A Modified Heuristic-Block Protocol Model for Privacy and Concurrency in Cloud

Akhilesh Kumar Bhardwaj
Research Scholar
Punjab Technical University
India

Dr. Surinder
Associate Professor
H.C.T.M, Kaithal
India

Dr. Rajiv Mahajan
Professor & Principal
C.T.I.T., Jalandhar
India

***Abstract*—With boost in the figure of cloud users and the magnitude of sensitive data on cloud, shielding of cloud has become more important. Competent methods are consistently desirable to ensure the information privacy and load management of outsource data on un-trusted cloud servers. The base of our proposed idea is the chronological display of metaheuristic firefly algorithm and blocks based Merkle hash tree protocol. This pool of combination significantly reduces the communication delay and I/O costs. The projected scheme in addition considers the dynamic data operations at block level while maintaining the equivalent security assurance. Our method makes use of third party auditor to periodically verify the data stored at cloud provider side. Our elucidation removes the burden of verification from the user side and alleviates both the user's and storage service's fear about data outburst and data corruptions.**

Keywords—Cloud Computing; TPA; Firefly; MHT; NTRU; LZW

I. Introduction

Cloud computing is a network-dependent environment, which aims to share computations or resources. The most vital negative aspect, as observed by the organizations looking ahead to transfer to the cloud is confidential data protection and application safekeeping along with communication interlude. In this paper, a simple data protection and load management protocol model has been proposed to overcome the existing negativities coupled with cloud.

The idea behind cloud computing has been introduced after the emergence of distributed computing, parallel computing and grid computing [5]. During the past few years, cloud computing has been widely adopted because the corporate require an increasingly proficient means of exploiting its IT investment [3].

In fact, clouds are dependent on Internet and they attempt to mask the complexity for the clients [1]. Cloud computing usage has become more prevalent and most of the companies have started utilizing the services from cloud computing [2].

The cloud computing model is widely accepted because it offers access to computing as well as storage as per requirement, in addition to boundless resources [4]. Some of the features of cloud computing include ubiquity, increased reliability, being virtual, adaptability, scalability, quick suppleness, abundant tendency, planned service, increased intelligence, autonomic efficient control and high quality of service "QoS" [7].

The cloud model provides numerous advantages to each and every cloud stakeholders such as cloud providers (CPs), cloud consumers (CCs) and service providers (SPs). Yet, there are also several unlocked issues available in this model, which affects the reliability to a greater extent [6].

The data residing in a cloud is subjected to severe problems and hence, currently, more number of researchers and projects has given utmost interest towards providing improved data security in cloud computing [10].

More recently, it is highly essential to learn and examine the way the cloud computing and its applications operate on clouds. In addition, it is also necessary to observe the level of privacy offered by the cloud computing services and the determination of the kind of cloud computing service to be used by the users becomes more vital. Examining the performance and the security issues of real cloud environments seems to be difficult because testing in real environments can be more costly, unrepeatable and time-consuming [8].

The security and performance associated with the entire system are also affected by the novel data storage paradigm in Cloud [12]. The cloud provider is responsible for preventing the unauthorized insiders or the malicious outsiders from accessing the data and personal information that is available in the host database and to assure data security [13].

Data that is securely stored in the server will be also under problem, when a hacker attacks several servers for obtaining the information. One security mechanism of cloud computing, which can avoid security violations, is the management reliability [14]. Safe access to the cloud services can be rendered by cloud authentication systems that utilize various methods such as simple text password, third party authentication, graphical password, biometric and 3D password object [11].

Of the serious challenges posed in cloud computing, mutual authentication is more important. With mutual authentication, both the parties involved in communication can authenticate each other prior to the initiation of communication. Several authentication methods can be used for authenticating the user.

Few authentication methods like, plain password authentication can be implemented without much difficulty. But, they are commonly feeble and primitive [9]. Making use of a reliable third party auditor, who serves as the user for evaluating and revealing the risk of cloud storage services as per user request, can be a better way of assuring data security [10].

Third Party Authentication can be considered as a form of scrutiny. Private audit-ability and public audit-ability are the two classifications of third party authentication. The private audit-ability may result in large scheme efficiency. But, the public audit-ability only enables everyone including the client, who is the owner of data, to insist the cloud server for the rightness of data storage without owning private information. Third - party auditor (TPA) aids in auditing the data of the client, so that the trouble of the data owner in handling the data can be eliminated. TPA audits to see if the data stored in the cloud is unharmed or not and thus, avoids the client from taking part. This audit performed by TPA is more essential because it accomplishes economies of scale for Cloud Computing. The released audit assists the owners in assessing the risks that are related with the cloud data services accessed. The report can be advantageous to the cloud service provider for enhancing their cloud-dependent service platform [15].

II. Related Work

The current technological advancements have led cloud computing to be more popular and successful. Yet, severe problems in security and privacy may arise, if the data and business applications are outsourced to a third person.

Zhifeng Xiao and Yang Xiao [16] have suggested plenty of methodologies for third party authentication that help in handling storage and data transaction in a secure way. The objective of all their works is to give a complete review of all the security and privacy issues in cloud environments.

The users can make a choice of the third-party auditor (TPA), if the public auditability for cloud storage is enabled. This step is more essential for the users because the TPA, who they choose, would verify the integrity of the outsourced data and they need not bother about it. More secure and successful way of introducing TPA can be accomplished, only if the auditing process does not cause vulnerabilities to data security, in addition to not increasing user's burden further. **Cong Wang [17]** has put forward a more protective cloud storage system that supports public auditing with privacy-preserving ability. They have also broadened their outcomes in a way that the TPA is rendered with the power to carry out audits for multiple users at the same time

In a distributed storage system that lacks central authority, it is difficult to provide security along with multiple function support**.** **Hsiao-Ying Lin *et al*. [18]** have presented a threshold proxy re-encryption scheme, which is integrated with a decentralized erasure code for developing a secure distributed storage system. Technically, their chief contribution is that the proxy re-encryption system would assist both the encoding operations, which are carried out on the encrypted messages, and the forwarding operations that are performed on the encoded and the encrypted messages.

The cost associated with handling data can be lowered by outsourcing the data backups from off-site to third-party cloud storage services. But, security assurance for the outsourced data is highly essential and at the present moment, the third party does this job. Hence **Yang Tang *et al.* [19]** have dealt with the design and implementation of FADE, which is a protected overlay cloud storage system that is capable of realizing fine-grained, policy-based access control and file assured deletion.

Cloud computing is turning out to be a novel computing model in the healthcare zones, though they have flourished in the other business areas. Most of the healthcare organizations have begun transferring their electronic health information to the cloud environment. **Assad Abbas *et al.* [20]** have proposed a cloud service in the health sector, wherein, the cloud serves as a medical record storage center along with the ability to perform the transfer of electronic medical records between various hospitals and health centers.

In cloud computing, the major issue of concern is that the cloud providers should be more certain about the protection of their infrastructure. This issue needs more consideration because the outsiders, other clients or any of the unauthorized cloud employees may have access to the data in an unlawful manner. **Ching-Nung Yang [21]** have proposed a cloud security services, which incorporates key agreement and authentication. Here, the secure cloud computing (SCC) has been developed with the utilization of Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing. The SCC that is employed can be of two classes. The former uses a trusted third party (TTP) and the latter does not make use of a TTP.

The need for ensuring data security is rising constantly and in particular, the hybrid cloud computing model requires data protection to a larger extent. **Jingxin K. Wang [22]** have put forth a number of methods for providing user data security that comprises of single encryption, multi-level virtualization and authentication interface. This work can be widened to the state, where CA system is either lacked or crashed.

A two layer encryption based approach has been suggested by **Mohamed Nabeel and Elisa Bertino [23]** in order to work out the problem by delegating as much of the access control enforcement responsibilities as feasible to the cloud while decreasing the information exposure risks due to colluding users and cloud. They have demonstrated that this problem was NP-complete and furthermore have suggested new optimization algorithms. By utilizing partial relationships among ACPs, they had furthermore plan to further decrease the computational cost.

Faraz Fatemi [24] have offered an efficient and scalable user authentication scheme for cloud computing environment. A client-based user authentication agent has been introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a-service application has been used to confirm the process of authentication for unregistered devices.

G. Jai Arul Jose [25] has offered an security system providing authentication, confidentiality and data integrity of user's data by joining the cloud computing framework with cluster load balancing, SSL over AES and secure session.

E.M. Mohamad [26] has provided on-demand security options by making selection from different encryption algorithms. They are examined based on NIST statistical testing and implemented as pseudo random number generator (PRNG). Performance calculation is done by testing encryption speed.

V. Nirmala [27] has proposed user authentication scheme in which data is divided into blocks and applied with AES encryption after the generation of hash value for each block. Further, the Hash code is also implemented to check the data integrity. The cloud here is used to storing encrypted data and generating hash while rest of work takes place at user side.

The paper [22] suggests that making use of user data at the time of commercialization can end up in a great issue. The security and privacy of commercial data of the user is much preferred than other factors, while the user wants to establish cloud computing in their company. Certain problems of security in cloud computing still persist, in particular, the inter-cloud operations. The cloud providers need to meet the standard of inter-cloud operation interfaces.

The data security ensured through Privacy-Preserving Public Auditing is stated in [17], wherein, TPA is employed to achieve greater efficiency. Yet, the efficiency of their work during multiple auditing tasks seems to be lower. It is also found that the security and efficiency obtained from their work is not that much better, when an extensive investigation is made.

When a cloud system is being developed, several issues (that reduce the level of security) need to be considered with utmost care. People may find difficulty in accessing all their data of interest from the cloud data center. This is because various cloud service providers store the required data. Hence, a state of uncertainty arises amid the users, if they access data through cloud service providers.

The data privacy issue that is encountered during third party auditing cannot be cleared entirely with the introduction of the encryption method. But, it can simply be transformed into the complex key management domain. The cloud model brings about a lot of latest security confronts, which have not been fine tacit. To overcome these drawbacks of privacy and concurrency, the proposed article presents a modified firefly – merkle hash tree protocol model. The model can be further extended for different communication scenario in the future.

III. Proposed Model

Cloud computing configuration contains two foundation layers: a virtualization layer and a management layer [30]. In the virtualization layer, we catch the actual platforms and servers that host the virtual machines and have virtualization enabled hardware. In the management layer, we come across the modules accountable for enabling the complete operations detailed for the cloud.. Ensuring the integrity of data storage is the primary difficulty in Cloud Computing. Hence, to overcome this difficulty, a simple data protection and load management protocol model (where data is encrypted using Advanced Encryption Standard before it is launched in the cloud) has been proposed.

In the proposed FMHP (Firefly-Merkle Hash Tree Protocol) model, the firefly algorithm is implemented for file encryption and integrity verification, while MHT helps in load management and files compression.

Here, a third party auditor (TPA) would assist the cloud client for ensuring the integrity of the dynamic data placed in the cloud. During the auditing period, the client's participation is considered by the TPA to check whether the client data is left undamaged or not. By doing so, the levels of economy of cloud computing can be achieved.

The proposed cloud computing model could fix the serious problems, namely public authentication, load balancing and dynamic data integrity. The effort is divided into different modules including design and execution of a FMH protocol to overcome the problem of public authentication and load management (while maintaining file server based data integrity), assessment of various threats on the security of cloud environment, evaluation and analysis of security and performance parameter like encryption time, decryption time, throughput and network delay and ensuring appropriate load balancing with metrics like throughput, response time, migration time, scalability and fault tolerance.

A. Proposed Algorithm

Step 1

User Login from the Client Software

Step 2

Establishment of Validation

TPA Registration - Main Server Login: Username, Password, MAC address will send to the Main Server.

Step 3

First Encryption of Username, Password and MAC address using AES and fully Homomorphic Algorithm

*1) Input of A; SK (username, password, MAC)) /*SK – Signature Name*/*

2) Input of B; BK (where BK is the apply AES algo first and then apply gates operation to convert plain SK text to cipher text)

*3) Output; LK+ 1(output of signature in cipher text form) /*LK – Final Signature*/*

Step 4

TPA Server will verify the Signature in the Database: If signature gets match then reply to user with success message as well as to main server with success message.

Step 5

TPA Server will perform Handshaking procedure 10 times with recently authorize client based on the specific format in which TPA server send message to client 10 times asking "Show Your Identity". In respect the client reply, TPA communicates with following format to server "Yes Authenticated: IP, MAC, Name of OS, Hardisk Address". If out of 10, 9 responses are found true then TPA issues Session Number to Main server respect to the Client.

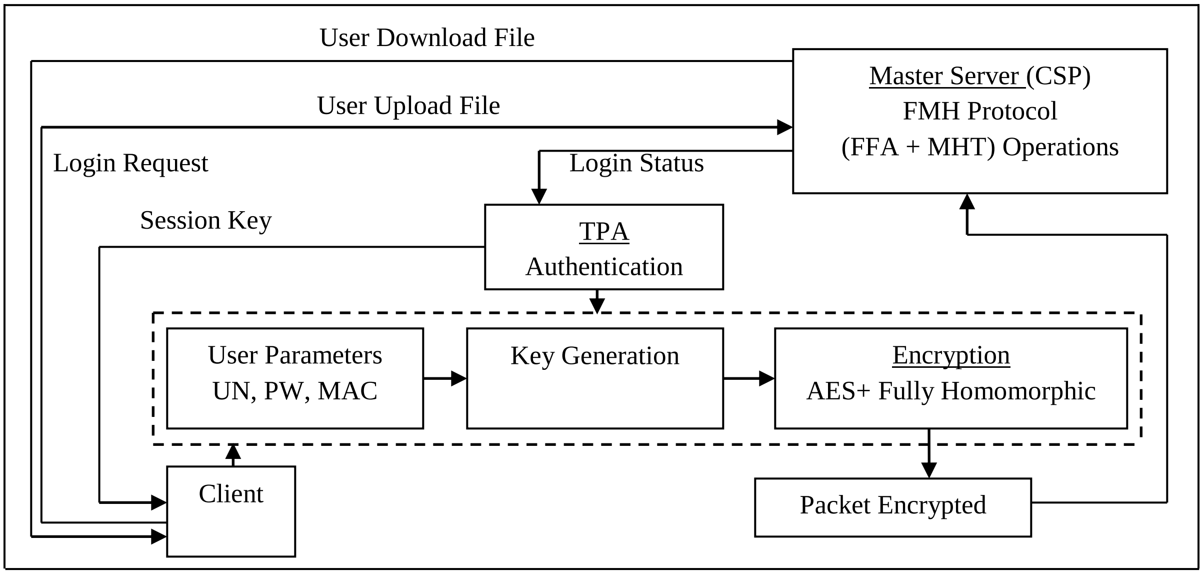

Fig. 1. TPA-FMHP based Proposed Cloud Security Model

Step 6

a) TPA sends prime number to the client who is going to upload the file.

b) Client receives the public and private key (computed by MS using NTRU algorithm)

/*NTRU (N-th degree Truncated Polynomial Ring Unit Algorithm) is based on polynomial arithmetic and provides very fast computation for the encryption and decryption of the message*/

1) The operations are based on objects that are in a polynomial ring: $R = Z [X] / (XN - 1)$

2) The polynomials, present in the ring have integer coefficients and degree $N – 1$:

Key Generation:

/*NTRU involves a public key and a private key. The public key is used for encrypting message and can be known to everyone. Messages encrypted with this key can only be decrypted in a reasonable amount of time using the private key*/

1) For the encryption, let m be the polynomial representing a message. We choose a small polynomial r as the random blinding polynomial, and compute the ciphertext $c = p*r*h + m \bmod q$.

2) For the decryption of c, $a = f*c \bmod q$ *is computed firstly, where the modulo q operation is done in an appropriate interval. Then the plaintext* $m = a \bmod p$ *is recovered.*

/*NTRU based convolution product computation algorithm is widely used in software implementation [28] */

Both A and B

PK1 + 1 ← generate an initial key of fireflies (LK)

/*pass Generated key from NTRU to initiate Firefly as well as convert plain text to cipher on every rotation*/

For (A + 1) do (where A would 1 to n value)

A (plaintext)

$\omega 4 \leftarrow$count (n) apply encryption till of n

TK$\leftarrow \omega 4$

$\alpha B \leftarrow E_{PK}$ (plaintext)(conversion of plaintext into ciphertext)

Step 7

Compression Process

a) Take ciphertext file generated on above steps.

b) Convert the file into the binary form using MHT hash function algorithm.

c) Split the binary content in 32 bit blocks using MHT.

d) Pass these 32 bit blocks into LZW string compression algorithm. It returns compressed blocks.

e) Arrange the blocks in tree format.

f) Assemble various chunks starting from the root till all blocks are covered using DFS support.

g) All blocks are then converted into string and write a new file.

/* LZW sting Compression algorithm is dictionary based algorithm which output a code for a character. Input data to compress is read from the file. Output codes have less number of bits than input data [29]*/

```
String s, char c;
s- Get input character
While (there is still input character)
ch- transfer input string to ch.
If (ch is in dictionary)
Generate its codeword;
Else
Update ch and get next character to ch and
Again search data in dictionary;
```

```
        If (it is not present in dictionary) then
        Add that string to dictionary;
        End if;
```

Decompression process

/*In LZW decompression algorithm, it needs to take the stream of code output from the compression algorithm, and use them to exactly recreate the input stream*/

```
        ch = output code
        While (there is still data to read)
        Code =get input character;
        If (code is not in the dictionary)
        Entry =get translation of code;
        Else
        Entry=get translation of output code;
        Output entry;
        ch =first character in entry
        Add output code + c to the dictionary
        Output code = code;
```

/*In decompression algorithm, code will be searched in dictionary and its character will be output*/

Step 8

Decryption using firefly algorithm

```
    B
    A←$D_{SK}$ (B) /* only B can decrypt the result. Here B will generate hash and send back to A*/
    If R= 1 then /*1=true 0=false*/
    TK=$D_{SK}$ (put cipher text)/* convert cipher text to plain*/
    End if
        End for
            End.
```

Step 9

Concurrency Management using MHT algorithm

a) Initiate from the root. Root will update all the child nodes (connected to the parent node) using Merkle hash tree algorithm.

b) The process terminates as all nodes of the network are updated.

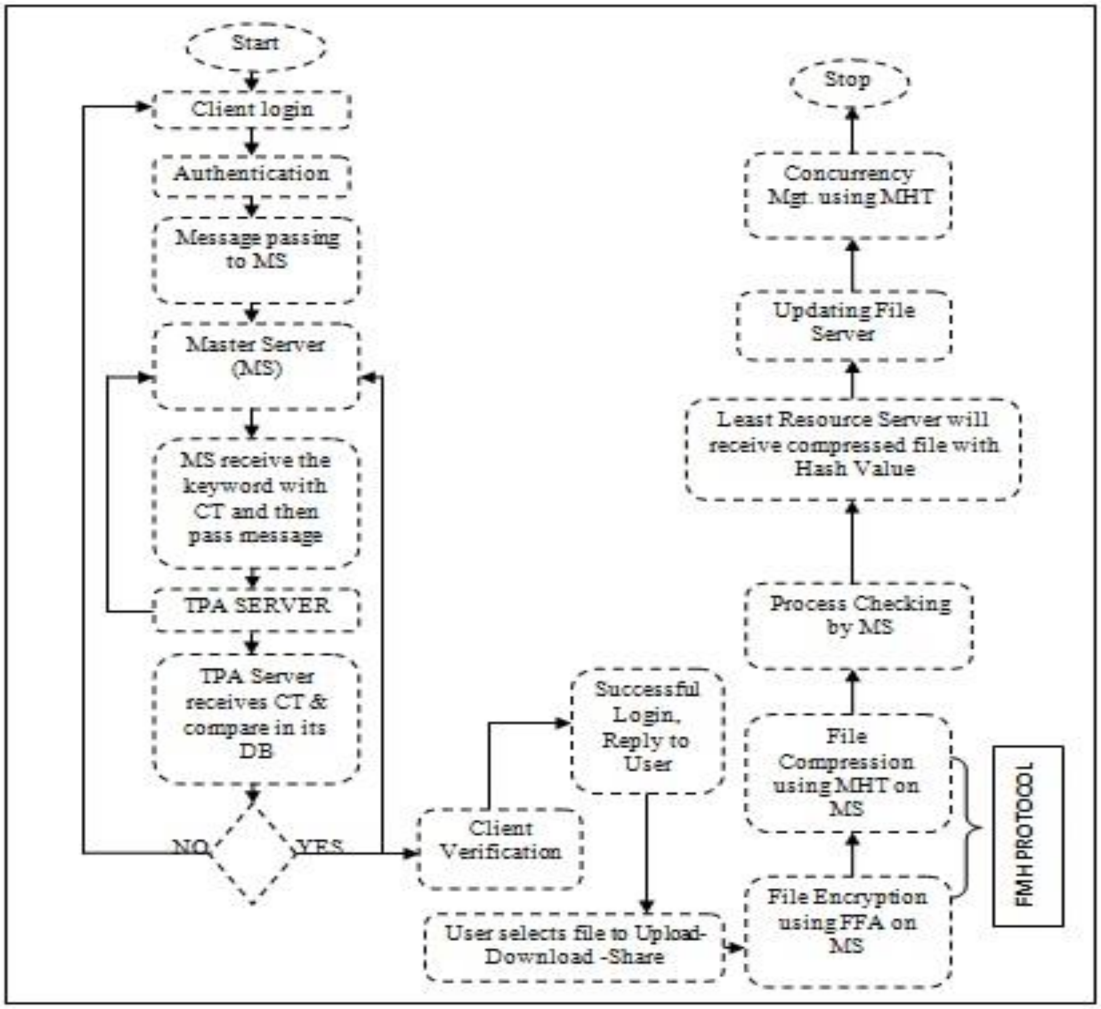
Start
Client login
Authentication
Message passing to MS
Master Server (MS)
MS receive the keyword with CT and then pass message
TPA SERVER
TPA Server receives CT & compare in its DB
NO
YES
Client Verification
Successful Login, Reply to User
User selects file to Upload-Download -Share
File Encryption using FFA on MS
File Compression using MHT on MS
FMH PROTOCOL
Process Checking by MS
Least Resource Server will receive compressed file with Hash Value
Updating File Server
Concurrency Mgt. using MHT
Stop

Fig. 2. Flow Chart of the Proposed System

I. Conclusion

The payback of the clouds computing is to accomplish the economics of scale, diminish the expenses on technology infrastructure, improves ease of access and monitoring the projects more efficiently. In addition, ensuring the security of client's data is the prime focus. In this paper, the cloud computing key issues are discussed and new integrated protocol model for information protection and load management is suggested.

The performance of the proposed system will be evaluated and justified in preventing anxious attacks on the security of cloud environment. Assessment and investigation of security and performance parameters will be the part of the apprehension along with ensuring suitable load balancing.

The potential work can be constructive to expand the security and performance of cloud computing during different communication modules.

References

[1] Farzad Sabahi, "Cloud Computing Security Threats and Responses", In the Proceeding of IEEE 3rd International Conference on Communication Software and Network, pp. 245-249, May 2011.

[2] Xiang Tana, Bo Aib, "The Issues of Cloud Computing Security in High-speed Railway ", In the Proceeding of IEEE International Conference on Electronic & Mechanical and Engineering and Information Technology, pp. 4358-4363, Aug 2011.

[3] Yanuarizki Amanatullah, and Heru Purnomo Ipung, "Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective", In the Proceeding of IEEE International Conference on ICT for Smart Society (ICISS), pp. 1-4, June 2013.

[4] Qiang Guan, Chi-Chen Chiu and Song Fu, "CDA: A Cloud Dependability Analysis Framework for Characterizing System Dependability in Cloud Computing Infrastructures", In the Proceeding of IEEE 18th International Conference on Dependable Computing, pp. 11-20, Nov 2012.

[5] WANG En Dong WU Nan, LI Xu, "QoS-oriented Monitoring Model of Cloud Computing Resources Availability", In the Proceeding of IEEE International Conference on Computational and Information Sciences, pp. 1537-1540, June 2013.

[6] Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", In the Proceeding of IEEE International Conference on Clouding Computing (CLOUD), pp. 364-371, July 2011.

[7] Maha Attia Hana, "E-Government Cloud Computing Proposed Model: Egyptian E_Government Cloud Computing", In the Proceeding of IEEE International Conference on Advanced in Computing Communication and Information (ICACCI), pp. 847-852, Aug 2013.

[8] Wei Zhao, Yong Peng, Feng Xie, and Zhonghua Dai, "Modeling and Simulation of Cloud Computing: A Review ", In the Proceeding of IEEE International Conference on Asia Pacific Cloud Computing Congress (AP Cloud CC), pp. 20-24, Nov 2012.

[9] Nimmy K., M. Sethumadhavan, "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", In the Proceeding of IEEE fifth International Conference on Application of Digital Information and Web Technologies (ICADIWT), pp.101-106, Feb 2014.

[10] Shuai Han, Jianchuan Xing, "Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing", In the Proceeding of IEEE International Conference on Cloud Computing and Intelligence System (CCIS), pp. 264-268, Sept 2011.

[11] Dinesha H A, Agrawal V K, "Multi-level Authentication Technique for Accessing Cloud Services", In the Proceeding of IEEE International Conference on Computing Communication and Application (ICCCA), pp. 1-4, Feb 2012.

[12] Qian Wang, Cong Wang, and Kui Ren, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", In the Proceeding of IEEE Transaction on Parallel and Distributed Systems, Vol. 22, No. 5, pp. 847-859, May 2011.

[13] Ching-Nung Yang, Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", In the Proceeding of IEEE International Conference on Biometric and security Technology, pp. 259-266, July 2013.

[14] Sue-Chen Hsueh, Jing-Yan Lin, and Ming-Yen Lin, "Secure Cloud Storage For Convenient Data Archive Of Smart Phones", In the Proceeding of IEEE International Conference on Consumer Electronics, pp. 156-161, June 2011.

[15] Bhavna Makhija, VinitKumar Gupta, and Indrajit Rajput, "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 2, Feb 2013.

[16] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing" In the Proceeding of IEEE Conference on Communication Surveys & Tutorials, Vol. 15, No. 2, pp. 843-859, May 2013.

[17] Cong Wang, Sherman S.M. Chow, and Qian Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage", In the Proceeding of IEEE Transaction on Computers, Vol. 62, No. 2, pp. 362-375, Feb 2013.

[18] Hsiao-Ying Lin, and Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", In the Proceeding of IEEE Transaction on Parallel and Distributed Systems, Vol. 23, No. 6, pp. 995-1003, June 2012.

[19] Yang Tang, Patrick P.C. Lee, and John C.S. Lui, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", In the Proceeding of IEEE Transaction on Dependable and Secure Computing, Vol. 9, No. 6, pp. 903-916, Nov 2012.

[20] Assad Abbas and Samee U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds", Journal of Biomedical and Health Information, Vol. 18, No. 4, pp. 1431-1441, July 2014.

[21] Ching-Nung Yang, and Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", In the Proceeding of IEEE Transaction on Biometrics and Security Technologies (ISBAST), pp. 259-266, July 2013.

[22] Jingxin K. Wang, Xinpei Jia, "Data Security and Authentication in Hybrid Cloud Computing Model" In the Proceeding of IEEE International Conference on Global High Tech Congress on Electronic (GHTCE), pp. 117-120, Nov 2012.

[23] Mohamed Nabeel and Elisa Bertino, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transaction on Knowledge and Data Engineering, Vol. 26, No. 9, pp. 2268-2280, Sep 2014.

[24] Moghaddam, Faraz Fatemi, Shiva Gerayeli ; Rouzbeh, Sohrab ; Araghi, Sagheb Kohpayeh ; Alibeigi, Nima Morad ; Varnosfaderani, Shirin Dabbaghi, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", IEEE symposium, Kuala Lumpur, Malaysia, pp. 508-513, 2014.

[25] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network trends and Technology, Volume 1, Issue 1, pp 18-22, 2011.

[26] E. M. Mohamed, H.S. Abdelkadar, S.E. Etriby, "Enhanced Data Security Model for Cloud Computing", International Conference on Informatics and Systems, 2012.

[27] V. Nirmala, R. K. Shivanadhan, R. S..Lakshmi,"Data Confidentiality and Integrity Verification using User Authentication Scheme in Cloud", International Conference on Green High Computing, IEEE, pp 1-5, 2013.

[28] Xuexin Zheng, An Wang, Wei Wei, "First-order collision attack on protected NTRU cryptosystem", Microprocessors and Microsystems, Elsevier, pp 601–609, 2013.

[29] S. Kaur, V.S. Verma, "Design and Implementation of LZW Data Compression Algorithm", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[30] Patrascu, V.V. Patriciu, "Logging for Cloud Computing Forensic Systems", International Journal of Computer Communication and Control, ISSN 1841-9836, 10(2):222-229, April, 2015.