iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3157

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Prevention of Identity Leakage and Access Management Using Anony Control-F Attribute Based Encryption

Snehanka K. Patil[1], Manjusha Tatiya[2]
[1] *P.G. Student, Department of Computer Engineering, Indira College of Engineering and Management, Pune, Maharashtra, India*
[2] *Professor, Department of Computer Engineering, Indira College of Engineering and Management, Pune, Maharashtra, India*

Abstract: ***Network security is needed to protect to protect network. Cloud computing may be a revolutionary computing paradigm, that permits versatile, on-demand, and cheap usage of computing resources, but the data is outsourced to some cloud servers, and varied privacy concerns emerge from it. Numerous schemes Supported the attribute-based committal to writing are projected to secure the cloud storage. However, most work focuses on the data contents privacy and so the access management, whereas less attention is paid to the privilege management and so the identity privacy. Throughout this paper, a semi anonymous privilege management theme Anony Control is projected to handle not entirely the information privacy, but collectively the user identity privacy in existing access control schemes. Anony management decentralizes the central authority to limit the identity run and so achieves semi anonymity. Besides, it collectively generalizes the file access management to the privilege management, by those privileges of all operations on the cloud data is managed in associate passing fine-grained manner. Afterwards, the Anony Control-F is presented, that absolutely prevents the identity outflow and succeeds the whole obscurity. The protection analysis shows that each Anony management and Anony Control-F unit secure beneath the decisional linear Diffie–Hellman assumption, and new performance analysis exhibits the practicability of latest schemes.***
Keyword: Anonimity, Attribute-based cryptography, cloud computing, multi-authority obscurity.

I. INTRODUCTION

The Network Security of Internet is expanding with a tremendous speed so as internet. Security is an important factor that consists of the provisions of underlying computer network infrastructure and also policies adopted by the network administrator to protect the network. Cloud computing might be a revolutionary computing technique, by that computing resources unit provided dynamically via web and so the knowledge storage and computation area unit outsourced to someone or some party throughout a 'cloud' It greatly attracts attention and interest from every world and business as a result of the profit, but it put together features a minimum of three challenges that has to be handled before coming to our real world to the foremost effective of our information. Initial of all, information confidentiality have to be compelled to be bonded. The knowledge privacy is not solely regarding the knowledge contents. Since the foremost participating a vicinity of the cloud computing is that the computation outsourcing, it's way on the far side enough to easily conduct associate access management. Extra most likely, users got to manage the privileges of knowledge manipulation over totally different users or cloud servers. usually this can be often as a results of once sensitive information or computation is outsourced to the cloud servers or another user, that is out of users' management in most cases, privacy risks would rise dramatically as a results of the servers might illicitly examine users' data and access sensitive data, or totally different users is able to infer sensitive data from the outsourced computation. Therefore, not solely the access but put together the operation have to be compelled to be controlled. Secondly, personal info is in peril as a result of one's identity is each supported his information for the aim of access management. As people became additional involved regarding their identity privacy latterly, the identity privacy put together needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not grasp any client's personal information. Last but not least, the cloud computing system have to be compelled to be resilient at intervals the case of security breach throughout that some a vicinity of the system is compromised by attackers. Numerous techniques area unit planned to safeguard the info contents privacy via access management. Identity-based encoding (IBE) was initial introduced by Shamir [1], during which the sender of a message can specify associate identity specified alone a receiver with matching identity can decipher it. Few years' later, Fuzzy Identity-Based cryptography [2] is planned, that's to boot said as Attribute-Based encoding (ABE). In such cryptography theme, associate identity is viewed as a gaggle of descriptive attributes, and secret writing is feasible if a decrypter's identity has some overlaps with the one ordered go in the cipher text. Soon

©IJRASET (UGC Approved Journal): All Rights are Reserved

after, extra general tree-based ABE schemes, Key-Policy attribute-Based encoding (KP-ABE) [3] and Ciphertext-Policy Attribute primarily based cryptography (CP-ABE) [4], unit given to specific extra general condition than straightforward 'overlap'. They're counterparts to each different at intervals the sense that the selection of cryptography policy is made by fully completely different parties.

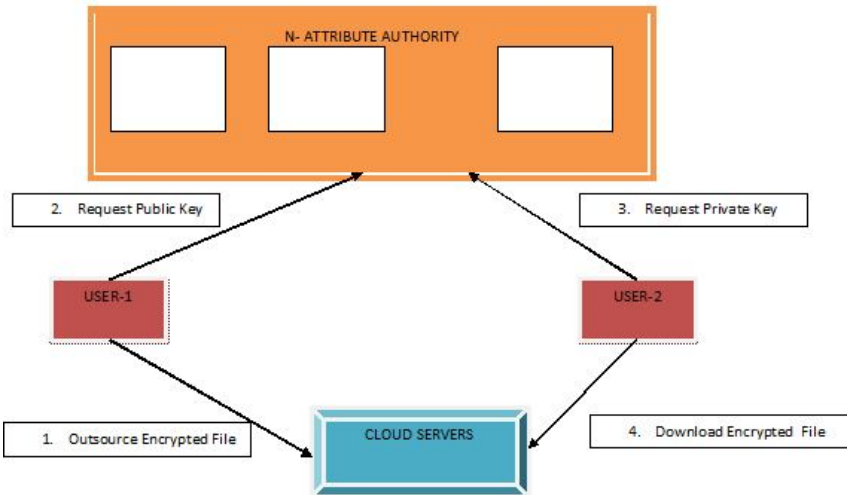


Fig.1. General flow of scheme

In the KP-ABE [3], a ciphertext is expounded to a collection of attributes, and a private secret's associated with a monotonic access structure kind of a tree, that describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user will decipher the ciphertext if and providing the access tree in his personal secret's happy by the attributes inside the ciphertext. However, the cryptography policy is delineating within the keys, that the encrypter does not have entire management over the cryptography policy. He has to trust that the key generators issue keys with correct structures to correct users. Once a re-encryption happens, all of the users inside the same system ought to have their personal keys re-issued so on gain access to the re-encrypted files, and this methodology causes tidy problems in implementation. On the other hand, those issues and overhead unit of measurement all resolved inside the CP-ABE [4]. In the CP-ABE, ciphertexts unit of measurement created with associate degree access structure, that specifies the cryptography policy, and private keys space unit generated per users' attributes. A user can decipher the ciphertext if and providing his attributes inside the private key satisfy the access tree set call at the ciphertext. By doing so, the encrypter holds the last word authority concerning the cryptography policy. Also, the already issued personal keys will never be changed unless the entire system reboots. Not like the information confidentiality, less effort is paid to protect users' identity privacy throughout those interactive protocols. Users' identities, that area unit delineate with their attributes, ar typically disclosed to key issuers, and conjointly the issuers issue personal keys per their attributes. But it seems natural that users unit of measurement willing to remain their identities secret whereas they until get their personal keys. Therefore, AnonyControl and AnonyControl-F is planned (Fig. 1) to allow cloud servers to manage users' access privileges while not knowing their identity data. Their main deserves are: 1) The projected schemes unit of measurement able to defend user's privacy against each single authority. Partial data is disclosed in AnonyControl and no data is disclosed in AnonyControl-F. 2) The projected schemes unit of measurement tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the complete system down. 3) Offered careful analysis on security and performance to point out practicableness of the theme AnonyControl and AnonyControl-F.

II. RELATED WORK

In [5] and [6], a multi-authority system is given during which each user has AN ID which they're going to act with each key generator or authority exploitation, totally different pseudonyms. One user's totally different pseudonyms unit of measurement tied to his personal key, but key generators never comprehend the private keys, and then they're not able to link multiple pseudonyms happiness to a similar user. Also, the whole attributes set is split into N disjoint sets and managed by N attributes authorities. During this setting, every authority is tuned in to exclusively a vicinity of any user's attributes that do not appear to be enough to figure out the user's identity. However, the theme projected by Chase et al. [6] thought of the essential threshold-based KP-ABE, that lacks generality at intervals the encryption policy expression. Many attribute based mostly encryption schemes having multiple authorities are projected later [7]–[10], however they either to boot use a threshold-based ABE [7], or have a semi-honest central authority [8]–

©IJRASET (UGC Approved Journal): All Rights are Reserved

[10], or cannot tolerate haphazardly many users' collusion attack [7]. The work by Lewko et al. [11] and Muller et al. [12] unit of measurement the foremost similar ones to during this they to boot tried to change the central authority at intervals the CP-ABE into multiple ones. Lewko et al. use a LSSS matrix as AN access structure, however their theme exclusively converts the AND, OR gates to the LSSS matrix, that limits their encoding policy to mathematician formula, whereas we tend to inherit the flexibility of the access tree having threshold gates. Muller et al. additionally supports exclusively reciprocally exclusive ancient type (DNF) in their encryption policy. Besides the particular proven fact that we tend to area unit able to specific haphazardly general encryption policy, this method to boot tolerates the compromise attack towards attributes authorities, that may not lined in many existing works. Recently, there to boot appeared traceable multi-authority ABE [13] and [14], that unit of measurement on the opposite direction of ours. Those schemes introduce responsibility mere malicious users' keys area unit often derived. On the other hand, similar direction as this theme is commonly found in [15]–[17], administrative unit try to hide encryption policy at intervals the ciphertexts, but their solutions do not stop the attribute revealing at intervals the key generation half.

III. PRELIMINARIES

Let G0 be a increasing cyclic cluster of prime order p and g be its generator. The linear map e ([18], [19]) is made public as follows: e : G0 × G0 → GT , where GT is that the codomain of e. The linear map e has the following properties: ∀u,v ∈ G0 and a, b ∈ Zp, e(ua,vb) = e(u,v)ab (bilinearity); for all u,v ∈ G0, e(u,v) = e(v, u) (symmetry); and e(g, g) = one (non-degeneracy). Definition 1: The Decisional linear Diffie-Hellman (DBDH) draw back in cluster G0 of prime order p with generator g is made public as follows: on input g, ga, gb, Gc ∈ G0 and e(g, g)z∈ GT , where a, b, c ∈ Zp, decide whether or not or not e(g, g)z = e(g, g)abc. The protection of the various ABE schemes [4], [20]–[23] and rely on the assumption that no probabilistic polynomial time algorithms can solve the DDH or DBDH draw back with non-negligible advantage (DDH assumption and DBDH assumption). This assumption is reasonable since separate exponent problems in sizable quantity field square measure wide thought-about to be refractory [24]–[28], and additionally the groups it's tend to selected square measure cyclic increasing groups of prime order, at intervals that DBDH issues square measure believed to be laborious The Lagrange constant i,S for i ∈ Zp and a collection, S, of elements in Zp: i,S(x) := j∈ S, j=i x i− −jj , which can be used within the polynomial interpolation at intervals the decoding formula. to boot, a simplex hash operate H : * → G0 is made public as a random oracle, which maps any attribute price to a random element in Zp.

A. Privilege Trees Tp

In this work, secret writing policy is depicted with a tree referred to as access tree. Each non-leaf node of the tree may well be a threshold component, and every leaf node is depicted by associate attribute. One access tree is required in every record to outline the key writing policy. During this paper, existing schemes square measure extended by generalizing the access tree to a privilege tree. The privilege during this theme is made public as rather like the privileges managed in standard operative systems. a data file has several operations feasible on itself, and each of them is allowed only to approved users with utterly totally different level of qualifications. For instance, may well be a privileges set of students' grades. Then, reading Alice's grades is allowed to her and her professors, but all different privileges ought to be verified only to the professors, therefore we'd wish to grant the "Read_mine" to Alice and each one different to the professors. each operation is expounded to 1 privilege p, that is depicted by a privilege tree Tp. If a user's attributes satisfy Tp, he is granted the privilege p. By doing therefore, not solely the file access management is completed however collectively management different possible operations, that produces the file dominant fine-grained and therefore acceptable for cloud storage service. In this theme, several trees square measure required in every record to verify users' identity and to grant him a privilege consequently. There are alleged to be r these quite structures, that mean there square measure utterly totally different privileges printed for the corresponding record. The privilege zero is unlined as a result of the privilege to scan the file, and different privileges might even be printed each that means (the m-th privilege does not primarily have further powerful privilege than the n-th one once m > n). The tree is analogous to the one printed in [4]. Given a tree, if numx is that the vary of the node x's kids node and kx is its threshold value zero < kx ≤ numx, then node x is assigned a true value if a minimum of kx kids nodes square measure assigned true value. Specially, the node becomes associate gate once kx = one associate degreed associate degree gate once kx = numx.

B. Satisfying the Privilege Tree

If a user's attributes set S satisfies the privilege tree Tp or the node x, we tend to tend to stipulate it as Tp(S) = one or x(S) = one severally. Tp (S) is calculated recursively as follows. If x may well be a leaf node, x(S) = one if and only if att(x) ∈ S. If x may well

©IJRASET (UGC Approved Journal): All Rights are Reserved

be a nonleaf node, x(S) = one given that a minimum of kx child nodes come one. For the basis node R p of Tp, Tp(S) = one only if Rp(S) = one.

IV. DOWNSIDE FORMULATION

A. System Model

In this system, there are a unit four styles of entities: N Attribute Authorities (denoted as A), Cloud Server, info householders and knowledge customers. User's area unit is usually a data Owner and a data client at an equivalent time. Authorities area unit assumed to own powerful computation skills, which they're supervised by government offices as a results of some attributes partially contain users' in person identifiable information. The full attribute set is split into N disjoint sets and controlled by every authority, so every authority is attentive to solely a part of attributes. A Data Owner is that the entity United Nations agency needs to source encrypted record to the Cloud Servers. The Cloud Server, who is assumed to own adequate storage capability, does nothing however store them. Newly joined information customers request non-public keys from all of the authorities, and that they don't apprehend that attributes are controlled by that authorities. Once the information customers request their non-public keys from the authorities, authorities jointly produce corresponding non-public key and send it to them. All information customers are able to transfer any of the encrypted info files, but only those whose private keys satisfy the privilege tree Tp can execute the operation related to privilege p. The server is delegated to execute academic degree operation p if and as long as the user's credentials area unit verified through the privilege tree Tp.

B. Threats Model

It is assumed that the Cloud Servers area unit semi-honest, UN agency behave properly in most of it slow but may conspire with malicious info customers or info householders to reap others' file contents to achieve illegitimate profits. However they're collectively assumed to understand legal profit once users' requests are properly processed, which suggests they're going to follow the protocol ordinarily. N authorities are assumed to be untrusted. That is, they'll follow our planned protocol ordinarily; however attempt to notice out the utmost quantity knowledge as achievable singly. Additional specifically, we tend to tend to assume they are interested by users' attributes to achieve the identities, but they're going to not conspire with users or different authorities. This assumption is analogous to many previous researches on security issue in cloud computing (see [20], [29]–[31]), and it's collectively low-cost since these authorities area unit going to be audited by government offices. Assumption is relaxed and allows the collusion between the authorities. Data shopper's area unit untrusted since they are random users as well as attackers. They'll move with different info shoppers to lawlessly access what they don't seem to be allowed to. Besides, do not take into consideration the identity outpouring from the underlying network since this can be trivially prevented by using anonymized network protocols (see [32], [33]).

C. Security Model

To formally define the protection of this AnonyControl, we tend to initial give the next definitions. Setup → PK, MKk: This algorithmic program takes nothing as input except implicit inputs like security parameters. Attributes authorities execute this algorithmic program to jointly cypher a system-wide public parameter PK equally as academic degree authority-wide public parameter yk, and to singly cypher a passe-partout MKk. Key Generate(PK, MKk, Au) → SKu: This algorithm allows a user to maneuver with every attribute authority, and obtains a private key SKu just like the input attribute set Au. Encrypt(PK, M, pε) → (CT, VR): This formula takes as input the overall public key PK, a message M, and a collection of privilege trees p∈, where r is set by the encrypter. It is going to write in code the message M and returns a ciphertext CT and a verification set VR so as that a user will execute specific operation on the ciphertext if and as long as his attributes satisfy the corresponding privilege tree Tp. As defined, T0 stands for the privilege to browse the file. Rewrite (PK, SKu, CT) → M or verification parameter: This algorithm area unit going to be used at file dominant (e.g. reading, modification, deletion). It takes as input the overall public key PK, a ciphertext CT, and a private key SKu that contains a collection of attributes Au and corresponds to its holder's GIDu. If the set Au satisfies any tree inside the set pε, the algorithm returns a message M or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, UN agency uses VR to verify it, the operation request area unit planning to be processed. Next, define the protection of this AnonyControl with the subsequent game. Init: The person A declares the set of compromised authorities ⊂ A (where a minimum of two authorities in a {very} very don't seem to be management diode by A) that area unit below his management (remaining authorities A/ square measure controlled by the challenger). Then, he declares T0 that he needs to be challenged, throughout that some attributes square measure being in charged by the challenger's authorities. Setup*: The

©IJRASET (UGC Approved Journal): All Rights are Reserved

competition and therefore the somebody jointly run the Setup algorithm to receive the valid outputs. part 1: The somebody launches Key Generate algorithms to question for as many private keys as he needs, that correspond to attribute sets A1,. . ., Aq being disjoint in charged by all authorities , but none of these keys satisfy T0. Besides, he collectively conducts arbitrarily many computations practice the general public and secret keys that he has (belonging to compromised authorities). Challenge: The person submits two messages M0 and money supply of equal size to the challenger. The challenger flips a random binary coin b and encrypts Mb with T0. The ciphertext CT is given to the person. Section 2: half one is continual adaptively, but none of the queried keys satisfy T0. Guess: The person outputs a guess b of b. The advantage of degree somebody A throughout this game is outlined as Pr[b = b] − one 2 . Definition 2: Our theme is secure and indistinguishable against chosen-attribute attack (INDCAA) if all probabilistic polynomial-time adversaries (PPTA) have at the foremost a negligible advantage at intervals the on prime of game. Note that the IND-CAA made public on prime of implies IND-CCA since the somebody can conduct encryptions and decryptions mistreatment the overall public keys and secret keys it owns in section one and half 2 (but he cannot rewrite the target ciphertext since none of its secret keys satisfy T0).

D. Vogue Goals

Our goal is to appreciate a multi-authority CP-ABE which: achieves the protection made public above; guarantees the confidentiality of knowledge Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. For the visual comfort, ensuant notations are frequently used hereafter. American state denotes the k^{th} attribute authority; Au denotes the attributes set of user u; Au k denotes the set of Au controlled by Ak; and ATP denotes the attributes set included in tree Tp.

V. ANONYCONTROL CONSTRUCTION

A. Set up

At the system information half, anyone of the authorities chooses a linear cluster G0 of prime order p with generator g and publishes it. Then, all authorities severally and at random picks vk ∈ Zp and send Yk = e(g, g)vk to any or all or the other authorities UN agency one by one reason Y := k∈A Yk = e(g, g)k∈A vk . Then, every authority province arbitrarily picks N − one integers skj ∈ Zp(j ∈ \) and computes gskj . every gskj is shared with one another authority A j. Associate in Nursing authority province, once receiving N − one things of gs jk generated by A j , computes its secret parameter xk ∈ Zp as follows:

$$x_k = \left(\prod_{j\in\{1,\cdots,N\}\backslash\{k\}} g^{s_{kj}} \right) \Big/ \left(\prod_{j\in\{1,\cdots,N\}\backslash\{k\}} g^{s_{jk}} \right) = g^{\left(\sum_{j\in\{1,\cdots,N\}\backslash\{k\}} s_{kj} - \sum_{j\in\{1,\cdots,N\}\backslash\{k\}} s_{jk} \right)}$$

It is straightforward to look at that these haphazardly created integers satisfy k∈ A xk = one mod p. this will be a significant property that achieves compromise attack tolerance for our theme, which is able to be mentioned inside following section. Then, the master key for the authority state is MKk = {vk, xk}, and public key of the whole system is written as PK = Note that the time quality of the setup computation is O(N2) since every authority computes N − one things of gskj . However, this will be any reduced to O(N) by applying the subsequent easy trick. We have a tendency to tend to initial cluster the authorities into C clusters, and exchanges the parameters among the cluster entirely. Then, the time quality is reduced to O(C N) = O(N) since C may be a constant.

B. Keygenerate(PK, MKk, Au)

When a replacement user u with GIDu must hitch the system, he requests the private key from all of the authorities by following this technique that consists of two phases. 1) Attribute Key Generation: For any attribute i ∈ Au, each Last Frontier indiscriminately picks RI ∈ Zp to severally cipher the partial personal keys H(att(i))ri, Di = gri, that unit privately sent to the user u. Then, each authority Last Frontier indiscriminately picks dk ∈ Zp, computes xk · gvk · gdk and privately shares it with various authorities (i.e. unbroken secret to the user u). Then, he privately sends xk ·gdk to the user u (i.e. unbroken secret to various authorities). anyone of N authorities computes and sends the following term to the user u: D = xkgvk gdk = g + g wherever gvk acts as a system-wide key used to generate a valid secret key, but no single authority is during a position to infer its price. A legitimate D with a legitimate gvk square measure usually achieved on condition that all the authorities properly follow the protocol and conduct a joint computation. Then, the user computes the subsequent term that's that the attribute key for the attribute i (att(i) refers to the half in G0 like i):

©IJRASET (UGC Approved Journal): All Rights are Reserved

$$D = \prod x_k g^{v_k} g^{d_k} = g^{\sum v_k + \sum d_k}$$

Note that Di is computed firmly whereas not revealing individual gdk's to the user or revealing gdk to any attribute authority. This will be important among the tolerance to the compromise attack that is in a position to be mentioned later. 2) Key Aggregation: User u, once receiving D, Di 's and D i 's, aggregates the weather as his personal key: SKu = C. write in code (PK, M, p^u) The Data Owner encrypts the data with any existing trigonal secret writing theme, and generates the key writing key Ke. Then, he determines a gaggle of privilege trees p^u and executes Encrypt(PK, Ke, $\{T_p\}$). Keep in mind that the privilege tree in our theme relies on the brink gates. Here, Shamir's secret sharing technique [34] is directly accustomed implement the brink gate. Shamir's t-out of-n secret share theme permits one to divide a secret to n shares, and additionally the first secret square measure usually recovered with t of them. So, in our tree, the node value of the gate is recovered if and providing a minimum of kx values of children nodes square measure recovered in algorithmic manner. The random vary, that is employed to mask the key writing key Ke, is keep at the idea of the privilege tree and is secret shared to its children nodes, and also the secret shares among the children nodes unit of measurement secret-shared to their kids nodes, therefore thus forth till the algorithmic secret sharing reaches the leaf nodes. This is implemented among the subsequent technique. For each Tp, the formula initial chooses a polynomial qx for each node x in it. For every node x, sets the degree dx of the polynomial qx collectively however the brink value kx. Starting from the foundation node Rp, the formula indiscriminately picks sp ∈ Zp and sets qR p(0) := sp and indiscriminately chooses various coefficients for qR p. Then, for the other node x, the coefficients unit of measurement chosen willy-nilly and additionally the constant term is prepared as qparent(x)(index(x)) such qx(0) = qparent(x)(index(x)) (index(x) is that the index of the x's child nodes, and parent(x) is node x's parent node). Finally, he picks a random half h ∈ Zp such h−1 mod p exists, and calculates gh·s p, Dh−1, and additionally the ciphertext CT is created as CT = p∈, E0 = Ke · Y s0, C = ghs p, C ˆ = Dh−1 I ∈ ATp, ∀p∈ Note that Dh−1 is introduced to forestall key combination attack, that's comparable to the construct appeared in [4], however in numerous ways: they introduced such a inverse among the facility in key generation formula whereas we have a tendency to tend to can therefore among the key writing so as to achieve the de-centralization. Then, VR, that's disclosed entirely to the Cloud Server, is made for the aim of privilege verification. VR = {E p = Y s p} p∈{1,...,r-1}. Finally, information Owner sends CT, VR and additionally the encrypted file to the Cloud Server to share them with various information shoppers.

D. Decipher (PK, SKu, CT)

Every user among the system can transfer the ciphertext from the Cloud Server, but he is able to execute operations on encrypted information entirely once he successfully decrypts it. Firstly, we have a tendency to define a algorithmic formula decipher Node(CT, SKu, x), where x stands for a node among the privilege tree Tp. If the node x may well be a leaf node, we have a tendency to tend to let i be the attribute of the node x and outline as follows. If i ∈ Au, Decrypt Node (CT, SKu, x) = e(Di, Cx)/e(Di, Cx)

$$DecryptNode(\mathbf{CT}, \mathbf{SK}_u, x) = \frac{e(D_i, C_x)}{e(D_i', C_x')}$$

$$= \frac{e(g^{\sum d_k} \cdot H(att(i))^{r_i}, g^{q_x(0)})}{e(g^{r_i}, H(att(i))^{q_x(0)})} = e(g,g)^{(\sum d_k) \cdot q_x(0)}$$

If not, we tend to outline DecryptNode(CT;SKu; x) := ?. If x isn't a leaf node, the rule takings as follows: For all nodes z that area unit youngsters of x, it calls DecryptNode(CT;SKu; z) and stores the output as Fz. Let Sx be associate impulsive kx-sized set of kid nodes z specified Fz =6. If no such set exists then the node wasn't glad and the rule returns, otherwise, calculate

$$F_x = \prod_{z \in S_z} F_z^{\triangle_{d, s_x'}(0)}, \text{ where } \begin{cases} d = index(z) \\ S_x' = index(z) : z \in S_x \end{cases}$$

$$= \prod_{z \in S_z} (e(g,g)^{(\sum d_k) \cdot q_z(0)})^{\triangle_{d, S_x'}(0)}$$

$$= \prod_{z \in S_z} (e(g,g)^{(\sum d_k) \cdot q_{parent(z)}(d)})^{\triangle_{d, S_x'}(0)}$$

$$= \prod_{z \in S_z} (e(g,g)^{(\sum d_k) \cdot q_x(d)})^{\triangle_{d, S_x'}(0)}$$

$$= e(g,g)^{(\sum d_k) \cdot q_x(0)}$$

The interpolation above recovers the parent node's price by scheming coefficients of the polynomial and evaluating the p(0). We tend to direct the readers to [34] for complete calculation. A user recursively calls this formula, starting from the foundation node Rp of the tree Tp, once downloading the file. If the tree is glad, which means he is granted the privilege p, then rewrite Node(CT, SKu,Rp) = e(g, g)s p Finally, if the user is creating an endeavor to browse the file, the key writing key Ke square measure typically recovered by:

$$\frac{E_0}{\frac{e(C,\hat{C})}{e(g,g)^{s_0 \sum d_k}}} = \frac{K_e \cdot Y^{s_0}}{\frac{e(g,g)^{s_0(\sum d_k + \sum v_k)}}{e(g,g)^{s_0 \sum d_k}}} = K_e$$

Then, the data file square measure typically decrypted by exploitation it. Otherwise, if he must execute some operation on the data, he ought to be verified as a accredited user for the execution initial. If the execution wants the j-th privilege, the user recursively calls Decrypt(CT, SKu, x) starting from the premise node R j of the tree Tj to induce e(g, g)s j dk and any deliver the products Y s j with constant equation as above. The user sends it to the Cloud Server also as a result of the operation request. The Cloud Server checks whether or not Y s j = E j , and yield if they're doing equal each other. In fact, Y s j needs to be encrypted to avoid replay attack. This may be simply enforced by introducing any public key encoding protocol.

V. ACHIEVING OBSCURITY ABSOLUTELY

The Obscurity A semi-honest authorities is assumed in AnonyControl and conjointly assumed that they are about to not conspire with one another. This can be a necessary assumption in AnonyControl as a results of each authority is answerable of a collection of the overall attributes set, and for the attributes that it's answerable of, it's tuned in to the precise info of the key requester. If the information from all authorities is gathered altogether, the full attribute set of the key requester is recovered and then his identity is disclosed to the authorities. During this sense, AnonyControl is semi anonymous since partial identity data (represented as some attributes) is disclosed to each authority; however we are able to reach a full-anonymity and in addition alter the collusion of the authorities. The key purpose of the identity data escape we tend to tend to had in our previous theme likewise as every existing attribute based mostly secret writing schemes is that key generator or attribute formula one 1-Out-of-2 Oblivious Transfer
Bob indiscriminately picks a secret s and publishes gs to Alice.
Alice creates associate encryption/decryption key pair:
Alice chooses i and calculates E Ki = gr, E Ki−1 = gs/gr and sends E K0 to Bob.
Bob calculates E K1 = gs/EK0 and encrypts M0 exploitation E K0 and funds exploitation E K1 and sends a pair of cipher texts EE K0(M0), engineering science K1(M1) to Alice.
Meanwhile, Bob doesn't perceive that cipher text is decrypted.Algorithm a try of 1-Out-of-n Oblivious Transfer generator has to perceive the user's attribute to undertake and do therefore. We would like to introduce a replacement technique to let key generators issue the correct attribute key whereas not knowing what attributes the users have. A naive answer is to produce all the attribute keys of all the attributes to the key requester and let him opt for despite the wants. Throughout this technique, the key generator does not perceive that attribute keys he key requester picked, however we have got to completely trust the key requester that he will not decide any attribute key not allowed to him. To unravel this, subsequent Oblivious Transfer (OT) is leveraged.

A. 1-Out-of-n Oblivious Transfer

In associate 1-out-of-n OT, the sender Bob has n messages money supply,. . ., Mn, and conjointly the receiver Alice has to choose one Mi from those funds,. . ., Mn. Alice successfully achieves Mi while not knowing any useful data relating to different messages, and Bob does not perceive that Mi is picked by Alice. [35] is employed as a building block out of the numerous implementations [35]–[37], in our completely anonymous multi-authority CP-ABE within following section. Then the 1-out-of-2 OT (Algorithm 1) is employed, inside that Alice picks Mi from Bob's M0, M1, to introduce the 1-out-of-n OT delineated in formula a try of. In formula a try of, Alice will do Mi if and providing she picks ti for the i she wants the message and sk for any k = i. If she picks several tk's, some sk's area unit missing and he or she or he is not ready to recover any message.

B. Wholly Anonymous Multi-Authority CP-ABE

In this section, we have a tendency to tend to gift the thanks to deliver the products the full obscurity in AnonyControl to designs the wholly anonymous privilege management theme AnonyControl-F. The KeyGenerate formula is that the exclusively [*fr1] that leaks

©IJRASET (UGC Approved Journal): All Rights are Reserved

identity information to each attribute authority. Upon receiving the attribute key request with the attribute price, the attribute authority will generate H(att(i))ri and sends it to the requester where att(i) is that the attribute price and Little Rhody can be a random variety for that attribute. The attribute price is disclosed to the authority throughout this step. We are able to introduce the upper than 1-out-of-n OT to forestall this outflow. We tend to let each authority be guilty of all attributes happiness to identical category. For each attribute category c (e.g., University), suppose there are a unit k achievable attribute values (e.g., IIT, NYU, CMU ...), then one requester has at the foremost one attribute worth in one category. Upon the key request, the attribute authority can select a random vary number forty four for the requester and generates H(att(i))ru for all i ∈ . Once the attribute keys area unit ready, the attribute authority and the key requester area unit engaged throughout a 1-out-of-k OT where the key requester has to receive one attribute key among k. By introducing the 1-out-of-k OT in our KeyGenerate formula, the key requester achieves the proper attribute key that he desires, however the attribute authority does not have any helpful information relating to what attribute is achieved by the requester. Then, the key requester achieves the full obscurity in our theme and yet what share attribute authorities conspire, his identity info is unbroken secret.

VII. DISCUSSION

Trust of Users: Our AnonyControl-F to boot needs to trust the requester that he picks correct attribute keys comparable to his identity, but the requester can select exclusively one attribute key in one category, that's manner on top of the naive arrange higher than, and it isn't this paper's scope to ensure the truthful news of the attributes. To the best of our knowledge, it's assumed that another authentication (e.g., government check) is in place to verify the reported attributes in most of ABE-related works. Performance: the extra computation introduced in AnonyControl-F is solely several exponent calculations that are negligible. However, additional communication overhead could be a problematic issue in AnonyControl-F. For each attribute class, the user is concerned throughout a 1-out-of-n OT that desires O(n) rounds of communication. Therefore, the communication overhead grows from O(1) in AnonyControl to O(I) where I is that the size of the entire attribute set. This may be the foremost drawback of our wholly anonymous theme that has to be compelled to be resolved in our future work.

VIII. CONCLUSIONS

This paper proposes a semi-anonymous attribute-based privilege management theme AnonyControl and a fully anonymous attribute-based privilege management theme AnonyControl-F to handle the user privacy downside throughout a cloud storage server. Using multiple authorities inside the cloud ADPS, our planned schemes attain not exclusively fine-grained privilege management but conjointly identity obscurity whereas conducting privilege management supported users' identity knowledge. Extra considerably, our system can tolerate up to N − 2 authority compromise, that's terribly fascinating notably in Internet-based cloud computing atmosphere. We've got a bent to put together conducted detailed security and performance analysis that shows that AnonyControl every secure and economical for cloud storage system. The AnonyControl-F directly inherits the protection of the AnonyControl and so is equivalently secure as a result of it, however further communication overhead is incurred throughout the 1-outof-n oblivious transfer. One in every of the promising future works is to introduce the economical user revocation mechanism on high of our anonymous ABE. Supporting user revocation could be a crucial issue inside the $64000 application, and typically this can be often a wonderful challenge within the applying of ABE schemes. Making our schemes compatible with existing ABE schemes [39]–[40] World Health Organization support economical user revocation is one all told our future works.

IX. ACKNOWLEDGMENT

I might wish to specific my feeling to Prof. Manjusha Tatiya for providing adequate facilities to finish this paper. I specify my gratitude for her support and suggestions relating to thesis. I conjointly impart Department of computer engineering for support and encouragement.

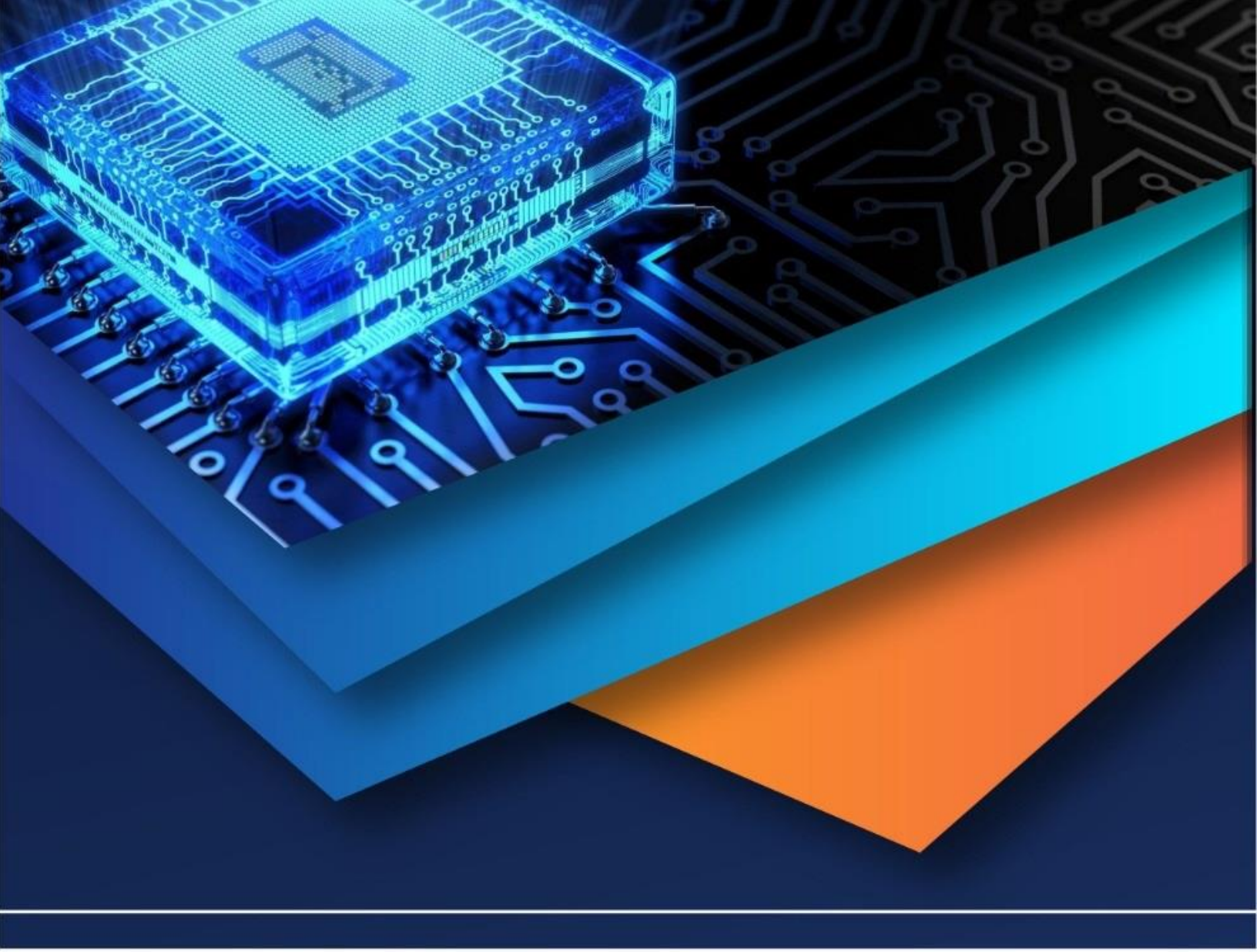
REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology.Berlin,Germany:Springer-Verlag,1985,pp.47–53.
[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. erlin,Germany:Springer-Verlag,2005,pp.457–473.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in roc. IEEE SP, May 2007, pp. 321–334.
[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.
[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

©IJRASET (UGC Approved Journal): All Rights are Reserved

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.
[8] V. Božovi´ c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283,2012.
[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing,"in Proc. IEEE 7th SOSE,-Mar.2013,pp.573–577.
[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr.2013, pp. 2895–2903.
[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology.Berlin,Germany:-Springer-Verlag-2011,pp.-568–588.
[12] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.
[13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011, pp. 386–390.
[14] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traito tracing," J. Comput. Inf. Syst., vol. 9, no. 7, pp. 2793–2800, 2013.
[15] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.
[16] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.
[17] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attributebased encryption supporting efficient decryption test," in Proc. 8th ASIACCS, 2013, pp. 511–516.
[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.
[19] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005.
[20] Liu, Z. Wan, and M. Gu, "Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," in Information Security Practice and Experience. Berlin, Germany: Springer-Verlag, 2011, pp. 98–107.
[21] A. Kapadia, P. P. Tsang, and S. W. Smith, "Attribute-based publishing with hidden credentials and hidden policies," in Proc. NDSS, 2007, pp. 179–192.
[22] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Proc. 4th Workshop Secure Netw. Protocols, Oct. 2008, pp. 39–44.
[23] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.
[24] T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacy preserving data aggregation without secure channel: Multivariate polynomial evaluation," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2634–2642.
[25] T. Jung and X.-Y. Li, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," IEEE Trans. Dependable Secure Comput.,to be published.
[26] X.-Y. Li and T. Jung, "Search me if you can: Privacy-preserving location query service," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2760–2768
[27] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, "Verifiable private multiparty computation: Ranging and ranking," in Proc. IEEE INFOCOM, Apr. 2013, pp. 605–609.
[28] L. Zhang, X.-Y. Li, and Y. Liu, "Message in a sealed bottle: Privacy preserving friending in social networks," in Proc. IEEE 33rd ICDCS, Jul. 2013, pp. 327–336.
[29] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar.2010, pp. 1–9.
[30] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.
[31] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keywordsearch over encrypted cloud data," in Proc. IEEE 30th ICDCS, Jun. 2010, pp. 253–262.
[32] Y. Liu, J. Han, and J. Wang, "Rumor riding: Anonymizing unstructured peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 464–475,Mar. 2011.
[33] Tor: Anonymized Network. [Online]. Available: https://www.torproject.org/, accessed 2014.
[34] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[35] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in Proc. 31st STOC, 1999, pp. 245–254.
[36] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," Commun. ACM, vol. 28, no. 6, pp. 637–647, 1985.
[37] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," IEEE Trans. Comput., vol. 53, no. 2, pp. 232–240, Feb. 2004.
[38] Ciphertext-Policy Attribute-Based Encryption Toolkit. [Online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.
[39] W. Ren, K. Ren, W. Lou, and Y. Zhang, "Efficient user revocation for privacy-aware PKI," in Proc. ICST, 2008, Art. ID 11.
[40] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,"IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)