ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

A Secure Multi-Owner Data Sharing and Load Balancing for Dynamic Groups in the Cloud

C.Suchithra[1], G.Appasami[2]

ME Student, Department of CSE, Dr.Pauls Engineering College, Villupuram, India.

Assistant Professor, Department of CSE, Dr.Pauls Engineering College, Villupuram, India.

ABSTRACT - Cloud computing is an emerging computing premise in which consists of a virtualized pool of highly scalable computing resources and provided as an internet based computing where many organizations store, reacquire and modify data among cloud users. Major problem in cloud computing is sharing data in a multi-owner manner, while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. The main aim is to provide secure multi-owner data sharing in dynamic groups. This poses a security challenge to the data stored inside cloud. As the result, the encryption computational cost is reduced; storage overhead and scheme are independent with the number of revoked users with rigorous proof and experiments. Load Balancing is also implemented to process the User requested job by allocating to the sub servers which will process the task by evaluating the CPU performance level.

KEYWORDS- Cloud computing, data sharing, privacy-preserving, identity privacy, dynamic groups.

I. INTRODUCTION

Cloud computing is a wide-ranging term that transmits hosted services over the internet and recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage. With cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost. With dropbox, for example, data is stored in the cloud (operated by amazon), and shared among a group of users in a collaborative manner. Let us consider a real time scenario. A professor allows his students and colleagues to share files stored in cloud. Those files may include internal assessment of students, his personal information, student's personal information, research details, other staff details etc. By utilizing cloud, students and other employees can get relevant information on a request basis. However, it poses some confidentiality risks. The cloud service provider or third party may not fully trusted by the users [2]. A possible approach would be to encrypt entire data files before outsourcing in order to achieve more integrity. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], the multiple-owner manner is more flexible in practical applications. On the other hand, an efficient membership re-vocation mechanism without updating of the secret keys of the remaining users minimize the complexity of key management , signed receipt is collected after every member revocation in the group it minimizes the multiple copies of encrypted file and also reduces computation cost.

II. RELATED WORK

Proposed a cryptographic storage system that enables secure file sharing from an untrusted server, named Plutus [4]. By dividing file into file groups and encrypting each file group with a unique lock group key, the data owner can share the file groups with others through delivering the corresponding group key, where the lock group-key is used to encrypt the lock-group keys.

In [5] untrusted server has two parts of files to be stored those: file metadata and file data. The file meta-data implies the access control information that includes a series of encrypted key blocks, each of which is encrypted under the symmetric key of authorized users.

It is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNL construction [10] is used for efficient key revocation.

To ensure security in distributed storage. Specifically the data owner encrypts blocks of content with unique and symmetric [6]. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key.

In [3], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Where any member in a group should be allowed to store and share data files with others.

Lu et al. [7] proposed a secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. However, user revocation is not supported in their scheme.

III. EXISTING WORKS

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable.

Disadvantages of Existing System

1) Only the group manager can store and modify data in the cloud.

2) The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

3) Identity transparency are not maintained for sharing a file in cloud group.

4) File sharing privacy not maintained.

IV. THE PROPOSED SCHEME

To solve the challenges presented above, this paper proposes an innovative approach for secure multi-owner data sharing scheme for dynamic groups in the cloud computing. It can be achieved by a technique called Attribute Based Encryption (ABE) in which each data files can be encrypted along with attributes relevant to the data file. During decryption, the user need to provide relevant attributes that satisfies the access structure of data file. Compared with the existing works the innovative approach offers unique features as follows:

1) Proposed system supports multiple users and each user can communicate with each other through data sharing and store data files with others by the cloud.

2) The complexity and size taken for encryption is independent with the number of revoked users in the system.

3) User revocation can be achieved without updating the private keys of the remaining users and signed receipts will be collected after any revocation that reduces duplication of encrypted copies;

4) Secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

5) Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

6) The group manager compute the revocation parameters and make the result public available by migrating them into the cloud.

Group Signature

The concept of group signatures was first introduced in [9] by Chaum and van Heyst. In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature’s originator when a dispute occurs, which is denoted as traceability [12].

Dynamic Broadcast Encryption

Broadcast encryption [10] enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in [8], which will be used as the basis for file sharing in dynamic groups.

Trusted Party Auditor

To check whether the data is modified or not, that is present in cloud, data owner assigns a third party called Trusted Party Auditor (TPA). Once the data owner sends the request to audit the data, TPA checks the integrity of the data by getting the hash code files from cloud server and top hash value from db and verifies the file using Merkle Hash Tree Algorithm. After each time period, the auditing information will be updated by the Trusted Party Auditor. If any file is missing or corrupted, email alert will be sent to data owner indicating that the data has been modified. The TPA can verify the file either by random or in manual way. Thus by allowing the Trusted Party Auditor to audit the data, Trustworthiness will be increased between the User and Cloud Service Providers.

Merkle Hash Tree

By using Merkle Hash Tree algorithm the data will be audited via multiple level of batch auditing process. The top hash value is stored in local database and other hash code files are stored in cloud. Thus the original data cannot be retrieved by anyone from cloud, since the top hash value is not in cloud. Even if any part of data gets hacked, it is of no use to the hacker. Thus, the security can be ensured

Step 1: A file is split up into „n‟ number of data blocks.

Step 2: Each data block is hashed and these hashes of data blocks are the leaves in hash tree.

Step 3: Nodes further up in the tree are the hashes of their respective children.

Step 4: Final hash value in a single node becomes a top hash value.

V. SYSTEM MODEL

The proposed system model can be explained with an example that a company uses a cloud to enable its staffs in the same group or department to share files and data. The system model consists of three different entities: the cloud

Server, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Figure 1.

To overcome this drawback, we propose secure storage for multi-owner data sharing authentication system in cloud. First, data will be uploaded in Encrypted format by the Data Owner in the Cloud Server. Once uploaded, the Cloud Server generates the Public and Private Keys. Then the data will be given to the Trusted Party Auditor for auditing purpose. The Auditor audits the data using Merkle Hash Tree Algorithm and stores in the Cloud Service Provider. If the user wants to View/Download the data, they have to provide the public key. The Data Owners will check the public key entered by the User. If valid, then the decryption key will be provided to the user to encrypt the data. The Load Balancing Concept is also implemented to process the User requested Job. First, the user request will be passed to the Cloud Service Provider‟s data center. The request is then queued up under the CSP‟s data center through communication channel. Then the job will be assigned to the sub server by keeping track of the CPU performance level that has minimum load.

Cloud Server

It is a large repository of resources which can be delivered to its customers as a service. The cloud servers are maintained by cloud service providers who are all responsible for storing sensitive information in the cloud and provides whenever needed. It is operated by CSPs and provides priced abundant storage services [3], [7], assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [12], [13].

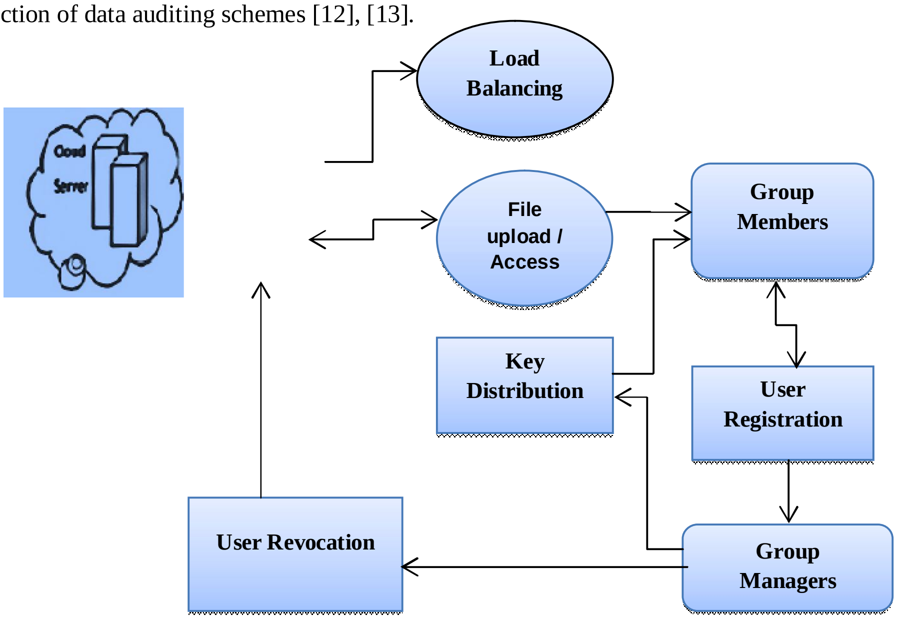


Figure 1. System Model

Group Manager

Group Manager is an entity who is going to store, share and manage data files stored inthe cloud. He is also responsible for granting new users to access and improve cloud performance based on a request from them. Hetakes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company.

Group Members

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. They initially get registered with cloud system to become a part of cloud and to use services offered. Example, the staff plays the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

User Registration

After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. User registered with their details such as identity (user name, password and email-id). During registration process, user got unique identity and access structure. This generates secret key for the members. For registered users they will obtain private key, that private key is used for group signature and file decryption. The Group manager adds the user identity (ID) to the group user list that will be used in traceability phase.

Key Distribution

Means of distributing secret keys by the group manager.Using public key cryptography and exchange of session keys that are valid only if the group members are not revoked from the group. Key can be updated by generating new key from an old key.

File Upload

To access the data that are stored in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete or modify the data that are stored in the cloud. If any request from revoked user, cloud server won't allow accessing the data.

File Deletion

File that are stored in the cloud can be deleted by either group member (i.e., the member who uploaded the file into the server) or by group manager. It allows data owners to delete their own files that are stored in the cloud. If any delete request from the group member, cloud server will verify the signature and delete the data file that are stored in the cloud.

User Revocation

User revocation is the process of removal of user from system user list which is performed by group manager. The system maintains Attribute History List (AHL) for each attributes. For the user to be revoked, his access structure is removed from AHL, so that they can't have more access to cloud. Upon receiving the resignation request from the group member, group member will be in revoked user list.

Load Balancing

Load balancing is a technique to distribute workload evenly across two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, maximize throughput, minimize response time, and avoid overload of any one of the resources. Using multiple components with load balancing instead of a single component may increase reliability through redundancy.

The users submit their diverse applications to the Cloud Service Provider through a communication channel. The requests from the users are queued up under the Cloud Service Provider‟s Data Center. The sub servers are then checked up for the minimum load with the CPU performance level of the currently executing task. The Cloud Service Provider then allocates the requested job to the sub servers that has minimum load to process the task in a First In First

Out (FIFO) manner. Thus the User requested job will be assigned to the available sub server which contains minimum load and it is concerned to process the User requested job.

The objective is to provide secure data storage, to maintain integrity of the data, to increase the user level of authentication and to improve the performance efficiently by 70-80% of balancing the load.

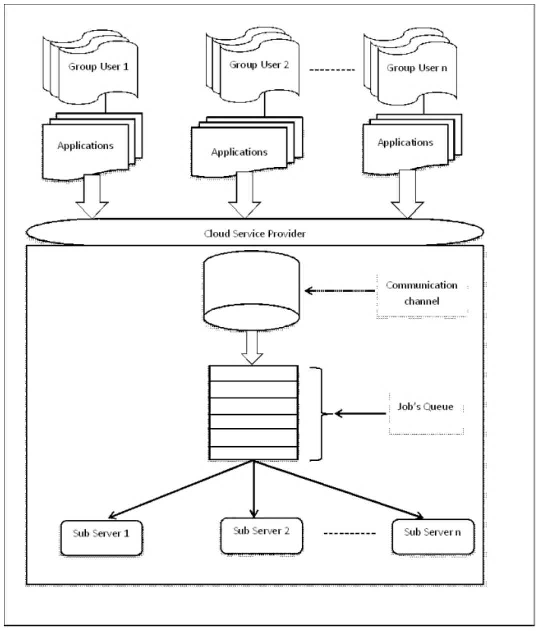


Figure 2. Load balancing process

VI. DESIGN GOALS

In this section, describe the main design goals of the proposed scheme as follows:

Access Control The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

Data confidentiality An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

Anonymity and traceability Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

Efficiency The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or reencryption operations.

VII. ACTIVITY DIAGRAM

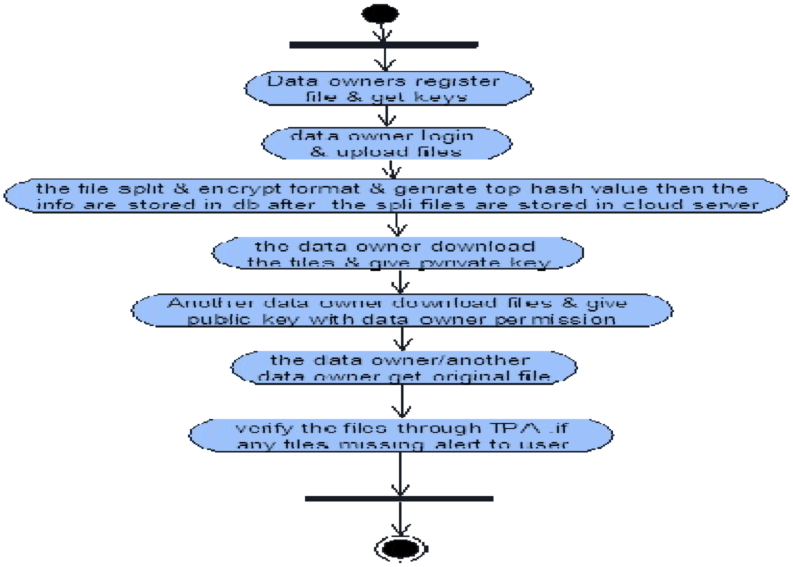

Data owners register file & get keys
data owner login & upload files
the file split & encrypt format & genrate top hash value then the info are stored in db after the spli files are stored in cloud server
the data owner download the files & give pvrivate key
Another data owner download files & give public key with data owner permission
the data owner/another data owner get original file
verify the files through TPA .if any files missing alert to user

Figure 3. Activity diagram

VIII. SIMULATION RESULTS

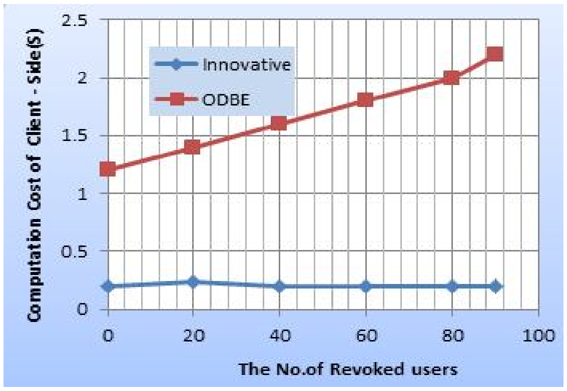
In this section, first analyze the storage cost and then perform experiments to test its computation cost.

Simulation

To study the performance, we have simulated using C programming language with GMP Library [14], Miracl Library [15], and PBC Library [16]. The simulation consists of three components: client side, manager side as well as cloud side. Both client-side and manager-side processes are conducted on a laptop with Core 2 T7250 2.0 GHz, DDR2 800 2G, Ubuntu 10.04 X86. The cloud-side process is implemented on a machine that equipped with Core 2 i3-2350 2.3 GHz, DDR3 1066 2G, Ubuntu 12.04 X64.

Client Computation Cost

The comparison on computation cost of clients for data generation operations between Innovative and the way that directly using the original dynamic broadcast encryption (ODBE) [11]. It is easily observed that the computation cost in Innovative is irrelevant to the number of revoked users. On the contrary, the computation cost increases with the number of revoked users in ODBE. From Figure 2, we can find out that sharing a 10- Mbyte file and a 100-Mbyte one, cost a client about 1.2 and 1.4 seconds in our scheme, respectively, which implies that the symmetrical encryption operation domains the computation cost when the file is large. The computation cost of clients for file access operation with the size of 10 and 100 Mbytes are illustrated in Fig. 2. Besides the above operations, need to be computed by clients in ODBE. Therefore, Innovative is still superior than ODBE in terms of computation cost.



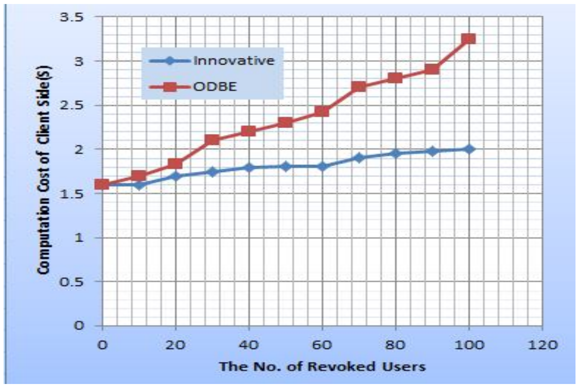


Figure 4. Comparison on computation cost for files generation between Innovative and ODBE.

Figure 5. Comparison on computation cost for file access between Innovative and ODBE.

Cloud Computation Cost

To evaluate the performance of the cloud in Innovative, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB, the test results are given in table 1. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations.

REQUEST	NO. OF REVOKED USERS		
	0	50	100
File Generation (100 MB)	0.065	0.154	0.271
File Generation (10 MB)	0.045	0.125	0.226
File Access (100 MB)	0.045	0.150	0.237
File Access (10 MB)	0.045	0.151	0.240
File Deletion (100 MB)	0.041	0.153	0.240
File Deletion (10 MB)	0.042	0.156	0.240

Table 1: Computation Cost of the Cloud (s)

IX. CONCLUSION

In this paper developed an Innovative approach for secure multi-owner data sharing for dynamic groups in an untrusted cloud. In this scheme a user is able to share data with others in the group without revealing identity privacy to the cloud. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. The storage overhead and the encryption computation cost are varied. Extensive analyses show that the proposed scheme satisfies the desired security requirements and it guarantees efficiency as well.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Ieee transactions on parallel and distributed systems, vol. 24, no. 6, june 2013

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc. of FC, January 2010, pp. 136-149.

[3] S. Yu, C. Wang, K. Ren, and W. Lou,“ Achieving secure, scalable and fine- grained data access control in cloud computing,” in Proc. of INFOCOM, 2010, pp. 534-542.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “plutus: Scalable secure file sharing on untrusted storage,” in Proc. Of FAST, 2003, pp. 29-42.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing remote untrusted storage,” in Proc. of NDSS, 2003, pp.131-145.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proc. of NDSS, 2005, pp. 29-43.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,”, in Proc. of AISIACCS, 2010, pp. 282-292.

[8] C. Delerablee, P. Paillier, and D. Pointcheval, “Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys,” in Proc. of Pairing, 2007, pp.39-59.

[9] D. Chaum and E. van Heyst, “Group Signatures,” in Proc. of EUROCRYPT, 1991, pp. 257-265.

[10] A. Fiat and M. Naor, “Broadcast Encryption,” in Proc. of CRYPTO, 1993, pp. 480-491.

[11] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[13] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.

[14] The GNU Multiple Precision Arithmetic Library (GMP), http:// gmplib.org/, 2013.

[15] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL), http://certivox.com/, 2013.

[16] The Pairing-Based Cryptography Library (PBC), http://crypto. stanford.edu/pbc/howto.html, 2013.

BIOGRAPHY

Mr. G. APPASAMI M.Tech., (Ph.D.) Since 2008 he has been working as Assistant Professor in the Department of Computer Science & Engineering in Dr. Pauls Engineering college. His Research interests include Data Mining, Operating systems, Computer Networks, Distributed computing, Data structures, Mobile computing and Cloud Computing.

Ms. C. SUCHITHRA received the B.Tech -Information Technology Degree from IFET College of Engineering, affiliated to Anna University in 2009 and currently pursuing his ME-computer Science Degree in Dr. Pauls Engineering College, affiliated to Anna University. Her area of interest includes Computer networks, Mobile Computing Distributed Computing and Cloud Computing.