iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: IX Month of publication: September 2017

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Access Privilege Control in Cloud and Achieving Obscurity with Totally Anonymous Attribute-Based Secret Writing Exploitation Fog Computing Conjointly Doing Keyword Looking Out

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

Abstract: Cloud computing may well be a revolutionary computing paradigm, that permits versatile, on-demand, and cheap usage of computing resources, but the information is outsourced to some cloud servers, and varied privacy issues emerge from it. Numerous schemes Supported the attribute-based secret writing are projected to secure the cloud storage. However, most work focuses on the information contents privacy and so the access management, whereas less attention is paid to the privilege management and so the identity privacy. Throughout this paper, we've got an inclination to gift a semi anonymous privilege management theme AnonyControl to handle not only the info privacy, but jointly the user identity privacy in existing access management schemes. Anony management decentralizes the central authority to limit the identity run and so achieves semi namelessness. Besides, it jointly generalizes the file access management to the privilege management, by that privileges of all operations on the cloud information may be managed in Associate in Nursing passing fine-grained manner. Afterwards, we tend to gift the Anony Control-F, that absolutely prevents the identity outflow and succeed the whole anonymity. Our security analysis shows that every Anony management and Anony Control-F area unit secure beneath the decisional linear Diffie–Hellman assumption, and our performance analysis exhibits the utility of our schemes.

Keywords: Anonymity, Attribute-based encryption, fog computing, namelessness, multi-authority, keyword searching

I. INTRODUCTION

CLOUD computing may be a revolutionary computing technique, by that computing resources unit provided dynamically via web and so the data storage and computation are outsourced to someone or some party throughout a ‘cloud'. It greatly attracts attention within the business world owing to the profit, but there are minimum of 3 challenges that possesses to be handled before returning to our reality to the foremost effective of information. Initial of all, information confidentiality ought to be secured. The data privacy is not solely regarding the data contents. However additionally users got to manage the privileges of knowledge manipulation over totally different users or cloud servers. Typically this can be often as a results of once sensitive data or computation is outsourced to the cloud servers or another user, that's out of users’ management in most cases, privacy risks would rise dramatically as a results of the servers could illicitly examine users’ data and access sensitive data, or totally different users will be able to infer sensitive data from the outsourced computation. Therefore, not solely the access but jointly the operation need to be controlled. Secondly, personal data is in peril as a result of one’s identity is technique supported his data for the aim of access management. As of us became further involved regarding their identity privacy recently, the identity privacy jointly has got to be protected before the cloud enters our life. Preferably, any authority or server alone should not get any client’s personal data. Last however not least, the cloud ADPS need to be resilient at intervals the case of security breach throughout that some a neighborhood of the system is compromised by attackers. varied techniques ar planned to stay safe 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 AN identity specified alone a receiver with matching identity can rewrite it. Few years later, Fuzzy Identity-Based coding [2] is planned, that's to boot remarked as Attribute-Based encoding (ABE). In such coding theme, AN identity is viewed as a bunch of descriptive attributes, and secret writing is feasible if and given that a decrypter’s identity has some overlaps with the one arranged enter the ciphertext. Soon after, further general tree-based

ABE schemes, Key-Policy Attribute-Based encoding (KP-ABE) [3] and Ciphertext-Policy Attribute primarily based coding (CP-ABE) [4], unit given to specific further general condition than straightforward 'overlap'. They're counterparts to each totally different at intervals the sense that the selection of coding policy is formed by fully different parties. within the KP-ABE [3], a ciphertext is expounded to a group of attributes, and a private secret's associated with a monotonic access structure. it's sort of a tree, that describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user will rewrite the ciphertext if and given that on condition that the access tree in his personal secret's happy by the attributes at intervals the ciphertext. However, the cryptography policy is drawn at intervals the keys, that the encrypted does not have entire management over the cryptography policy. AN encrypted must trust that the key generators issue keys with correct structures to correct users. moreover, once a re-encryption happens, all of the users at intervals identical system ought to have their personal keys re-issued so on gain access to the re-encrypted files, and this methodology causes some issues in implementation. On the other hand, those issues and overhead unit all resolved at intervals the CP-ABE [4]. within the CP-ABE, ciphertexts unit created with AN access structure, that specifies the cryptography policy, and private keys unit generated per users' attributes. A user can decrypt the ciphertext if and on condition that his attributes at intervals the private key satisfy the access tree arranged enter the ciphertext. By doing so, the encrypted holds the last word authority relating to the cryptography policy. Also, the already issued personal keys will never be changed unless the whole system reboots. not like the information confidentiality, less effort is paid to protect users' identity privacy throughout those interactive protocols. Users' identities, that unit drawn with their attributes, are usually disclosed to key issuers, and additionally the issuers issue personal keys per their attributes. but it seems natural that users unit willing to remain their identities secret whereas they get their personal keys. Therefore, AnonyControl and AnonyControl-F have planned which allow cloud servers to manage users' access privileges whereas not knowing their identity data. Their main deserves are: 1) The projected schemes unit able to protect user's privacy against each single authority. Partial data of identity is disclosed in AnonyControl and no data of identity is disclosed in AnonyControl-F. 2) The projected schemes unit tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down. 3) A careful analysis on security and performance has offered to point out usefulness of the theme AnonyControl and AnonyControl-F.

We planned a CP-ABE theme with securing the cloud mistreatment fog computing technology [17]. We tend to use this technology to launch misinformation attacks against malicious insiders that prevents them from characteristic the $64000 sensitive client information from faux chaffy information. Also we try to add here keyword searching method for bettor result which reduced the human effort.

II. LITERATURE REVIEW

In [5] and [6], a multi-authority system is given within which each user has associate degree ID (GID) which they'll act with each key generator (authority) exploitation fully totally different pseudonyms. One user's totally different pseudonyms unit of measurement tied to his personal key, however key generators never comprehend the private keys, then they're not able to link multiple pseudonyms happiness to identical user. Also, the entire attributes set is split into N disjoint sets and managed by N attributes authorities. during this setting, each authority is attentive to solely a specific region 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-about the essential threshold-based KP-ABE, that lacks generality at intervals the cryptography policy expression. many attribute based mostly cryptography schemes having multiple authorities are came into the image later [7]–[10], but they either to boot use a threshold-based ABE [7], or have a semi-honest central authority [8]–[10], or cannot tolerate many users' collusion attack [7]. The add [11] and [12] unit of measurement the foremost similar ones to ours during this they to boot tried to change the central authority at intervals the CP-ABE into multiple ones. A LSSS matrix is employed as associate degree access structure, however their theme alone converts the AND, OR gates to the LSSS matrix, that limits their cryptography policy to Boolean formula, whereas we tend to inherit the malleability of the access tree having threshold gates. Muller et al. to boot supports alone reciprocally exclusive ancient type (DNF) in their cryptography policy. Besides the particular incontrovertible fact that we tend to area unit able to specific haphazardly general cryptography policy, the system to boot tolerates the compromise attack towards attributes authorities, that won't lined in many existing works. Recently, there to boot appeared traceable multi-authority ABE [13] and [14].Those schemes introduce responsibility specific malicious users' keys area unit usually derived. On the opposite hand, in similar direction as this technique is commonly found in [15]–[16], administrative unit try to hide cryptography policy at intervals the ciphertexts, but their solutions reveal the attribute at intervals the key generation half. In [18] a distinct approach is introduced to shield sensitive knowledge with victimisation user behavior identification and decoy info referred to as as 'Fog Computing'. To some extent, these three works and ours complement each other within the sense that the combo of these two kinds protection can end in a really anonymous ABE.

III.SYSTEM OVERVIEW

Four varieties of entities: N Attribute Authorities (denoted as A), Cloud Server, information house owners and information customers. A user may be a knowledge Owner and a knowledge shopper at the same time. Authorities are assumed to possess powerful computation talents, and that they are supervised by government offices as a result of some attributes partly contains users' in person recognizable data. The entire attribute set is split into N disjoint sets and controlled by every authority, thus every authority is attentive to solely a part of attributes.

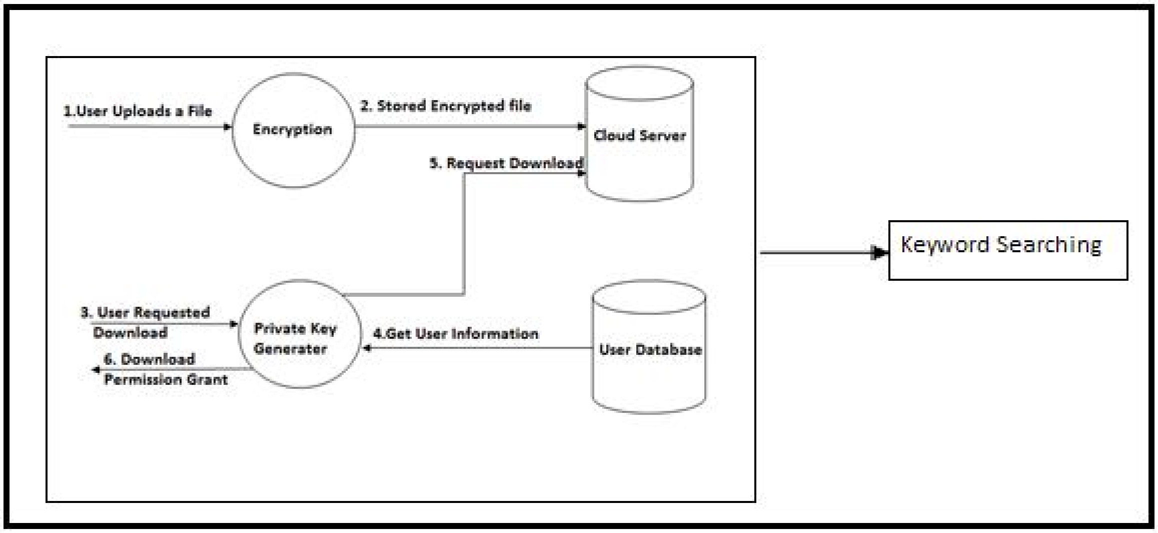

Fig. 1.System Overview

In our system we are trying to make decentralize system by using fog computing. In this system we are replacing drawbacks of cloud system such as assessing data. We reduce that method we provide high level security such as information assessing for particular country, area, domain, etc. if anyone want to try it interrupt to this then it got fake information also our system can store the IP address of that particular machine block it.

Here we make sure that to provide more facilities for users for their easy life those facilities is key word searching. It is more efficient to make user friendly system.

IV.DOWNSIDE FORMULATION

A. System Model

In our system, there are four varieties of entities: N Attribute Authorities (denoted as A), Cloud Server, information house owners and Data customers. Users are often a knowledge Owner and a knowledge Consumer at the same time. Authorities are assumed to own powerful computation talents, and that they are supervised by government offices as a result of some attributes partly 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 information files, however solely those whose non-public keys satisfy the privilege tree Tp will execute the operation related to privilege p. The server is delegated to execute associate degree operation p if and provided that the user's credentials are verified through the privilege tree Tp.

B. Threats Model

We assume the Cloud Servers ar semi-honest, who behave properly in most of your time however might conspire with malicious information Consumers or information house owners to reap others' file contents to gain illegitimate profits. however they're conjointly assumed to realize legal benefit once users' requests are properly processed, which means they'll follow the protocol normally. N authorities are assumed to be untrusted. That is, they will follow our planned protocol normally, but try to find out the maximum amount data as doable separately. More specifically, we tend to assume they're inquisitive about users' attributes to achieve the identities, however they'll not conspire with users or alternative authorities. This assumption is analogous to several previous researches on security issue in cloud computing (see [20], [29]–[31]), and it's conjointly cheap since these authorities are going to be audited by government offices. However, we will any relax this assumption and permit the collusion between the authorities in Section VI. Data shopper's area unit untrusted since they're random users including attackers. They will interact with alternative information shoppers to lawlessly access what they're not allowed to. Besides, we tend to don't take into account the identity outpouring from the underlying network since this will be trivially prevented by employing anonymized network protocols (see [32], [33]).

C. *AnonyControl Construction*

To formally outline the protection of our AnonyControl, we first provide the subsequent definitions. Setup → PK, MKk: This algorithmic program takes nothing as input except implicit inputs like security parameters. Attributes authorities execute this algorithmic program to collectively cypher a system-wide public parameter PK similarly as associate degree authority-wide public parameter yk, and to separately cypher a master key MKk. Key Generate(PK, MKk, Au) → SKu: This algorithmic program enables a user to move with each attribute authority, and obtains a personal key SKu similar to the input attribute set Au. Encrypt(PK, M, p∈) → (CT, VR): This algorithm takes as input the general public key PK, a message M, and a set of privilege trees p∈, wherever r is set by the encrypter. it'll encipher the message M and returns a ciphertext CT and a verification set VR in order that a user will execute specific operation on the ciphertext if and provided that his attributes satisfy the corresponding privilege tree Tp. As we defined, T0 stands for the privilege to browse the file. Decrypt (PK, SKu, CT) → M or verification parameter: This algorithmic program are going to be used at file dominant (e.g. reading, modification, deletion). It takes as input the general public key PK, a ciphertext CT, and a personal key SKu, that contains a set of attributes Au and corresponds to its holder's GIDu. If the set Au satisfies any tree within the set p∈, the algorithmic program returns a message M or a verification parameter. If the verification parameter is with success verified by Cloud Servers, who use VR to verify it, the operation request are going to be processed. Next, we tend to outline the protection of our AnonyControl with the following game. Init: The someone A declares the set of compromised authorities ⊂ A (where a minimum of 2 authorities in a very are not management led by A) that area unit below his control (remaining authorities A/ area unit controlled by the challenger). Then, he declares T0 that he desires to be challenged, during which some attributes area unit being in charged by the challenger's authorities. Setup∗: The contender and therefore the someone collectively run the Setup algorithmic program to receive the valid outputs. Phase 1: The someone launches Key Generate algorithms to query for as several non-public keys as he desires, that correspond to attribute sets A1,. . ., Aq being disjointly in charged by all authorities , however none of those keys satisfy T0. Besides, he conjointly conducts randomly several computations mistreatment the public and secret keys that he has (belonging to compromised authorities). Challenge: The someone submits 2 messages M0 and M1 of equal size to the contender. The contender flips a random binary coin b and encrypts Mb with T0. The ciphertext CT is given to the someone. Phase 2: part one is recurrent adaptively, however none of the queried keys satisfy T0. Guess: The someone outputs a guess b of b. The advantage of associate degree someone A during this game is outlined as Pr[b = b] − one two . Definition 2: Our theme is secure and indistinguishable against chosen-attribute attack (IND-CAA) if all probabilistic polynomial-time adversaries (PPTA) have at the most a negligible advantage within the on top of game. Note that the IND-CAA outlined on top of implies IND-CCA since the someone will conduct encryptions and decryptions mistreatment the general public keys and secret keys it owns in Phase one and part two (but he cannot rewrite the target ciphertext since none of its secret keys satisfy T0).

D. *Style Goal*

Our goal is to realize a multi-authority CP-ABE which: achieves the protection outlined 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, we regularly use the subsequent notations 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 formatting part, anyone of the authorities chooses a linear cluster G0 of prime order p with generator g and publishes it. Then, all authorities severally and randomly picks vk ∈ Zp and send Yk = e(g, g)vk to all or any other authorities United Nations agency one by one reason Y := k∈A Yk = e(g, g)k∈A vk .Then, each authority American state willy-nilly picks N − one integers skj ∈ Zp(j ∈ \) and computes gskj . Each gskj is shared with one another authority A j. Associate in Nursing authority American state, after receiving N − one items of gs jk generated by A j , computes its secret parameter xk ∈ Zp as follows:

$$Xk = (\Pi_{j\in\{1,\ldots N\}\{k\}} g^{skj})/(\Pi_{j\in\{1,\ldots N\}\{k\}} g^{skj})$$

$$=g(\Sigma_{j\in\{1,\ldots N\}\{k\}} skj - \Sigma_{j\in\{1,\ldots N\}\{k\}} skj)$$

It is simple to examine that these haphazardly made integers satisfy k∈A xk = one mod p. this can be a vital property which achieves compromise attack tolerance for our theme, which will be mentioned within the next section. Then, the passkey for the authority American state is MKk = {vk, xk},, and public key of the entire system is printed as PK ={G0, g, Y = e(g, g)vk} Note that the time complexness of the setup computation is O(N2) since each authority computes N − one items of gskj . However, this will be any reduced to O(N) by applying the following straightforward trick. we tend to initial cluster the authorities into C clusters, and exchanges the parameters among the cluster solely. Then, the time complexness is reduced to O(C N) = O(N) since C could be a constant.

B. Title and Author Details Keygenerate(PK, MKk, Au)

When a replacement user u with GIDu needs to hitch the system, he requests the non-public key from all of the authorities by following this method that consists of 2 phases. 1) Attribute Key Generation: For any attribute i ∈ Au, every Ak indiscriminately picks Ocean State ∈ Zp to severally cipher the partial private keys H(att(i))ri, Di = gri, that square measure in private sent to the user u. Then, every authority AK indiscriminately picks dk ∈ Zp, computes xk · gvk · gdk and in private shares it with alternative authorities (i.e. unbroken secret to the user u). Then, he in private sends xk ·gdk to the user u (i.e. unbroken secret to alternative authorities). Any one of N authorities computes and sends the subsequent term to the user u: D = πxkgvk gdk = $g^{\Sigma vk}$ + $g^{\Sigma dk}$ where gvk acts as a system-wide key wont to generate a valid secret key, however no single authority is in a position to infer its value. a legitimate D with a legitimate gvk are often achieved only if all the authorities properly follow the protocol and conduct a joint computation. Then, the user computes the subsequent term that is that the attribute key for the attribute i (att(i) refers to the part in G0 such as i): Di = H(att(i))ri · π(xk · gdk) = H(att(i))ri · g(dk) Note that Di is computed firmly while not revealing individual gdk's to the user or revealing gdk to any attribute authority. this can be vital within the tolerance to the compromise attack, which is able to be mentioned later. 2) Key Aggregation: User u, once receiving D, Di 's and D i 's, aggregates the elements as his non-public key: SKu = { D, ∀i ∈ Au : Di = g(dk) · H(att(i))ri, Di = gri }

C. Encrypt(PK, M, {Tp}p∈{0,…,r–1})

The Data Owner encrypts the info with any existing symmetric secret writing theme, and generates the secret writing key Ke. Then, he determines a group of privilege trees p∈ and executes Encrypt(PK, Ke,). Remember that the privilege tree in our theme is based on the brink gates. Here, Shamir's secret sharing technique [34] is directly wont to implement the brink gate. Shamir's t-out of-n secret share theme permits one to divide a secret to n shares, and also the original secret are often recovered with t of them. So, in our tree, the node worth of the gate is recovered if and providing a minimum of kx values of kids nodes are recovered in algorithmic manner. The random range, which is used to mask the secret writing key Ke, is keep at the basis of the privilege tree and is secret-shared to its kids nodes, and the secret shares within the kids nodes square measure secret-shared to their kids nodes, thus so forth till the algorithmic secret sharing reaches the leaf nodes. This is enforced within the following method. for every Tp, the formula initial chooses a polynomial qx for every node x in it. for every node x, sets the degree dx of the polynomial qx in concert but the brink worth kx. ranging from the root node Rp, the formula indiscriminately picks sp ∈ Zp and sets qR p(0) := sp and indiscriminately chooses alternative coefficients for qR p. Then, for the other node x, the coefficients square measure chosen randomly and also the constant term is ready as qparent(x)(index(x)) such that qx(0) = qparent(x)(index(x)) (index(x) is that the index of the x's kid nodes, and parent(x) is node x's parent node). Finally, he picks a random part h ∈ Zp such h−1 mod p exists, and calculates gh·s p, Dh−1, and also the ciphertext CT is formed 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 is comparable to the concept appeared in [4], but in different ways: they introduced such a inverse within the power in key generation formula whereas we tend to will thus within the secret writing in order to attain the de-centralization. Then, VR, that is disclosed solely to the Cloud Server, is created for the aim of privilege verification. VR = {E p = Y s p}p∈{1,...,r-1} Finally, knowledge Owner sends CT, VR and also the encrypted file to the Cloud Server to share them with alternative knowledge shoppers.

D. Decrypt(PK, SKu, CT)

Every user among the system will transfer the ciphertext from the Cloud Server, however he's ready to execute operations on encrypted knowledge solely once he with success decrypts it. Firstly, we outline a algorithmic formula decipher Node(CT, SKu, x), where x stands for a node within the privilege tree Tp. If the node x could be a leaf node, we tend to let i be the attribute of the node x and define as follows. If i ∈ Au,

Decrypt Node

(CT, SKu, x) = e(Di, Cx)/e(Di, Cx)

= e(g Σ dk · H(att(i))ri, gqx(0)) /e(gri, H(att(i))qx(0))

= e(g, g)(Σ dk)·qx(0)

If not, we tend to outline decipher Node(CT, SKu, x) := ⊥. If x isn't a leaf node, the formula yield as follows: For all nodes z that square measure kids of x, it calls decipher Node(CT, SKu, z) and stores the output as Fz. Let Sx be associate degree discretional kx-sized set of child nodes z such Fz = ∅. If no such set exists then the node wasn't glad and also the formula returns ⊥. Otherwise, compute

Fx = $\prod_{Z \in Sxz}$ FzΔds 'x(0) where d =index (z) Sx'= index (z):Z ∈ Sx

=$\prod_{Z \in Sx}$(e(g, g) Σ(dk). qz(0) Δd, s'x(0)

=$\prod_{Z \in Sx}$(e(g, g) Σ(dk). qparent (z)(d))Δd, s'x(0)

= $\prod_{Z \in Sx}$(e(g, g) Σ(dk). qx(d)Δd, s'x(0)

=e(g, g)(dk)·qx(0)

The interpolation higher than recovers the parent node's worth by scheming coefficients of the polynomial and evaluating the p(0). we tend to direct the readers to [34] for complete alculation. A user recursively calls this formula, ranging from the root node Rp of the tree Tp, once downloading the file. If the tree is glad, which implies he's granted the privilege p, then Decrypt Node(CT, SKu, Rp) = e(g, g)s pΣ dk Finally, if the user is making an attempt to browse the file, the secret writing key Ke are often recovered by:

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

Then, the info file are often decrypted by exploitation it. Otherwise, if he needs to execute some operation on the info, he should be verified as a licensed user for the execution initial. If the execution needs the j-th privilege, the user recursively calls Decrypt(CT, SKu, x) ranging from the basis node R j of the tree Tj to induce e(g, g)s j dk and any deliver the goods Y s j with the same equation as higher than. The user sends it to the Cloud Server as well because the operation request. The Cloud Server checks whether Y s j = E j , and yield if they are doing equal one another. In fact, Y s j ought to be encrypted to avoid replay attack. This can be merely enforced by introducing any public key encryption protocol.

VI. ACHIEVING FULL

Obscurity We have assumed semi-honest authorities in AnonyControl and we assumed that they're going to not conspire with one another. This is a necessary assumption in AnonyControl as a result of every authority is to blame of a set of the total attributes set, and for the attributes that it's to blame of, it is aware of the precise information of the key requester. If the data from all authorities is gathered altogether, the whole attribute set of the key requester is recovered and so his identity is disclosed to the authorities. during this sense, AnonyControl is semi anonymous since partial identity info (represented as some attributes) is disclosed to every authority, but we can achieve a full-anonymity and additionally enable the collusion of the authorities. The key purpose of the identity info escape we tend to had in our previous theme likewise as each existing attribute based secret writing schemes is that key generator or attribute Algorithm one 1-Out-of-2 Oblivious Transfer

Bob indiscriminately picks a secret s and publishes gs to Alice.

Alice creates associate degree 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 money supply exploitation E K1 and sends 2 cipher texts EE K0(M0), EE K1(M1) to Alice.

Alice will use r to decipher the specified cipher text EE Ki(Mi), however she cannot decipher the opposite one. Meanwhile, Bob doesn't understand that cipher text is decrypted.

Algorithm a pair of 1-Out-of-n Oblivious Transfer

Bob indiscriminately picks n secrets s1,. . ., metal and calculates ti as follows:

$\forall i \in$: $t_i = s_1 \oplus \cdots \oplus s_{i-1} \oplus M_i$

for every $i \in$, Bob and Alice square measure engaged in a 1-out-of-2 OT wherever Bob's initial message is ti and also the second message is si. Alice picks ti to receive if she needs Mi and si otherwise.

once Alice receives n elements, she has $t_i = s_1 \oplus \cdots \oplus s_{i-1} \oplus M_i$ for the i she needs and sk for k = i, she can recover the Mi by $M_i = t_i \oplus s_{i-1} \oplus s_{i-2} \oplus \cdots \oplus s_1$ authorities in our scheme problems attribute key supported the reported attribute, and also the generator needs to understand the user's attribute to try and do thus. we want to introduce a replacement technique to let key generators issue the right attribute key while not knowing what attributes the users have. A naive answer is to provide all the attribute keys of all the attributes to the key requester and let him choose no matter he needs. During this method, the key generator does not understand that attribute keys the key requester picked, but we've got to totally trust the key requester that he won't pick any attribute key not allowed to him. To unravel this, we leverage the subsequent Oblivious Transfer (OT).

A. 1-Out-of-n Oblivious Transfer

In associate degree 1-out-of-n OT, the sender Bob has n messages M1,. . ., Mn, and also the receiver Alice needs to select one Mi from those money supply,. . ., Mn. Alice with success achieves Mi without knowing any helpful info regarding alternative messages, and Bob doesn't understand that Mi is picked by Alice. We use [35] as a building block out of the many implementations [35]–[37], in our totally anonymous multi-authority CP-ABE within the next section. We use the 1-out-of-2 OT (Algorithm 1), within which Alice picks Mi from Bob's M0, M1, to introduce the 1-out-of-n OT delineated in formula a pair of. In formula a pair of, Alice can do Mi if and providing she picks ti for the i she needs the message and sk for any k = i. If she picks many tk's, some sk's square measure missing and she or he isn't able to recover any message.

B. Totally Anonymous Multi-Authority CP-ABE

In this section, we tend to gift the way to deliver the goods the total obscurity in AnonyControl to styles the totally anonymous privilege control theme AnonyControl-F. The KeyGenerate formula is that the solely half that leaks identity info to every attribute authority. Upon receiving the attribute key request with the attribute worth, the attribute authority can generate H(att(i))ri and sends it to the requester wherever att(i) is that the attribute worth and Ocean State could be a random number for that attribute. The attribute worth is disclosed to the authority during this step. It is introduced the higher than 1-out-of-n OT to forestall this leakage. we tend to let every authority be to blame of all attributes belonging to identical class. for every attribute class c (e.g., University), suppose there square measure k doable attribute values (e.g., IIT, NYU, CMU ...), then one requester has at the most one attribute worth in one class. Upon the key request, the attribute authority will choose a random range atomic number 44 for the requester and generates H(att(i))ru for all i ∈ {1…..k}. After the attribute keys square measure prepared, the attribute authority and the key requester square measure engaged during a 1-out-of-k OT wherever the key requester needs to receive one attribute key among k. By introducing the 1-out-of-k OT in our KeyGenerate algorithm, the key requester achieves the right attribute key that he needs, however the attribute authority doesn't have any useful info regarding what attribute is achieved by the requester. Then, the key requester achieves the total obscurity in our theme and notwithstanding what percentage attribute authorities collude, his identity info is unbroken secret.

VII. SYSTEM ANALYSIS

A. Tolerance Against Authorities

Collusion or Compromise Attack In the projected theme, associate degree authority AK generates a group of random secret parameters and shares gskj it with other authorities via secure channel, and xk is computed based on this parameters. it's believed that DDH downside is uncontrollable within the cluster G0 of prime order p, therefore gskj doesn't leak any applied mathematics info regarding skj . This implies though associate degree mortal is in a position to compromise up to (N − 2) authorities, there square measure still 2 parameters skj unbroken unknown to the mortal. So, the mortal isn't ready to guess the valid gvk , and he fails to construct a legitimate secret key. Hence, the theme achieves compromise tolerance to up to (N − 2) authorities compromise. But, if we tend to scale back the time complexness of the setup section by dividing authorities into many clusters having C authorities in every, attackers can compromise C − one authorities during a cluster to form valid master keys of that cluster. Therefore, there's a trade-off between tolerance and complexness. However, since the number of authorities is usually not terribly Brobdingnagian, and also the setup is one-time operation at the terribly starting of the system setup, It is suggested to exploitation the initial setup formula whose complexity is O(N2). Note that the compromised authorities square measure ready to issue valid attribute keys that they're to blame of, so the ciphertexts whose privilege trees have solely those attributes might be lawlessly decrypted if the offender issue all doable attribute keys to himself. But, since the authority's square measure well protected servers, it's exhausting to compromise even one authority, and the likelihood of compromising enough authorities to illegally decipher some ciphertext is extremely low.

B. Tolerance against Users' Collusion Attack

In order to access a plaintext, attackers should recover Y s0 = e(g, g)s0 vk , which may be recovered providing the attackers have enough attributes to satisfy the tree T0. When two completely different keys' elements square measure combined, the combined key cannot undergo the polynomial interpolation within the decryption formula attributable to the various randomizers in every key. Therefore, a minimum of one key ought to be valid to satisfy a privilege tree.

C. Formal Proof

With same properties (indistinguishability of skj 's and inability of interpolation exploitation completely different users' keys), we square measure able to formally prove that AnonyControl and AnonyControl-F square measure each secure. To be granted the file access privilege (Tp = T0), one has to recover Y s0 from E0 = Ke · Y s0, whereas one has to recover Y s p if he needs alternative privileges. they're primarily identical parameters with completely different values, so it's enough to prove that no polynomial time adversaries have important advantage in our security game (Section IV, outlined just for the file access privilege) to indicate the safety of our schemes rather than proving it for all privileges. Theorem 7.1: If associate degree mortal includes a non-negligible advantage in our security game (Section IV), there exists a minimum of one probabilistic polynomial-time formula UN agency will solve the DBDH downside (Section III) with a non-negligible advantage. Proof: Suppose a probabilistic polynomial-time adversary's advantage in our security game is .we tend to prove that the following DBDH game are often solved with a bonus a pair of . Let e : G0 × G0 → GT be a linear map, where G0 is a increasing cyclic cluster of prime order p and g is its generator. Initial the DBDH contestant flips a binary coin μ, and he sets (g, A, B, C, Z) := (g, ga, gb, gc, e(g, g)abc) if $\mu = 0$; otherwise he sets (g, A, B, C, Z) := (g, ga, gb, gc, e(g, g)z), where a, b, c, z ∈ Zp square measure indiscriminately picked. The contestant then provides the machine g, A, B, C, Z = g, ga, gb, gc, Z . The machine sim then plays the role of a contestant within the following DBDH game. Init: The mortal A controls the set of compromised authorities ⊂ A (where a minimum of 2 authorities during a square measure not controlled by A), and remaining authorities A/ square measure controlled by sim. Then, he declares a T0 that he needs to be challenged, within which some attributes square measure being in charged by the simulator's authorities A/ (i.e., non-compromised authorities). Setup: sim sets a = dk, b = d vk k , c = s0, where d1, . . . , dn, v1, . . . , vn, s0 ∈ Zp square measure all indiscriminately chosen. Meanwhile, he sets the parameter Y := e(A, B) = e(g, g)ab and gives this public parameter to A.

Phase 1: A queries for as several non-public keys as he needs, which correspond to the attributes sets A1, . . . , Aq being disjointly in charged by all authorities , however none of them satisfy the T0. sim, once receiving the key queries, computes the elements privately keys to reply the A's requests. For all attributes i ∈ Au, he indiscriminately picks Ocean State ∈ Zp, and computes Di := A · H(att(i))ri, Di := gri . Then, sim returns the created non-public keys to A. Challenge: The mortal A submits 2 challenge messages m0 and money supply to the contestant. The contestant flips a binary coin γ, and returns the subsequent ciphertext to A. CT* = T0, E0 = mγ · Z, i∈AT0 If $\mu = 0$, Z = e(g, g)abc. Note that a = dk, ab = vk and c = s0, and that we have Z = e(g, g)abc = (e(g, g)ab)c = Y s0 and Di = g dk H(att(i))ri . Therefore, CT* could be a valid ciphertext of the message mγ , and Di could be a valid element of the non-public key. Otherwise, if $\mu = 1$, Z = e(g, g)z. Then, we have E0 = mγ · e(g, g)z. Since z ∈ Zp could be a random part, E0 could be a random part in GT from A's perspective (if DBDH is hard within the prime order cluster GT), so CT∗ contains no info regarding m γ .

Phase 2: Repeat section one adaptively. Guess: A submits a guess γ of γ . If $\gamma = \gamma$, sim outputs $\mu = 0$, indicating that it absolutely was given a legitimate DBDH-tuple (g, A, B, C, Y s0), otherwise it outputs μ = one, indicating that he was given a random 5-element tuple (g, A, B, C, Z). As shown within the construction of the sport, the machine sim computes the general public parameter and also the non-public key within the same method as our theme. When $\mu = 1$, the adversary A learns no info regarding γ , so we have Pr[$\gamma = \gamma$ |μ = one] = Pr[$\gamma = \gamma$ |$\mu = 1$] = 1 a pair of. Since the machine sim outputs his guess μ = one once $\gamma = \gamma$, we've got Pr[$\mu = \mu$|μ = one] = Pr[$\gamma = \gamma$ |$\mu = 1$] = 1 a pair of. If $\mu = 0$, the mortal A gets a legitimate ciphertext of mγ . A's advantage during this state of affairs is by definition, so we have Pr[$\gamma = \gamma$ |$\mu = 0$] = a pair of one + . Since the machine provides his guess μ = zero once $\gamma = \gamma$, we've got Pr[μ = μ|$\mu = 0$] = Pr[$\gamma = \gamma$ |$\mu = 0$] = one a pair of + . the advantage during this DBDH game is:

Pr[$\mu = \mu|\mu = 0$]Pr[$\mu = 0$] + Pr[μ `= $\mu|\mu = 1$]Pr[$\mu = 1$] −1/2

$=1/2\cdot (1/2+\epsilon) +1/2\cdot 1/2-1/2$

$= \epsilon /2$

To conclude, the advantage for a PPTA within the DBDH game is a pair of if the advantage for a polynomial-time mortal in our security game is . Therefore, if associate degree mortal includes a non-negligible advantage in our security game, he has a non-negligible advantage to unravel the DBDH downside. Based on the idea that no PPTA will solve the DBDH problem with non-negligible advantage, it are often deduced that no mortal has important advantage in our security game. Therefore, our AnonyControl is secure per the definition in Section IV.

1) Security of AnonyControl-F: the sole distinction between AnonyControl and AnonyControl-F is that the recently introduced 1-out-of-n OT throughout the KeyGenerate formula. Therefore, as long because the introduced OT doesn't leak information regarding the attributes that square measure transferred via it, AnonyControl-F leaks the maximum amount as info as AnonyControl will. Since the 1-out-of-n OT employed in our work is proved to be secure [35], AnonyControl-F is as secure as AnonyControl. A Data Owner is that the entity WHO desires to source encrypted file to the Cloud Servers. The Cloud Server, WHO is assumed to own adequate storage capability, will nothing however store them. new joined information shoppers request personal keys from all of the authorities, and that they don't apprehend that attributes square measure controlled by that authorities. once the information shoppers request their personal keys from the authorities, authorities conjointly produce corresponding personal key and send it to them. All information shoppers square measure ready to transfer any of the encrypted information files, however solely those whose personal keys satisfy the privilege tree Tp will execute the operation related to privilege p. The server is delegated to execute AN operation p if and given that the user’s credentials square measure verified through the privilege tree Tp.

Authorities square measure assumed to own powerful computation talents, and that they square measure supervised by government offices as a result of some attributes partly contain users’ in person recognizable data. The complete attribute set is split into N is joint sets and controlled by every authority, thus every authority is awake to solely a part of attributes. Mistreatment fog computing several issues like looking key word are often simply solved.

There will be extra modifications in this system.

1) Causing generated key to email ID of the user WHO requested the file for transfer.

2) Looking keywords in encrypted information by mistreatment fog technique.

3) generate fake document for unwanted users who try to assessing information.

4.)Collect information of such fake users like their IP address and make sure to block them.

5) Also add new feature that is key word searching.

VIII. MATHEMATICAL MODEL

Input – uploaded file Encrypted formF{a,b,c,…..n}

Output-Decrypted file E {a,b,c,…n}

Steps :

A. User A is uploaded file F having data

B. Encryption key k generated

C. Apply K on file F {a,b,c,..n}=>E{a,b,c,…n} On download request generate private key
p= (c) = cdmodn

D. Valid used can access file i.e download filei.e user name && pass word && security question = true -> original file download

E. File can encrypted DECRYPT(m) = memod n.

F. User name && password && security question = false -> duplicate file download.

G. Q i.e IP for fake users for(Q=0; Q<=255;Q++) [{192.10.14.236,192.45.236.478,…..etc} collect]

H. By using fog computing data (N) stored in DB Search key words K(1,2,3,…,n).

IX.PERFORMANCE ANALYSIS

Here we analysis our system on the basic of their actually result shown by the system. Following figures show that exact what happened when fog technique used then exactly memory they used for performing operation.

TABLE I
FAKE ACCESS VS REAL ACCESS

Fog Computing

#Fake Access		#Real Acess	
System Count	Real Count	System Count	Real Count
10	10	20	20

Table II
Memory used in keyword searching in time

Keyword	Memory	Time (ms)
Exact	225	11.2
Fuzzy	243	6.2

Table III.
Different type of searching techniques.

Search Techniques	Memory Uses(MB)	
	Documents in Cloud	DBLP Dataset
Exact	238	236
Fuzzy	235	232

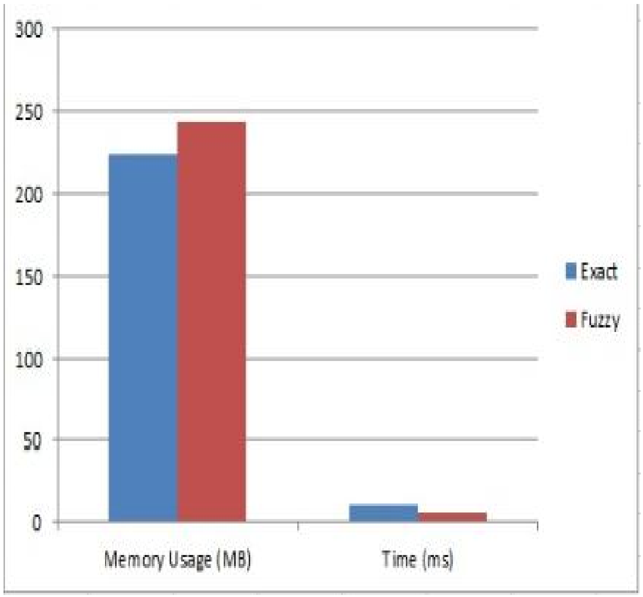

Fig. 2 Graph od Memory Usage

Figure 2 shows the graph of memory usage. So by their results our system can be is better than previous system.

X. 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 deal with the user privacy disadvantage throughout a fog storage server. victimization multiple authorities inside the fog ADPS, our planned schemes attain not only fine-grained privilege management but collectively identity obscurity whereas conducting privilege management supported users' identity information. Further 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 an inclination to collectively conducted careful security and performance analysis that shows that AnonyControl every secure and economical for fog storage system. The AnonyControl-F directly inherits the protection of the AnonyControl and thus is equivalently secure as a result of it, however further communication overhead is incurred throughout the 1-out-of-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 may be a crucial issue inside the $64000 application, and this is this can be often a wonderful challenge inside 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.

XI.ACKNOWLEDGMENT

I would like to express my gratitude to Prof. Manjusha Tatiya for providing me adequate facilities to complete this paper. I express my gratitude for her support and suggestions regarding dissertation. I also thank 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

[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.573–57

[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. 2895–2903EEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. ,JANUARY-2015 JUNG et al.: CONTROL CLOUD DATA ACCESS PRIVILEGE AND ANONYMITY-19

[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. 201

[17] [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 a

[20] nd B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005. J. Liu, Z. Wan, and M. Gu, “Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cl

[21] oud computing,” in Information Security Practice and Experience. Berlin, Germany: Springer-Verlag, 2011, pp. 98–107.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 attributebased 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, “Privacypreserving 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.

[26] 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

[27] 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.

[28] 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.

[29] 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

[30] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. IEEE 30th ICDCS, Jun. 2010, pp. 253–262.

[31] 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

[32] Tor: Anonymized Network. [Online]. Available: https://www.torproject.org/, accessed 2014

[33] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979

[34] M. Naor and B. Pinkas, “Oblivious transfer and polynomial evaluation,” in Proc. 31st STOC, 1999, pp. 245–254.

[35] S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” Commun. ACM, vol. 28, no. 6, pp. 637–647, 1985.

[36] 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.

[37] Ciphertext-Policy Attribute-Based Encryption Toolkit. [Online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.

[38] W. Ren, K. Ren, W. Lou, and Y. Zhang, “Efficient user revocation for privacy-aware PKI,” in Proc. ICST, 2008, Art. ID 11.

[39] 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.