2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)
International Institute of Information Technology (I²IT), Pune

Secure Cloud Storage Using AES Encryption

Babitha.M.P
Department of Information Technology
Government Engineering College
Idukki,Kerala
Email:babithamooleparampil@gmail.com*

K.R. Remesh Babu
Department of Information Technology
Government Engineering College
Idukki,Kerala
Email: remeshbabu@yahoo.com

***Abstract*—In cloud computing distributed resources are shared via network in open environment. Hence user can easily access their data from anywhere. At the same time there exist privacy and security issues due to many reasons. First one is dramatic development in network technologies. Another is increased demand for computing resources, which make many organizations to outsource theirdata storage. So there is a need for secure cloud storage service in public cloud environment where the provider is not a trusted one. This paper addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different security services like authentication, authorization and confidentiality along with monitoring in delay. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on a cloud. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.**

Keywords—Cloud Computing; Cloud Security; AES; DES; Encryption; Decryption; QoS.

I. INTRODUCTION

The cloud computing model integrates several technological advancements such as virtualization, web services, and Service Level Agreement (SLA) management for enterprise application. Due to rapid development in technologies more and more service providers and customers moving towards cloud environment. Today military, government and commercial enterprise systems are using different cloud services to provide network connectivity and high service availability to the end users. Cloud providers offer their services in three fundamental models [1]: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Even though cloud computing has many advantages when compared with the traditional data storage mechanisms; security concern is a barrier for choosing cloud computing from the consumers viewpoint. The researchers are done several studies related to security issues in cloud [14]. Cloud infrastructure is mainly available in public and private mode. Private cloud is dedicated to a single customer or organization. The hosted services are offered to limited number of peoples, this minimizes the security concern. In public cloud, the infrastructure is owned and managed by cloud provider itself. Hence security and confidentiality of data is an important concern [2][3]. As the number of cloud users increases day by day, the Quality of Service (QoS) management is another important issue. QoS management incloud computing environment refers to the activities in QoS specification such as evaluation, prediction, aggregation and control of resources to meet end-to-end user and application requirements.

With the emergence in technologies a large number of organizations like IBM, Google, Yahoo, eBay etc., have already invested in cloud computing. Large number users share huge amount of data at high speeds from geographically dispersed locations. But in real cloud computing environment existing solutions are prone to failure and security compromise in many areas: computing performance, cloud reliability and information security [3]. Present approaches are not sufficient to ensure data security for end users. The proposed approach provide a clear and concise view of delay within real cloud computing environments and inform cloud users about unauthorized access to their data through an SMS alert system. This paper discusses different research works [15][16][17] done for management and monitoring of different QoS parameters in cloud. And also provides an abstract view of encryption techniques AES, DES and RSA.

The rest of the paper is organized as follows. Section II contains literature survey. Then section III providesthe detailed description of the proposed scheme. Section IV contains performance evaluation. Finally, section V gives the concluding remark of the whole paper.

II. LITERATURE REVIEW

In order to make data scalable and secure in cloud environment researchers proposed several methods.

The paper [14] studied different security issues in service delivery models of cloud computing. They also suggest an integrated security model for providing different levels of security to data in cloud infrastructure. The threats and attacks that are possible to launching cloud computing data storage are studied in [2] and then proposed a new security mechanism. Integrity of the data during the transmission can be guaranteed by the SSL protocol applied. In file uploading and downloading session MD5 checksum is used for providing authentication and authorization. The paper [3] discussed about the new challenges in large scale cloud computing, such as reliability and security. They also analyzed two important features of distributed storage; capability of distributed storage and information security in cloud computing using CAP Theorem. Attribute based encryption and efficient key management are used for data security in paper [18]. The data will be encrypted under a set of attributes and multiple users decrypt their data using assigned key. The

owner can encrypt data without even knowing the Access Control List (ACL). The important feature of this system is that it prevents user collusion issue. The paper [4] studied problem of ensuring integrity of data in cloud computing. To verify the integrity of dynamic data, it used a third party auditor (TPA) that will improve the Proof of Retrievability (PoR) model by manipulating Merkle Hash Tree (MHT) for block tag authentication. A distributed scheme to provide data security in the cloud using homomorphism token proposed in paper [6]. This model stores the data and identifies tamper occurred at the cloud server. It also provides facilities for data updating, deletion and a solution to avoid collusion attacks of server modification due to unauthorized users. In this model a homomorphic token using universalhash function used for the verification of erasure-coded data and for identification of misbehaving servers. The paper [7] has done a comparative study between different encryption methods-AES, DES and RSA based on analysis of simulation time for encryption and decryption. They concluded that AES algorithm is better than DES and RSA.

The next section discuss about some research works focused on QoS monitoring and management in cloud. It considered different parameters rather than security like throughput, delay, SLA violation etc. Each work has its own advantages and limitations.

A method for QoS monitoring and management is proposed in [15]. Here System of Systems (SoS) approach used for QoS monitoring, management and response for enterprise systems which provide cloud services. This technique is an extension of Paul Hershey and Donald Runyon proposed SOA Monitoring for Enterprise Computing Systems. A step by step approach to monitoring and management of QoS metrics along with data security was proposed in this paper. A multi-dimensional frame work called Enterprise Monitoring, Management, and Response Architecture (EMMRA) for Cloud Computing Environments (EMMRA CC) is used for this monitoring. The three dimensions are:

- Response Time (X dimension) defines time-based services based on measurement time intervals (MTIs).
- Domains (Y dimension) detect and respond to enterprise events.
- Planes-usage, control, management, and cyber security (Z dimension) introduces structures that monitor and manageend-to-end events.

A new-fangled monitoring system called Cloud Monitoring System (CMS) for strengthens QoS during SLA negotiation is proposed in paper [16]. The negotiation between consumers and Service providers is periodically evaluated and reports are generated in an absolute process. If any local changes occurred, each network element will generate alarms to ensure that global parameters are not violated. Also the failed nodes can be noticed, which will increase the efficiency of cloud environment and attracts more consumers. The paper [17] proposed a middleware that automatically manage the resource allocation of services in enterprise cloud environment and provided a cost-effective and secure way for accessing cloud services. Agent technology was used for monitoring the requested QoS Requirements and SLAs. The agent technology used unified format of data files for different system modules to communicate. For different levels of development, this system provided different API for developers for system interface, management and monitoring. The limitation was lack of self-learning algorithm to determine the time for automatic resource allocation.

III. System Model

Before discussing about the proposed system in detail, we have to know about security issues in cloud environment and importance of AES among other encryption algorithms.

A. Cloud Computing Security Issues

1) Cloud Security: Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security [9]. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

2) Security Issues Associated with the Cloud: There are several security issues exist with in cloud computing. Selection of cloud vendors, users should ask about seven safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability [10]. The Cloud Security Alliance (CSA) has identified security issues in different cloud domains and also provide security guidances [8]. A survey of security issues in cloud in service delivery models and given a detailed analysis each security issue in [14]. Data Center Knowledge is a leading online source of daily news, they analysed data center security issues. They reports Security Breaches, Data Loss, Outages occurred in cloud [5].

B. Encryption algorithms

The encryption algorithms mainly categorized into two:Symmetric and Asymmetric key encryptions. In symmetric key encryption single secret key is used for both encryption and decryption. In asymmetric key, encryption is performed using public key and decryption using secret key. AES and Data Encryption Standard (DES) are two symmetric key encryption methods. Rivest-Shamir-Adleman (RSA) is example for asymmetric key encryption.

*1) DES:*The algorithm also referred as Data Encryption Algorithm (DEA). For DES data are encrypted in 64 bits blocks using 56 bit key. This algorithm transform 64 bit into a 64 bit output through a series of steps. The same steps and key is used for decryption also. In the initial step the 64 bit plain text passes through an initial permutation. Next phase consist of 16 rounds of both permutation and substitution functions. Last round consist of 64 bit output: the left and right half of the output is swapped, this will generate the pre-output. In the last step reverse of initial permutation is applied to the pre-output, which produces 64 bit cipher text. DES finally and definitively proved insecure in July 1998 by the Electronic Frontier Foundation (EFF), they announced that the DES

encryption is possible to broken by using special purpose DES cracker machine that was built for $250,000. According to them less than three days needed for breaking DES encryption. Fortunately there are a number of alternatives to DES like AES, Triple DES. DES is more vulnerable to brute force attack because of its short key length (56 bit).

2) AES: This algorithm was published by National Institute of Standards and Technology (NIST) in 2001. AES is symmetric block cipher that is intended to replaces DES. The cipher takes plaintext of size 18 bit. The key length can be 128,192,256 bits. The algorithm referred to as AES-128, AES-192 and AES-256 depending on key length. The cipher consists of N rounds depends on key length: 10 rounds for a 128 bit key, 12 rounds for a 192 bit key and 14 rounds for 256 bit key. First N-1 rounds consist of 4 transformation functions-One permutation (ShiftRows) and three substitutions (Substitute bytes, MixColumns, AddRoundKey). Final round of both encryption and decryption consist of only 3 stages. Substitute bytes use S box for byte by byte substitution. MixColumns makes use of arithmetic over GF (2^8) AddRoundKey is simple bit-wise XOR of current block with a portion of expanded key.

*3) RSA:*Ron Rivest, Adi Shamir and Len Adleman at MIT published Rivest-Shamir-Adleman scheme in 1978. RSA is a block cipher. In RSA the plaintext and cipher text are integers between 0 and n-1. The typical size of n is 1024 bit. Encryption and decryption are of the following form for a plain text block M and cipher text block C.

$$C = M^e \bmod n \quad (1)$$

$$M = C^d \bmod n = M^{ed} \bmod n \quad (2)$$

Here "*e*" and "*d*" are public and private keys. The RSA has been used in various applications like e-commerce trade which ensures integrity, confidentiality, authentication and non-repudiation.

C. Why AES Encryption ?

1) Comparative analysis: Table I shows the comparative analysis of encryption algorithms - DES, AES and RSA based on key length, cipher type, block size, security, easiness in hardware and software implementation, encryption/decryption speed etc. A comparative study between different encryption methods-AES, DES and RSA based on stimulated time for encryption and decryption has done in [7]. Different size text files are used as input for evaluate the encryption and decryption time. Based on their experiments they concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. Based on their results they reached in a conclusion that AES algorithm is much better than DES and RSA algorithm. From table I show that RSA is least secure and AES is most secure and faster one. Now a days an important problem faced by all organization and providers is that fastest and secure delivery of services to the customers. Security of any system also depends on user satisfaction level. Hence the proposed system provided security to user data through encryption before uploading on the cloud. AES algorithm is used for data encryption and decryption, since it is faster and secure than other algorithms.

TABLE I. COMPARATIVE ANALYSIS BETWEEN AES, DES AND RSA

Features	DES	AES	RSA
Developed	1977	2000	1977
Key Length	56 bits	128,192,256 bits	More than 1024 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Block size	64 bits	128 bits	Minimum 512 bits
Security	Not secure enough	Excellent secured	Least secure
Hardware & Software Implementation	Better in hardware than software	Better in both	Not efficient
Encryption and Decryption	Moderate	Faster	Slower

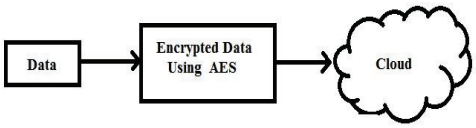

Fig. 1. Data Encryption with AES

D. Problem Statement

The data storage in cloud is similar to data stored in other storage devices but in remote locations. In cloud the user can access their data at anytime from anywhere. Three aspects of information security have to consider when using cloud services: confidentiality, integrityand availability. Public cloud infrastructure provide scalable and on demand data storage. This avoids the burden of creation and maintenance of private infrastructure for data storage. The customers get several benefits like reliability, availability with minimum cost and effort. But there exist some security and privacy risks. One important problem among them is confidentiality of customer data. One common solution to maintain data confidentiality is encryption. To ensure effectiveness of encryption there must use efficient encryption algorithm. In cloud computing environment where large amounts of data transmission, storage and handling occur, hence also need to consider processing speed as well as computational efficiency of encryption algorithm. In this case symmetric encryption algorithm is more suitable than asymmetric encryption algorithm.

To address the above problems and increase the number of customers, this paper proposes a new approach based on AES encryption technique. Fig.1 shows the security model of proposed approach. The proposed approach will ensure the following features:

- Confidentiality -The cloud storage provider don't know any information about customer data.
- Integrity - Any unauthorized access to customer data is handled by SMS alert mechanism.

Along with this, the existing features of cloud was also supported, i.e.

- Availability- Customer can access their data from any machine at any time using their secret file_id.
- Data sharing-Customers can provide access to their datawith trusted parties.

Most of the previous studies are not done experiments in real cloud environment. So a more reliable and secure effective system which is tested in real environment is needed for secure data storage.

E. System Module

The proposed system contains three components: one cloud controller, consumer and different nodes. Delay measurement was performed based on the request and response time during file upload. Fig. 2 shows the overall system architecture.

1) User Registration: Each user has a unique account. Hence, each users have to register initially before them accessing the cloud system. The registration is done by the user only once to create an account with username and password. Then she/he can login into the system from anywhere using the username and password and can also upload/download files through file upload and download module.

*2) File Uploading/Downloading:*User can login from any-where using her/his username and password and upload file, using their own file key. And later she/he can download the file using the same key. When uploading the file the content will encrypted using AES encryption before saved in to the database. Also the content will distributed to different blocks. So the chance for attack and uploading time are reduced. If there occur any unauthorized access an SMS alert will send to the authorized user.

3) Delay Calculation: In real cloud environment due to increase in number of users, the data traffic become high. This will affect overall system performance. The huge data traffic result delay and congestion. In real environment different factors causes the delay i.e. size of uploaded file, network speed etc. The model proposed here measure the delay occured when uploading files with different size at different time in a real cloud platform. When uploading a file initially the file split into different blocks before encryption. The size of each block depends on the file size. Delay metric is calculated as the sum of delay occurred during block wise uploading to different location in cloud database.

$$Delay = T_s - T_b \quad (3)$$

The observed delay is caculated using equation (3); which is the difference between time after uploading and time before uploading. Delay is calculated using the equation 4. It is the sum of delay occured during blockwise upload of file in three cloud location.

$$D_T = D_{c1} + D_{c2} + D_{c3} \quad (4)$$

T_s= Time after successful upload

T_b= Time before uploading

D_T=Total Delay

Here C_1, C_2 and C_3 denote three cloud locations. The contentof each blocks stored in three cloud locations.

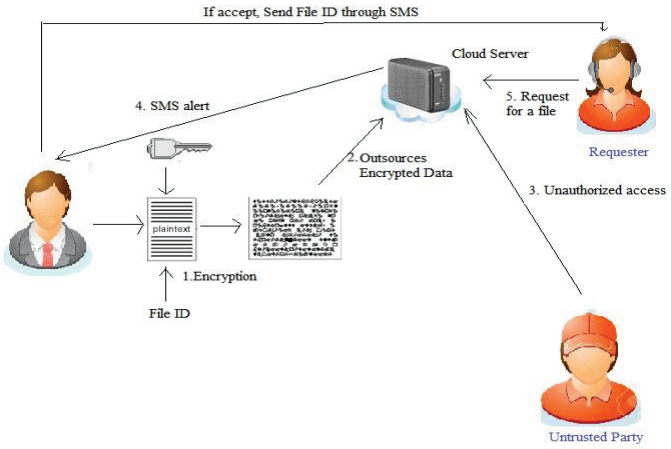

Fig. 2. System Architecture

4) Data security: 128 bit AES encryption is used for provide security to the user uploaded data. AES is a fast symmetric encryption algorithm.

IV. Result

The proposed system built on a prototype of an online file processing application. The application was hosted in an online cloud database provided by the cloud provider GoDaddy. GoDaddy is a US based cloud service provider. A GoDaddy account was created for running the application. In this model one system is act as the controller. Anybody can access the application from anywhere at any time over internet. JAVA and JSP are the programming languages used for creating this application. Graphical user interface (GUI) was created with HTML. Fig. 2 shows the overall system architecture and activities in proposed model. One important application of this system is secure sharing of confidential data like medical record, personal information, financial information etc. Suppose a user wants to access our application for uploading their confidential data, she/he must register with their valid email_id and mobile number with our system. The username and password for their account is user defined and not system defined. After successful registration they can login as a user. Then user can upload the confidential file through file upload module. Before uploading file to cloud, the user gets a window for encrypting their file as individual blocks. Then click the save button after setting a secret fileID for future accessing and sharing. The file will upload to the GoDaddy server database. In the case of medical record, user can share record with their doctor at anytime from anywhere, there is no need for keeping their files with them always as hard copy or soft copy. Only need is to remember their secret file ID. The file ID may be numbers, alphanumeric characters or special characters anything as user wish or they

can use a combination of these as file ID. There is no limitation for length of file_id. The user can view time taken for uploading their file.

A. Security

The proposed model used 128 bit AES encryption. The encryption consists of 10 rounds for 128-bit keys. In this model, the file was split into different blocks depending on file size. Then individual blocks are encrypted separately. After block wise encryption each block uploaded to cloud at different locations with file_id and block_id. If anybody like cloud provider, try to access a file directly from the server, they can't get whole data, since it stored at different locations and also in encrypted form. Hence the person who knows secret file_id can retrieves data. The proposed system provides an online editing facility, i.e. user can edit their data and then uploaded on to cloud without downloading to their system. Only the actual user can use this facility while others can only view data. Fig. 3 shows the diagrammatic representation of file encryption

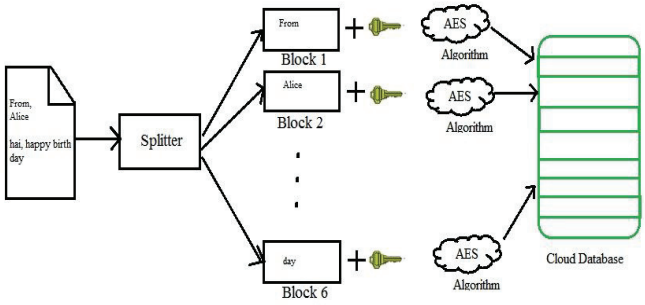

Fig. 3. Encryption

B. Delay

Delay is the prime factor considered while evaluating the QoS in every system. Delay depends on various factors, including mis-configuration of software stack, blocked ports in network, and data processing delays. In this system file uploading and downloading delay was monitored at different time interval. Table III shows observed delay and calculated delay when uploading files with different sizes. Table II shows delay during block wise upload. Calculated delay is the sum of block wise delay. Fig.4 shows time taken for uploading files with different sizes. Fig.5 shows the delay variation over time. From Fig.7, shows the variation in observed delay and the computed delay. Fig. 6 represents the delay occurred during block wise uploading. The delay may vary based on the size of data being processed. In addition, there are various factors that affect delay in the system: network speed is one important factor during real time execution.

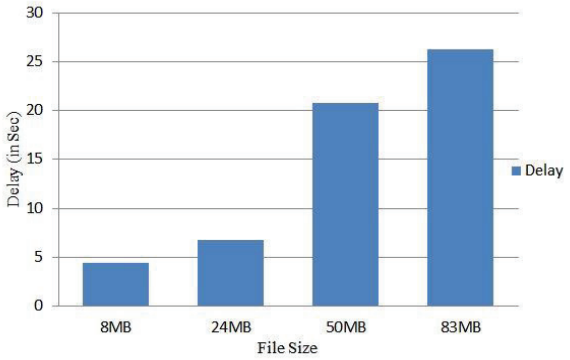

Fig. 4.Delay occur when uploading files with different size

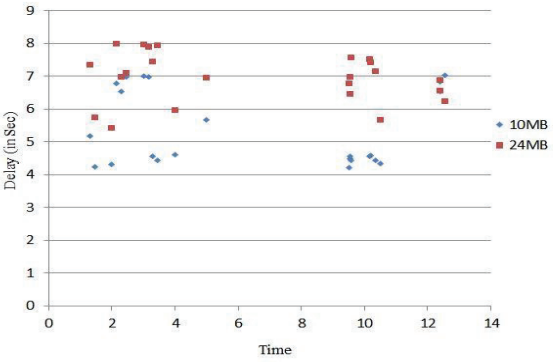

Fig. 5. Variation in Observed Delay and Calculated Delay

TABLE II. DELAY OCCUR DURING BLOCK WISE UPLOAD

File Size (MB)	Cloud 1(Sec)	Cloud 2(Sec)	Cloud 3 (Sec)
8	1.0570	1.0143	1.0266
24	2.0170	2.0140	1.0170
50	4.0610	3.0510	5.0710
83	8.5792	1.8943	3.8683

TABLE III. VARIATION IN OBSERVED DELAY AND CALCULATED DELAY

File Size (MB)	Observed Delay (Sec)	Calculated Delay (Sec)
8	4.4280	2.7671
24	7.8080	6.7490
50	20.7790	20.4570
83	26.2830	23.4980

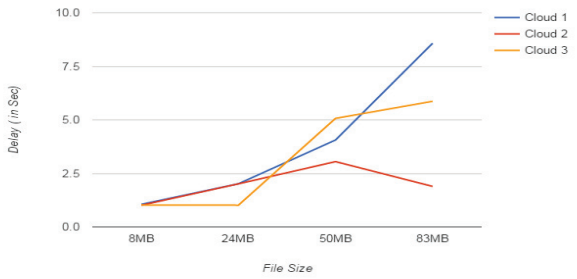

Fig. 6. Delay occur during block wise upload

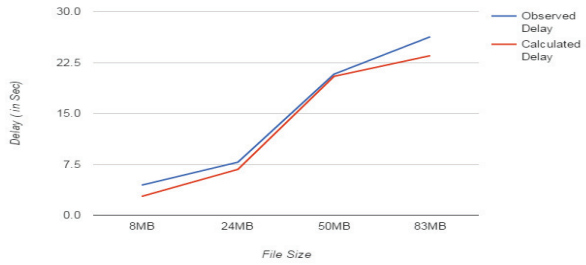

Fig. 7. Variation in Observed Delay and Calculated Delay

C. *Authentication and Authorization*

User authentication is performed through password verification. Each user has a unique user id and password for their account. During registration user set his/her own user_id and password by which they can access their account for uploading their text files. When uploading file, each user have a unique file_id for future access to their data. If user enters correct user name and password he/she get access to their account. Otherwise error message will be generated. Authorization is the process of verifying user's privilege to access something. In the proposed system, during unauthorized access to a particular file an SMS alertsystem is used to inform actual owner. Each file uploaded in cloud has a unique file_id. Authorized users can use this ID for downloading and editing their uploaded data. If somebody tries to access another person's file, an alert SMS will send to the actual owner's mobile number which he/she provided during the time of registration. Fig.8 shows the working model of user authorization module.

V. Conclusion and Future Scope

This paper studied existing security issues in cloud computing environment and proposed a new method for securing cloud data in real environment. 128 bit AES encryption is used for providing confidentiality, authenticity and access control. Then performance of proposed approach was analyzed based on delay. From this analysis we observed that there is drastic increase in delay with increase in file size. Future work proposes a new method for intelligent data storage in which the storage nodes are evaluatedbased on the previous attack history.

References

[1] P. Mell, Grance, "The NIST definition of cloud computing", Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145.

[2] Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, "Securing Data Storage in Cloud Computing", J. of Security Engineering, June 2012, pp.252-259.

[3] C.W. Hsu, C.W. Wang, Shiuhpyng Shieh, "Reliability and Security of Large Scale Data Storage in Cloud Computing", part of the Reliability Society Annual Technical Report 2010.

[4] Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in CloudComputing", IEEE Systems Journal, Vol.9, No.1, August 2015.

[5] http://www.datacenterknowledge.com/archives/2015/03/16/security-breaches-data-loss-outages-the-bad-side-of-cloud/

[6] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Ensuring data storage security in Cloud Computing", IEEE 17th International Workshop on Quality of Service (IWQoS) 2009, pp. 1 - 9

[7] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol.13, Iss. 15, Vol. 1, 2013.

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, retrieved on 19th November 2015.

[9] Wentao Liu, "Research on cloud computing security problem and strategy", IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1216-1219.

[10] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853, retrieved on 6th March 2016.

[11] Deyan Chen, Hong Zhao, "Data Security and Privacy ProtectionIssues in Cloud Computing", IEEE International Conference on Computer Science and Electronics Engineering, 2012, pp 647-651.

[12] Ateniese, Giuseppe, "Provable data possession at untrusted stores". ACM Conference on Computer and Communications Security. ACM Press; 2007, pp. 598-609.

[13] Ashalatha R, Vaidehi M, "The Significance of Data Security in Cloud: A Survey on Challenges And Solutions on Data Security", International Journal of Internet Computing, Vol, 1, Iss. 3, 2012, pp.15-18.

[14] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, Iss. 1, Jan 2011, pp.1–11.

[15] Paul C. H., S Rao, C B. Silio, A Narayan, "System of Systems for Quality-of-Service Observation and Response inCloud Computing Environments", IEEE Systems Journal. Vol.9, No.1, March 2015, pp. 212-222.

[16] D Ardagna, G Casale, M Ciavotta, J F Perez, W Wang, "Quality-of-service in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications, 5:11, 2014, pp. 1-17.

[17] S.Lee, D.Tang, T.Chen, W.C.Chu, "A QoS assurance middleware model for enterprise cloud computing", IEEE 36th Int. Conf. on Computer Software and Application Workshops, 2012, pp. 322-327.

[18] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters ,"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", ACM Conference on Computer and Communication (CCS 2006), pp. 89-98.