is permitted and gains a trapdoor tr. However, the cloud server will solely take a look at whether or not the 2 cipher texts contain an equivalent info and can't decode them exploitation the trapdoor. The legitimate users access information per their attributes and may decode their cipher texts or take a look at the cipher texts. If the legitimate users satisfy the access structure for the take a look at, they will get the take a look at results of the cipher texts from the cloud server. If the legitimate users satisfy the access structure for the decoding, they will decode the cipher texts.

An integrated KP-ABEwET theme consists of six algorithms: Setup, Encrypt, KeyGen, and Trapdoor, decode and check. Here, we have a tendency to let M be plaintext house and C be cipher text area.

(1) Setup (k): It takes a security parameter k as input, so it outputs the general public parameters pp and pk and also the master mk.
(2) Encrypt (M; pk; S; S0): It takes a message M a pair of M, public key pk and 2 sets of attributes S; S0 as inputs, so it outputs the cipher text CT a pair of C.
(3) KeyGen(T; T0; S; S0; pp; mk): This rule takes as inputs the master mk, 2 access trees T; T0, and 2 sets of attributes S; S0 that satisfy T(S) D one and T0(S0) D one, and it later on outputs the personal key sk.
(4) Trapdoor (S0; T0; mk): It takes mk, T0 and S0 as inputs, and it outputs the trapdoor td.
(5) Decrypt(CT ; sk; S; S0): It takes as inputs a cipher text CT a pair of C; S; S0 and also the non-public key sk, and it outputs the message M if T(S) D one and T0(S0) D one. Here, CT is encrypted victimization the sets S and S0.
(6) Test(CTA; CTB; tdA; tdB; S0): Suppose that CTA may be a cipher text of the sets of attributes reserves and SA0 which CTB may be a cipher text of the sets of attributes SB and SB0. This algorithm takes as inputs 2 cipher texts CTA; CTB, the trapdoors tdA; tdB and also the set S0 of attributes that satisfy T0A(S0) D one and T0B(S0) D one, so it outputs one if CTA and CTB contain an equivalent message; otherwise, it returns zero.

B. Security Model

Here, the protection model of the projected theme and also the security model of authorization area unit conferred.

First, we tend to American state ne unidirectional against chosen-cipher text attack (OW-CCA) for KP-ABEwET below a selected set of attributes, as follows.

Game 1: Suppose that A is that the soul. A announces a group of attributes that he needs to be challenged, shown as S.

(1) Setup. The competition C takes a security parameter k as input and outputs public parameters pp to A with the Setup formula of KP-ABEwET.
(2) Phase one. A performs the subsequent varieties of queries polynomials repeatedly.

Key retrieve queries: A performs any queries for personal keys for several access structures Ti, wherever S 2= Ti for all i. C sends sk to A.

Decryption queries: A performs several queries for cipher texts. C runs the rewrite formula and outputs the plaintext reminiscent of the cipher text or? to A.

Trapdoor queries: C runs the Trapdoor formula and outputs td to A.

(3) Challenge: C indiscriminately chooses a message M a pair of M, sets CT D Encrypt (pk; M) and sends CT to A as his challenge cipher text.
(4) part 2: Phase one is perennial. The constraints area unit that CT doesn't seem within the coding queries.
(5) Guess: A outputs a guess M two M and wins the sport if M D M.

The advantage of A is First State ned as Pr[M D M].

De nation 5: The KP-ABEwET theme is OW-CCA secure if the advantage of all polynomial time adversaries is negligible within the on top of game.

Finally, we tend to First State ne a testable against chosen-cipher text attack (T-CCA) of authorization for KP-ABEwET below the chosen sets of attributes, as follows:

Game 2: Suppose that A2 is associate degree individual. A2 announces 2 sets of attributes S and S0 that he desires to be challenged. Here, (S \ S0) D ?, S is employed for coding, and S0 is employed for the trapdoor.

(1) Setup. The competition, C, takes a security parameter k as input and outputs public

parameters pp to A2 by mistreatment the Setup formula of KP-ABEwET.

(2) Phase one. A2 performs the subsequent kinds of queries polynomials over and over. Key retrieve queries: A2 performs several queries for personal keys for any access structures Ti and T0j, where

S 2= Ti for all i and S0 2= T0j for all j. C sends sk to A2. Decoding queries: A2 performs several queries for cipher texts. C runs the decode algorithmic rule and out-puts the plaintext akin to the cipher text or ? to A2.Trapdoor queries: C runs the Trapdoor algorithmic rule and outputs td to A2.

Test queries: C runs the check algorithmic rule and outputs 1 for equality cipher texts and 0 for unequal cipher texts or?.

(3) Challenge: C chooses a random variety # two f0; 1g. If # D 1, then C chooses one message M, sets

CT1 D Encrypt (pk; M); CT2 D Encrypt (pk; M)

and sends CT1 ; CT2 to A2 as his challenge cipher texts. If # D 0, C chooses 2 unequal messages, money supply and M2; sets

CT1 D Encrypt (pk; M1); CT2 D Encrypt(pk; M2) and sends CT1 ; CT2 to A2 as his challenge cipher texts.

(4) Part 2: Phase one is recurrent with the conditions that CT1 and CT2 don't seem in decoding queries and CT1 and CT2 don't seem in check queries.

(5) Guess: A2 outputs a guess # and wins the sport if # D #, which means one for money supply D M2 or zero for money supply 6DM2.

The advantage of A2 is First State need as jPr[# D #] 1=2j. First State nation 6: The KP-ABEwET theme is T-CCA secure in terms of authorization if the advantage of all polynomial time adversaries is negligible within the previously mentioned game.

IV.OUR CONSTRUCTIONS

The following section presents the projected KP-ABEwET theme. Setup (k): It takes a security parameter k as input and outputs public parameters pp as follows:

(1) Generate linear teams, G1; G2 and jG1j D alphabetic character; jG2j D q, and select a random generator g 2 G1. Then, let e V G1 G1 ! G2 be a linear map.

(2) Let A be a universe of properties of attributes. For simplicity, we have a tendency to take the rst A parts of Zq because the universe, formally as 1; 2; jAj (mod q).

(3) Let H1 V f0; 1gjAj G2! f0; 1gkCl, H2 V f0; 1gjAj G2 ! G1, and H3 V 5G1 f0; 1gkCl! f0; 1gk be hash functions, wherever l is that the length of the weather of Zq.

(4) Choose x1; x2; ; xjAj; y1; y2 two Zq arbitrarily, then output public keys pk,

X1 D gx1 ; ; XjAj D gxjAj ; Y1 D e(g; g)y1 ; Y2 D e(g; g)y2 , and also the passkey mk, (x1; x2; ; xjAj; y1; y2).

Encrypt (M; pk; S; S0): It takes a message M, public key pk and 2 sets of attributes S; S0 as inputs, wherever (S \ S0) D ;,S is used for coding, and S0 is employed for testing. Then, it outputs the cipher text as follows:

Choose r1; r2; r3 a pair of Zq at random, and so formulate the following:

CT D (S; S0; C1 D gr1 ; C2 D M k r1 H1(S; Y1r2); C3 D Mr1 H2(S0; Y2r3); C4 D fEi D Xir2 gi2S ;

C5 D fEj D Xjr3 gj2S0 ; C6 D H3(Mr1 ; C1; C2; C3; C4; C5))

KeyGen (T; T0; S; S0; pp; mk): This algorithmic program takes the passkey mk, 2 sets of attributes S; S0 satisfying T(S) D one and T0(S0) D one and (S0 TS) D ? as inputs, and it outputs the non-public key as follows:

The algorithmic program chooses a polynomial qx for every node x within the tree T. The polynomials area unit chosen from prime to bottom, ranging from the basis node r. the small print area unit conferred as follows:

For each node x in T, it sets the degree dx of the polynomial qx to be one but the edge price kx of that node, which suggests that dx D kx.

V. SECURITY ANALYSIS

The following section provides the protection proof of the conferred KP-ABEwET theme.

Theorem 2: Our projected theme is OW-CCA secure against the resister World Health Organization is permitted with a trapdoor supported the BDH assumption within the random oracle model.

Proof: Suppose that A is that the resister that may break the bestowed KP-ABEwET theme. Then, there's AN algorithmic rule C to solve the BDH drawback with a non-negligible advantage. Given a 4-tuple (g; A; B; C) D (g; ga; gb; gc), the target of algorithmic rule C is to calculate e(g; g)abc. Init Suppose that there's a universe. A chooses a group of Paste your text here and click on "Next" to look at this text editor do it's issue.

Don't have any text to check? don't have any text to check? Click "Select Samples". Phase 1 A performs the subsequent sorts of queries poly-nominally times.

H1-query: A could issue queries to the random oracle H1. to retort to those queries, C maintains a listing of tulles H1. every component within the list may be a tulle of the shape (S ; ;). The list is at first empty. Responding to question (S ;), C runs as follows:

If the question (S ;) already seems within the H1 list within the type (S ; ;), then C responds to A with H1(S ;) D.
Otherwise, C simply takes 2 G2, so it responds to A with H1(S ;) D . C adds the tulle (S ; ;) to the H1 list.

Key retrieve queries: A performs several queries for private keys for several access structures T, wherever S doesn't satisfy T. C sends sk to A as follows:

(1) C builds 2 algorithms: SatT and DNSatT, as follows:

SatT(Tx ; S; vx): This algorithmic program constructs the polynomials for the nodes of associate degree access sub-tree with a sates dysfunction root node once Lone-Star State (S) D one. It takes as inputs a group of attributes S, associate degree access tree Lone-Star State and a random range vx 2 Zp, and it outputs a polynomial qx of degree dx for the foundation node x as follows:

Let qx (0) D vx and indiscriminately select dx different points of the polynomial qx to construct qx . The algorithmic program constructs polynomials for every kid node x0 of x by death penalty the algorithmic program SatT(Tx0 ; S; qx (index(x0))).

DNSatT(Tx ; S; gvx): This algorithmic program constructs the polynomials for the nodes once Lone-Star State (S) D zero. It takes a group of attributes S, associate degree access tree Lone-Star State and a random part gvx a pair of G1, wherever vx a pair of Zp, and it outputs a polynomial qx of degree dx for the basis node x as follows:

Because Lone-Star State (S) D 0, the foundation node has but dx satis disjunction kids. Suppose that sx is that the range of sates disjunction kids of x, which means that sx < dx . The algorithmic program chooses a random range vx0 a pair of Zp for every satis disjunction kid x0 of x. Let qx (index(x0)) D vx0 and indiscriminately select different dx sx points of the polynomial qx to construct qx We acquire qx ( ) for every node in T as follows.

VI. PERFORMANCE EVALUATION

We in theory analyze the straight line quality of the projected theme and alternative PKEwET schemes in Table one. we have a tendency to describe the process quality in terms of the involution operation E and also the pairing operation P. we tend to denote the quantity of attributes needed within the cipher-text by jSC j and jSC0 j. In Table 1, CEnc, CDec and C Test represent the cryptography algorithms, decoding algorithms and check algorithms, severally. Lollop said genus represents the proof of authorization. From the second to the fourth columns, we tend to gift the process complexities of CEnc, CDec and C Test. The 5 column indicates whether or not the underlying schemes area unit attribute primarily based. The sixth column shows whether or not the schemes have the proof of authorization. The seventh column highlights the safety levels of the schemes. The last column presents the underlying assumptions for guaranteeing the safety.

From Table one, we have a tendency to observe that the process com-laxity of our theme depends on the amount of attributes needed by the cipher text. as a result of our theme incorporates the ABE state of affairs, it's going to not be as client because the current works. The trade off is adjusted whereas providing the protection of user identities. Moreover, in distinction to previous works, our theme additionally permits the users to get ne-grained authorization of cipher texts. To the simplest of our information, Ma et al. rest given four varieties of authorizations in [29]. we tend to nd that our projected theme will perform the authorization and take a look at in an exceedingly additional edible manner as a result of in our theme, we are able to perform the authorization mistreatment the attributes of users. moreover, for the time, the proof of authorization is evidenced supported the tDBDH assumption.

VII. CONCLUSION

In this paper, a replacement cryptosystem known as key-policy attribute-based encoding with equality check (KP-ABEwET) is pre-scented. To the most effective of our information, KP-ABEwET is that the rst commit to mix the general public key encoding supporting equality check with key-policy attribute-based secret writing. The planned theme are often viewed as AN extension of attribute-based encoding with keyword search (ABEwKS) with the distinction that it will check whether or not the cipher texts contain a similar info that were encrypted by completely different public keys. In distinction to previous schemes with equality check, the new theme supports testing the cipher texts with ne-grained authorization and additionally hides the identity of the user. Moreover, the projected theme is unidirectional secure against chosen-cipher text attack (OW-CCA) supported the linear Dif e-Hellman (BDH) downside. Moreover, a replacement computational downside known as twin-decision additive Dif e-Hellman downside (tDBDH) is projected and is proved to be as laborious because the DBDH downside. Finally, the protection model of authorization is conferred, and therefore the security of authorization supported the tDBDH assumption is proved within the random oracle model. To the simplest of our information, this work is that the RST to prove the protection of authorization in such a state of affairs.

VIII. REFERENCES

[1] A. Boldyreva, S. Fehr, and A. O'Neill, ``On notions of security for deter-ministic encryption, and ef cient constructions without random oracles,'' in Proc. Annu. Int. Cryptol. Conf., 2008, pp. 335 359.

[2] A. Sahai and B. Waters, ``Fuzzy identity-based encryption,'' in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2005, pp. 457 473.

[3] C. Wang, W. Li, Y. Li, and X. L. Xu, ``A ciphertext-policy attribute-based encryption scheme supporting keyword search function,'' in Proc. CSS, 2013, pp. 377 386.

[4] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart, ``Deterministic encryption: De nitional equivalences and constructions without random oracles,'' in Advances in Cryptology CRYPTO (Lecture Notes Com-put. Science), vol. 5157. Berlin, Germany: Springer-Verlag, Aug. 2008, pp. 360 378.

[5] M. Bellare, A. Boldyreva, and A. O'Neill, ``Deterministic and ef - ciently searchable encryption,'' in Proc. Annu. Int. Cryptol. Conf., 2007, pp. 535 552.

[6] M. Nishioka, ``Perfect keyword privacy in PEKS systems,'' in Provable Security. Berlin, Germany: Springer, 2012, pp. 175 192.

[7] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, ``Expressive search on encrypted data,'' in Proc. 8th ACM SIGSAC Symp. Inf., 2013, pp. 243 252.

[8] J. Li and L. Zhang, ``Attribute-based keyword search and data access control in cloud,'' in Proc. 10th Int. Conf. Comput. Intell. Secur. (CIS), Nov. 2014, pp. 382 386.

[9] J. Han, W. Susilo, Y. Mu, and J. Yan, ``Privacy-preserving decentralized key-policy attribute-based encryption,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150 2162, Nov. 2012.

[10] S. Li and M. Z. Xu, ``Attribute-based public encryption with keyword search,'' Chin. J. Comput., vol. 37, no. 5, pp. 1017 1024, 2014.

[11] P. Liu, J. Wang, H. Ma, and H. Nie, ``Ef cient veri able public key encryption with keyword search based on KP-ABE,'' in Proc. 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA), Nov. 2014, pp. 584 589.

[12] A. Lewko and B. Waters, ``Decentralizing attribute-based encryption,'' in Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn., 2011, pp. 568 588.

[13] S. Hohenberger and B. Waters, ``Online/of ine attribute-based encryp-tion,'' in Proc. Int. Workshop Public Key Cryptogr., 2014, pp. 293 310.

[14] P. Datta, R. Dutta, and S. Mukhopadhyay, ``Fully secure online/of ine predicate and attribute-based encryption,'' in Proc. ISPEC, 2015, pp. 331 345.

[15] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong , ``Probabilistic public key encryption with equality test,'' in Proc. Cryptogr.-Track RSA Conf., 2010, pp. 119 131.

[16] S. Ma, Q. Huang, M. Zhang, and B. Yang, ``Ef cient public key encryption with equality test supporting exible authorization,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 458 470, Mar. 2015.

[17] S. Ma, ``Identity-based encryption with outsourced equality test in cloud computing,'' Inf. Sci., vol. 328, pp. 389 402, Jan. 2016.

[18] L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, ``Ef cient and secure identity-based encryption scheme with equality test in cloud computing,'' Future Generat. Comput. Syst., vol. 73, pp. 22 31, Aug. 2017.

Cite this article as :

Dr. Gopal Sakarkar, Mrunal Prabhakar Rohad, Rahul Ashwani Gupta, "Attribute-Based Encryption with Equality Test in Cloud Computing Using Key-Policy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 835-844, March-April 2019. Journal URL : http://ijsrcseit.com/CSEIT1952252