IJITKM 0973-4414 Volume-8, Number-2 Jan-Jun 2015 pp. 99-114 available online at www.csjournalss.com

Novel Approach to Ensure Data Security in Cloud Computing

Sonia Bassi[1], Anjali Chaudhary[2]
[1] M.Tech Student, Department Of Computer Science, KITM, Kurukshetra
[2] Assistant Professor, Department Of Computer Science, KITM, Kurukshetra
sonia_bassiin@yahoo.com

Abstract-Cloud computing is an emerging and increasingly popular computing paradigm, which provides the users massive computing, storage, and software resources on demand . Because system resources are essentially shared by many users and applications, an excellent task scheduling scheme is critical to resource utilization and system performance. Cloud computing is very flexible and cost reducing to do this task. The security issues are organised into several categories – availability, reliability, data protection, ownership, trust, identity etc. In this paper, it is discuss about some of the techniques that were implemented to protect data. It is also discuss about architecture to protect data in cloud. Data encryption algorithms would not be of much use if it is secure enough but slow in performance. There are many popular secret encryption algorithms i.e. AES, DES, 3DES, the blowfish, MD5, RSA. In this paper, the two of the popular secret key encryption algorithms i.e. DES and the blowfish have been implemented. DES (Data Encryption Standard) is currently the most widely used block cipher in the world. It is largely used in banking sector. The Blowfish algorithm was introduced in 1993 and it is a variable length key, 64- bit block cipher. It is often used in software applications.

Keywords: Cloud computing; Data Security; AES; the Blowfish; Encryption Algorithms.

1. INTRODUCTION

Cloud Computing is rapidly growing area in the IT security space. Cloud is computing model that refers to both the applications derived as services over the internet and hardware and system software that provides those services.

Cloud computing is model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The data can be stored remotely in the cloud by the users and can access using thin clients as and when required. When a local network is connected to a cloud network, in which some part of the network data is broken out from the local network and placed in the cloud, but critical data resides in the local network itself. In this case, the Cloud provider does not have any privilege of accessing the data physically which is in the local network. But in some cases, the cloud needs to access some information which is in local network, during that access; there exist the possibility of unauthorised access of the local network resources. It describes the typical problem in network security where the information can face active attacks and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. The passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the cloud network.

Our aim is to provide more efficient data security in cloud system. When the total data of the local network resides within the cloud where the local network and the authorised users can access their data physically in the cloud. At that instant of time, there exists a possibility of unauthorised users to enter and access the data in the cloud. In this situation, the virtual machines are allotted to the users. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways. Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. Our work provides more knowledge in this dimension and also predicts the future threats likely to be faced by Cloud Computing and solutions to these threats.

The proposed model combines the various cryptographic techniques together to achieve data security in cloud. The proposed model handles maximum attacks. This paper is structured as follow: Section 2 summarizes the literature survey for data security in cloud. In Section 3, a proposed architecture is described to solve the security issue of cloud computing. Section 4 provides the implemented algorithms used in this paper. In Section 5, a proposed model is describe to solve the security issues in cloud computing. In

section 5, conclusion and future work is described.

2. Literature Survey

Juels et al. (2007) described a formal Proof of Retrievability (POR) model for ensuring the remote data integrity. Their scheme com- bines spot-checking and error-correcting code to ensure both possession and recovery of files on archive service systems. Shacham and Waters (2008) built on this model and constructed a random linear function based Homomorphic Authenticator. This enables unlimited number of queries and requires less communication overhead. Wang et al. (2009) described a homomorphism distributed verification scheme using Pseudorandom Data to verify the storage correctness of user data in cloud. Wang et al. (2010) discussed the drawbacks of using ordinary encryption techniques and suggested that these techniques are not useful over cloud because for this user should have pre knowledge about the encrypted cloud data. Their model is based on symmetric searchable encryption method. They gave design for existing crypto- graphic primitive and order preserving symmetric encryption (OPSE). Security analysis shows its success rate for one too many mapping and for ranked keyword search. This model did not provide any information about the security attacks, confidentiality and integrity. This model is not well suited for preserving security. In 2011, Singhal and Raina, presented a comparative analysis between AES and RC4 for better utilization. In 2012, Ajey et al. defined cloud computing as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. "Cloud computing continues to gain acceptance as a critical way to deliver on-demand information and resources to customers," The cloud architecture is implemented in such a way that it provides you the flexibility to share application as well as other network resources. In 2013, Louai A et al shows several threats to data privacy, confidentiality and integrity over the cloud. The threats include abuse and nefarious use of cloud computing, insecure API's malicious insiders, shared technology vulnerabilities, data loss or leakage, account or service hijacking and unknown risk profile. In 2014, Dr. L. Arockiam et al proposed a new cryptographic technique in which encrypted data is stored on storage servers while secret key(s) are retained by data owner himself. Along with encryption, obfuscation technique is used to increase the confidentiality of data.

3. ARCHITECTURE OF DATA SECURITY

Architecture has been proposed to implement the data security in cloud computing using symmetric cryptography technique. The proposed architecture is based on block based symmetric cryptography algorithm, which is very efficient and secured. Different experiment are done on existing algorithm and on comparing of those algorithm, block based symmetric cryptography algorithm is better. This proposed architecture using block based symmetric cryptography has the better speed of storing data, when compared with the existing encryption algorithm. The proposed algorithm improves encryption of data secured by inserting the symmetric layer. Symmetric encryption is the oldest and best known technique.

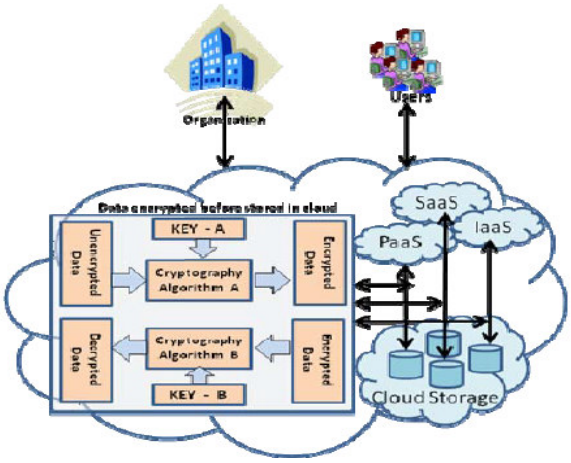

Figure 1: Architecture for Data security in Cloud

The secret key to generate the cipher text, which can be a number, or a word, or just a string of random block letters, is applied to the text of a message to change the content in a particular way. This cipher text may be as simple as shifting each letter by a number of places in the alphabet. As both sender and recipient know the secret key, they can encrypt and decrypt all messages that used by this key. A random number is used for generating the initial key. This key will be used for encrypting the given source file using proposed encryption algorithm with the help of encryption key number. The symmetric encryption approach is divided into two types, one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography. In this proposed architecture block symmetric cryptography was used, so its efficiency and security. In the proposed technique a common key was used in between sender and receiver, which is known as private key. The private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where 254 cipher texts decrypted by same private key into plain text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information.

4. IMPLEMENTED ALGORITHMS

The following secret key encryption algorithms were chosen for implementation, i.e.

* DES

* Blowfish

Data Encryption Standard (DES)

DES (Data Encryption Standard) is presently the most widely used block cipher in the world. In May 1973, NIST

(then NBS) called for possible encryption algorithms for use in unclassified adopted encryption algorithm and is in many standards around the world (e.g. Australian Standard AS2805.5-1985). One of the largest users of the DES is the banking sector. It is for this use that the DES was primarily standardized, with ANSI reconfirming its use for 5 year periods - in future it will be replaced with AES. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

Blowfish: Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Though it suffers from weak keys problem, no attack is known to be successful against it.

5. PROPOSED MODEL

In this paper we proposed a secure cloud framework where security can achieve. For this we proposed an architecture which is java based. By using this architecture we can provide security to the cloud environment and to the user. Any normal can register their detail in this environment and according to the detail Admin of the cloud provide a user id and password. Proposed framework has been structured to provide complete security to the data throughout the entire process of cloud computing, be it in cloud or in transit. Thus, multiple mechanisms and available techniques are applied to shield the critical information from unauthorized parties. The proposed frame work is divided into four phases.

First phase deals with registration of the user to CSP.

Second phase deals with the data storage at cloud storage.

Third phase deals with the authentication of user on data retrieval request.

Forth and last phase deals with the retrieval of data from cloud by the authenticated user and verification of integrity of the retrieved data, thereby providing data back to authorized user with passing all security mechanisms.

5.1. Phase 1 (Registration of cloud user to cloud service provider)

(As shown in figure 2) First of all, the user will have to register himself with the cloud service provider by providing its details like user name, password, and registered mobile number. CSP database will prevent the data from account hijacking and job inside attack.

After verifying the user particulars the CSP generates an OTP and send it to the cloud user which is re entered by the user and verified by the CSP; this policy prevents the user account from unauthorized person login.

The user will have to enter a CAPTCHA as well which make it secure from the software designed for cracking password. This concept assures the manual entering of the user information.

5.2. Phase 2 (Storing of data in cloud storage)

(As shown in figure 3) This phase transmit and store the data securely to the cloud in encrypted form. This phase further divided into sub sections to encrypt data at user end and encryption at CSP end.

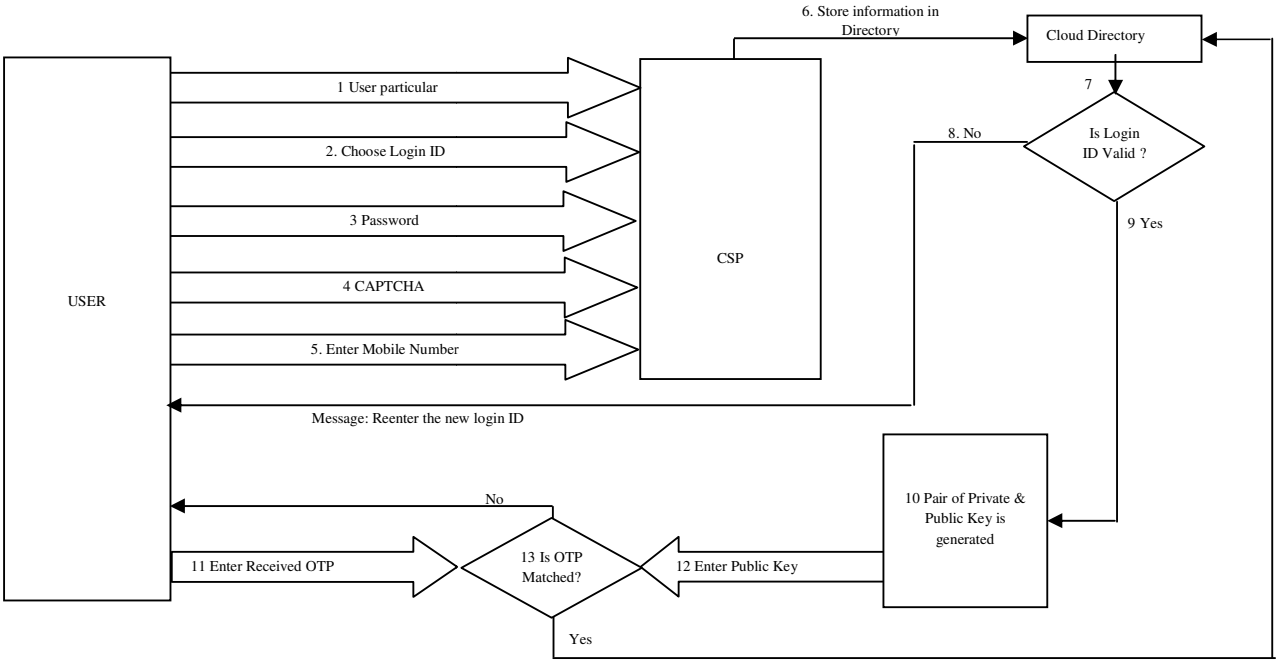

Figure 2: Registration of cloud user to cloud service provider

5.2.1. Encryption at user end

After the successful enrolment at the CSP, now the data should be transferred to cloud storage. The user encrypt the data by applying the DES symmetric key algorithm and store the public key generated at the user end database itself against the file ID allotted to file encrypted. Now plain text will be translated to cipher text 1. The DES algorithm is adopted as a very powerful algorithm as compared to DES algorithm.

5.2.2. Encryption at CSP end

The CSP receives cipher text 1 of the sent file and then apply another asymmetric key cryptographic technique Blowfish at his end. This technique generates a pair of public and private key. The cipher text 1 is again encoded with the public key generated by the Blowfish algorithm

Now each file stored is encrypted twice, which eliminates the drawbacks of the past proposals by various researcher

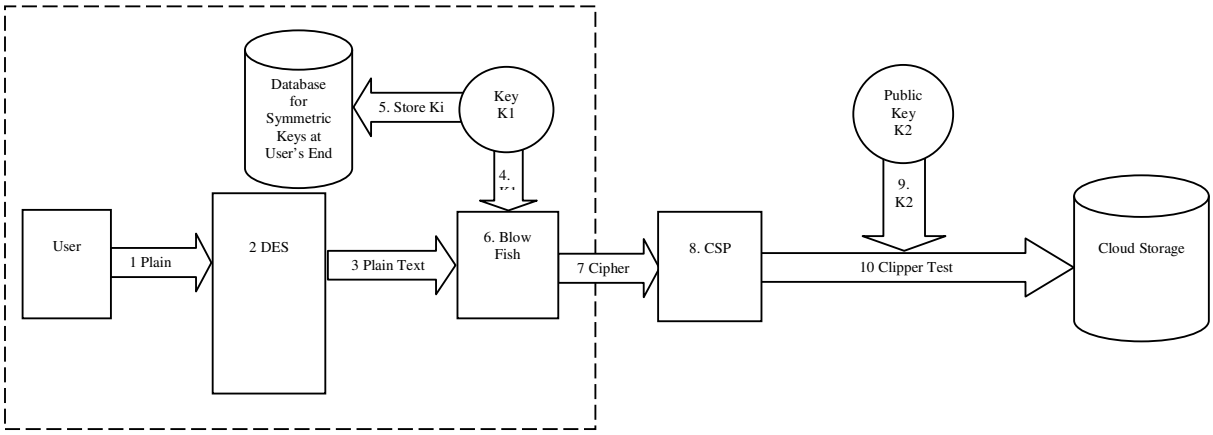

Figure 3: Storing of data in Cloud storage

5.3. Phase 3 (User Authentication on data retrieval request)

(As shown in figure 3) The user has to be authenticated by the CSP before the granting permission for the data retrieval. The user has to pass his login id, password and CAPTCHA to cloud service provider. The CSP matches and verifies the credential passed with the details maintained in its cloud directory. The CSP then send an OTP to the user registered mobile number. The user re enters the OTP to the CSP; CSP matches it and allow the user to access cloud storage.

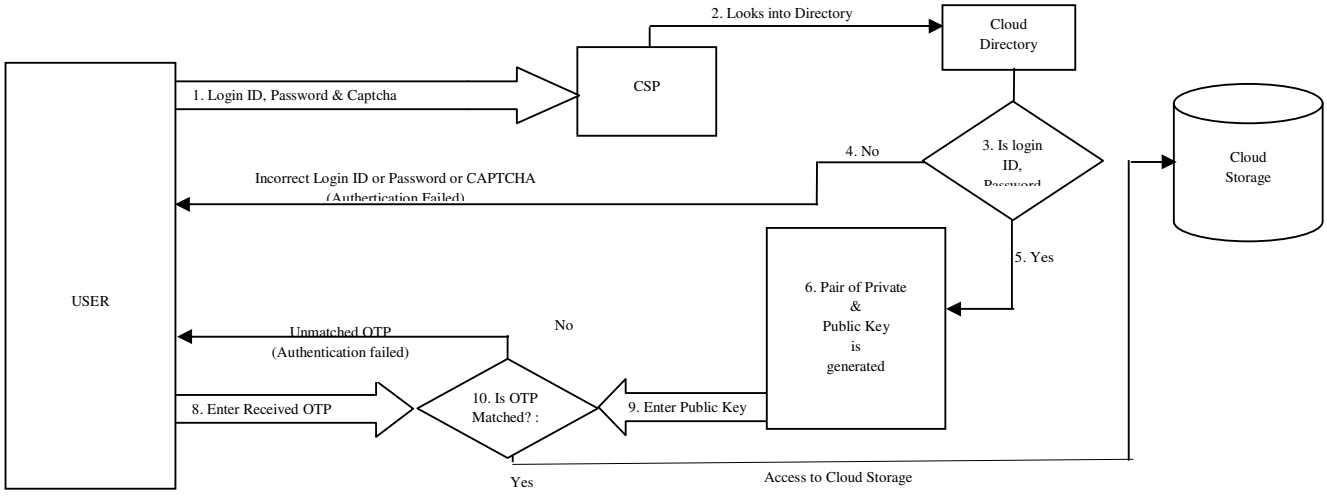

Figure 4: User's Authentication on data retrieval request

5.4. Phase 4 (Retrieval of data and Integrity verification)

(As shown in figure 5) At last whenever the data is retrieved from CSP end in encrypted mode, the authenticated user will check its own database for the private key and public key against the file ID and transform the data back in plain text mode. The user transforms the cipher text 2 into cipher text 1 by Blowfish private key, and then cipher text is converted to Plain text by DES symmetric key.

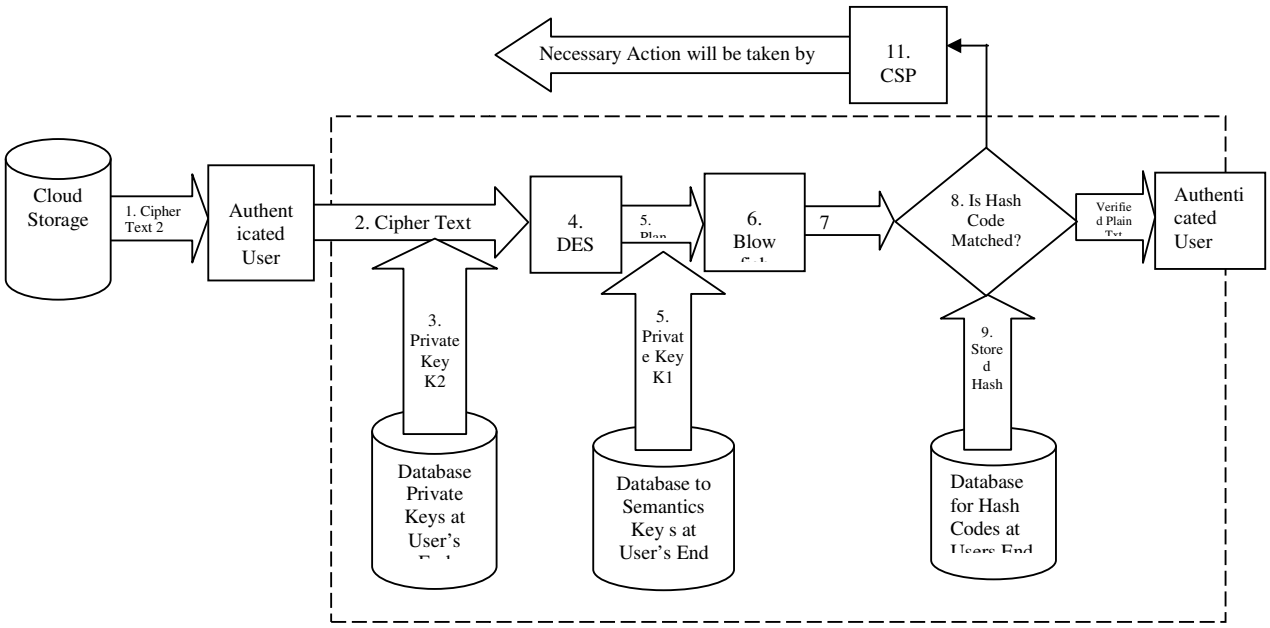

Figure 5: Retrieval of data and Integrity verification

6. SECURITY ANALYSIS

The proposed algorithm is enough secure so that the cloud user can submit its data to the cloud storage with no issues at all. The proposed algorithm can prevent all these threats and attacks listed as under:

- Service Provider Security Issues
- Secure stored data.
- Man-in-the Middle attack
- Side channel attack
- Insecure Cryptographic storage/ Poor encryption technology
- Service or account hijacking
- Data loss and leakage
- Malicious insiders/ Inside-job attack
- Authentication attacks

7. CONCLUSION & FUTURE SCOPE

This paper proposed a new combined algorithm for cloud data storage environment to achieve the objective of maximizing the data owners control on data. The performance and efficiency of the proposed algorithm is highly secure and privacy aware for all cloud environment.

In near future the algorithm can be improved with the advanced encryption algorithm concepts. The above concept will be implemented and tested against the various security attacks in comparison of the rest all papers discussed in related work for the exact competitive edge in the Cloud storage.

REFERENCES

[1] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, Keynote Paper, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA), Sept. 25-27, 2008, Dalian, China.

[2] Weiwei Lin, Chen Liang, James Z. Wang, and Rajkumar Buyya. Bandwidth-aware divisible task scheduling for cloud computing, Software: Practice and Experience[J], ISSN: 0038-0644, Wiley Press, New York, USA, 2013 (in press, Article first published online: 23 NOV 2012).

[3] National Bureau of Standards - Data Encryption Standard, FIPS Publication 46, 1977.

[4] NIST, "Advanced Encryption Standard Call", NIST, 1997. http://www.nist.gov/aes/

[5] Schneier, B.: "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings (Dec. 1993), Lecture Notes in Computer Science (LNCS), Springer-Verlag, Vol. 809, pp. 191-204, 1993, ISBN 3-540-58108-1.

[6] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 1, January 2012.

[7] Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive. Report 2008/175; 2008a.

[8] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print Archive. Report 2008/489, 2008b.

[9] Juels A, Burton J, Kaliski S. PORs: proofs of retrievability for large files. Proceedings of CCS '07, p. 584–597, 2007.

[10] Kamara S, Lauter K. Cryptographic cloud storage. Lecture Notes in Computer Science 2010;6054:136–49.

[11] Prasad P, Ojha B, Shahi RR, Lal R. 3 dimensional security in cloud computing. Computer Research and Development (ICCRD) 2011;3:198–208.

[12] Popa RA, lorchJR, MolnarD, WangHJ, ZhuangL, Enabling security in cloud storage SLAs with cloud proof. Technical report. Microsoft Research May 2010.

[13] ShachamH, WatersB. Compact Proofs of Retrievability, Proceedings of Asia crypt '08,5350,p.90–107,2008.

[14] Sood SK, Sarje AK, SinghK. A secure dynamic identity based authentication protocol formulti-server architecture. Journal of Network and Computer Applications 2011;34(2):609–18.

[15] Wang C, CaoN, LiJ, RenK, LouW. Secure ranked keyword search over encrypted cloud data. Journal of the ACM 2010;43(3):431–73.

[16] WangC, WangQ, RenK, LouW. Ensuring data storage security in cloud computing, quality of service, 2009, IW QoS IEEE17 the international workshop, p.1–9,2009.