Data storage lock algorithm with cryptographic techniques

Anitha K. L.[1], T.R. Gopalakrishnan Nair[2]
[1]Bharathiar University, India
[1,2]Networks and Security Research Group, Advanced Research Centre, Rajarajeswari Group of Institutions, India

Article Info

Article history:

Received Nov 26, 2018
Revised Mar 27, 2019
Accepted Apr 10, 2019

Keywords:

Cloud service provider
Cryptography
Data storage
Decryption
Encryption

ABSTRACT

The cloud computing had its impact far and wide, and Enterprise solutions are getting migrated to different types of clouds. The services are delivered from the data centers which are located all over the world. As the data is roaming with less control in any data centers, data security issues in cloud are very challenging. Therefore we need multi-level authentication, data integrity, privacy and above all encryption to safeguard our data which is stored on to the cloud. The data and applications cannot be relocated to a virtual server without much degree of security concern as there can be much confidential data or mission-critical applications. In this paper, we propose Data Storage Lock Algorithm (DSLA) to store confidential data thereby provides secure data storage in cloud computing based on cryptographic standards.

Corresponding Author:

Anitha K. L.,
Research Scholar, Bharathiar University,
Coimbatore, India.
Email: anithakl07@gmail.com

1. INTRODUCTION

A cloud is a collection of resources which are virtualized that hosts a variety of different workloads and can be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machine. It supports self-recovering, redundant and significantly scalable programming methods that allow workloads to recover from many necessary hardware or software failures and monitor resource use in real time to enable rebalancing of allocations when needed [1]. The popular algorithms include the Data Encryption Standard (DES) [2], and the Advanced Encryption Standard (AES) [3]. The AES algorithm was published by the National Institute of Standards and Technology (NIST) in 2001. AES is a symmetric block cipher which is proposed to replace DES as the approved standard for an extensive collection of applications. Whitfield Diffie and Martin Hellman introduced an algorithm called the Diffie-Hellman algorithm (DH) in 1976 [4], accomplished drastic changes in cryptography, presenting the first asymmetric cryptographic algorithm. Rivest, Shamir and Adelman defined their well-known Rivest-Shamir-Adleman (RSA) algorithm [5] in 1978. The RSA algorithm has since that time reign absolute as the most extensively accepted and implemented a general-purpose approach to public-key encryption. In 1985, Victor Miller (IBM) and Neil Koblitz (University of Washington) discovered Elliptic Curve Cryptography (ECC) which can be used, as an alternative mechanism to implement public key cryptography [6]. ECC algorithms rely on the algebraic structure of elliptic curves over finite fields. Nowadays cloud service provider offers server side security to retain control for the customer's data. We can't make sure that the user's data are vulnerable to attacks or a data breach. Therefore to ensure security and privacy in cloud there is a need for a client side encryption mechanism to safeguard our data. Thus the user data will stay protected whoever be the entity that controls the entire computing environment. Thus the user data in the cloud remains in encrypted form until the user decrypts it in client side. This mode of encryptions is required to safeguard our data from hacking, malicious attacks and vulnerabilities. Now we are proposing an algorithm by which, extra layer of security can be given to potentially vulnerable data using the client controlled approaches. This will enable in realizing storage lock system with cryptography in realizing the data in user protected foliage.

In this paper, Section 2, we introduce the discussion of related work. Section 3 describes data storage and in section 4, the detailed description of the proposed algorithm for secure data storage in the cloud has been discussed. Result and Analysis showed in section 5. Finally, section 6 describes the conclusion.

2. RELATED WORKS

Recent technological advances relieve an explosive growth in the usage of the remote storage system, namely the cloud-based storage services. The outsourced data brings several cloud-specific security issues like confidentiality, integrity and privacy of the data. Therefore, the data security remains a dominating hurdle to the development and widespread use of cloud storage. The users outsource their data on remote servers, which are controlled and managed by Cloud Service Providers (CSPs). However to provide data intended to be kept secret in multi-tenant environments becomes very challenging. Encrypting data at the client side is a good alternative to mitigate such approaches of data confidentiality [7, 8]. The user is preserving the decrypting keys out of reach of the cloud provider. However, this method gives rise to several key management concerns, such as storing and maintaining the keys' availability at the client side. The aspects like ease of use, ease of deployment, flexibility, robustness and performance need to consider for defining the solutions for integrity and confidentiality of outsourced data. Authors [9] proposed a cryptographic scheme for cloud storage, based on original usage of ID-Based Cryptography (IBC) to ensure the confidentiality of data. In this plan, every client acts as a Private Key Generator (PKG) for encrypting the data to store in the cloud by computing an ID-based pair of keys which allows data access to be managed by the data owner. The flexible sharing approach provided by using a per data ID-based key. Based on a content hash keying method, a client side de-duplication scheme for cloud applications has been proposed to improve the computation complexity at the customer side [10].

CloudaSec [11] uses a public key based solution for improving the confidentiality of data in cloud storage environments and enhancing dynamic sharing among users. To ensure the confidentiality of data, the data owner uploads the encrypted data to the cloud and integrates the deciphering key encrypted into the metadata. Moreover, CloudaSec incorporates a conference key distribution scheme, based on parallel Diffie-Hellman exchanges, to guarantee backwards and forward secrecy. Hence, only authorized users can access metadata and decipher the decrypting data keys. Authors investigated the various security frameworks for the mobile cloud computing environment. Due to the resource limitation of mobile devices, most of the security frameworks offload processor intensive jobs on the cloud [12]. To accomplish a secure mobile cloud computing environment, service providers have to address the security threats about the network security, data security, data confidentiality, and data breach issues and so on. Moreover, new security risk arises due to lack of complete isolation among virtual machine instances running on the same physical server. Based on Attribute-based signature (ABS) scheme, authors proposed a new provenance system with fine-grained access control [13]. The user's anonymity is guaranteed by, incorporating ABS and group signature approaches. The user access is moved to the cloud server with broadcast encryption thereby the computation and communication overhead for the data owner is reduced. The security vulnerabilities like Identity Management Systems (IDM) server compromise, mobile device compromise, and traffic interception is identified in [14] and developed an architecture called consolidated IDM (CIDM) for separating the authorization credentials to prevent illegal access in case of IDM compromise or traffic interception. It adds a second layer of authentication using human-based challenge-response to guard against mobile device compromise. The experiments prove that compared to the current IDM systems, CIDM offers its clients with enhanced security guarantees and that it has less energy and communication overhead. The authors investigate an approach to ensure trust and provenance in the cloud-based services with the help of digital signatures using properties or the attributes derived from their construction and the software behaviour. As service execution proceeds, the keys are generated dynamically by the features obtained. A multidimensional key generation approach is introduced wherein it maps from multi-dimensional feature space directly to a key space. An entropy algorithm is developed to evaluate the entropy of the key space [15]. Authors proposed multi-factor biometric fingerprint authentication and protection gateway [16] in which the enterprises can protect their customer's sensitive data in a public cloud environment. The authentication credentials of the users will not be revealed to the cloud service provider and other malicious users thereby providing high security for the users and attains data privacy. To preserve the privacy of the key bit of information from indoor or outdoor malicious attackers, the authors implemented data anonymization and advanced tokenization approaches as vital part of protection gateway. In cloud computing environment, security needs an exact point of view and can be created by the trust, mitigating protection towards a trusted third party [17]. Here the authors proposed a solution by incorporating PKI (Public Key Infrastructure), SSO (Single-Sign-On) and LDAP (Lightweight Directory Access Protocol) to ensure authentication, availability, integrity and confidentiality of data and the communications. With this solution, essential trust is sustained, by a horizontal level of service which is available to all the implicated entities, which realizes a security mesh.

In the common environment of cloud computing there is a dire need for incorporating client controlled encryption capability to bringin assured data protection against the probable security gaps existing in any particular cloud system. Implementing a client controlled security strategy mainly leverages by taking control of the protection of the data client can deposit in remote machines. As we discussed earlier most successful data protection is possible through data encryption technology. As the cloud systems has caught strategic paths through which data has to run back and forth from central cloud area, it calls for specific encryption-decryption process to be generated for this purpose. We developed a Data Storage Lock Algorithm which addresses this issue and successfully resolves the security challenges.

3. DATA STORAGE

Cloud storage allows data owners to remotely store their data and access them via networks at any time and from anywhere. Despite the obvious benefits such as improved scalability and accessibility, outsourcing data to the cloud brings new security issues to the cloud data security. Once the data gets outsourced, the data owners abandon the control over the destiny of their data. The server may conceal data loss accidents to uphold the reputation or reject the information, which is not in use or not often accessed to keep storage space. Cloud as a new way to reduce the complexity and costs and face it much better in this economy. In the case of traditional computing, setup requires the user to be in the same place where the device, is located wherein the cloud allows you to store, access and modify your data from any location with your internet-enabled device. The information stored on a local computer can be kept on to the cloud and accessed from any computing devices. The user does not know where the data gets stored, how secure the data will be. Authors proposed smart cloud architecture called Smart Cloud Data Manager [18] which handles security issues in the cloud. Authentication, authorization, data splitting, encryption, data backup, data access control rights by verification needs to ensure for providing more security for the data. In [19], the authors proposed architecture for examining whether security metrics in a security SLA has met. Moreover, these structures need to be secured. Hence to ensure the safety of the data, end users who are accessing the cloud services have to analyze their data how sensitive it is and how much security it needs. Therefore it is necessary to use encryption standards to secure our very sensitive data before outsourcing to cloud.

Cloud computing is rapidly becoming a mainstay in today's digital world because of its greater flexibility, ease of access, and capacity compared to traditional storage and data sharing methods. Before putting data onto the public cloud, the cloud user should ensure the type of data or application (whether it is sensitive or not), security environment provided for data storage and the service-level agreement. Therefore, several safety measures have to be set up, to survive with the newly-visible cloud concerns, namely outsourcing encrypted data and periodically checking data integrity and availability. For example, storing encrypted data yields to be a cumbersome key management and access control, and regularly checking massive amounts of data tightens the bandwidth consumption. Some cryptographic techniques needed for ensuring security and privacy in clouds. We can use encryption techniques for protecting data in multitenant environments as we don't have full control.

4. PROPOSED MODEL (DATA STORAGE LOCK ALGORITHM)

Let us assume that there are n data centers; dc1, dc2,……,dcn and storage space as ss1, ss2,……,ssn. The user accessing the cloud service has to register the cloud with signature information. The data classifies into two: confidential data (cd) and non-confidential data (nd).

Initialization

- Data Center: dc
- Storage Space: ss
- Private Key: Pk.
- SecureKey: sKEY
- Input data: data.
- Confidential data: cd
- Cipher Text: C1, C2
- Cryptographic hash function: Hs ()
- Transport Layer Security: TLS

```
Steps
1. User: inputs signature info.
2. Key Generator: Pass=numeric (signature info)
−   Pk= Hs (pass, random ())
−   return (Pk) to user
−   store (Pk) to CSP.
3. User:  Login (Pk)
        if (authenticated)
              Billing for storage space
        else
              go to step 1.
4. CSP: store(Pk, dci, ssi)  where i=1,2,….,n.
5: User: if (data==cd){
            a) C1=EncryptAES (data, KAES)
           b) sKEY=EncryptRSA(KAES , RSApub)
         c) C2=HMAC(Message)+C1
}
else
c=encrypt (data) using TLS in server side.
6. Cloud Storage: Store encrypted data.
7. For downloading the data, the user has to be authenticated using the private key Pk.  If authentication is
successful, the user gets encrypted data.
8. The user can use sKEY and decryption algorithms to retrieve the original data.
        a) KAES = DecryptRSA(sKEY, RSApri)
        b) data = DecryptAES (C1, KAES)
```

Figure 1 shows the secure data storage and Figure 2 shows the consumer accessing cloud services to download data. The authors [20] proposed a workflow of the user accessing the cloud services for secure data storage by using the private key. Here we use our proposed "Data Storage Lock Algorithm" to provide security for the confidential data. In DSLA, the user has to input signature information. The key generator generates a private key by using the cryptographic hash function. The users as well as the Cloud Service Provider (CSP), get the private key of the user to provide more security. The CSP identifies the user by the private key. CSP maintains an index table consists of private key, datacenter id, storage space id. The user can log into the cloud by using the private key and can request for the storage space by pay-as-you-go model. The CSP verifies the private key and allocates the block of space required by the user. Non-confidential data should be encrypted, by using TLS. Many storage service providers use TLS. The confidential data needs to be encrypted, in client side before uploading to the cloud storage. Therefore we need to create a secure key (sKEY) for the confidential data encryption.

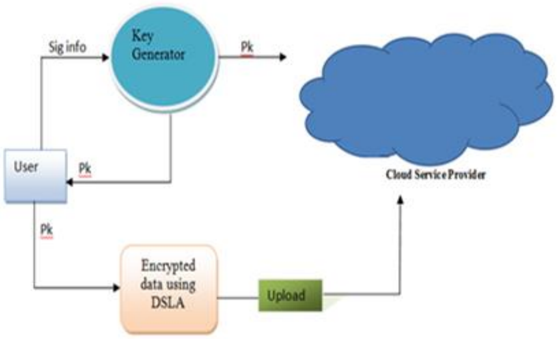


Figure 1. Secure data storage

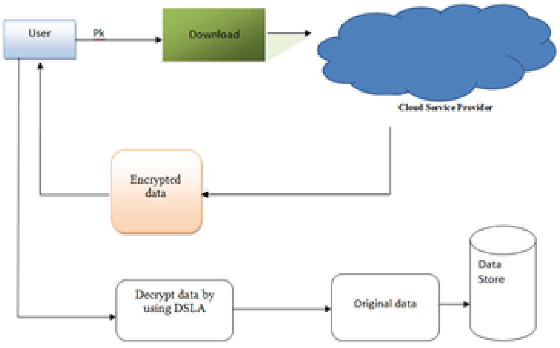


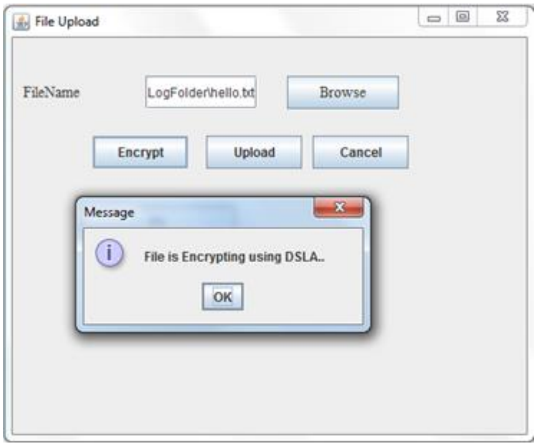
Figure 2. User accessing cloud services to download data

In DSLA, we integrate AES [3] algorithm and RSA algorithm [5] to provide more security for our data. In the first phase, we generate a key by encrypting AES key and RSA public key by using RSA algorithm. In the second phase, the data will be encrypted, by using AES algorithm. Then the encrypted message can be uploaded to the cloud storage. As we use encryption standard to encrypt the confidential data, the data should not be deleted, modified or fabricated during storage. Only authenticated users can access the data storage space thereby no data leakage during storage. The legitimate user can access the data at any time from any computing device. To provide integrity to the encrypted data, hash-based message authentication code (HMAC) [21] is used to attach a message along with encrypted data.

For downloading the data, the user has to login using the private key (Pk). The private key locks the storage space for a user. The CSP checks the index table for Pk. If found, the data center id (dci) and the storage space id (ssi), is identified. The user can download the data from the data center. Figure 5 and Figure 6 shows the time taken for encrypting and decrypting the data of various sizes using DSLA. DSLA provides an efficient locking system and encryption approach that does not produce significant overheads, as well as ensures data availability and retrieval. And also it prevents cloud providers accessing the users' original data.

5. RESULTS AND ANALYSIS

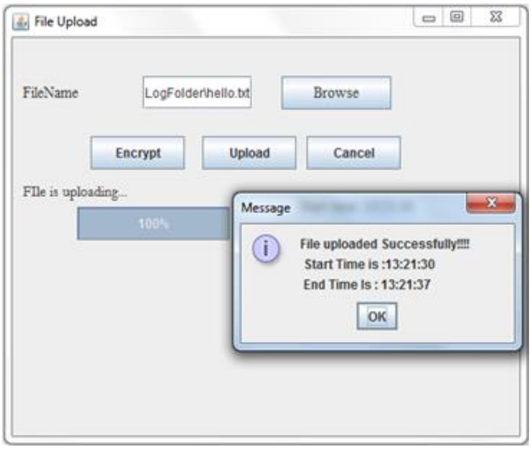
In every approach developing a simulation environment is very vital inorder to verify the proposed algorithms and its performance. To test this client controlled encryption scheme in cloud environment an experimental implementation and performance evaluation of Data Storage Lock Algorithm is arrived at using Eclipse IDE and java. Figure 3 and Figure 4 shows encrypting and uploading a file using DSLA algorithm.



FileName LogFolder\hello.txt

File is Encrypting using DSLA..

Figure 3. Encrypting file using DSLA algorithm



FileName LogFolder\hello.txt

FIle is uploading...

File uploaded Successfully!!!!
Start Time is :13:21:30
End Time Is : 13:21:37

Figure 4. Data uploaded using DSLA algorithm

Multilevel configuration of secure data management and Data Storage Lock Algorithm (DSLA) to store confidential data that provide higher degree of secure data storage in cloud computing. The complex paradigm of cloud performance and user engagements of various levels of inter-nodal transactions, mitigation of data leak is a vital challenge. To ensure improved security and confidential level on private data, encryption algorithms are engaged in a multi-level configuration between the user end and the cloud clusters. Confidential data can be stored and retrieved from cloud with sufficient security management, which is in high demand today for enterprise computing integration. The response is scalable with high-speed processors, and to estimate this response, sample runs were done, on lower level processors. Table 1 and Table 2 shows the encryption and decryption time for the file size in kilo bytes and mega bytes. Figure 5 and Figure 6 shows one of the response graphs for encryption and decryption. The initial load given is 10 kilobyte, and it systematically improved to 5 megabytes. The response indicates that the time consumed for a higher amount of data on the dead weight data of 10 kilobytes is marginally small. It ensures that overloading the data into high-security storage and processing will not consume much time affecting the total performance of the job executed by the cloud processors.

It proves that very low level of overhead is added, by DSLA approach on confidential data. Here we applied a new method of deeper level security lock provisions on confidential data of business enterprises and high-security institutions such that they can govern the confidentiality of data storing and retrieval. To realize this approach we used combinations of standard approaches to security like AES and RSA algorithms.

Table 1. Encryption and decryption of data of file size in KB using DSLA

File Size (in kilo bytes)	Encryption (in ms)	Decryption (in ms)
10	295	15
50	295	15
100	296	16
150	296	16
200	296	16
250	296	16
300	296	16

Table 2. Encryption and decryption of data of file size in MB using DSLA

File Size (in mega bytes)	Encryption (in ms)	Decryption (in ms)
1	296	16
2	297	16
3	297	17
4	297	17
5	298	18

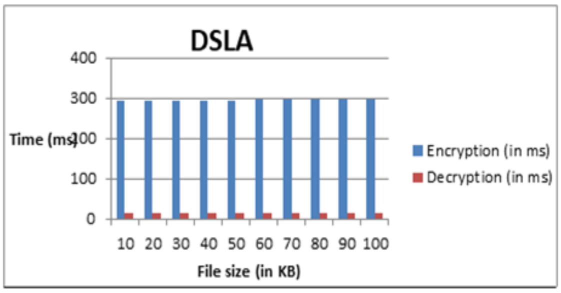


Figure 5. Encryption and decryption of data of file size (in kilo bytes)

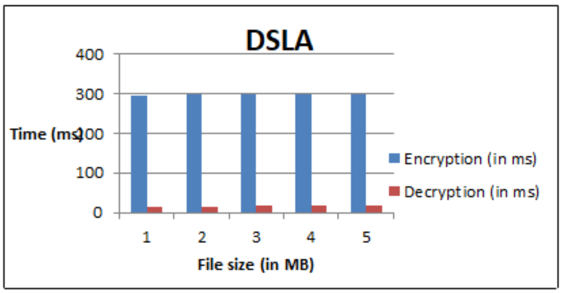


Figure 6. Encryption and decryption of data of file size (in megabytes)

6. CONCLUSION

In this paper, we presented issues in cloud computing such as security, service availability and authentication. The spotlight of the paper is the introduction of Data Storage Lock Algorithm (DSLA). This algorithm is used, for the safe storage of confidential data onto the cloud. Here we check the authenticity of a user who accesses the cloud storage by using the private key (Pk) which is stored onto the Cloud Service Provider. The private key is used, for locking the storage space allocated to a user in any data center. The user can download or access their data at any time by using the private key. The fast retrieval of data is possible by maintaining an index table in the Cloud Service Provider. It enables a scenario in which confidential data can be stored and retrieved from the cloud with sufficient security management with data encryption approaches.

REFERENCES

[1] G. Boss, P. Malladi, D. Quan, L. Legregni,H. Hall. *Cloud Computing*, 2007. www.ibm.com/ developerworks/ websphere/zones/hipods/

[2] National Bureau Of Standards NIST. Data encryption standard (des). Technology,46-3(46):1-26, 1999.

[3] N FIPS. 197: Announcing the advanced encryption standard (aes) Technology Laboratory, National Institute of Standards, 2009(12):8-12, 2001.

[4] W. Diffie and M. Hellman. New directions in cryptography, 1976.

[5] R. Rivest, A. Shamir, and L. Adleman. “A method for obtaining digital signatures and public-key cryptosystems. Commun,” *ACM*, 21(2):120-126, 1978.

[6] D. Hankerson, A. Menezes, and S. Vanstone. “Guide to Elliptic Curve Cryptography,” Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[7] S. Kamara and K. Lauter. “Cryptographic cloud storage,” In *Proceedings of the 14th International Conference on Financial Cryptography and data security*, FC'10, Berlin, Heidelberg, Springer-Verlag, 2010.

[8] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. “Controlling data in the cloud: outsourcing computation without outsourcing control,” In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 85-90. ACM, 2009.

[9] N. Kaaniche, A. Boudguiga, and M. Laurent. “ID based cryptography for cloud data storage,” In *IEEE Sixth International Conference on Cloud Computing, Santa Clara*, CA, USA, June 28-July 3, 2013, pages 375-382, 2013.

[10] N. Kaaniche and M. Laurent. “A secure client-side deduplication scheme in cloud storage environments,” In *6th International Conference on New Technologies, Mobility and Security, NTMS 2014*, Dubai, United Arab Emirates, March 30-April 2, 2014, pages 1-7, 2014.

[11] N. Kaaniche, M. Laurent, and M. El Barbori. “Cloudasec: A Novel Public-key Based Framework to Handle Data Sharing Security in Clouds,” In *Proceedings of the 11th International Conference on Security and Cryptography - Volume 1: SECRYPT, (ICETE 2014)* ISBN 978-989-758-045-1, pages 5-18, 2014.

[12] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani. “Towards secure mobile cloud computing: A survey,” *Future Generation Computer Systems*, Volume 29 Issue 5, Pages 1278-1299. Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands, July 2013.

[13] Jin Li , Xiaofeng Chen, Qiong Huang, Duncan S. Wong. “Digital provenance: Enabling secure data forensics in cloud computing,” *Future Generation Computer Systems*, Volume 37, Pages 259-266, July 2014.

[14] Issa Khalil, Abdallah Khreishah, Muhammad Azeem. “Consolidated Identity Management System for secure mobile cloud computing,” *Computer Networks,* Volume 65, Pages 99-110, June 2014.

[15] Bin Ye, Gareth Howells, Mustafa Haciosman and Frank Wang. “Multi-dimensional key generation of ICMetrics for cloud computing,” *Journal of Cloud Computing Advances, Systems and Applications*, vol. 4, no. 19, 2015.

[16] Nagaraju, S. & Parthiban,“Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway,” *L. J Cloud Comp,* vol. 4, no. 22, 2015.

[17] Dimitrios Zissis, Dimitrios Lekkas. Addressing cloud computing security”, *Future Generation Computer Systems* Volume 28, Issue 3, Pages 583-592., March 2012.

[18] Anitha K L, T.R. Gopalakrishnan Nair. “A Smart Cloud Architecture to handle Security Issues and Vulnerabilities in Cloud,” *IEEE sponsored International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, Publisher: IEEE, Volume 3, pages 1-6. DOI: 10.1109/INVENTIVE.2016.7830166, 2016.

[19] SA de Chaves, C. B. Westphall, and F. R. Lamin. “SLA Perspective in Security Management for Cloud Computing,” *6th International Conference on Networking and Services (ICNS), IEEE*, pages 212-217, 2010.

[20] Anitha K L, T.R. Gopalakrishnan Nair, “Secure Cloud Data Storage with Cryptographic Intervention for premier enterprise data”, *Global Journal of Engineering Science and Researches, ICRTCET-2018*, ISSN: 2348 – 8034, Pg.No: 714 – 720, March 2019.

[21] Arasu, S. Ezhil, B. Gowri, and S. Ananthi. "Privacypreserving public auditing in cloud using HMAC algorithm." *International Journal of Recent Technology and Engineering (IJRTE)*, 2013.

BIOGRAPHIES OF AUTHORS

Anitha K. L. is a research scholar in the Department of Computer Science, Bharathiar University, Coimbatore, India. Anitha K L received post graduate degree in Master of Computer Applications and B.Sc. degree in Computer Science from the University of Kerala. Her research interests include cloud computing security, virtualization, data center networking and distributed computing.

T. R. Gopalakrishnan Nair, a Fellow of Institution of Engineers, has 34 years of experience in professional field spread over Research, Industry and Education. Currently, he is the Rector for Rajarajeswary Group of Institutions in India. He was the Aramco Endowed Chair in Technology in PM University, KSA. He holds degrees M.Tech. (I.I.Sc., India) and a Ph.D. in Computer Science. His areas of interest include Advanced networks, Cognitive Systems and Multidisciplinary studies including Brain and physical systems. He is a senior member of IEEE, ACM and few other professional bodies.