Control Identity Leakage in Cloud Data and Achieve the Full Anonymity

[1]R Shiva Shankar, [2]K Sravani, [3]J Raghaveni, [4]D Ravibabu

[1,2,3,4]Dept. of CSE, SRKR Engineering College, Bhimavaram, West Godavari, AP, India

Abstract

We propose an Attribute-Based Encryption system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. A semi-anonymous privilege control scheme Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a semi-functional form and then arguing security. Our security analysis shows that both Anony Control and Anony Control-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

Keywords

Anony Control and Anony Control_F, Attribute Based Encryption System

I. Introduction

A number of computing concepts and technologies are combined in Cloud Computing to satisfy the computing needs of users, it provides common business applications online through web browsers, while their data and software's are stored on the servers [1]. This is an approach that is used to maximize the scope or step up capabilities robustly without investing in new infrastructure, sustenance new personnel or licensing new software. It provides tremendous storage for data and rapid computing to customers over the internet.

Data security is one of the aspects of the cloud which prohibit users from using cloud services [2]. There is fear between the data owner's especially in large organizations that their data possibly misuse by the cloud provider without their knowledge. Data security of the user's can be ensured by using the concept of virtual private networks, firewalls, and by enforcing other security policies within its own circumferences [3-4]. Security is consequently an extensive element in any cloud computing environment, because it is crucial to assure that only authorized access is sanctioned and protected behaviour is accepted. Any kind of security and privacy contravention is critical and can produce crucial results [5-6]. As soon as the strict regulations and policies are taken against privacy in cloud, more and more personnel will feel save to adopt cloud computing.

A client may be individual or a big organization but all are having same concern i.e. data security, so data security is dire consequence. Data security at different levels is the vital matter of this technology [7]; it can be categorized into two categories: Security at External level and Security at Internal Level. Security at External level states that data is unsecure opposed to third party, cloud service provider or network intruder. Security at Internal level states that data is unsecure opposed to authorized users or employee of an organization [8]. This system provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication.

In practice, this provides a reasonable guarantee that one is communicating with precisely. The website that one intended to communicate with, as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party [9]. Secure Server Plus application has mainly double login security. That is, after logging into the application user receives a secret key on his registered gmail id. This secret key has to be entered in the pop-up box displayed after logging into SSP Application. This application has two functionalities, Encryption and Decryption. Encryption is the functionality in which the file to be sent over mail in firstly divided into 4 equal parts in byte format and then encrypted using different encryption algorithms .After Encryption files would be sent to recipient through Gmail At the recipient end. He will download the files and using SSP Application data in files would be decrypted and merged [10].

II. Related Work

There are numerous work carried in the field of data protection at cloud. Many models, schemes and techniques are proposed for data security. M. Sugumaran et al [10] illustrates a couple of techniques that resolves the security of the data and proposes architecture to safeguard the data in cloud. In proposed architecture the encrypted data is stored in cloud using cryptography technique i.e. located on block cipher. Cindhamani.J et al [3] proposed an enhanced frame work for data security in cloud which follows the security polices such as integrity, confidentiality and availability. Parameters they used are 128 bit encryption, RSA algorithm and Trusted Party Auditor (TPA). Before storing the data into the cloud, the data owner assigns the privileges that who will access the data. After assigning the privileges they encrypt the data and stores into the cloud. Dharmendra [4] proposed the unified data encryption architecture which ensures the data security and privacy with reasonable performance overhead of computing system. It is based on multilevel identity encryption approach with two level/factor identity verification process. Dr. L. Arockiam et al [5] achieves the data confidentiality in cloud storage with two different techniques i.e. encryption and obfuscation. Encryption encrypts the alpha-numeric and alpha data while obfuscation encrypts the numeric data. Both are done on user side. First, the user has to encrypt the data using any technique then he stores the data into cloud storage. Taeho Jung et al [14] use two schemes to control the data privacy and the identity privacy. One is the Anony Control scheme i.e. semi anonymous privilege control scheme which not only addresses the data privacy but also the user identity privacy in extant access control schemes. It decentralizes the central authority to restraint the identity leakage and thus achieves semianonymity. Another is the AnonyControl-F scheme that controls the identity leakage and achieves the full anonymity. Eman M.Mohamed et al [6] Exhibits the data security model that is based on the analysis of cloud architecture and implemented software to intensify endeavor in data security model for cloud computing. Hu Shuijing [7] described the enormous essentials in cloud computing, such as security key technology, regulation and standard etc and discussed manner in which they are addressed. In this Proposed model data is protected against all threats i.e. internal and external, thread during, transits as well as when data at rest. The security of many ABE schemes [12], [13]–[17] andours rely on the assumption that no probabilistic polynomial time algorithms can solve the DDH or DBDH problem with non-negligible advantage (DDH assumption and DBDH assumption). This assumption is reasonable since discrete logarithm problems in large number field are widely considered to be intractable [16]–[19], and the groups we chose are cyclic multiplicative groups of prime order, in which DBDH problems are believed to be hard.

Encryption policy is described with a tree called access tree. Each non-leaf node of the tree is a threshold gate,and each leaf node is described by an attribute. One access treeis required in every data file to define the encryption policy.In this paper, we extend existing schemes by generalizing the access tree to a privilege tree. The privilege in our scheme is defined as similar to the privileges managed in ordinary operating systems. A data file has several operations executable on itself, and each of them is allowed only to authorize users with different level of qualifications.

III. Problem Formulation

A. System Model

In our system, there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and a Data Consumer simultaneously.

Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but 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 delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

B. Threats Model

We assume the Cloud Servers are semi-honest, who behave properly in most of time but may collude with malicious Data Consumers or Data Owners to harvest others' file contents to gain illegal profits. But they are also assumed to gain legal benefit when users' requests are correctly processed, which means they will follow the protocol in general. N authorities are assumed to be untrusted. That is, they will follow our proposed protocol in general, but try to find out as much information as possible individually. More specifically, we assume they are interested in users' attributes to achieve the identities, but they will not collude with users or other authorities. This assumption is similar to many previous researches on security issue in cloud computing and it is also reasonable since these authorities will be audited by government offices. However, we will further relax this assumption and allow the collusion between the authorities .Data Consumers are untrusted since they are random users including attackers.

IV. Methodlogies

A. Attribute-based encryption for fine-grained access control of encrypted data

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). I develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

B. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Attribute Based Encryption (ABE) [13] determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptions can require that a user obtain keys for appropriate attributes from each authority be-fore decrypting a message. Chase [5] gave a multi-authority ABE scheme using the concepts of a trusted Central Authority (CA) and Global Identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially entrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, i propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

C. Secure Threshold Multi Authority Attribute Based Encryption Without a Central Authority

An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each cipher text. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trusted central authority which can decrypt every cipher text in the system. This central authority would endanger the whole system if it's corrupted. This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encrypted can encrypt a message such that a user could only decrypt if he has at least d k of the given attributes about the message for at least t+1, t≤n/2 honest authorities of all the n attribute authorities in the proposed scheme. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme.

D. Registration Based Social Authentication Module

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's Registration.

E. Security Module

Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees.

F. Attribute Based Encryption

Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. The attribute-based encryption has been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext.

G. Multi-authority

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

V. Implementation

Algorithm for simple triple DES

```
Step 1: myEncryptionKey = "ThisIsSparta ThisIs Sparta";
Step 2: myEncryptionScheme = DESEDE_ ENCRYPTION_ SCHEME;
Step 3: arrayBytes = myEncryption Key. getBytes(UNICODE_ FORMAT);
Step 4 : ks = new DESedeKeySpec(arrayBytes);  Step 5:  skf = SecretKeyFactory .getInstance (myEncryptionScheme);
Step 6:  cipher = Cipher.getInstance (myEncryptionScheme);
Step 7: key = skf.generateSecret(ks);
```

Algorithm for Single Encrypt

```
Step 1: cipher.init(Cipher.ENCRYPT_MODE, key);
Step 2: byte[] plainText=unencryptedString.getBytes(UNICODE_ FORMAT);
Step 3: byte[] encryptedText = cipher.doFinal (plainText);
Step 4: encryptedString = new String(Base64 .encodeBase64(encryptedText));
```

Algorithm for Single Encrypt

```
Step 1: cipher.init(Cipher.DECRYPT_MODE, key);
Step 2: byte[] encryptedText = Base64. decodeBase 64(encryptedString);
Step 3: byte[] plainText = cipher. doFinal (encryptedText);
Step 4: decryptedText = new String(plainText);
```

VI. Result Analysis

In the presents of performance evaluation based on our measurement on the implemented prototype system of AnonyControl-F. To the best of our knowledge, this is the first implementation of a multi-authority attribute based encryption scheme. Our prototype system provides five command line tools.

AnonyControl-setup: Jointly generates public key and N master keys.

AnonyControl-keygen: Generates a part of private key for which attribute set it is responsible

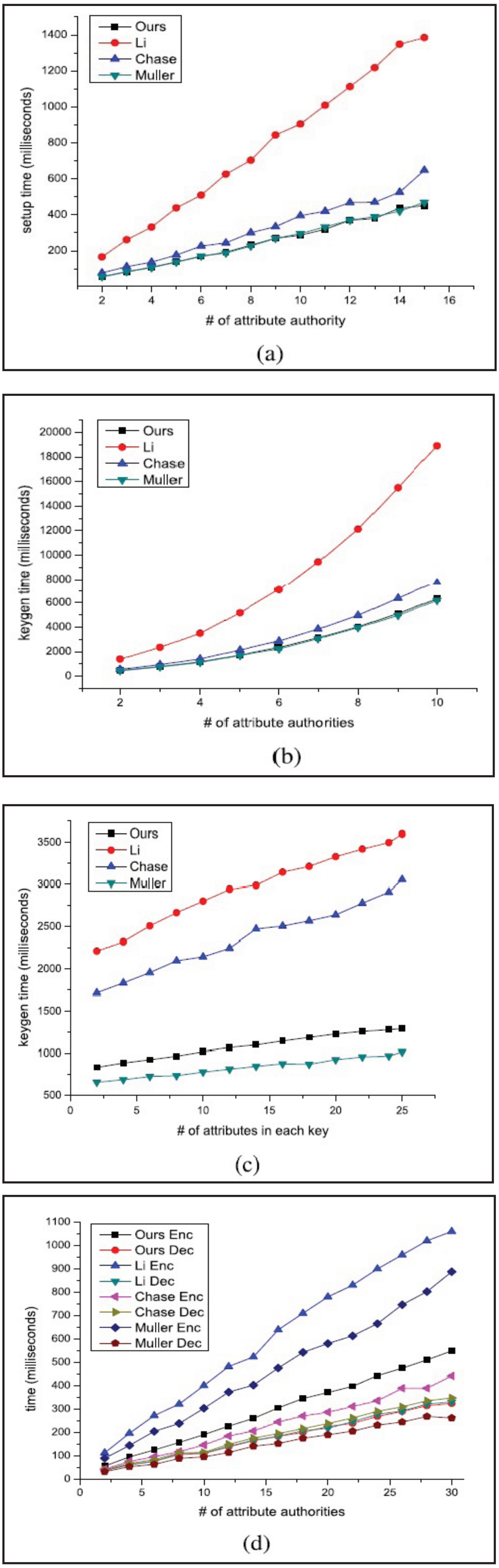
AnonyControl-enc: Encrypts a file under r privi lege trees.

AnonyControl-dec: Decrypts a file if possible.

AnonyControl-rec: Decrypts a file and re-encrypts it under different privilege trees.

Fig. shows the computation overhead incurred in the core algorithms Setup, Key Generate, Encrypt, and Decrypt under various conditions. We additionally implemented three similar works (Li [13], Chase [13], and Muller [12]) under the same condition (same security level and same environment) for the comparison purpose. Particularly, in Fig. A (e), we set only one privilege for the file access, and we measured the time to create one privilege tree and calculate its verification parameter in Fig. A (f) In general, the computation overhead of Li [13] is much higher than others because their scheme involves many more exponentiations and bilinear mappings due to the accountability. The encryption/decryption under different file sizes did not show big differences when file sizes are large (≥20MB), because the run times are dominated by the symmetric encryption (AES-256). Finally, only our run times are plotted in Fig. 7(f) because the privilege creation is the unique process in our scheme.

- Setup time
- Keygen time with different authority's#. 20 attributes per key.
- Keygen time with different attributes #. 4 authorities.
- Encryption and decryption time with different attributes number. File size is 100KB.
- Encryption and decryption time with different file size. 20 attributes in T0.



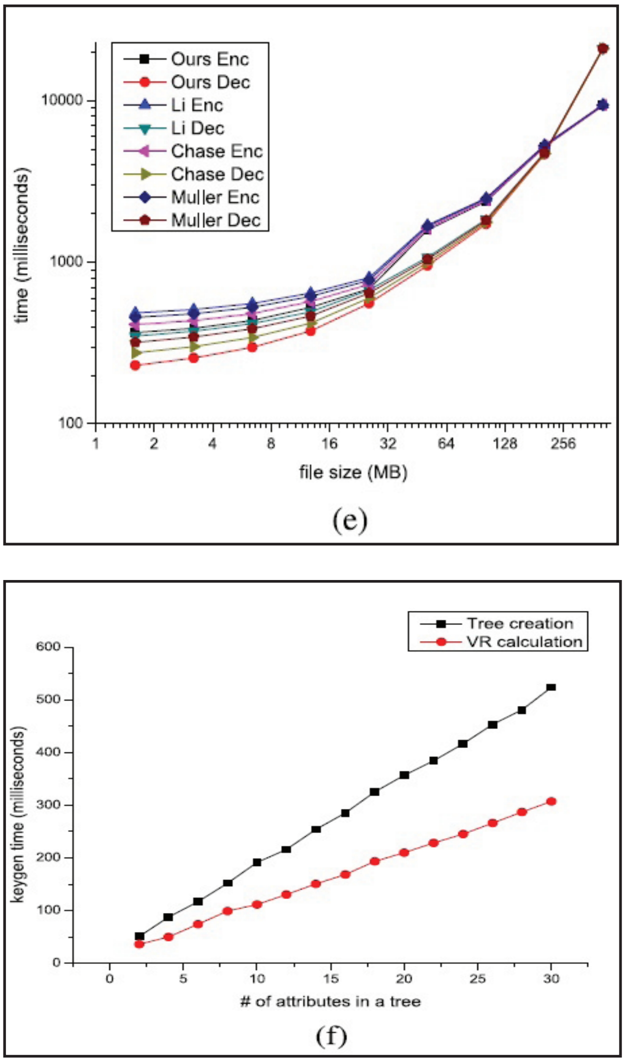


Fig. 1: Experiment Result on our Implemented Prototype System

VII. The Cloud Service Composition Model

The Architecture encompasses bee agents and their interaction structure.

- Employee forager bee agent
- Scout and onlooker bee agent
- Hive - Resource agent

There are a variety of users in the cloud platform. The cloud users must define their budgetary requirements based on technical and functional considerations.

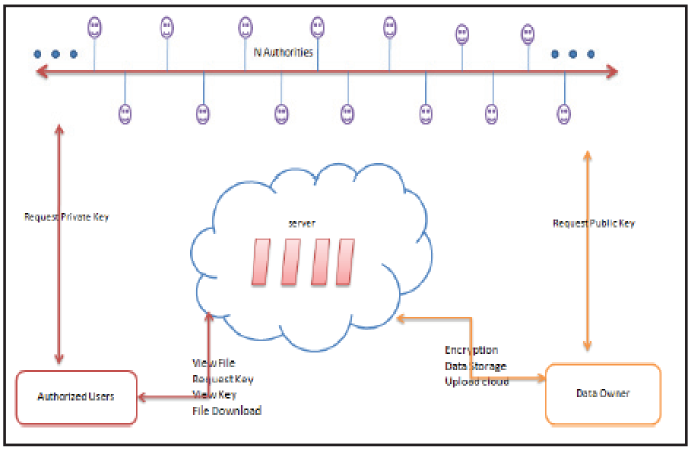


Fig. 2: System Architecture

VIII. Conclusion

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes that support efficient user revocation is one of our future works.

References

[1] A. Shamir,"Identity-based cryptosystems and signature schemes," In Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai, B. Waters,"Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, 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, B. Waters,"Ciphertext-policy attributebased encryption," In Proc. 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, 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, 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, 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, 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, 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, B. Waters,"Decentralizing attribute-based encryption," In Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[12] S. Müller, S. Katzenbeisser, 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, 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, J. Xu,"Fully secure multi-authority attribute-based traitor tracing," J. Comput. Inf. Syst., Vol. 9, No. 7, pp. 2793–2800, 2013.

[15] S. Hohenberger, 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, H. Li, "Anonymous attributebased encryption supporting efficient decryption test," In Proc. 8th ASIACCS, 2013, pp. 511–516.

[18] D. Boneh, M. Franklin,"Identity-based encryption from the weil pairing", In Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.

[19] A. Sahai, B. Waters,"Fuzzy identity-based encryption," Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005.

R. Shiva Shankar is currently an Assistant Professor in the Department of Computer Science and Engineering at the SRKR Engineering College (India). He received his master of technology degree from the Andhra University, Visakhapatnam, India. His M. Tech degree includes Computer Science and Technology.