ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Enhanced Authentication Architecture for Cloud Computing System

Lalit Gehlod*[1], Vishal Deep Rathore[2]
Computer Science Department, IET-DAVV, Indore, India
lalitgehlod@yahoo.co.in

Abstract

Cloud computing is a powerful tool for computation ability. This provides various diverse services and platforms for develop and manage user data in a remote storage. In this context, cloud also provides the ability to share and transfer large amounts of data in an efficient manner. In this paper, we have proposed new security architecture for cloud computing system. This ensures secure authentication system and hiding information from others. In this a diverse light weight AES algorithm based cryptographic solution is proposed for optimizing security. This model also includes one time password system for user authentication process.

Keywords: Cloud Computing; Security Architecture; AES; onetime password; MD5.

1. Introduction

Cloud Computing is a new computing model that delivers the computing missions on a resource pool that includes a large amount of computing resources. It is the result of development of infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). With broadband Internet access, Internet users are able to acquire computing resource, storage space and other kinds of software services according to their needs. In cloud computing, with a large amount of various computing resources, users can easily find their solutions with the resources provided by a cloud. This brings great flexibility for the users. Using cloud computing services, users can store their critical data in cloud data centers and can access their data from anywhere using the Internet. Users do not need to worry about system or disk crash.

One of the essential characteristics of cloud computing security is protecting integrity, availability and confidentiality of data stored in the cloud data centers. Data will be accumulated and transferred in a shared environment which is managed by various cloud service providers, and it is expected to be located in a discrete country that has their own set of rules and guidelines. It could face a several kind of rules and guidelines which might uncover it partially or completely even when it placed in the national borders. The data could be transferred to a third party who may use it for legal or illegal purposes, for instance, in advertisements, which might lead to considerable security problems. Integrity of files or data that is sorted in the cloud data centers has to be insured without downloading it, as it will be expensive for users, especially with huge quantity of data. Furthermore, data is always dynamic either in the data center or anywhere else, so it could be modified, altered, removed and so on [2].

As data is stored in different data centers that located at discrete locations, so data availability will become a major concern by some factors such as bandwidth efficiency, one data center or server is partly or completely unavailable and so on. For example, Microsoft's Azure is a cloud service provider faced severs degradation for nearly 22 hours by the reason of problems related to network upgrading [3]. A cloud service provider also has to make certain its computing resources are fully usable and available at all times. Computing resources could be unapproachable for many reasons such as natural failure or denial of service.

Protecting data privacy is another significant characteristic in cloud computing security. Cloud computing provides a shared environment, that make use of sharing infrastructure. So, unauthorized uses of data may be possible in this environment. Sharing the cloud computing resources with protecting customer's privacy is a major challenge. For delivering a secure multi-tenancy in the cloud computing, data isolation is a major concern. User's data should be isolated from another user's data. As the data may be transferred between countries, so it could face different kind of rules and guidelines and legal systems. Data secrecy might be utilized for ensuring the customers data privacy and security.

In these days, different security models and algorithms have used in cloud computing environment. Unfortunately, these models have failed to solve all most all the security threats. Additionally, various online businesses require high capacity security models in cloud computing domains. Security models that are developed and currently used in the cloud computing environments are mainly used for providing security for a file and not for the communication. Furthermore, present security models are sometimes uses secured channel for communication. However, this is not cost effective process. Yet again, it is rare to find a combined work of main server security, transaction between them and so on. Few models attempt on discussing about all, but they are completely dependent on user's approach. Few models have proposed about hardware encryption system for secured communication system. The concept is usually direct but the implementation is relatively problematic. Moreover, hardware encryption is helpful only for the database system but not for other security problems. User authentication based detection technique is currently very important thing. This method is rarely discussed in the recently used models for ensuring security in cloud computing.

In this paper, we have proposed a model an enhanced authentication architecture for cloud computing system. Here files are encrypted with AES algorithm. In this model encryption keys are generated randomly by the authentication server using MD5 algorithm. Two servers, computing server and authentication server are used here for ensuring high security. This model also helps to solve many security issues like malicious intruders, hacking, etc. of cloud computing system.

2. Related Work

There are various models have already been proposed and done on cloud computing security in recent times. Identification based cloud computing security architecture have been worked out by different researchers [4]. But only identification of the authorized user does not all the time prevent hacking or misusing of data or data intruding in the cloud data center of cloud environment. Yao's Garbled Circuit has proposed a model which used for secure data saving in cloud servers [5, 6]. It is also an identification based model. The flaw in this model is that it does not guarantee for whole cloud computing system's security. Researches into ensuring security in whole cloud computing platforms have already worked out in different structures and models. AES algorithm based file encryption system is used in some of these models [7, 8]. But these models store both the encryption key and encrypted file in single database server. Only a single successful malicious attack on the server may disclose the whole information about the files and the owners the file to the hacker which is not accepted from any cloud service provider. Some other models and secured architectures have been proposed for ensuring security in cloud computing environment [9, 10]. Although these models ensures secured communication between users and servers, but they do not encrypt the information loaded on cloud servers. For better security ensuring methods, the uploaded information on the server needs to be encrypted so that none can be able to know about the file information and its location. There are some other secured models for cloud computing environment have been proposed [13, 14]. But, these models have also failed to ensure all the issues of cloud computing security architecture [15].

To provide security Kawser et al suggest a cryptographic approach [1] in 2012, in this proposed model they have worked with the following security algorithms like RSA encryption algorithm for secured communication between users and the cloud servers. AES encryption algorithm is used for securing files. The MD5 hashing algorithm is used to cover the tables from users. One time password is used for authentication.

In this model first the client has to make login to the server. One time password has been used to authenticate the user. The communication between the client and the cloud service provider is secured by using RSA algorithm. An authenticated client encrypts the file by system's public key. After receiving an encrypted file from the client it will immediately decrypt it using its private key. Similarly, when the client receives an encrypted file from the system the client's browser will decrypt it with RSA algorithm using the client's private key.

When a file is uploaded by a client the system server encrypts the file using AES encryption algorithm using randomly generated key by system server. This particular key is used for encrypting and decrypting a file of a user for that moment. The key is kept in the database table of the system server along with the user account name using MD5 hashing.

When the user wants to download a file he/she is required to select that particular file, then server automatically recover the key for the requested file from the main system server. The system matches the user account id saved in its database table with the id saved in the storage server after using md5 hashing.

3. Proposed Model

A. Problem Domain

That is much simpler approach where a single cryptographic algorithm is used for an individual work. But each security algorithm having their own advantages and flaws, more over it there are more secure cryptographic schemes are also available for securing data. Author of [1] proposed model using RSA encryption system which is deterministic. For this reason, it becomes delicate in long run process. There are several goals that are required to achieve is to propose a new security model which is light resource consuming and provide efficient and adaptable security under given cloud environment. Proposed model will help to improve the less running time.

B. Solution Domain

To optimize the problem specified in the problem domain new security architecture is proposed. We have designed and implemented a controlled AES algorithm [16] based cryptographic scheme for data security. The overview of the proposed security architecture for cloud computing system is shown in Figure 1.

This system is designed in three different phases. First a desktop based client application that is used to connect to the server system. Clients can upload and download their files through this application. Second is a cloud data center, which is a file server, which is used to store the files in the system in a cryptographic manner. Third is an authentication server. This server works as a security server which contains all the information of the clients and is used for authentication of the user. This server also stores the several file information like key information, file name, date and time along with the user id of respected clients to provide the authentication and file exchange.

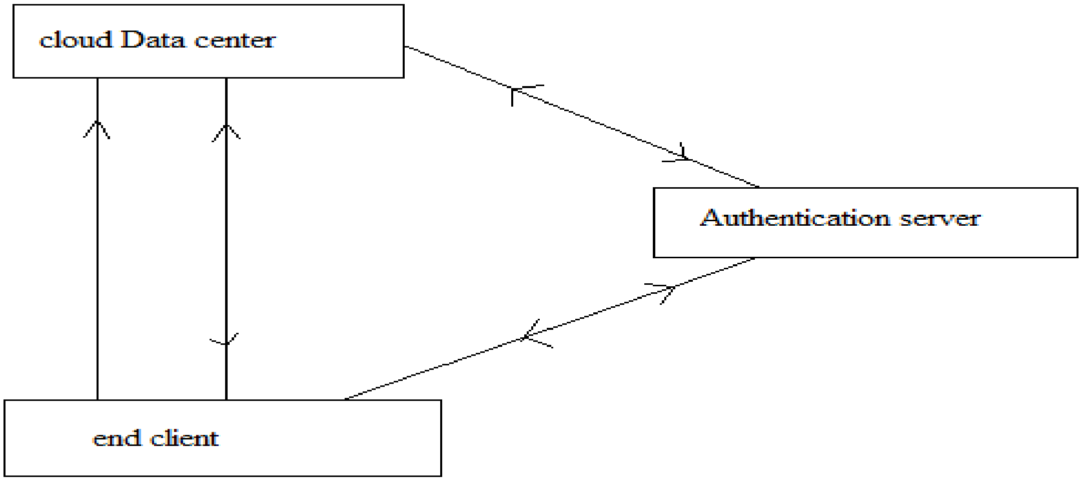

Figure 1. Proposed Security Model

In this model, all the users must pass through the user registration process. In this process the user should provide their basic details to get registered into the system. So it is a basic information collection process. Certain security questions are required to submit at the time of registration which is further used for providing the authentication of the user. The client will pass these information through the client connector which is an additional GUI developed in order to connect with the remote server.

In the proposed security model one time password has been used for the authentication of the user. The password is used to make the user account inaccessible and secured from the unauthorized user. But the passwords defined by the user can be compromised. To overcome this difficulty one time password is used in the proposed security model. Thus, whenever a user access to the cloud system, he/she will be redirected to the authentication server. The authentication server asks certain security questions to the user and the user have to respond with security answers. After getting the answers server matches it with the answers stored at the time of registration. After the successful matching authentication server provides a onetime password to the user. The system will generate this password randomly. User has to respond it back to the authentication server and matching is performed. This newly generated single password will be used only once to login into the system. Therefore, at a same time a check to determine the validity of the user is also performed. As a result only authorized user will be able to connect to the cloud system. By this process, the existence of an unauthorized user will be pointed out. Now authentication server redirects the user to cloud data center.

Once the user is connected with the cloud server, he/she can upload or download the file(s). The first time when the user connected with the server he/she can only upload file. After that user can be able to upload, download and manage their files. In the proposed model AES encryption algorithm is used for making the file transfer safe. The pictorial representation of uploading the file from the user's end to the cloud data center is shown in Figure 2.

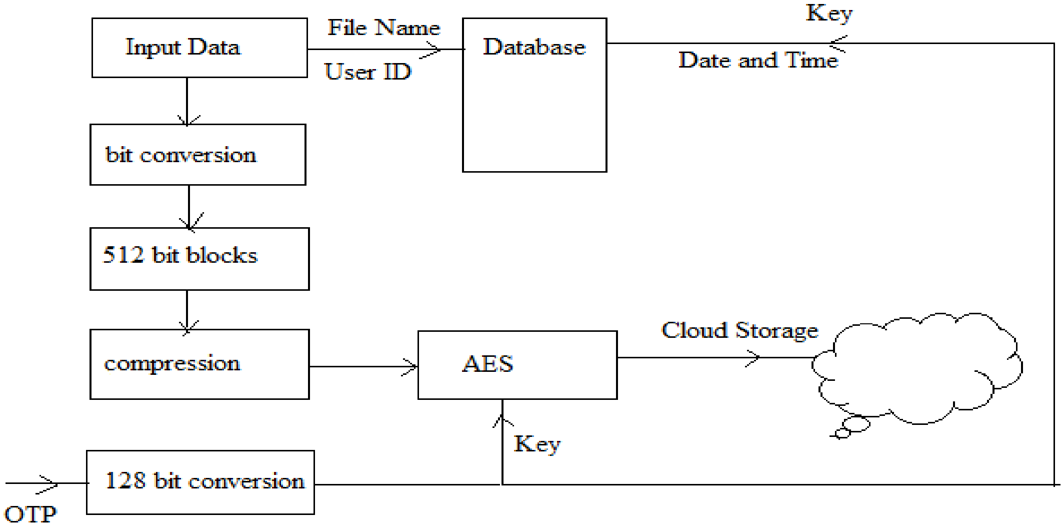

Figure 2. File Uploading Process

Every time when the user requests for uploading the file, the authentication server sends one time password for an individual file. This one time password provided by the authentication server works as an encryption key for that particular file. . This one time password is converted into the 128 bits using MD5 algorithm. The system at the user side first accepts the file input to be uploaded. The file is converted into the size of 512 bit block. These file blocks are compressed using a default Java compressor. After getting compressed blocks, each block is encrypted using secured AES cryptographic algorithm. This key and compressed file blocks are applied to the AES encryption algorithm in that end. After encryption, file blocks are transferred to the cloud data center for storage. When the encrypted file blocks are gathered at the data center zipped into a single encrypted file. The information regarding file like file name, user id, key, date and time is stored on the authentication server. So keeping the file and encryption key on different server ensures that unauthorized person cannot retrieve the key to decrypt a particular file for a particular user by simply gaining access and observing the database table of the authentication server. As a result the key becomes hidden and safe for that particular file.

Whenever the user wants to download a file it first required to connect through the client connector in order to connect with the remote server. Now the user requests for a file to be downloaded. The pictorial representation of downloading the file from the cloud data center is shown in Figure 3.

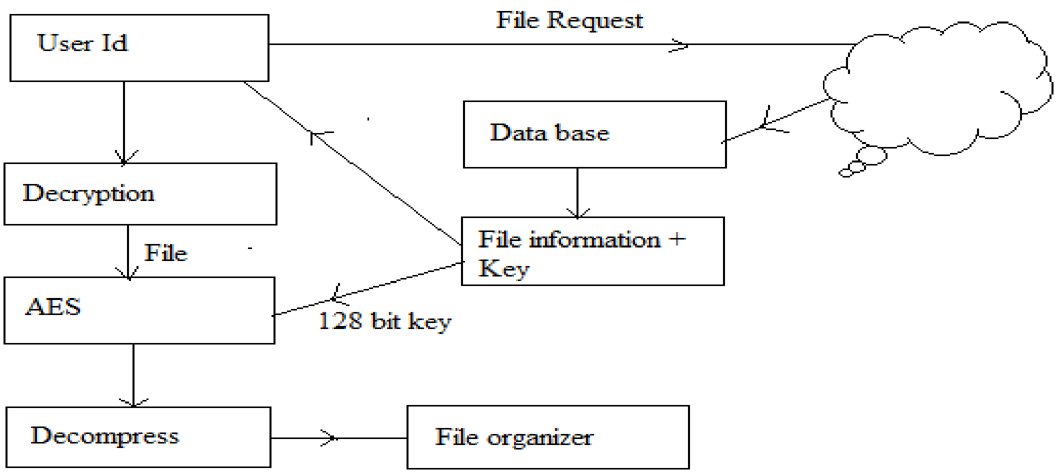

Figure 3. File Downloading Process

The user first chooses the particular file to be downloaded from the list of uploaded files. When he/she request for a particular file, the cloud data center unzipped the encrypted file into the number of encrypted file blocks and these encrypted file blocks are transferred over the network to the user's system. Then data center requests the authentication server to send the particular encryption key for that file. The authentication server sends this key to the user's system. Now the user has both the encrypted file blocks along with an encryption key. File blocks and encrypted key are applied to the AES decryption algorithm at user end. After decryption original file blocks are obtained which passed through the Java default decompression algorithm. After applying decompression process on file blocks, all the blocks are reorganized into the single file and this file is ready for use.

4. Results Analysis

This section discusses the results obtained after successful implementation of the desired cryptographic technique for cloud data center security. The performance of the proposed methodology is evaluated on various parameters. Number of files with different sizes, extensions, and contents are applied to the proposed model which helped to demonstrate the model with better results and to prove the efficiency of the overall model.

A. Accuracy

The accuracy of data is a parameter of data validity. In other words, this provides the measurement of how accurate the data is stored on the cloud servers and recovered them during access.

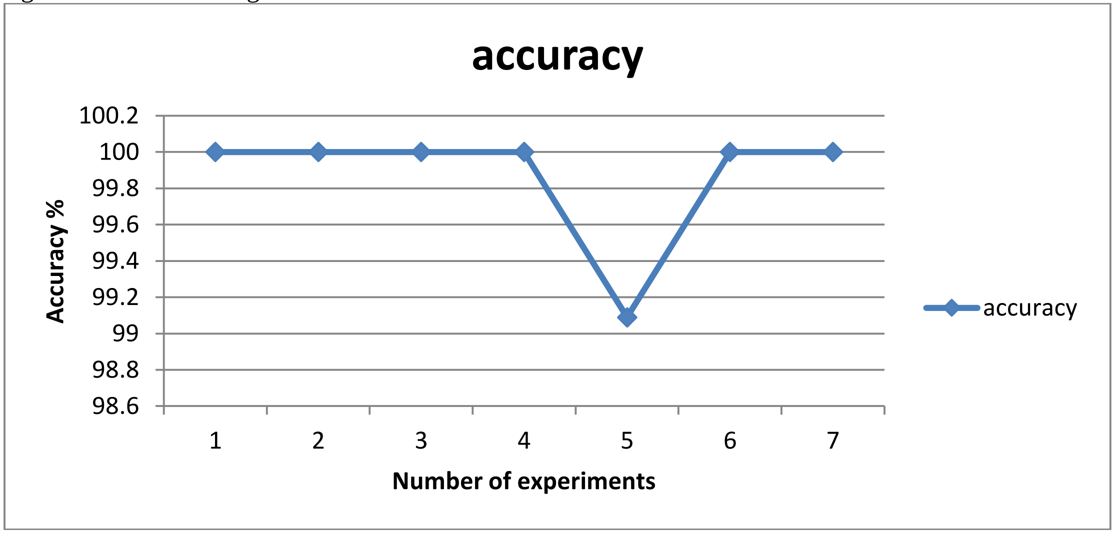

Figure 4. Accuracy

The figure 4 provides the information about the accuracy of data during the cryptographic data access. In this diagram X axis represents the number of experiments and Y access provides the accuracy of in percentage.

B. Request and Response Time

The amount of time required to access a data file as the request is known as request time and the total time the server takes to response to specific request is termed as the response time. Figure 5 shows the request and response time of the designed system.

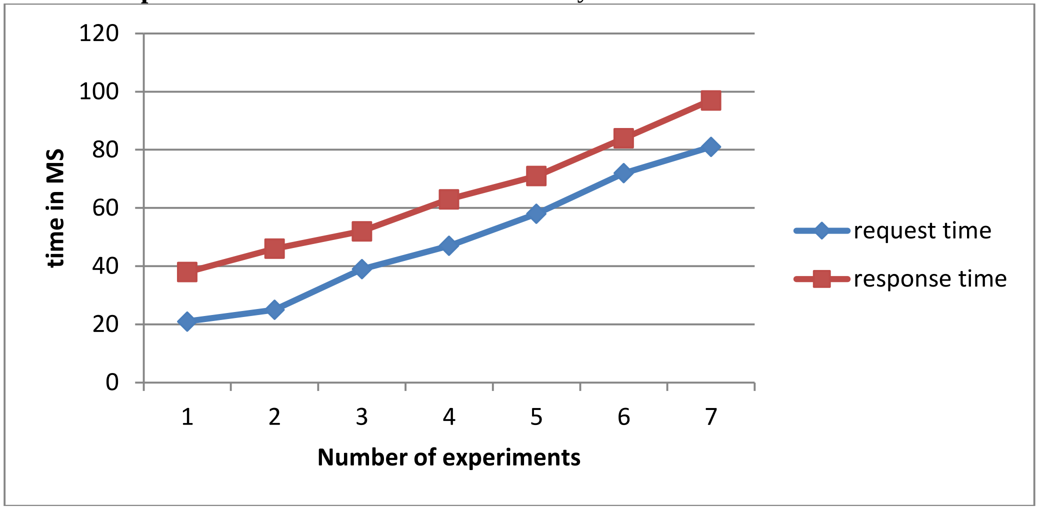

Figure 5. Request and Response Time

The given figure describes the time complexity of the designed system. The request and response time are basically a time overhead that is required to process a request of file access. That involves the user and data identification, encryption and decryption over the requested data. Therefore, according to the size of data and data type that is fluctuating. In this diagram the blue line represents request time and the red line shows the request time consumed. Additionally the X axis provides the number of different experiments performed with increasing size of data and Y axis provides the amount of time consumed in MS.

C. Memory Use

The amount of main memory required processing the request and response for access or uploading a file is given as memory used. Figure 6 demonstrates the memory requirement for both the scenarios (file upload and download from data centers). In the given diagram the blue line shows the memory consumption during the file upload process. On the other hand red line shows the memory during file downloading.

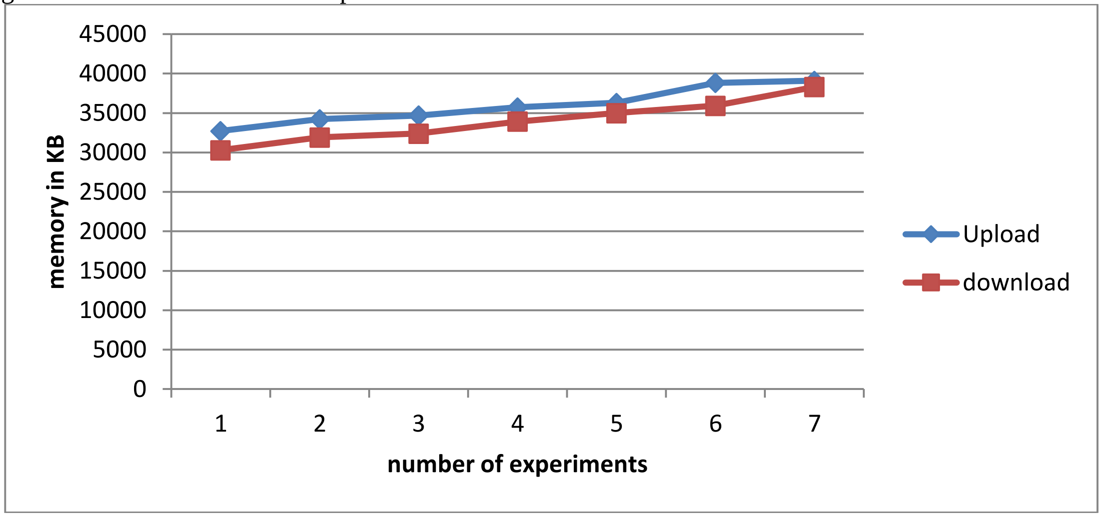

Figure 6. Memory Used

In the figure 6 the X axis shows the different number of experiments and the Y axis provides the memory consumed in terms of KB.

The performance result shows the effectiveness of the proposed system. The computational and storage complexity indicates that the system consumes additional time as time overhead for authentication and cryptographic approach of data protection. The performance of the system is summarized using a performance summary table given using table I.

Table 1. Advantages of the proposed work

S. No.	Parameter	Performance
1	Data validity	The system is able to recover data efficiently and accurately. Therefore system is adoptable.
2	Time complexity	The system introduces additional time overhead during request processing for file access and privacy management.
3	Memory complexity	The system consumes less memory during the cryptographic approach.

5. Conclusion

In this paper, we have proposed enhanced authentication architecture for cloud computing environment which includes 3rd party authentication server, AES file encryption system, one time password to authenticate users. Using MD5 algorithm for key generation makes the file safe from brute force attack. Keeping the encrypted file and encryption key on different server make this model highly secured. This model ensures security for whole cloud computing structure.

Here, the various parameters such as execution time and memory complexity are subsequently low because this model requires the implementation of only AES algorithm and does not require multiple algorithms for encryption. This model shows accurate results which make this model efficient. In our proposed system, an intruder cannot easily get information and upload or download the files because he needs to take control over both cloud server and authentication server, which is quite hard to do. Developed in a cloud environment, in this model each individual servers have assigned their respective task here. Without being authenticated a user can not be able to view the file information so, file is secured from unauthorized access.

6. Acknowledgements

The Authors are willing to express their profound gratitude and heartiest thanks to all the researchers in the field of cloud computing architecture’s security. The concerning paper is only used for educational research and development purpose that is not tested for industrial protocols.

Finally, I wish to thank my parents for their support and encouragement throughout my study.

References

1. *Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.*
2. *C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in Cloud Computing,” in 2009 17th International Workshop on Quality of Service, 2009, pp. 1–9.*
3. *W. a Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing,” in 2011 44th Hawaii International Conference on System Sciences, 2011, pp. 1–10.*
4. *Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, “Identity-Based Authentication for Cloud Computing”, CloudCom 2009, LNCS 5931, pp. 157–166, 2009.*
5. *Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, “Twin Clouds: Secure Cloud Computing with Low Latency”, CASED, Germany, 2011.*
6. *Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, “Twin Clouds: Secure Cloud Computing with Low Latency”- Extended Abstract, CASED, Germany, 2011.*
7. *Luis M. Vaquero, Luis Rodero-Merino, Daniel Morán, “Locking the sky: a survey on IaaS cloud security”, Computing (2011) 91:93–118*
8. *Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman, “FADE: Secure Overlay Cloud Storage with File Assured Deletion”, 2010*

9. *Thuy D. Nguyen, Mark A. Gondree, David J. Shifflett, Jean Khosalim, Timothy E. Levin, Cynthia E. Irvine, "A Cloud-Oriented Cross-Domain Security Architecture", The 2010 Military Communications Conference, U.S. Govt.*
10. *Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", US National Science Foundation under grant CNS-0831963, CNS-0626601, CNS-0716306, and CNS-0831628, 2009.*
11. *Younis A.Younis, Madjid Merabti and Kashif Kifayat, "Secure Cloud Computing for Critical Infrastructure: A Survey" ISBN: 978-1-902560-27-4 2013 PGNet.*
12. *K Patidar, R Gupta, G Singh, M Jain, P Srivastava, "Integrating the Trusted Computing Platform into the Security of Cloud Computing System", International Journal of Advanced Research in Computer Science and Software Engineering volume 2 issue 2 February 2012*
13. *Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Secure Data Storage and Retrieval in the Cloud", University of Texas, 2011*
14. *John Harauz, Lori M. Kaufman, Bruce Potter, "data Security in the World of Cloud Computing", The IEEE Computer SOCIETIES, August, 2009*
15. *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for cloud computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010*
16. *Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", 1999*
17. *Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001*
18. *Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January 2010*