ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Multilevel Security Approach for Cloud Data Storage

A.Balasubramanyan [1], Dr. D .Chitra [2]

P.G. Student, Department of Computer Science and Engineering, P. A. College of Engineering and Technology, Pollachi, India[1]

Professor and Head, Department of Computer Science and Engineering, P. A. College of Engineering and Technology, Pollachi, India[2]

ABSTRACT: Cloud computing brought flexibility, scalability, and capital cost savings to the IT industry. In more companies turn to cloud solutions, securing cloud based service becomes increasingly important, because for many organizations, the final barrier to adopting cloud computing is sufficiently secure. The users rely on cloud storage as it is mainly because cloud storage is available to be used by multiple devices at the same time. The flow and storage of data on the cloud environment in plain text format may be main security threat. The security issues associated with data storage over cloud is a major discouraging factor for potential adopters. The existing work for cloud security is to using cryptography approach. A novel approach to cloud security is to implement by using multilevel security system. The combination of cryptography, session management, log management system provides to high level security in the cloud storage. The multi level security system is to reduce the malicious activity and increase the security level in the cloud storage. The multilevel security system for cloud storage is also support to avoid duplication and maintain unnecessary disk utilization to increase the cloud server performance. Through analysis investigating data privacy and efficiency is to assure in the proposed system in cloud environment. Experiments on the real-world data set further to show the proposed approach indeed introduce low overhead on computation and resource communication.

KEYWORDS: Cloud Computing, Crypto systems, Log management system, Session key generation, Cloud storage security, Deduplication.

I. INTRODUCTION

Cloud Computing refers to both applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service. The datacenter hardware and software is called a Cloud. The Cloud is made available in a pay-as-service manner to the general public, the service being sold is Utility Computing. The cloud model for enabling 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 [1]. Cloud computing is an internet based resource sharing technique. Based on the technology domain usage it can be divided in four following major types [1], [2].

1. **Private Cloud:** The Cloud-based solution is provisioned and used by a single enterprise. The services in a private Cloud are consumed by multiple users, and the services are managed operated and owned by the enterprise itself, a third party and combination of between them [3].

2. **Community Cloud:** This type of cloud infrastructure is targeted towards a selected group or community of consumers belonging to organizations with related goals [4]. It may be managed by one or more of the organizations involved, or by some third party.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

3. **Public Cloud:** The public Cloud is the provisioning of Cloud-based solutions is publicly available for open use. The services are ubiquitous available through an Internet connection but this deployment model is rising many security and privacy concerns [5].

4. **Hybrid Cloud:** The hybrid level cloud infrastructure comprises of two or more forms of the previous cloud infrastructures where interactions among the different infrastructures are made possible by using standardized or proprietary data and application interaction methods [3].

The service means different types of applications provided by different servers across the cloud. There are three types of service deployment models provided by the cloud are [2].

1. **Software as a Service (SaaS):** In SaaS, the user uses different software applications from different servers through the Internet. The client will have to pay for the time he uses the software. The software that does a simple task without any need to interact with other systems makes it an ideal candidate for Software as a Service [6].

2. **Platform as a Service (PaaS):** PaaS provides all the resources that are required for building applications and services completely from the Internet, without downloading or installing software [4]. PaaS services are software design, development, testing, deployment, and hosting. The platform as a service is implemented with the help of virtualization approach.

3. **Infrastructure as a Service (IaaS):** It is also known as Hardware as a Service (HaaS). It offers the hardware as a service to an organization so that it can put anything into the hardware. The rent resources allowed by IaaS to the user are Server space, Memory, Storage space [7].

II. RELEATED WORK

Different types of approaches are developed in the past decades by researchers for solving, cloud computing security problems. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not practical solution due to the expensiveness in input and output transmission cost across the network. Besides, it is often insufficient to detect the data corruption only at the same time accessing the data, as it does not give users correctness assurance for those un accessed data and might be too late to recover the data loss or damage.

The burden can be resolved by few researchers introduced the public auditing service using Third Party Auditor (TPA) to audit the outsourced data at needed. TPA has a problem in the case of unencrypted public cloud data. Besides, encryption does not completely solve the problem of protecting data privacy against third party auditing. The existing work is based on cryptography approach either tokenization approach provides the privacy preserving on cloud storage. The number of cryptography approaches such as symmetric or asymmetric approach used to implement the secure cloud data storage.

Merkle [26] proposed a paper to describe a number of cryptographic protocols. Certainly, these are not only possible valuable tools to the system designer can be achieved and provide feasible solutions to problems of recurring interest. It gives only basic ideas and methods to implement public crypto systems. But it doesn't have an enhancement for the cloud security solution.

Boneh [13] proposed a short signature scheme based on the Computational Diffe-Hellman assumption on certain elliptic and hyper-elliptic curves. The signature length is half the size of a Digital Signature Algorithm for a similar level of security. This short signature scheme is designed for systems signatures are typed in by a human or signatures are sent over a low-bandwidth channel. It has a problem in Key generation on high bandwidth.

Ateniese [23] proposed a new idea for Storage outsourcing is a rising trend to prompts a number of interesting security issues, many of have been extensively investigated in the past. Provable Data Possession (PDP) is a topic that

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

has only recently appeared in the research literature. The main issue is to frequently, efficiently and securely verify that a storage server is faithfully storing its client's outsourced data. The storage server is assumed to be entrusted in terms of both security and reliability. The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. PDP technique allows outsourcing of dynamic data that is efficiently supports operations, block modification, deletion and append.

Ateniese and Kamara [20] provide a framework for building public-key Homomorphic Linear Authenticator from any identification protocol satisfying certain homomorphic properties. The research shows to turn any public-key Homomorphic Linear Authentication into a publicly verifiable Proofs of Storage with communication complexity independent of the file length and supporting an unbounded number of verifications. This research illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use Proofs of Storage based on factoring.

Erway [25] proposed a Dynamic Provable Data Possession because storage-outsourcing services and resource-sharing networks have become popular the problem of efficiently proving the integrity of data stored at entrusted servers has received increased attention. The Provable Data Possession (PDP) model, the client preprocesses the data and sends it to an entrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted without downloading the actual data. But the problem is original PDP scheme applies only to static files.

Anna Lisa Ferrara [22] experiments provide strong evidence that batching short signatures is practical, even in a setting an adversary can inject invalid signatures. These results apply to standard and Identity-Based signatures, exotic short ring and group signatures are increasingly being considered for privacy-critical applications. At a deeper level, results indicate that efficient batching depends heavily on the underlying design of a signature scheme, particularly on the placement of elements within the elliptic curve subgroups signature and the comparable size and security, yet the latter scheme can batch more than 250 signatures per second, implementation clocks in at fewer than 40. The advantage of these scheme designers should take these considerations into account of proposing new pairing-based signature schemes.

Chander Kant, yogesh Sharma [30] proposed Enhanced Security Architecture for Cloud Data Security. The author defines the cloud architecture with configured samba storage and cryptographic encryption techniques. The cloud architecture deployed with samba storage uses operating system feature specifying permission values for three attributes User, Owner, Group and maps it to cryptographic application to performs cryptographic operations. Cryptography application supports symmetric and asymmetric encryption algorithm to encrypt and decrypt data for uploading and downloading within cloud storage. A username and password based authentication mechanism for users and digital signature scheme for data authenticity are defined within cloud architecture.

Mary Michael [31] proposed the method of Delegating Log Management to the Cloud Using Secure Logging In this method investigate the tough challenges against the secure cloud management service. It provides a comprehensive solution for storing and maintains log records in a server operating in cloud-based environment. Also address security and integrity issues not only just during the log generation phase but also during other stage in the log management.

III. MULTILEVEL SECURITYAPPROACH FOR CLOUD SYSTEM

The cloud data security contains traditional approaches like third party auditing, homomorphic linear encryption, random masking, short signature, and provable data positioning method, remote positioning method has their own disadvantages in cloud security domain. Its challenge work to provide the efficient security method for cloud data

Fig. 1. Multi Level Security System Cloud Architecture

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

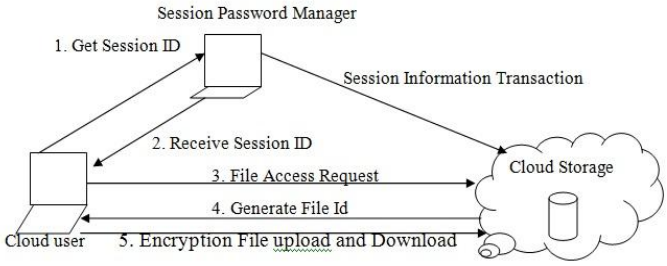

Fig. 1. Multi Level Security System Cloud Architecture

owner and cloud service provider. The Multilevel security system cloud storage architecture is shown in Fig. 1. There are three basic types of entities in the system: Cloud User, Session Password Manager, and Cloud Storage Server.

Cloud User: An entity, user performs data storage and retrieval operations over cloud storage. The user will access the resources inside the organization and also shared cloud storage environment.

1. **Session Password Manager:** Once correct user credentials are matched in the data base the next screen will be generate the session password using the mobile App. Each time user login the random session password generating to increase data integrity in the cloud data storage.

2. **Cloud Storage Server:** The cloud servers provides data storage space and maintain resources required for data computations. The cloud storage servers are maintained by the Cloud Service Provider (CSP).

IV. CRYPTOGRAPHY APPROACH

Cryptography is a method to provide the data security in the cloud network. The original text is called as plain text and sometimes called as clear text. The plain text is covert in to cipher text format is called as Encryption. The cipher text is convert into plain text is called as Decryption. Encryption is performed in the source place and Decryption is performed by destination place. There are two types of algorithms used for cryptography method one is symmetric approach and another is asymmetric approach. In symmetric approach encryption and decryption is used same key for data security. The different symmetric algorithm comparison is presented in Table 1. The asymmetric approach encryption and decryption is used different keys it is suitable for shared network data transmission.

PARAMETERS	DES	3DES	AES
Block Size	64 bits	64 bits	128 bits
Key length	56 bits	112,168 bits	128,192,256
Number of Rounds	16	48	10,12,14
Security level	Not enough	Adequate	Excellent
Execution time	Slow	Very slow	More fast

TABLE I. SYMMETRIC ALGORITHM COMPARISON

The comparison of symmetric algorithm Advanced Encryption Standard (AES) is the best algorithm for secure data storage in the cloud domain. AES algorithm used key size is 128 bits, 192 bits or 256 bits. The bits within such sequences will be numbered starting at zero and ending at one less than the sequence length. All byte values in the AES algorithm will be presented as the concatenation of its individual bit values 0 and1 between braces in the order {b7, b6, b5, b4, b3, b2, b1, b0}. These bytes are interpreted as finite field elements using a polynomial representation.

$$b_7x_7 + b_6x_6 + b_5x_5 + b_4x_4 + b_3x_3 + b_2x_2 + b_1x + b_0 = \sum_{i=0}^{7} b_ix_i \quad (1)$$

The AES algorithm performs four functions in each round encryption and inverse function of four operations performed in the decryption.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

1. **SubBytes:** The SubByte transformation is a non-linear byte substitution that operates independently based on the S- Box substitution table. In S-Box one byte is substituted for another based on substitution algorithm. Apply the transformation function over GF (28).

$$b_i' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \quad (2)$$

2. **ShiftRows**: The ShfitRows performs the bytes in the last three rows of the state are cyclically shifted over different number of bytes. Row zero of the state is not shifted, row one is shifted one byte, row two is shifted two bytes and row three is shifted three bytes. ShiftRows function transformation proceeds as follows.

$$S'r, c = Sr(c + shift(r, Nb)) \bmod Nb \quad \text{for } 0<r<4 \text{ and } 0 \le c < Nb \quad (3)$$

3. **MixColumns**: The MixColumns provides by mixing data within columns. The four bytes of each column in the state are treated as a four byte number and transformed to another four byte number. The MixColumns polynomial function is given below.

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \quad (4)$$

4. **AddRoundKey:** The actual encryption is performed in the AddRoundKey function, each byte in the state is XORed with the sub key. Each round key consists of Nb words from the key schedule is given below.

$$[s'_{o,c}, s'_{1,c}, s'_{2,c}, s'_{3,c},] = [s_{o,c}, s_{1,c}, s_{2,c}, s_{3,c},] \oplus [w_{roud * Nb + c}] \quad (5)$$

V. DYNAMIC SESSION CREATION APPROACH

The user session is more important in the cloud data security. Each time user will login using separate user session identification number. The dynamic session identification algorithm is given below.

Step 1: Generate the user key for each login P= (F, B) and B (F, R) = Pd. R is the random number provided by the server. The Pd is the dynamic session identification for authentication.

Step 2: Generate the secure session identification using the simple linear function. The x_i is one digit of the password and y_i is the random number provided by the server and **a** is the remain secret.

$$B(x_i) = ax_i + y_i \bmod Z \quad (6)$$

Step3: To perform the random number calculation is implemented by using the randomized liner function as given below.

$$B_{xi} = \begin{cases} k1 = (ax_1 + y_1 + x_2 + c) \bmod z, i = 1 \\ k_i = (ak_{i-1} + y_i + x_i + c + x_{i+1}) \bmod z, i = 2,..n \end{cases} \quad (7)$$

The **a** is constant the user needs to remember but **c** is not. The most interesting of the function is that c will be a random number which the user randomly picks each time the user tries to login to the system. Since gcd (a, Z) =1, the above function is also a bijective function regardless of the c value. Because c is also unknown to server, the server knows that $c \in \{0, 1,\ldots, Z-1\}$.

Step4: The generated dynamic session identification number is displayed using mobile application implemented with the help of J2ME programming. Once the session identification number is matched with the server the user will access the corresponding file resources in the cloud storage.

The existing method the authors only focusing cryptography, one time password, Third party auditor methodology to investigate. The novel approach for privacy and preserving cloud data using multilevel security approach is to combine model to provide efficient system to enable security in cloud data storage. The dynamic session key generation is used to access the user resources only matching the session key in the database. The multilevel security system to minimize the security loop holes and enable data integrity in the cloud.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

V1. LOG MANAGEMENTAPPROACH

The security in the public cloud, log management is more important. The logs and data status are maintained by the separate third party auditors. Using TPA log management to reduce the overall burden to cloud data owner and cloud service providers. The Fig.2 shows the diagrammatic representation of log management system.

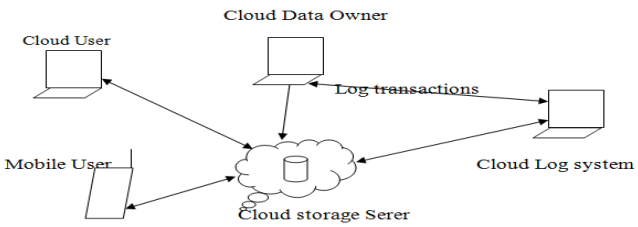

Fig. 2. Log Management Architecture

The log management system will maintain the user access log database. The cloud log system should be listening in the data transmission in the cloud network. The malicious activity will occur in the cloud access immediately log system sends the report to the data owner. There are four functional components in a cloud logging management system

1. **Cloud User:** The cloud user is the end user to access the resource in the cloud storage through the cloud service provider. The cloud user accesses the cloud resources based on the user credentials.
2. **Cloud Data Storage:** The cloud data storage consists of user resources and data storage. The cloud data server provides the resource access to the cloud data owner and cloud end user in the public and private cloud networks. The user will access the files using simple query language and Graphical User Interface system.
3. **Cloud Data Owner:** The cloud data owner is the initiate the data stored in the cloud storage. The cloud data owner to provide the access permission to the cloud users.
4. **Cloud Log Management:** The cloud log management system contains the log monitor and log management. The major functionalities of the log monitor system is to monitor and review log data, generating the queries to retrieve and analyze the log data retrieved from the cloud.

Log management system is very important for proper functioning of any organization information processing systems. It is also very expensive to maintaining log data of many organizations over long periods of time. The unauthorized persons some time possible to access the log files to create overhead to the data owner and cloud service providers. The problem is overcome by using an effective secured cloud base log management system with required protocols and methods that strengthen the security of query execution over a logging cloud database. The log analyzer and log monitor applications running inside the log management system. The log greeting message is automatically send to the data owner in the cloud through third party mail server.

VI. EXPERIMENTAL RESULTS

The Cryptography approach module is implemented by using Advanced Encryption Standard (AES) algorithm. The size of key length is 256 is used for this module to increase the cloud security. The user login using user credentials and select the size of the file and upload the file to the cloud. The file is uploading in to the cloud storage the encryption is done by using AES 256 algorithm. The encryption and decryption using AES 256 algorithm is implementing with the help of JavaScript programming language in Netbeans Integrated Development Environment is shown in Fig. 3. The files are stored using HeidiSQL Database. The user downloads the file and performs the reverse operation of AES to get their original data in the cloud.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

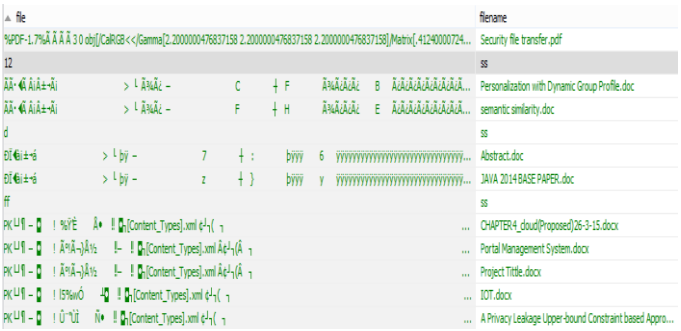

Fig. 3. Encryption Using AES 256 Algorithm

The session key management module is implemented with the help of J2ME mobile application environment. The user will login using username and password. The username and passwords are matched in database the random virtual key is automatically generated for each user. The random virtual key is entering into the mobile application and click to calculate button to create the session key for the user session is shown in the Fig. 4.

Fig. 4. Session Key Generator

The cloud disk utilization is more important to improve the cloud server performance. The replication of file storage is wastage of disk space. The disk space wastage is to minimize by using the file key technique. At the time of file upload the data owner using file key to store the file in the data base. The same file key and same file name are repeated in the time of uploading the server generate the error message and stop the process. The user status is recorded in log file. The log files are maintained by the Third Party Auditor. The log admin to maintain the log is very important to avoid malicious activity in the cloud storage. The un-authorized user try to enter and access the original file the log report is send to the data owner. The file size, file name and user name is status is periodically monitor in cloud log server is shown in Fig. 5.

Fig. 5. Cloud Log Management

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

The major security loop holes are identified in the proposed system and try to reduce the security risks in the cloud data storage. The proposed cloud security system is adopting both private and public cloud environment.

VII. CONCLUSIONS AND FUTURE WORK

The multilevel security for cloud data storage approach is to design to overcome recent security issues in the hybrid level cloud domain. The AES 256 algorithm is to reduce the data hacker attacks and improve the system security in the cloud. The session random key generation approach is to prevent the malicious user activity in the cloud domain. The log management system is to monitor the user activity in the cloud server.

The research work is extending to focus on data security in the local level. The proposed model the user will login using user credentials and upload the file to the cloud. The file is successfully uploaded in the cloud storage after only the encryption is performed to implement the security in the cloud. The forthcoming work the data owner will encrypt the file using cryptography algorithm and store the virtual drive in the local system to upload the content to the cloud server. The prospective model the data owner encrypted file will be uploading to the cloud storage to enable high level data security in the cloud network.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, Accessed April 2010.
[2] F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54, 2012.
[3] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of con-temporary research in business, Vol.3, No 9, p. 1323-1329, 2012.
[4] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.
[5] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.
[6] S. Subashini and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul.,2010.
[7] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld,Available: http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1 [Mar. 13, 2009].
[8] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730.
[9] C. Wang, Q. Wang, K. Ren, and W. Lou (2010), 'Privacy-Preserving Public Auditing for Storage Security in Cloud Computing', Proc.IEEE INFOCOM '10.
[10] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009), 'Above the Clouds: A Berkeley View of Cloud Computing', Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley.
[11] Cloud Security Alliance (2010), 'Top Threats to Cloud Computing', http://www.cloudsecurityalliance.org.
[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li(2011), 'Enabling Public Auditability and Data Dynamics for Storage Security in Cloud mputing', IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859.
[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song(2007), 'Provable Data Possession at Untrusted Stores',Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609.
[14] 14. M.A. Shah, R. Swaminathan, and M. Baker (2008), 'Privacy-Preserving Audit and Extraction of Digital Contents', Cryptology ePrint Archive, Report 2008/186.
[15] A. Juels and J. Burton, S. Kaliski (2007), 'PORs: Proofs of Retrievability for Large Files', Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597.
[16] Cloud Security Alliance(2009), 'Security Guidance for Critical Areas of Focus in Cloud Computing', http://www.cloudsecurityalliance.org.
[17] H. Shacham and B. Waters(2008), 'Compact Proofs of Retrievability', Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107.
[18] C. Wang, K. Ren, W. Lou, and J. Li(2010), 'Towards Publicly Auditable Secure Cloud Data Storage Services', IEEE Network Magazine, vol. 24, no. 4, pp. 19-24.
[19] R. Curtmola, O. Khan, and R. Burns(2008), 'Robust Remote Data Checking', Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS '08), pp. 63-68.
[20] G. Ateniese, S. Kamara, and J. Katz(2009), 'Proofs of Storage from Homomorphic Identification Protocols', Proc. 15th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT), pp. 319-333.
[21] D. Boneh, B. Lynn, and H. Shacham (2004), 'Short Signatures from the Weil Pairing', J. Cryptology, vol. 17, no. 4, pp. 297-319.
[22] A.L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen (2009) , 'Practical Short Signature BatchVerification',Proc. CryptographersTrack at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA), pp. 309-324.
[23] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik (2008), 'Scalable and Efficient Provable Data Possession', Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10.
[24] C. Wang, Q. Wang, K. Ren, and W. Lou (2012), 'Towards Secure and Dependable Storage Services in Cloud Computing', IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

[25] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia (2009), 'Dynamic Provable Data Possession', Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222.
[26] R.C. Merkle (1980), 'Protocols for Public Key Cryptosystems', Proc. IEEE Symp. Security and Privacy.
[27] T. Schwarz and E.L. Miller (2006), 'Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage', Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06).
[28] R. Curtmola, O. Khan, R. Burns, and G. Ateniese (2008), 'MR-PDP: Multiple-Replica Provable Data Possession', Proc. IEEE Int'l Conf.Distributed Computing Systems (ICDCS '08), pp. 411-420.
[29] Cong Wang, Kui Ren(2013), 'Privacy-Preserving Public Auditing for Secure Cloud Storage', IEEE Transactions On Computers, VOL. 62, NO. 2, pp 362-375.
[30] Chander Kant, yogesh Sharma (2013), 'Enhanced Security Architecture for Cloud Data Security', International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3,Issue 5, May 2013.
[31] Mary Michael, J.Mary Metilda (2014), 'Delegating Log Management to the Cloud Using Secure Logging', International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 788-793.