Limitation of cloud data entry authority and obscurity with fully unknown characteristic-Based Encryption

Mr. B. RAJINI KANTH

Asst. Professor

Department of CSE

Mr. UGADI SIVA KUMAR

M.Tech in Computer Science

Department of CSE

Malla Reddy Institute of Technology, Maisammaguda, Dhulapally Post, Secunderabad and Telengana State, India.

Abstract:

Cloud computing is a modern computing paradigm, which permits flexible, on-demand, and occasional-price utilization of computing assets, however the information is outsourced to some cloud servers, and diverse privacy worries emerge from it. Diverse schemes primarily based at the attribute-based totally encryption have been proposed to at ease the cloud garage. But, maximum work makes a specialty of the facts contents privacy and the get right of entry to control, even as less attention is paid to the privilege manipulate and the identification privateness. Here we gift a semi-anonymous privilege manage scheme AnonyControl to deal with now not most effective the statistics privacy, however also the person identification privateness in existing access manipulate schemes. AnonyControl decentralizes the significant authority to restrict the identification leakage and for this reason achieves semi-anonymity. Except, it also generalizes the document access control to the privilege manage, by using which privileges of all operations on the cloud statistics can be managed in a first-class-grained way. Eventually, we present the AnonyControl-F, which fully prevents the identification leakage and reap the total anonymity. Our safety analysis suggests that each AnonyControl and AnonyControl-F is comfortable underneath the decisional bilinear Diffie–Hellman assumption, and our overall performance evaluation reveals the feasibility of our schemes.

Index Terms: Anonymity, multi-authority, attribute-based encryption.

Introduction:

CLOUD computing is a modern computing method, with the aid of which computing sources are supplied dynamically thru internet and the records storage and computation are outsourced to someone or some birthday celebration in a 'cloud'. It substantially draws attention and hobby from both academia and industry because of the profitability, but it also has at the least 3 demanding situations that ought to be dealt with earlier than coming to our actual life to the nice of our information. Initially, records confidentiality needs to be guaranteed. The statistics privacy isn't always best approximately the information contents. Since the maximum attractive a part of the cloud computing is the computation outsourcing, it's far a long way past sufficient to just behavior an access manage. Much more likely, users need to control the privileges of data manipulation over other customers or cloud servers. That is due to the fact when touchy statistics or computation is outsourced to the cloud servers or any other consumer, which is out of customers' manage in most cases, privacy dangers could rise dramatically due to the fact the servers might illegally investigate customers' facts and get right of entry to touchy statistics, or other customers might be in a position to infer touchy records from the outsourced computation. Consequently, not simplest the get entry to but also the operation must be controlled. Secondly, non-public statistics (defined with the aid of every consumer's attributes set) is at risk because one's identity is authenticated based on his facts for the purpose of get right of entry to manage (or privilege manipulate on this paper). As human beings are becoming more worried approximately their identification privateness nowadays, the identity privacy additionally wishes to be included earlier than the cloud enters our life. Ideally, any authority or server by me should now not recognize any client's private statistics. Last however no longer at-least, the cloud computing machine ought to be resilient in the case of safety breach in which some part of the machine is compromised by means of attackers.

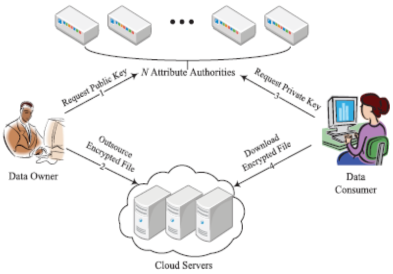


Fig. 1. General flow of our scheme.

Numerous strategies had been proposed to guard the information contents privacy via access management. Identification-based totally encryption (IBE) became first brought by using Shamir, in which the sender of a message can specify an identity such that most effective a receiver with matching identification can decrypt it. Few years later, Fuzzy identity-based totally Encryption is proposed, which is also called Attribute based totally Encryption (ABE). In such encryption scheme, identification is regarded as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the only precise in the cipher-text. Soon after, more standard tree-primarily based ABE schemes, Key-policy attribute-based totally Encryption (KP-ABE) and Cipher-text policy characteristic- primarily based Encryption (CP-ABE), are offered to specific greater well-known condition than simple 'overlap'. They are the counterparts to each other inside the sense that the decision of encryption policy (who can or cannot decrypt the message) is made by using extraordinary parties.

In the KP-ABE, a cipher-text is associated with a set of attributes, and a non-public secret's related to a monotonic get admission to shape like a tree, which describes this user's identity (e.g. IIT AND (Ph.D OR master)). A person can decrypt the cipher-text if and only if get right of entry to tree in his personal key's satisfied by using the attributes inside the cipher-text. However, the encryption coverage is described within the keys, so the encrypter does not have complete control over the encryption coverage. He has to accept as true with that the key mills problem keys with correct systems to accurate users. Moreover, whilst a re-encryption occurs, all of the customers inside the same device must have their personal keys re-issued in an effort to advantage get admission to the re-encrypted documents, and this system causes vast troubles in implementation. Alternatively, the ones troubles and overhead are all solved inside the CP-ABE. Within the CP-ABE, cipher-texts are created with an access structure, which specifies the encryption coverage, and private keys are generated in line with customers' attributes. A user can decrypt the cipher-text if and best if his attributes within the non-public key fulfill the get right of entry to tree precise in the cipher-text. Through doing so, the encrypted holds the closing authority approximately the encryption policy. Additionally, the already issued private keys will never be changed except the entire system reboots. Unlike the statistics confidentiality, much less effort is paid to shield customers' identity privacy for the duration of those interactive protocols. Customers' identities, which can be described with their attributes, are usually disclosed to key issuers, and the issuers trouble personal keys in step with their attributes. But it seems natural that users are willing to hold their identities secret at the same time as they nevertheless get their private keys. Therefore, we propose AnonyControl and AnonyControl-F (Fig. 1) to allow cloud servers to govern users' get right of entry to privileges without knowing their identification statistics.

Their most important merits are:

1) The proposed schemes are able to shield consumer's privacy in opposition to each single authority. The partial facts are disclosed in AnonyControl and no data is disclosed in AnonyControl-F.

2) The proposed schemes are tolerant in opposition to authority compromise, and compromising of as much as (N −2) government does no longer bring the whole gadget down.

3) We offer particular evaluation on protection and performance to expose feasibility of the scheme AnonyControl and AnonyControl-F.

4) We first of all put in force the actual toolkit of a multi-authority primarily based encryption scheme AnonyControl and AnonyControl-F.

2. Related Work:

Here a multi-authority gadget is presented in which each user has an identity and they are able to interact with every key generator (authority) the use of exceptional pseudonyms. One person's unique pseudonyms are tied to his personal key; however key generators in no way recognize approximately the personal keys, and for that reason they aren't capable of link more than one pseudonyms belonging to the identical consumer. Additionally, the complete attributes set is divided into n disjoint sets and managed by using n attributes government. On this placing, each authority is aware of only a part of any person's attributes, which are not sufficient to parent out the person's identity. However, the scheme proposed by way of chase et al. considered the simple threshold-based totally kp-abe, which lacks generality in the encryption coverage expression. Many characteristic based totally encryption schemes having more than one authorities have been proposed afterwards, but they both additionally employ a threshold-based totally abe, or have a semi-sincere vital authority, or can't tolerate arbitrarily many customers' collusion assault.

The work by Lewko *et al.* and Muller *et al.* are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones. Lewko *et al.* use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates. Muller *et al.* also supports only Disjunctive Normal Form (DNF) in their encryption policy. Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works. Recently, there also appeared traceable multi-authority ABE, which are on the opposite direction of ours.

Those schemes introduce accountability such that malicious users' keys can be traced. On the other hand, similar direction as ours can be found, who try to hide encryption policy in the ciphertexts, but their solutions do not prevent the attribute disclosure in the key generation phase. To some extent, these three works and ours complement each other in the sense that the combination of these two types protection will lead to a completely anonymous ABE.

3. PRELIMINARIES:

The security of many ABE schemes and ours rely upon the belief that no probabilistic polynomial time algorithms can remedy the DDH or DBDH problem with non-negligible gain (DDH assumption and DBDH assumption). This assumption is cheap given that discrete logarithm troubles in huge variety area are broadly taken into consideration to be intractable, and the companies we selected are cyclic multiplicative organizations of top order, in which DBDH problems are believed to be hard.

A.Privilege Trees Tp: In our paintings, encryption coverage is defined with a tree called get right of entry to tree. Every non-leaf node of the tree is a threshold gate, and each leaf node is defined by an attribute. One get right of entry to tree is required in every statistics document to outline the encryption policy. We extend existing schemes via generalizing the get right of entry to tree to a privilege tree. The privilege in our scheme is defined as similar to the privileges controlled in normal running systems. A statistics report has several operations executable on itself, and each of them is permitted only to authorized users with different level of qualifications. For example, read mine, read all, delete, alter, create is a privileges set of students' grades. Then, analyzing Alice's grades is permitted to her and her professors, but all different privileges should be legal only to the professors, so we need to supply the "read mine" to alice and all different to the professors.

Each operation is related to one privilege p, which is defined with the aid of a privilege tree tp. If a user's attributes fulfill t_p, he's granted the privilege p. with the aid of doing so, we not handiest controls the record get admission to but additionally manipulate other executable operations, which makes the record controlling fine-grained and as a result suitable for cloud storage provider.

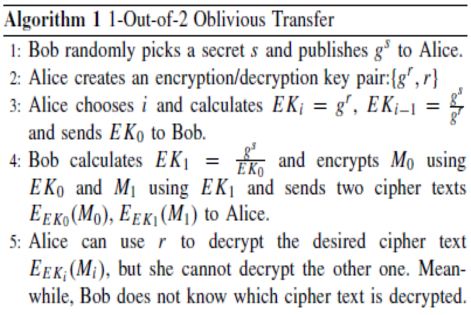
In our scheme, several trees are required in every data file to verify users' identity and to grant him a privilege accordingly. There are supposed to be *r* these kind of structures, which means there are *r* different privileges defined for the corresponding data file. The privilege 0 is defined as the privilege to read the file, and other privileges may be defined arbitrarily (the *m*-th privilege does not necessarily have more powerful privilege than the *n*-th one when $m > n$). The tree is similar to the one defined in [4]. Given a tree, if *numx* is the number of the node *x*'s children node and *kx* is its threshold value $0 < kx \leq numx$, then node *x* is assigned a true value if at least *kx* children nodes have been assigned true value. Specially, the node becomes an OR gate when $kx = 1$ and an AND gate when $kx = numx$.

B. Satisfying the Privilege Tree: If a user's attributes set *S* satisfies the privilege tree *Tp* or the node *x*, we define it as $T_p(S) = 1$ or $x(S) = 1$ respectively. *Tp(S)* is calculated recursively as follows. If *x* is a leaf node, $x(S) = 1$ if and only if $att(x) \in S$. If *x* is a non-leaf node, $x(S) = 1$ only when at least *kx* child nodes return 1. For the root node *Rp* of *Tp*, $Tp(S) = 1$ only if $Rp(S) = 1$.

4. PROBLEM FORMULATION:

A. System Model: In our device, there are 4 forms of entities: N attribute government (denoted as A), Cloud Server, facts owners and information clients. A person may be a facts owner and a statistics consumer simultaneously. Government are assumed to have powerful computation abilties, and they're supervised by using government places of work due to the fact a few attributes partially include users' individually identifiable facts. The entire characteristic set is split into N disjoint units and managed by means of each authority, therefore each authority is privy to simplest part of attributes. A facts owner is the entity who wishes to outsource encrypted information report to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage potential, does nothing however store them.

Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree *Tp* can execute the operation associated with privilege *p*. The server is



Algorithm 1 1-Out-of-2 Oblivious Transfer

```
1: Bob randomly picks a secret $s$ and publishes $g^s$ to Alice.
2: Alice creates an encryption/decryption key pair:$\{g^r, r\}$
3: Alice chooses $i$ and calculates $EK_i = g^r$, $EK_{i-1} = \frac{g^s}{g^r}$
   and sends $EK_0$ to Bob.
4: Bob calculates $EK_1 = \frac{g^s}{EK_0}$ and encrypts $M_0$ using
   $EK_0$ and $M_1$ using $EK_1$ and sends two cipher texts
   $E_{EK_0}(M_0), E_{EK_1}(M_1)$ to Alice.
5: Alice can use $r$ to decrypt the desired cipher text
   $E_{EK_i}(M_i)$, but she cannot decrypt the other one. Mean-
   while, Bob does not know which cipher text is decrypted.
```

delegated to execute an operation *p* if and only if the user's credentials are verified through the privilege tree *Tp*.

B. Threats version: We anticipate the cloud servers are semi sincere; who behave properly in most of time however may additionally collude with malicious facts clients or facts owners to reap others' record contents to advantage unlawful profits. But they're also assumed to gain prison benefit whilst users' requests are efficaciously processed, which way they will observe the protocol in general. N governments are assumed to be un-trusted. This is, they will comply with our proposed protocol in standard, however attempt to find out as much facts as feasible in my opinion. Greater specially, we assume they are inquisitive about customers' attributes to gain the identities, but they will now not collude with customers or different government. This assumption is just like many preceding researches on security trouble in cloud computing, and it is also affordable considering the fact that these authorities could be audited via the authorities' places of work. But, we will further loosen up this assumption and permit the collusion between the authorities in phase 6. Records customers are un-trusted seeing that they're random customers which include attackers. They'll collude with other facts purchasers to illegally get entry to what they're no longer allowed to. Except, we do not recall the identification leakage from the underlying network in view that this may be trivially prevented by using anonymized network protocols.

C. Security Model: To officially outline the security of our anonycontrol, we first supply the subsequent definitions. Set up→p_k, mk_k : this algorithm takes nothing as enter besides implicit inputs which includes safety parameters. Attributes government execute this set of rules to jointly compute a device-huge public parameter p_k as well as an authority-huge public parameter y_k , and to personally compute a master key mk_k . key generate(p_k, mk_k, a^u) → sk_u: this set of rules permits a consumer to engage with each attribute authority, and obtains a personal key sk_u similar to the input characteristic set au.

Init: The adversary *A* declares the set of compromised authorities {*Ak*} ⊂ **A** (where at least two authorities in **A** are not controlled by *A*) that are under his control (remaining authorities **A**/{*Ak* } are controlled by the challenger). Then, he declares *T*0 that he wants to be challenged, in which some attributes are being in charged by the challenger's authorities.

Setup: The challenger and the adversary jointly run

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

the Setup algorithm to receive the valid outputs.

Phase 1: The adversary launches Key Generate algorithms to query for as many private keys as he wants, which correspond to attribute sets $A_1, \ldots, A_q$ being dis-jointly in charged by all authorities {A_k }, but none of these keys satisfy *T*0. Besides, he also conducts arbitrarily many computations using the public and secret keys that he has (belonging to compromised authorities).

Challenge: The adversary submits two messages *M*0 and *M*1 of equal size to the challenger. The challenger flips a random binary coin *b* and encrypts *Mb* with *T*0. The cipher-text **CT** is given to the adversary.

Phase 2: Phase 1 is repeated adaptively, but none of the queried keys satisfy *T*0.

D. Design Goals:

Our purpose is to achieve a multi-authority CP-ABE which achieves the safety described above; ensures the confidentiality of records consumers' identification information; and tolerates compromise attacks on the authorities or the collusion assaults by way of the government.

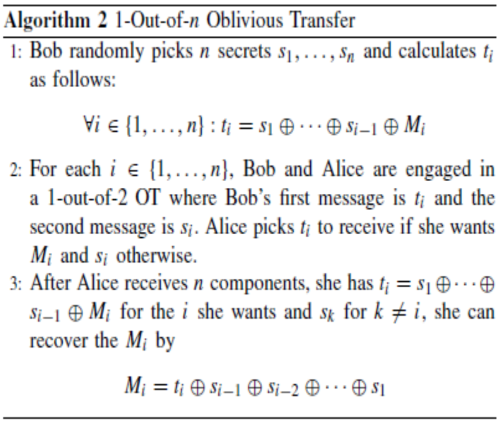
5. ACCOMPLISHING COMPLETE ANONYMITY:

A. Setup:

At the system initialization phase, any one of the authorities chooses a bilinear group G0 of prime order *p* with generator *g* and publishes it. We've assumed semi sincere government in AnonyControl and we assumed that they'll not collude with each other that is a important assumption in AnonyControl because every authority is in price of a subset of the complete attributes set, and for the attributes that it is in price of, it knows the exact facts of the important thing requester. If the facts from all the government are accumulated altogether, the entire characteristic set of the important thing requester is recovered and as a result his identity is disclosed to the authorities. In this sense, AnonyControl is semi-anonymous when you consider that partial identity records (represented as a few attributes) is disclosed to every authority, but we are able to acquire a full-anonymity and additionally permit the collusion of the authorities.

$$\begin{aligned} F_x &= \prod_{z \in S_z} F_z^{\Delta_{d,s'_x}(0)}, \text{ where } \begin{cases} d = index(z) \\ S'_x = index(z) : z \in S_x \end{cases} \\ &= \prod_{z \in S_z} \left(e(g,g)^{(\sum d_k)\cdot q_z(0)}\right)^{\Delta_{d,S'_x}(0)} \\ &= \prod_{z \in S_z} \left(e(g,g)^{(\sum d_k)\cdot q_{parent(z)}(d)}\right)^{\Delta_{d,S'_x}(0)} \\ &= \prod_{z \in S_z} \left(e(g,g)^{(\sum d_k)\cdot q_x(d)}\right)^{\Delta_{d,S'_x}(0)} \\ &= e(g,g)^{(\sum d_k)\cdot q_x(0)} \text{ (using polynomial interpolation)} \end{aligned}$$

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



Algorithm 2 1-Out-of-*n* Oblivious Transfer

1: Bob randomly picks n secrets $s_1, \ldots, s_n$ and calculates t_i as follows:

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

2: For each $i \in \{1, \ldots, n\}$, Bob and Alice are engaged in a 1-out-of-2 OT where Bob's first message is t_i and the second message is s_i. Alice picks t_i to receive if she wants M_i and s_i otherwise.

3: After Alice receives n components, she has $t_i = s_1 \oplus \cdots \oplus s_{i-1} \oplus M_i$ for the i she wants and s_k for $k \neq i$, she can recover the M_i by

$$M_i = t_i \oplus s_{i-1} \oplus s_{i-2} \oplus \cdots \oplus s_1$$

B. Fully anonymous multi-authority cp-abe: In this segment, we gift the way to obtain the overall anonymity in anonycontrol to designs the fully nameless privilege manipulate scheme anonycontrol-f. The key-generate set of rules is the only element which leaks identification facts to every attribute authority. Upon receiving the characteristic key request with the attribute cost, the characteristic authority will generate $h(att\ (i\ ))^{r}_{i}$ and sends it to the requester wherein att (i) is the attribute price and r_i is a random quantity for that attribute. The attribute cost is disclosed to the authority on this step.

C. Discussions:

1) Trustfulness of customers: Our AnonyControl-F additionally wishes to believe the requester that he choices accurate characteristic keys similar to his identification, however the requester can pick out handiest one attribute key in a single category, that's plenty better than the naive idea above, and it is not this paper's scope to guarantee the honest reporting of the attributes. To the high-quality of our information, it's miles assumed that a few different authentication (e.g., authorities test) is in vicinity to verify the reported attributes in maximum of ABE-related works.

2) Overall performance: The extra computation added in AnonyControl-F is simply numerous exponent calculations, which are negligible.

$$\begin{aligned} DecryptNode(\mathbf{CT}, \mathbf{SK}_u, x) &= \frac{e(D_i, C_x)}{e(D_i', C_x')} \\ &= \frac{e(g^{\sum d_k} \cdot H(att(i))^{r_i}, g^{q_x(0)})}{e(g^{r_i}, H(att(i))^{q_x(0)})} \\ &= e(g,g)^{(\sum d_k)\cdot q_x(0)} \end{aligned}$$

However, more communique overhead is an intricate trouble in AnonyControl-F. For every attribute category, the person is involved in a 1-out-of-n OT which desires O(n) rounds of communique. Therefore, the conversation overhead grows from O(1) in AnonyControl to O(I) in which I is the size of the complete attribute set. That is the principle disadvantage of our completely anonymous scheme, which ought to be solved in our destiny paintings.

6. PERFORMANCE EVALUATION:

On this segment, we present the performance evaluation based totally on our measurement on the implemented prototype system of anonycontrol-f. To the first-class of our information, that is the first implementation of a multi-authority attribute based totally encryption scheme. Our prototype gadget offers five command line tools. Anonycontrol-setup: jointly generates a public key and n grasp keys. Anonycontrol-keygen: generates part of personal key for the characteristic set it's far responsible for. Anonycontrol-enc: encrypts a file beneath r privilege timber. Anonycontrol-dec: decrypts a record if feasible. Anonycontrol-rec: decrypts a report and re-encrypts it below. This toolkit is based totally on the cp-abe toolkit that is to be had online, and the complete system is applied on a linux device with intel i7 2nd gen @ 2.7ghz and 2gb ram. Fig. 2 shows the computation overhead incurred in the core algorithms Setup, KeyGenerate, Encrypt, and Decrypt under various conditions.

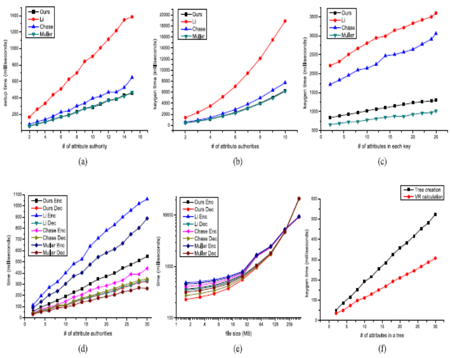


Fig. 2. Experiment result on our implemented prototype system. (a) Setup time. (b) Keygen time with different authorities #. 20 attributes per key. (c) Keygen time with different attributes #. 4 authorities. (d) Encryption and decryption time with different attributes number. File size is 100KB. (e) Encryption and decryption time with different file size. 20 attributes in T_0. (f) Time to create a privilege tree and decrypt a verification parameter from it.

7. CONCLUSION AND POSSIBLE EXTENSIONS:

This project proposes a semi-anonymous characteristic-based totally privilege control scheme AnonyControl and a completely-nameless characteristic-based privilege manage scheme AnonyControl-F to deal with the person privateness hassle in a cloud storage server. The usage of more than one authority in the cloud computing system, our proposed schemes achieve now not best satisfactory-grained privilege control but additionally identification anonymity even as engaging in privilege manage based on users' identification information. Greater importantly, our gadget can tolerate as much as N − 2 authority compromise, that's quite optimal especially in internet-based totally cloud computing environment. We additionally conducted designated security and performance evaluation which suggests that AnonyControl each at ease and green for cloud garage device. The AnonyControl-F without delay inherits the safety of the AnonyControl and as a result is equivalently comfortable because it, but extra verbal exchange overhead is incurred for the duration of the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient person revocation mechanism on pinnacle of our anonymous ABE. Supporting user revocation is an essential trouble within the real application, and this is a exceptional mission within the utility of ABE schemes. Making our schemes well suited with existing ABE schemes who guide greenconsumer revocation is considered one of our destiny works.

REFERENCES:

[1] 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.

[2] 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.

[3] 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.

[4] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key*

Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[5] 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.

[6] 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.

[7] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.

[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005.

Guide Details

Mr. B. RAJINI KANTH was born in India in the year of 1985. He received B.Tech degree in the year of 2009 & M.Tech PG in the year of 2013 from JNTUH. He was expert in Web Technologies, Data Structures & Cloud Computing subjects. He is currently working as An Asst. Professor in the CSE Department in Malla Reddy Institute of Technology, Maisammaguda, Dhulapally Post, Secunderabad, Telangana State, India .

Mail ID: mail2rajanikanthb@gmail.com

Student Details

Mr. UGADI SIVA KUMAR was born in India. He pursues M.Tech degree in Computer Science & Engineering in CSE Department in Malla Reddy Institute of Technology, Maisammaguda, Dhulapally Post, Secunderabad and Telengana State, India.

Mail id: ugadisivakumar@gmail.com