www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19574-19579

A Review On Data Security in Cloud Environment

Varsha Yaduvanshi, Asst.Prof. Manish Rai, Prof.(Dr.) Mohit Gangwar
Department of Computer Science and Engineering RKDF College of Engineering,
Bhopal, INDIA
varshayaduvanshi40@gmail.com
Department of Computer Science and Engineering RKDF College of Engineering,
Bhopal, INDIA
Manishrai2587@gmail.com
Department of Computer Science and Engineering Bhabha Engineering Research Institute,
Bhopal, INDIA
mohitgangwar@gmail.com

Abstract—**The primary use of cloud computing is information storage. Cloud provides enormous capability of storage for cloud users. It is lot of reliable and versatile to users to store and retrieve their information at anytime and anyplace. It is an progressively growing technology. Nowadays, several enterprises have started using cloud storage because of its benefits. Even though the cloud continues to gain popularity in usability and attraction, the issues belong information security, data privacy and alternative data protection problems. Security and privacy of information stored in the cloud are major setbacks within the field of Cloud Computing. Security and privacy of the information stored in cloud are the key issues. This paper offers the brief discussion on cloud data security.**

Keywords—Cloud computing, cloud security, services, data encrytion

I. INTRODUCTION

As per the definition provided by the National Institute for Standards and Technology (NIST)“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) which can be rapidly provisioned and free with minimal management effort or service provider interaction”. It represents a paradigm shift in information technology many of us are likely to see in our lifetime.

While the customers are excited by the opportunities to cut back the capital price, and therefore the likelihood to divest themselves of infrastructure management and concentrate on core competencies, and specially the agility[1]offered by the on-demand provisioning of computing, there are issues and challenges which require to be addressed before a ubiquitous adoption could happen.
A cloud can be defined as a pool of virtualized computer resources. A cloud can:

•Host a range of various workloads, as well as batch-style back-end jobs and interactive, user-facing applications

•Allow workloads to be deployed and scaled-out quickly through the fast provisioning of virtual machines or physical machines

•Support redundant, self-recovering, extremely ascendible programming models that enable workloads to endure several unavoidable hardware/software failures

•Monitor resource use in real time to alter rebalancing of allocations when required [4]

Recent developments within the field of cloud computing have vastly modified the approach of computing in addition with the concept of computing resources. In a cloud primarily based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users

•The transmission of personal sensitive information to the cloud server,
•The transmission of information from the cloud server to clients' computers and
•The storage of clients’ personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are vulnerable to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. Cloud computing comes with various possibilities and challenges simultaneously. Of the challenges, security is considered to be essential barrier for cloud computing in its path to success[5]

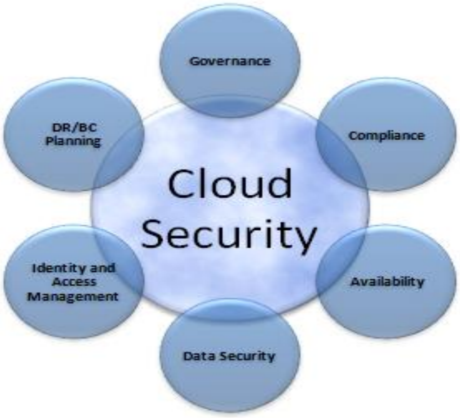

FIGURE 1 : CLOUD SECURITY

IIDATA SECURITY

Data security refers to protecting digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security additionally protects data from corruption. The main priority for organizations of every size and genre is data security.

Data security can also be called as information security (IS) or computer security. Some examples of data security are technologies include software/hardware disk encryption, backups, data masking and data erasure.

A key data security technology measure is scrambling, wherever digital information, software/hardware, and hard drives are scrambled and rendered unreadable to unauthorized users and hackers.

Data security is additionally vital for health care records, therefore health advocates and medical practitioners within the U.S. and other countries are working toward implementing electronic medical records (EMR) privacy by making awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

Cloud computing has reworked organizations approach IT, enabling them to become more agile, introduce new business models, gives lot of services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, below totally different service and deployment models, and might coexist with other technologies and software design approaches.

Maintaining control over the information is paramount to cloud success. A decade ago, enterprise data generally resided within the organization's physical infrastructure, on its own servers in the enterprise's data centre, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, however physically reside in infrastructure owned and managed by another entity. [7]

Classical Encryption

Many encryption algorithms are available that are used in information security. These algorithms can be classified as classical encryptions [8]. These encryption algorithms are based on two general principles namely substitution cipher, within which each element in the plaintext is mapped into another element, and transposition cipher, in which elements in the plaintext are rearranged. Out of the various encryption algorithms, few algorithms are described in this section.

A. Caesar Cipher

Caesar cipher [9] could be a classical substitution cipher and it is one of the simplest examples of substitution cipher. It replaces alphabet of letter in the plain text, with a letter 3 places previous of it. For example, "HELLO" could be a plain text that can be converted into "KHOOR" as cipher text. One can see that such a cipher cloud be difficult to break. This cipher can be broken by brute force attack as at the end there are only 25 possible available options of key.

B. Playfair Cipher

Next example of classical substitution cipher is Playfair cipher that contains a square matrix of 5X5 alphabetical letters organized in an acceptable manner. The user will choose a key and place it within the matrix. The rest of the letters of English alphabet from the key are then they are one by one placed in the matrix of Playfair cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter with „x‟. Otherwise if the pair is with completely different alphabetical letter sand resides within the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters is in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters is neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters.

C. Vigenere Cipher

Vigenere cipher [10] compared with Caesar cipher provides some level of security with the introduction of a keyword. This key word is repeated to cover the length of the plain text that is to be encrypted. Example is given below:

KEY : f a u z a n f a u z a n
Plain text : c r y p t o g r a p h y
Cipher : H R S O T B L R U O H L

As it may be seen from that above given example, "fauzan" is a keyword and plain text is "cryptography" that is encrypted into "HRSOTBLRUOHL". This is done using Vigenere table which contains alphabets in form of rows and columns left most column. The left most column indicates keyword and top most row indicates plaintext and at the junction of two alphabetical letters resides our replacement. After individually transforming every letter, user gets an encrypted message.

D. Rail fence technique

This is one among the transposition ciphers, within which the plain text is written down as a sequence of diagonal and then read as a sequence of rows. As an example, to encipher the message "hai welcome" with a rail fence of depth 2,

h i e c m
a w l o e

Now the encrypted message is "hiecmawloe". In this technique the same alphabets in the plaintext is rearranged. This technique alone cannot be adequate for information security.[11]

Advance Encryption

Advanced Encryption Standard (AES), additionally known as Rijindael is used for securing information. AES could be a symmetric block cipher that has been analysed extensively and is used widely now-a-days. AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, User decides to use cloud services and can migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best mere services offered by provider.

DOI: 10.18535/ijecs/v5i12.57

When migration of data to the chosen CSP happens associated in future whenever an application uploads any data on cloud, the information can first encrypted using AES algorithm and then sent to provider. After encryption, information is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anyplace on cloud. This includes all types of data.

This encryption solution is transparent to the application and can be integrated quickly and easily without any modifications to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server may be put in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for large vary of applications.

Hashing

Hashing produces a unique, fixed-length signature for a message or data set. Each "hash" is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be reversed or deciphered. Hashing then, though not technically an encryption method as such, is still helpful for proving data hasn't been tampered with.[15]

III. CLOUD AND ITS SERVICES

The word "cloud" is mostly used in science to describe a vast agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not further inspected in a given context. The word cloud was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics[12]

A cloud service can be defined as any resource which is provided over the Internet. The most commonly used cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). [13]

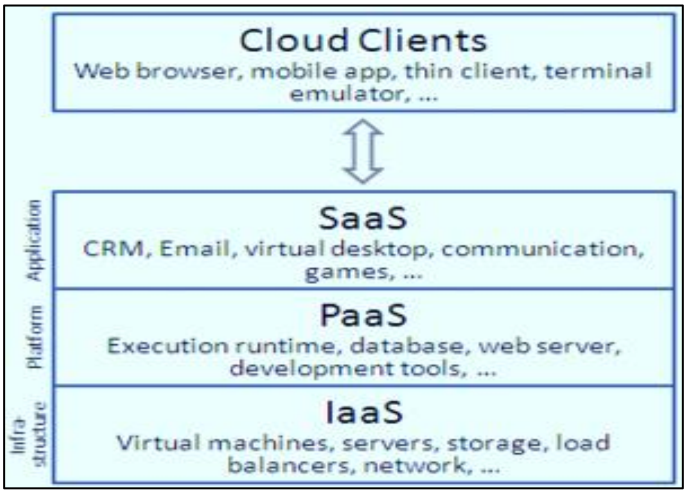
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

FIGURE 2 : CLOUD SERVICES

A. *Software as a Service (SaaS):*

In this , a complete application is provided to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers "side, there is no requirement for upfront investment in servers or software licenses, while for the provider, the costs are minimized, as only a single application needs to be hosted & maintained. Today SaaS is offered by companies like Google, Sales force, Microsoft, Zoho, etc.

B. Platform as a Service (Paas):

Here, a layer of software or development environment is encapsulated &provided as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers gives a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE,Ruby etc. Google's App Engine, Force.com, Etc. are some of the examples of PaaS.

C. Infrastructure as a Service (Iaas):

IaaS provides basic storage and computing capabilities as Standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some examples are Amazon, Go Grid, 3 Tera, etc[14]

IV.LITERATURE REVIEW

[1] **Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA, "Security and Privacy Issues in Cloud Computing",** In this the author has described that Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount importance. Many research issues are yet to be identified. Cryptographic methods are used to give secure communication between the user and the cloud. Symmetric encryption has the speed and

DOI: 10.18535/ijecs/v5i12.57

computational efficiency to handle encryption of vast volumes of information in cloud storage. This paper has proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is explained in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the information of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders

[2] Er. Ashima PansotraandEr, SimarPreet Singh, DAV University, Jalandhar, "Cloud Security Algorithms" International Journal of Security and Its Applications Vol.9, No.10 (2015) This paper describes that cloud computing appears very useful service for many people; every third person is using cloud in different ways. Because of its flexibility, several persons are transferring their data to cloud. Cloud computing prove a very successful application for organisations. As organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anyplace anytime easily. As people are saving their personal and important data to clouds, so it becomes a major problem to store that data safely.

Many algorithms exist for the data security like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric, in which 2 different keys are used for encryption and decryption. These algorithms are not secure, there is need to enhance the security of algorithms.

[**3] Santosh Kumar and R. H. Goudar "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012,** In this paper the author has discussed the architecture and popular platforms of cloud computing. The author also addressed challenges and problems of cloud computing in detail. In spite of the several limitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises. Cloud Computing initiatives could affect the enterprises within two to three years as it has the potential to significantly change IT.

[**4] Pankaj Sareen, Baddi University of Emerging Sciences & Technology, "Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud", IJARCSSE, Volume 3, Issue 3, March 2013,** This paper suggests that in today's global competitive market, companies must innovate and get the most from its resources to succeed. This needs enabling its employees, business partners, and users with the platforms and collaboration tools that promote innovation. Cloud computing infrastructures are next generation platforms that can provide tremendous value to companies of any size. Cloud Computing provides Software, Platform, Infrastructure, Storage, Security, Data, Test Environment etc. as a service. Clients would be able to access their applications and data from anyplace at any time. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. It would also bring hardware costs down. This paper also describes that you would not need a large hard drive because you would store all your data on a remote computer. However the biggest concerns about cloud computing are security and privacy. The idea of handling over important data to another company worries some people. Corporate executives might hesitate to take benefit of a cloud computing system as they cannotstore company's information under lock and key. The author also discussed the Concept of Virtualization in Cloud Computing as any discussion of cloud computing typically starts virtualization. Virtualization is using computer resources to imitate other computer resources or whole computers. The author also discussed the characteristics, applications and various forms of Virtualization.

[5] Monjur Ahmed and Mohammad Ashraf Hossain, Daffodil Institute of IT, Dhaka, Bangladesh, "CLOUD COMPUTING AND SECURITY ISSUES IN THECLOUD", (IJNSA), Vol.6, No.1, January 2014, Cloud computing has enormous prospects, but however the security threats embedded in cloud computing approach are directly proportional to its offered benefits. Cloud computing is a great opportunity and lucrative option for both the businesses and the attackers – either parties can have their own benefits from cloud computing. The huge possibilities of cloud computing cannot be ignored solely for the security problems reason – the on-going investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security problems could severely affect could infrastructures. Regardless of the nature of security issues, it can be undoubtedly concluded that the severe adverse effects as a consequence of security breaches in cloud computing, the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

[6] Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby, Menofia University, Menofia, Egypt, "Data Security Model for Cloud Computing", Journal of Communication and Computer 10 (2013), In this paper the author discusses that according to the simulation results, in the authentication phase in the proposed data security model, OTP is used as two-factor authentication software. OTP archived more password strength security than other authentication systems (BIN and static password). This appears by comparing between OTP, BIN, and static password authentication systems based on the space time size and entropy bits. From the simulation results of the second phase in the proposed data security model, test the proposed system in Ubunto Amazon Micro Instance EC2, and from randomness and performance evaluation to eight modern encryption algorithms AES is the best encryption algorithm in Ubunto Amazon Micro Instance EC2. In addition to the randomness and performance evaluation, data integrity must be ensured. Moreover, the proposed data security model encourages users to use true-crypt to encrypt his/her sensitive data.

Said Aminzou, Brahim ER-RAHA, Youness Idrissi Khamlichi, Karim Afdel, Mustapha Machkour, in their work entitled “Towards a Secure Access to Patient Data in Cloud Computing Environments,” **[16] Said Aminzou, Brahim ER-RAHA, YounessIdrissiKhamlichi, KarimAfdel, Mustapha Machkour, “Towards a Secure Access to Patient Data in Cloud Computing Environments,” 978-14 799. {) 324-5/ 13/$31.00 -20 13 IEEE,** pointed that in the modern health service, data are stored in a Data Center and only authorized users can access it. However, this Data are prone to be exposed to a number of attacks; especially by the Cloud provider's Personnel with privileged access. To avoid illegal access to comprehensive content of data center including patient’s information. They propose in this article a mechanism using the content-based watermarking technique. Information of patient and a digest are encrypted, before being embedded into LSB's biplane of image associated to the patient. This image is integrated directly into the database. Hadoop system with the integrate functions; HOFS and Map Reduce will play the key roles for our solution. In this paper, they have implemented a security architecture using watermarking and encryption techniques to secure the management of medical image and patient’s data in cloud environment. The presented method and architecture will be helpful for enhancing data security in public and private cloud. So, the proposed method will play an important role in the future.

Chao YANG, Weiwei LIN*, Mingqi LIU, in their work entitled “A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security**,” [17] Chao YANG, Weiwei LIN*, Mingqi LIU, “A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security,” 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies,** indicated that the technology of cloud has been expanding in past years because of its power to allow on-demand, elastic, authentic and affordable services to users. With the increased use of cloud application being available, the serious concern is cloud data security. In order to ensure data security in cloud data storage, a novel triple encryption scheme is proposed in this paper, which combines HDFS files encryption using DEA and the data key encryption with RSA, and then encrypts the user's RSA private key using IDEA. We implement the triple encryption scheme in Hadoop-based cloud data storage and experiment studies were conducted to verify its effectiveness.

Johannes K. Chiang, Eric H.-W. Yen, Yen-Hua Chen in their work entitled “Authentication, Authorization And File Synchronization On Hybrid Cloud -On Case Of Google Docs, Hadoop, And Linux Local Hosts,” **[18] Johannes K. Chiang, Eric H.-W. Yen, Yen-Hua Chen, “Authentication, Authorization And File Synchronization On Hybrid Cloud -On Case Of Google Docs, Hadoop, And Linux Local Hosts,” 2013 International Symposium on Biometrics and Security Technologies ,978-0-7695-5010-7/13 $26.00 © 2013 IEEE DOI 10.1109/ISBAST.2013.22,** showed that Cloud computing brings more flexible options for the Small and Medium Business (SMB). With the help of public cloud, such as Google Docs, the SMB’s are able to share their business information in lower cost but higher efficiency. Integrity between local storages and the clouds is a critical issue, which often messes up the SMB’s digital assets in a hybrid environment. The downside makes SMBs reluctant to embrace cloud technology, though they may benefit from it in the long-term. The drawback comes from two aspects: “the information chaos” and “the management crisis”. The chaos originates from the possibility of information inconsistency among replicas in different places. On the other hand, the managerial crisis lies in the non-trustable access to the digital assets. Our research refers to the de facto open standards, viz. OpenID and O'Auth, to solve the problem by identity authentication and access right authorization on the hybrid cloud.

QIAN Quan, WANG Tin Hong, ZHANG Rui, XIN Ming-jun , in their work entitled “A Model of Cloud Data Secure Storage Based on HDFS,” **[19] QIAN Quan, WANG Tian-hong, ZHANG Rui, XIN Ming-jun , “A Model of Cloud Data Secure Storage Based on HDFS,” 978-1-4799-0174-6/13/$31.00 2013 IEEE.**

] indicated that as more and more organizations and individuals tend to outsource their data to cloud storage, the security and user privacy protection attract more attention. Previous work mostly focused on the user identity authentication to keep the security, while in this paper, a novel model of cloud secure storage is proposed, which combines the Hadoop distributed file system (HDFS) with symmetric and public-key cryptography.

This discussion is summarized in following table.

TABLE 1: Summery of Related work.

S. No .	Authors	Advantages	Limitations
	Dr. L. Arockiam, S. Monikandan	symmetric encryption algorithm for secure storage	Method is same for all data.
2	Er. AshimaPansotraandEr. SimarPreet Singh	organisations can store large amount of data	Time Efficiency gets sacrificed.
3	Santosh Kumar and R. H. Goudar	Symmetry Based Encryption	Authentically is missing.
4	PankajSareen, Baddi	Concentrate on Virtualization	Missing other aspects
5	Monjur Ahmed and Mohammad Ashraf Hossain	Data Security	Lacking other data related aspect.
6	Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby	Concentrate on only Encryption of Data	Lacking other data related aspect.
16	Said Aminzou, Brahim ER-RAHA, YounessIdrissiKhamlichi, KarimAfdel,	this article a mechanism using the content-based	Memory Issue is there.

	Mustapha Machkour	watermarking tedmique	
17	Chao YANG, Weiwei LIN*, Mingqi LIU	Work on Encryption and authentication	Did not used Dynamic authentical.
18	Johannes K. Chiang, Eric H.-W. Yen, Yen-Hua Chen	Authentication, Authorization And File Synchronization	Less Time Efficient .
19	QIAN Quan, WANG Tian-hong, ZHANG Rui, XIN Ming-jun	Based on HDFS	Less Time Efficient .

CONCLUSION

There are several advantages of using cloud computing like efficiency, quick deployment, improved accessibility etc. However, there are yet many practical issues that have to be solved. In this paper we discussed about the cloud, data security in cloud. This paper also explains the data security in cloud, types of encryption techniques. Also we briefly explain the types of services provided by cloud.

REFERENCES

[1] JaydipSen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA, “Security and Privacy Issues in Cloud Computing”

[2] Er. Ashima Pansotra and Er. Simar Preet Singh, DAV University, Jalandhar, “Cloud Security Algorithms” International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360

[3] Santosh Kumar and R. H. Goudar “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey”, International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

[4] Pankaj Sareen, Baddi University of Emerging Sciences & Technology, “Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud”, IJARCSSE, Volume 3, Issue 3, March 2013

[5] Monjur Ahmed and Mohammad Ashraf Hossain, Daffodil Institute of IT, Dhaka, Bangladesh, “CLOUD COMPUTING AND SECURITY ISSUES IN THECLOUD”, (IJNSA), Vol.6, No.1, January 2014

[6] Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby, Menofia University, Menofia, Egypt, “Data Security Model for Cloud Computing”, Journal of Communication and Computer 10 (2013)

[7] CSO, “ Data Security in the Cloud ”Gartner Inc., “Worldwide Cloud Services Market Is Expected to Surpass $109 Billion in 2012,” press release, September 18, 2012

[8] Vamsee Krishna, Yarlagadda And Sriram Ramanujam, “Data Security in Cloud Computing”, Journal of Computer and Mathematical Sciences, Vol.2 (1), pp 15-23, 2011.

[9] Dr. A. Padmapriya, P. Subhasri,” Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security”, International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4,pp 1067-1071, 2013

[10] Quist-Aphetsi Kester, “A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher”, International Journal of Advanced Technology & Engineering Research (IJATER),
Volume 3, Issue 1, pp 141-147, 2013.

[11] Dr. L. Arockiam, S. Monikandan, St. Joseph‟s College, Trichy, Tamilnadu, India, “Data Security and Privacy in Cloud Storage using
Hybrid Symmetric Encryption Algorithm”, IJARCCE, Vol. 2, Issue 8, August 2013

[12] https://en.wikipedia.org/wiki/Cloud_computing

[13]http://searchcloudprovider.techtarget.com/definition/cloud-services

[14]http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[15]http://datashieldcorp.com/2013/06/04/3-different-data-encryption-methods/

[16] Said Aminzou, Brahim ER-RAHA, Youness Idrissi Khamlichi, Karim Afdel, Mustapha Machkour, “Towards a Secure Access to Patient Data in Cloud Computing Environments,” 978-14 799. {} 324-5/ 13/$31.00 -20 13 IEEE

[17] Chao YANG, Weiwei LIN*, Mingqi LIU, “A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security,” 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies

[18] Johannes K. Chiang, Eric H.-W. Yen, Yen-Hua Chen, “Authentication, Authorization And File Synchronization On Hybrid Cloud -On Case Of Google Docs, Hadoop, And Linux Local Hosts,” 2013 International Symposium on Biometrics and Security Technologies ,978-0-7695-5010-7/13 $26.00 © 2013 IEEE DOI 10.1109/ISBAST.2013.22.

[19] QIAN Quan, WANG Tian-hong, ZHANG Rui, XIN Ming-jun , “A Model of Cloud Data Secure Storage Based on HDFS,” 978-1-4799-0174-6/13/$31.00 ©2013 IEEE