Meta Data Integrity Verification With Face Recognition Authentication Technique In Cloud Computing

Dr. P. Senthil Kumari, Dr. A.R.Nadira Banu Kamal

Abstract: Cloud computing makes data available to the end user in a 24 x 7 x 365 access time, anywhere and anything. Tsunami of Internet of Things (IoT) connections and data relies more on the Cloud servers where data storage and access takes place. Cloud computing technology has multiple internal and external cloud servers together to provide high interoperability capabilities associated with a single or multiple Cloud Service Provider (CSP). The most attractive cloud service is Data Outsourcing. Any type of data file (text, word, audio, video, image, excel and portable document format files) will be encrypted first using hybrid algorithm ECC-AES (Elliptic curve Cryptography – Advanced Encryption Standard). Then file is outsourced to the cloud. Any authenticated user whose face is recognized for authentication can download the file and decrypt the cipher file. Receiver should decrypt the encrypted file using the same hybrid algorithm ECC-AES. Integrity of the outsourced file is checked using meta data integrity verification technique of parent directory path ID. This paper discusses about three different entities: sender, receiver and attacker with three different ports whose keys are checked for processing. Cyber storms come from clouds, so that security for IoT devices is not enough. Plain text attack, Cipher text attack, Chosen cipher text attack, Chosen plain text attack, brute force attack and dictionary attack are prevented in this paper.

Index Terms : Cloud Computing, Integrity, Meta data, ECC and AES encryption algorithms.

1. INTRODUCTION

CLOUD computing is a pay-per-use business model (gas, water, electricity and landline phone). Computational resources and services can be used, retrieved and implemented using the concept of utility computing [1]. There are a lot of cloud computing solutions from IT giants such as Google, Amazon, Microsoft and IBM. Cloud storage is an emerging solution that puts users' to store resources on the cloud [2]. Data centers are the cloud servers where all necessary data and software are stored at a remote location. Data center environment allows business enterprises to run applications faster, with easier manageability and less maintenance effort [3]. The movement of data to centralized services could affect the privacy and security of users' interactions with the files stored in the cloud storage space.

Integrity monitoring is needed to avoid threats from hackers for any outsourced encrypted cloud data. Data integrity is the accuracy and consistency of stored cloud data. Many integrity methods are developed to help the cloud users [4]. To overcome data integrity problems, many Proof of Retrievability (PoR) techniques, Provable Data Possession (PDP) techniques and cryptographic hash functions are practically used. Public key based (Digital Signature Algorithm) authentication using SHA-256 digest, Multi Authority Attribute Based Encryption and Hash based Message Authentication code with MD5 are used for integrity verification in various papers. In this paper, meta data integrity is verified with face recognition authentication technique.A major usage of metadata is to find relevant information for users and identify resources. Various national governmental organizations collect metadata of telecommunication activities including internet bandwidth traffic. Government organizations store metadata relating to electronic mails, telephone calls, web pages and IP connections regularly in several countries. Two types of attacks are available in cloud computing: passive attacks and active attacks. In the case of passive attack, attacker does not harm the system. The attacker tries to get the information from the sender/receiver from their communication message. Passive attacks can be prevented by encrypting the data. Active attacks harm the system by changing the data integrity and availability. Active attacks are easily detected by CSP, but not prevented from hackers. ECC is an asymmetric encryption algorithm which needs two keys for encryption and decryption. ECC 160-bit algorithm provides same level of security for encrypted cloud data as RSA (Rivest-Shamir-Adleman) 1024-bit algorithm performs. AES is a symmetric encryption algorithm which provides better processing time, minimal storage requirements and a single secret key for encryption and decryption. When comparing the performance evaluation, if AES 128-bit is compared with AES 192-bit key, the power and time consumption increase by 8%. In the proposed work, AES 128-bit is used. ECC and AES are discrete logarithm protocols which have the capacity to provide the required non-linearity for the self contained safety communication between paired hardware devices. The rest of the paper is structured as follows: Section II includes the existing works related to various integrity verification techniques, the proof of retrievability techniques, provable data possession techniques, etc and various authentication techniques used for the cloud computing applications. Section III describes the detailed implementation of the metadata integrity verification technique. Section IV presents the results and discussion of the proposed method and section V gives the conclusion and future work of this paper.

- *Senthil Kumari. P, Assistant Professor, Department of Computer Science, Thassim Beevi Abdul Kader College for Women, Kilkarai. E-mail: senthilmathimca@gmail.com*
- *Nadira Banu Kamal. A, R,, Principal, Mohamed Sathak Hamid College of Arts and Science for Women, Ramanathapuram. E-mail: nadirakamal@gmail.com*

2 RELATED WORKS

IoT applications spread from industrial automation to home purpose cloud computing and health-care. Smart homes will rely upon IoT devices to monitor the house temperature, baby sitters, gas leakages, harmful intrusions and several other parameters relating to the house and its inhabitants. In healthcare applications, IoT devices are used to perform

continuous biological monitoring (ECG (Electro Cardio Gram) and BP (Blood Pressure)), drug administration, elderly monitoring conditions and habits for an improved lifestyle [1]. A theoretical framework was proposed by Bowers. K. D et al. for the design of PORs [5]. Proof of Retrievability scheme divided a file into set of blocks and then encoded with error correcting codes. Check blocks called sentinels are embedded for each block. Any person who wants to verify the integrity specifies the positions of sentinels. A new variant on the Juels-Kaliski protocol was proposed by them and described a prototype implementation [6]. Static archival of large files was focused. This scheme made use of spot checking and error correcting codes. Merkle Hash Tree (MHT) and AES algorithm are used to maintain data integrity at the not trust worthy server in the research proposal of Poonam M. Pardeshi et al. [7]. Third Party Auditor (TPA) acted on behalf of client for data integrity checking and sent an alert to notify the status of the stored data. Assurance of recovery of data, in case of data loss or corruption, by providing a recovery system was proposed. A survey of techniques and tools used for cloud data integrity verification was presented by Princelly Jesu et al. [8]. Selection of the integrity methods may depend on the type of data and its size. The survey summarized the drawbacks of all the methods with different considerations. Distributed Denial of Service (DDoS) attack is the result of multiple compromised systems flooding the targeted system with more traffic. Novel varieties of DDoS attacks were discussed by Qiao Yan et al. and gave a survey of preventive methods for DDoS attacks using Software Defined Networking (SDN) [9]. Implementation details of SDN to prevent DDoS attacks were presented. An application based on Hadoop and MapReduce framework was proposed by Rajat Saxena et al. [10]. Paillier Homomorphic Cryptography (PHC) system used homo-morphic encryption on data blocks. Homo-morphic encryption allows certain types of computations to be carried out on ciphertext and produces an encrypted result which decrypted matches the result of operations performed on plaintext. A survey on information integrity techniques was presented by Rohini G. Khalkar et al. [11]. In Proof of Retrievability (PoR) technique, data recovery is possible. In Provable Data Possession (PDP), data need not to be downloaded for verification. Novel resource allocation strategy to prevent DDoS attacks for every cloud customer was proposed by Shui Yu et al. dynamically [12]. Intrusion prevention servers filtered out attack packets and the quality of the cloud service for users was guaranteed to prevent DDoS attack. A mathematical model to meet the needs of the resource investments based on queuing theory was established. Various problems for encrypted cloud data storage and solutions were presented by Sultan Aldossary et al. [13]. A major issue was sharing data in the cloud when the CSP was mistrusted. Some techniques that protected the data stored in CSP were mentioned. More secure cloud storage will lead to more acceptances from the people and the trust on the cloud will increase. A novel integrity auditing scheme for cloud data sharing services characterized by multi user modification, public auditing, efficient user revocation as well as practical computational / communication auditing performance was proposed by Vedire Ajayani et al. [14]. User impersonation attack can be resisted by their scheme which was not considered in the existing techniques that supported multi user modification. Any person who is not authorized can verify the data integrity. This proposal was presented by Yuan Zhang et al. which prevented against opponents and harmful intention having auditors [15]. A method to hide the sensitive data was developed to protect against intruders and prevented cloud malware threat. Digital money block chain transactions produce messages to avoid secret cooperation between untrusted Third Party Auditors (TPA) and CSPs. An efficient distributed metadata management scheme in Cloud Computing was proposed by Yiixue Wang et al. [16]. Metadata services can be enhanced by various techniques: parent directory based path ID distribution method, imitating hierarchical based directory, mutual assistance of two layers cache method, close familiarity algorithm and the application of database server to metadata backend tool. Rajkumar Chalse et al. presented a detailed analysis of the cloud security problem [17]. Also the different problems in a cloud computing system and their effect upon the different cloud users were analyzed. It provided a comparably scalable, position independent and low cost platform for client's data. Mohammed Faez et al. proposed a model for integrity verification by using TPA. A safety method guaranteed availability and consistency of encrypted cloud data stored in CSPs [18]. Subashini. S et al. proposed a new methodology which might not completely help in restricting a hacker to access the data. New method will make the data invaluable, if it was extracted by a hacker intentionally but at the same time ensured the quality of the data that was provided to its respective owner [19]. A metadata based data segregation and storage methodology was proposed and also solutions to access this segregated data were found. This method proved that data was invaluable during static residence and gets valuable value only during data acquisition or updation. Anitha. R et al. devised a new research method for encrypted cloud data using metadata. The metadata created based on DCMI (Dublin Core Metadata Initiative) standards gave a new way for safety transactions in CSP [20]. Security was ensured by cipher key generated from the attributes of metadata by providing two novel features: a). Data owner has full rights over encryption and decryption keys b). High level complications of the key are generated by using feistel structure in a different way. A new research proposal to retrieve encrypted cloud data from cloud servers is proposed by Anitha. R et al. using metadata technology [21]. Retrieval of query from the cloud user is performed efficiently. Latency of data retrieval is reduced in the proposed method. Bloom filter is the data structure used for data retrieval. Charmee et al. presented a survey on various integrity verification techniques [22]. Message Digest (MD5) cryptographic hash function reads the file and compresses. Compressed content is input to MD5 function which generates the message digest. Encrypted message digest is appended with the original file content within predefined tag. Kaiping Xue et al. proposed a solution for safety of encrypted cloud storage from EDoS (Economic Denial of Sustainability) attacks and provided resource consumption accountability [23]. The scheme used CP-ABE (Ciphertext Policy Attribute Based Encryption) and met specific standards with arbitrary access policy of CP-ABE. ECC and AES algorithms when combined as a hybrid algorithm provide advantages in key length, processing requirements, storage space and high level of security. Nishaal J et al. presented a comparative evaluation of encryption algorithms for router communication [24].

3 META DATA INTEGRITY VERIFICATION TECHNIQUE AND FACE RECOGNITION AUTHENTICATION TECHNIQUE

Meta data integrity verification technique is implemented in Java using JDK 1.8, Front end tool – Visual C#, IDE – Net beans 8.0, Windows 7 ultimate (X86) (32 bit) Operating System and back end tool - Wamp server 2.0. Cloud computing environment has three entities: Data owner (Sender), Data user (Receiver) and Cloud server. Hacker (Attacker) wants to intrude and get the original message from the sender to receiver. Integrity techniques are used to avoid hacking of the data. In order to prevent the original data from being attacked by the intruder, data owner saves the metadata of the plain file and uploads into the cloud server. Sender encrypts the file which he wants to outsource using ECC-AES hybrid encryption algorithm and uploads into the cloud server. The original file to be outsourced is encrypted using AES but the secret key used for encryption is generated using ECC algorithm. Sender sends the key to the authenticated user. Authenticated user who wants to download the encrypted file sends a request to the CSP. CSP verifies the authentication of the user. Face of the user is captured using camera. It is stored as JPG (Joint Photographic Experts Group) file. Cloud server will have a database of photographs for the authenticated users. If the current photo taken for the user is matched with any one of the photos in the database, then the user is an authenticated person. User is allowed to download the outsourced encrypted file. Receiver has to decrypt the file using the same ECC-AES hybrid encryption algorithm and the same key used by the file owner. Now, authenticated user gets the plain file which is uploaded by the data owner. User generates the metadata of the plain file. If the newly generated metadata is matched with the metadata which is uploaded by the file owner, then metadata integrity is verified. Sender, receiver and attacker will have three different IP addresses and ports. Keys also are verified by the CSP. Text files can be sent in two different modes: chat mode and File Transfer Protocol (FTP) mode. Small size of text files can be sent in chat mode. Large size of files with various extensions (text, word, audio, video, image, excel and portable document format files) can be sent in FTP mode. Text files which are sent in chat mode are intruded by the attackers. Plain text attack, Cipher text attack, Chosen cipher text attack, Chosen Plain text attack, brute force attack and dictionary attack are prevented by the CSP. Metadata integrity is verified for the files which are sent in FTP mode.

4 RESULTS AND DISCUSSION

Registration of authenticated user is performed. User's name is entered first. Any person's face who wants to get access to the cloud resources is captured first by clicking Face input. Then "Submit" button is enabled. New message box appears. Click "Ok". This process is shown in Figure 1. In the next window, click "Face recognition". If the captured photo is matched with the photo in the database, then a message such as "Matched. Welcome Client" appears in the run time window. This process is shown in Figure 2.

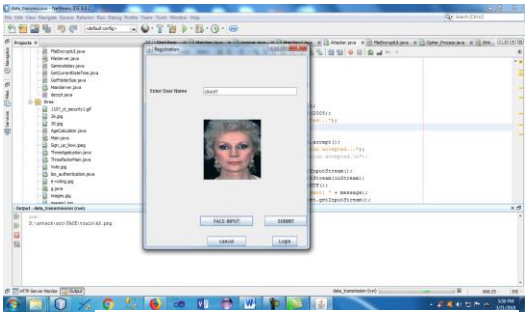

Figure 1. *Capturing of the user's face*

Captured user's face is compared with the faces in the CSP's database. If a match occurs, user is authenticated to access the resources. This procedure is shown in Figure 2.

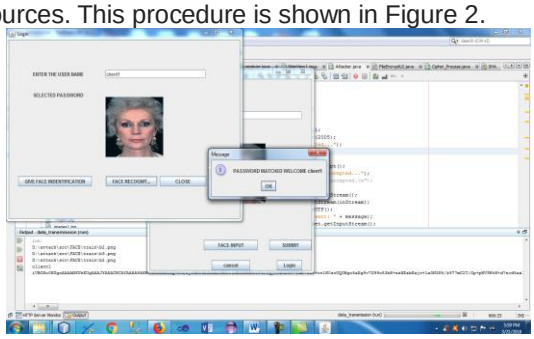

Figure 2. *Notification of the authenticated Client*

Different windows are used for sender, receiver and attacker with separate ID, IP addresses, port numbers and keys. Attacker tries to intrude in the communication between sender and receiver by giving chat message "hi". This step is shown in figure 3. Various types of attacks are detected by CSP. Detection of Plain text attack is shown in figure 4. Detection of Chosen Ciphertext Attack is shown in figure 5. Sender will stop sending further messages once he is notified the detection of any type of attacks. Separate drop down list boxes are used for various fie types (text, word, audio, video, image, excel and portable document format files), algorithms to be used for encryption (AES, DES, ECC, ECC-AES and blow fish), operation modes of cipher (Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB) mode and Output Feed Back mode) and key sizes to be used (32 bit, 64 bit, 128 bit, 256 bit and 512 bit) which is shown in figure 6.

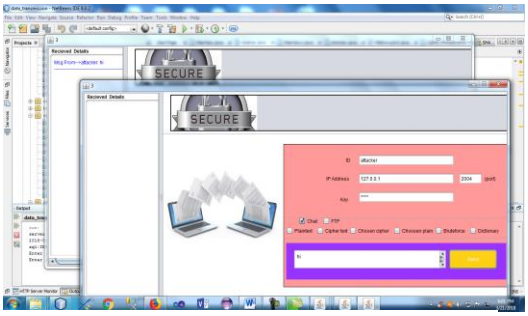

Figure 3*. Attacker's window with IP address*

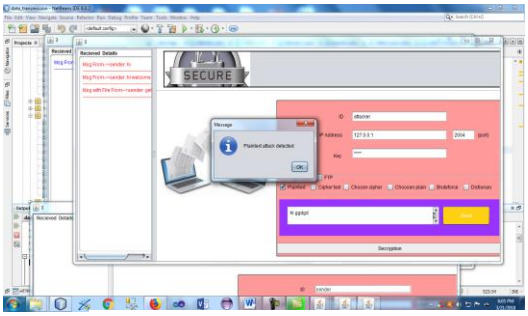

***Figure 4**. Detection of Plain text Attack*

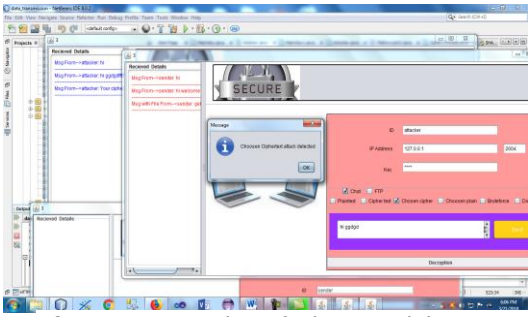

***Figure 5**. Detection of Chosen Ciphertext Attack*

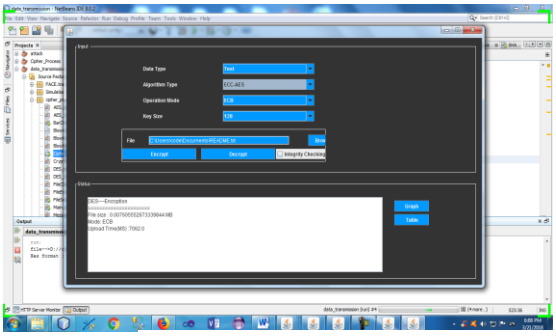

***Figure 6.** Various File Type, Algorithm, Operation mode, key size chosen for the file to be uploaded*

Data verification time is the time taken for checking different types of data for accuracy and inconsistency. Data owner upload time and verification time of ECC-AES encrypted cloud data files are compared with AES and DES algorithms which is depicted in Table 1.

TABLE 1

UPLOAD AND VERIFICATION TIME

No.	Algorithms	Upload Time (ms)	Verification Time (ms)
1.	DES	7062	5886
2.	AES	2578	6918
3.	ECC-AES	67	17

Upload time comprison chart indicates that ECC-AES hybrid algorithm consumes less time when compared with DES and AES which is shown in figure 7.

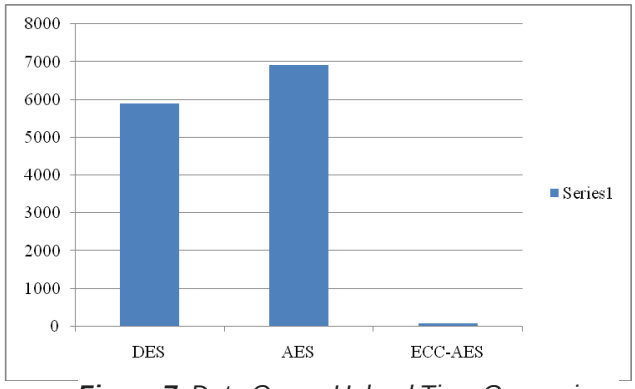

***Figure 7.** Data Owner Upload Time Comparison*

Verification of transparency time comparison chart indicates that ECC-AES hybrid algorithm consumes less time when compared with DES and AES which is shown in figure 8.

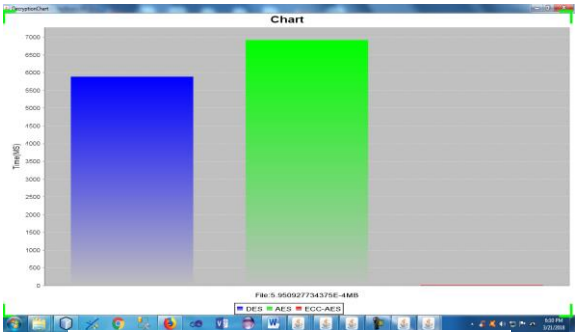

***Figure 8.** Verification Time Comparison*

Data owner upload time is compared with ABE-POP (Attribute Based Encryption – Partially Outsourced Protocol) and ABE-FOP (ABE – Fully Outsourced Protocol) of Kaiping Xue et al. [23] and verified that the proposed work gives lesser data owner upload time and verification of transparency time. Partially Outsourced Protocol specified an expected maximal download times, and data owners remain offline unless it wants to increase the value. Fully Outsourced Protocol in which the data owner cannot set an expectation of download time. Data owner would be offline for a long time, in this case, the data owner can delegate to the cloud.

5 CONCLUSION AND FUTURE WORK

In this paper, metadata integrity verification is proposed with face recognition authentication technique. This method has the advantage of faster encryption time since this method uses hybrid of encryption algorithms (ECC and AES). However, the major disadvantage of this method is that it requires 32 bit OS for processing. Hence, the future work shall be extended to remove the drawback.

REFERENCES

[1] Michele De Donno, Alberto Giaretta, Nicola Dragoni and Antonio Bucchiarone and Manuel Mazzara, “Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era”, Future Internet 2019, 11, 127, 30 pages, doi: 10.3390/ fi11060127, www.mdpi.com/ journal/ futureinternet

[2] Yun Xue Yan, Lei Wu, Wen Yu Xu, HaoWang and ZhaoMan Liu, “Integrity Audit of Shared Cloud Data with Identity Tracking”, Hindawi, Security and Communication

Networks,Volume 2019, Article ID 1354346, 11 pages, https://doi.org/10.1155/2019/1354346

[3] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.

[4] Neha Thakur and Aman Kumar Sharma, "Data Integrity Techniques in Cloud Computing: An Analysis", International Journals of Advanced Research in Computer Science and Software Engineering, Volume-7, Issue-8, DOI: 10.23956/ ijarcsse/V7I8/0141, August 2018, pp. 121-125.

[5] Bowers K. D., A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation", in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, (New York, NY, USA), ACM, 2009, pp. 43–54.

[6] Juels. A and B. S. Kaliski, Jr., "PORs: proofs of retrievability for large files," in CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, (New York, NY, USA), ACM, 2007, pp. 584–597.

[7] Poonam M. Pardeshi and Deepali R. Borade, "Improving Data Integrity for Data Storage Security in Cloud Computing", IJCSNS International Journal of Computer Science and Network Security, Vol. 15(6), June 2015, pp.75-82.

[8] Princelly Jesu. A and Ramesh Kumar. S, "A Survey of Techniques and Tools Used for Cloud Data Integrity Verification", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4(2), Feb 2016, pp.1923-1928.

[9] Qiao Yan, F. Richard Yu, Qingxiang Gong and Jianqiang Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE Communications Surveys & Tutorials, Vol. 18(1), First Quarter 2016, pp. 602-622.

[10] Rajat Saxena and Somnath Dey, "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing", Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), Procedia Computer Science 89 (2016), pp. 142 – 151.

[11] Rohini G. Khalkar Ms. and Prof. Dr. S.H.Patil, " Data Integrity Proof Techniques in Cloud Storage", International Journal of Computer Engineering & Technology (IJCET), Vol. 4(2), March – April (2013), pp. 454-458.

[12] Shui Yu, Yonghong Tian, Song Guo and Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE Transactions on Parallel and Distributed Systems, Vol. 25(9), Sept - 2014, pp. 2245 - 2254.

[13] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7(4), 2016, pp. 485-498.

[14] Vedire Ajayani, K. Tulasi and Dr P. Sunitha, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", International Journal of Advanced Technology and Innovative Research, Vol. 8(16), Oct-2016, pp. 3146-3152.

[15] Yuan Zhang, Chunxiang Xu, Hongwei Li and Xiaohui Liang, "Cryptographic Public Verification of Data Integrity for Cloud Storage Systems", IEEE Cloud Computing published by the IEEE computer society, September / October 2016, pp.44-52.

[16] Yiixue Wang and Hai Tao Lv, "Efficient Metadata management in Cloud Computing", in the Proceedings of IEEE 3rd International Conference on Communication Software and Networks, 27 – 29 May 2011, DOI: 10.1109/ ICCSN. 2011.6014777

[17] Rajkumar Chalse, Ashwin Selokar and Arun Katara, "A New Technique of data integrity for analysis of the Cloud Computing Security", in the proceedings of 5th International Conference and Computational Intelligence and Communication Networks, 27-29 September 2013, DOI: 10.1109/CICN.2013.103

[18] Mohammed Faez Al - Jaberi and Anazida Zainal, "Data Integrity and privacy model in cloud computing", in the proceedings of International Symposium on Biometrics and Security Technologies (ISBAST), 26-27 August 2014, DOI: 10.1109/ISBAST.2014.7013135

[19] Subshini. S and Kavitha. V, "A Metadata Based Storage Model for Securing Data in Cloud Environment", in the proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 10-12 October 2011, DOI: 10.1109/ CyberC.2011.76

[20] Anitha. R and Saswati Mukherjee, "Data Security in Cloud for Health Care Applications", Advances in Computer Science and Its Applications, Lecture Notes in Electrical Engineering 279, DOI: 10.1007/978-3-642-41674-3 167, Springer-Verlag Berlin Heidelberg 2014, pp. 1201-1209.

[21] Anitha. R and Saswati Mukherjee, "'MaaS': Fast retrieval of data in cloud using metadata as a service", Arabian Journal for Science and Engineering, August 2015, Vol. 40, Issue 8, pp. 2323–2343.

[22] Charmee V. Desai and Gordhan B. Jethva, "Survey on Data Integrity checking Techniques in Cloud Storage", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 12, Dec 2014, pp. 292-295.

[23] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong and Peilin Hong, "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage", IEEE Transactions on Information Forensics and Security, February 2018, pp. (99):1-1.

[24] Nishaal J. Parmar and Pramode K. Verma, "A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchange System", Security and Communication Networks, Volume 2017, Article ID 1467614, January 2017, 7 pages, https://doi.org/10.1155/2017/1467614.