Security Threats - Main Hindrance to the Wide Acceptance of Cloud Computing Services

Prashant Rewagad
Head of the Department
Department of Computer Science and Engg
GHRIEM, Jalgaon

Yogita Pawar
ME (CSE) Student
Department of Computer Science and Engg
GHRIEM, Jalgaon

ABSTRACT

Cloud computing has become new trend, which many enterprises wants to incorporates in their working. Since it relies on sharing of computing resources rather than having local servers or personal devices to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)[3] It is used in consumer-oriented applications such as financial portfolios delivering personalized information, or power immersive computer games. The cloud computing however, has not gained wide acceptance. For which the main reason is security issue. Cloud computing is surrounded by many security issues like securing data, data integrity and examining the utilization of data in cloud by the cloud computing vendors This paper is study of various security threats posed to the data stored in cloud and also threats concerned to both user and vendors in cloud computing. This is a literature survey of various key security threats associated with cloud computing. It also includes a critical analysis of various research papers on same grounds. At the same time it discusses various security models and tools proposed in those papers in order to protect data confidentiality and provide security to the data in cloud computing.

Keywords

Trusted cloud computing, Cloud networking and cloud computing.

1. CLOUD COMPUTING

A. Introduction

The cloud computing is a model for enabling convenient ,on demand network access to a shared pool of configurable resources such as networks, servers, files storage ,applications and services. The Cloud Computing buzz is growing every day with a growing number of businesses and government establishments opting for cloud computing based services [11].

Cloud computing is a type of computing that is comparable to grid computing. Cloud computing relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios or even to deliver personalized information, or power immersive computer games[11].

To do this, cloud computing networks use large groups of servers, usually those with low-cost consumer PC technology, with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Cloud computing has started to obtain mass appeal in corporate data centers as it enables the data center to operate like the Internet work through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner.

B. Cloud services

a. CloudMe

Cloud Me is a best example of cloud storage services, wherein a client can Access, upload and download files from anywhere, even from his very handheld equipments like smart phone. He can access online storage, Photos, Music, Movies, Application development, Calendar, Mail, Media Player, Word Processors etc. It can be used to schedule daily meetings and to set up reminders for birthdays and anniversaries. It has both free and premium signup. It also offers a platform for web developers Platform as a service, PaaS. The guest account is facilitated with free 3GB of CloudMe drive storage.

b. Cloudo

Cloudo is a hosted service in cloud computing, wherein there is no hardware or software to setup and maintain, and the DDE is fully accessible from any internet connected device. Other advantages of utilizing hosted software include centralizing data backup, updates, and security at the data center as well as the benefits of lower cost which can be associated with the administration of a single global instance of software versus many local instances.

c. Mint

It is a personal finance tool based on cloud computing which can manage the money transactions. It came into the market in September 2007. It is recipient of more than 30 prestigious web awards from the CNN Money, Time, Business Week, PC Mag etc. The client has to create an account to have access to all balances transactions together on the web or on the iPhone. All your money related accounts viz. bank accounts, credit card, loans, stock brokerage and other investments in one place. Barclays, ABN Amro and few Europe based banks are supported but one must check at Mint for the specific details.

2. SECURITY ISSUES

A. Problem related to IP Address

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack.

Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward.

B. Problem related to attacks [4]

a. Problem Related to passive Attacks

In passive attacks in cloud, the attacker only watches the transmission of cloud data’s and does not try to modify data packets or don’t do anything that user may realize that someone's watching him. Further it is divided into two types.

b. Release of Message Contents

In release of cloud message contents, the attacker only looks the messages and reads them in an unauthorized way.

c. Traffic Analysis

In traffic analysis, the attacker mask (does not change) the message in such a way that the authorized user either cannot access it or cannot understand the message properly.

d. Problem Related to Active Attacks

This attack involves reading of data messages along the messages and read them in an unauthorized way. In this case, sometimes, the attacker creates his new message and sends it to the destination instead of the original. In such an attack, the actual path of the data changes and the message is sent from user C while it appears to be coming from user A to userB. Sometimes unauthorized user may appear to be an authorized one to the other users as shown below:

In such case, attacker manipulates everything according to his wish. In former case, the message is modified by the attacker. So such an active attack is called modification of messages. In the latter one the message appears to be coming from an authorized user while it is not so; this attacker is called Masquerade.

e. Problem Related to Session level DOS

When a client is successfully authenticated by a service and a secure session is established with the service, the service keeps track of the session until the client cancels it or the session expires. Every established session counts against the limit for the maximum number of active simultaneous sessions with a service. When this limit is reached, clients that attempt to create a new session with that service are rejected until one or more active sessions expire or are canceled by a client. A client can have multiple sessions with a service, and each one of those sessions’ counts toward the limit.

f. Problem Related to Port level DOS

The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. We call this kind of an attack a Distributed Denial of Service (DDoS) attack. Here the hacking program blocks the port that the server sends message.

g. Problem Related to packet level DOS

A packet denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

h. Problem Related to Dictionary Attacks

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities’ dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list called a dictionary (from a prearranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phase dictionary attack) or a bible etc. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily-predicted variations on words, such as appending a digit

i. Problem Related to “Man in the Middle Attack” and Eavesdropping

In the man-in-the-middle attack (often abbreviated MITM), or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straight forward in many circumstances.

j. Problem related to Smurf Attack and Viruses

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. (Sending a packet with someone else's return address in it is called spoofing the return address.) The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

3. LITERATURE SURVEY

This is a brief discussion of the selected ten papers relating to provide data security in cloud computing. Along with the details in paper, its merit and demerits are also discussed, at the end.

Uma Somani, Kanika Lakhani and Manish Mundra [1]: proposed an architecture wherein digital signature along with RSA algorithm, to encrypt the data while transferring it over the network. According to them in order to get rid of problems like security of data, files system, backups, network traffic, host security, their architecture proves to be useful. Since digital signature demonstrates authenticity of a digital document and RSA is the most secure asymmetric algorithm, it solves the dual problem of authentication and security.

This work ensures users about data integrity and prevention of security attacks. Hence the contribution is remarkable but it implies limitation in terms of increasing the cost and processing time

G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom [2]: dealt with the problem of data security in cloud computing with somewhat same approach. They made use of RSA Public keys and Private Keys generated for public and private access. Certificate Binary file is used inside control node configuration file to make sure cloud data flow securely. After certificate activation the control node sends data through Secure Socket Layer. Finally AES algorithm is used for encryption .This unique combination makes this solution best to prevent different types of attacks.

The strength of their work is strong data security against various attacks. The distinguishing part is if a user attempts to login falsely for many times, the system automatically slow down the service and temporarily stop the account service for the particular user.

Volker Fusenig and Ayush Sharma [3] tackle the problem of data security with a new approach called cloud networking. It involves addition of networking functionalities to cloud computing. The architecture and functions between the architectural elements are shown in Figure below.

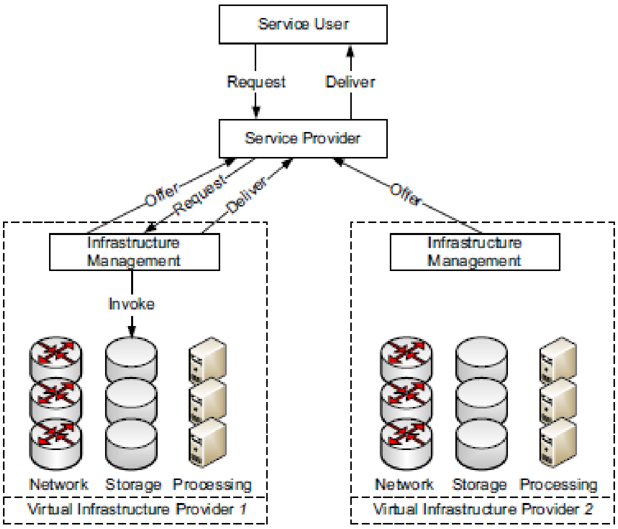

Fig 3.1: An overview of proposed solution[1]

This architecture consists of three functional entities: the service user, the service provider, and the virtual infrastructure provider. The figure shows the different functions which are used to interact between these entities. This architecture preserves the security goals of service users while at the same time benefiting from the flexible and dynamic placement of virtual resources at different virtual infrastructure providers.

The innovative concept proved to be useful but its strength depends on the strategy chosen to enforce security.

On similar footsteps Zhang Xin Lai Song-qing and Liu Nai-wen [4] designed a security cloud cube model: CCM DSM (Cloud Computing Multi-dimension Date Security). Their model makes use a hierarchical defending architecture with three layers wherein first layer for users' authentication (digital certificates), second layer for encryption of users' data and third layer for fast recovery of users' data.

The proposed work addresses Multi-dimension Data Security but is only applicable to sales applications. Hence it is not widely accepted solution.

M. Sudha, Dr.Bandaru Rama Krishna Rao and M. Monica [5] proposed a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality. Cloud environment is created using wired and wireless LAN networks wherein programming is done using JAVA. And Advanced Encryption Standard security algorithm is used for ensuring security in the framework.

This work is on same terms as discussed earlier; just the difference is it takes care of data confidentiality only while downloading any file from cloud server at the client’s end. The weakness is that it requires compatibility between cloud services

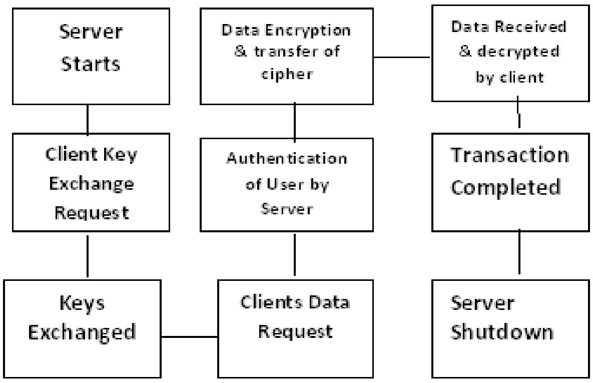
Server Starts
Data Encryption & transfer of cipher
Data Received & decrypted by client
Client Key Exchange Request
Authentication of User by Server
Transaction Completed
Keys Exchanged
Clients Data Request
Server Shutdown

Fig 3.2: An overview of Data Protection framework[5]

As per Eman M.Mohamed and Hatem S. Abdelkader [6] Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. Thus their paper investigates the basic problem of cloud computing data security. They presented the data security model of cloud computing based on the study of the cloud architecture. They implemented software to enhance work in a data security model for cloud computing. Finally they applied this software in the Amazon EC2 Micro instance for evaluation process.

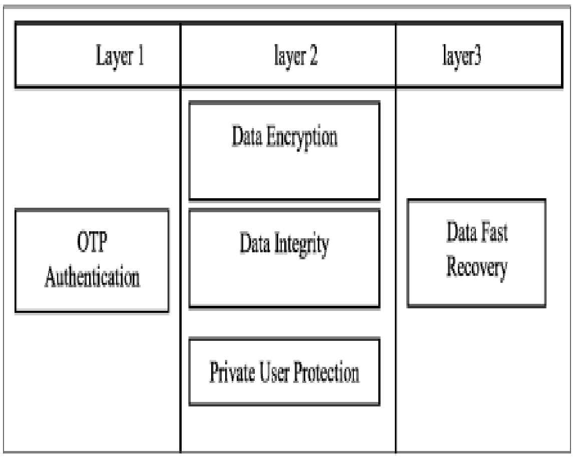

Fig 3.3: A Proposed data security model in cloud computing[6]

As per Deyan Chen and Hong Zhao [7] from the consumers' perspective, cloud computing security concerns are specially data security and privacy protection issues which remain the primary inhibitor for adoption of cloud computing services. They provided a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then they discussed some current solutions in their paper. Those solutions includes a fully homomorphic encryption scheme developed by IBM in June 2009. This scheme allows data to be processed without being decrypted. Then decentralized information flow control (DIFC) and differential privacy protection technology applied by Roy I and Ramadan HE into data generation and calculation stages in cloud and put forth a privacy protection system called airavat.. This system can prevent privacy leakage without authorization in Map-Reduce computing process. Finally, they described in their paper future research work about data security and privacy protection issues in cloud.

The strength of their work is the framework proposed to address data security and privacy. The weakness is that it just a theory which depends on other scheme and policies for its implementation.

D.Kesavaraja, R.Balasubramanian and D.Sasireka [8] proposed Cloud Data Servers concept. It is used as novel approach for providing secure service to e-business. Numbers of users surfing the Cloud for various purposes increases day by day. For this we need highly safe and persistent services. Usually hackers target particular Operating Systems or a Particular Controller. Inspite of several ongoing researches Conventional Web Servers and its Intrusion Detection System might not be able to detect such attacks. So they have implemented a Cloud Data Server with Session Controller Architecture using Redundancy and Disconnected Data Access Mechanism. They generated the hash code using MD5 algorithm. With the help of which even the attacks can be circumvented, which are undefined by traditional Systems .They have implemented Cloud Data Sever using Java and Hash Code backup Management using My SQL. They have also used AES Algorithm for providing more Security for the hash Code. The CDS using the Virtual Controller controls and monitors the Connections and modifications of the page so as to prevent malicious users from hacking the website. In this proposed approach an activity analyzer takes care of intimating the administrator about possible intrusions and the counter measures required to tackle them. The efficiency ratio of the approach is 98.21% compared with similar approaches, according to them.

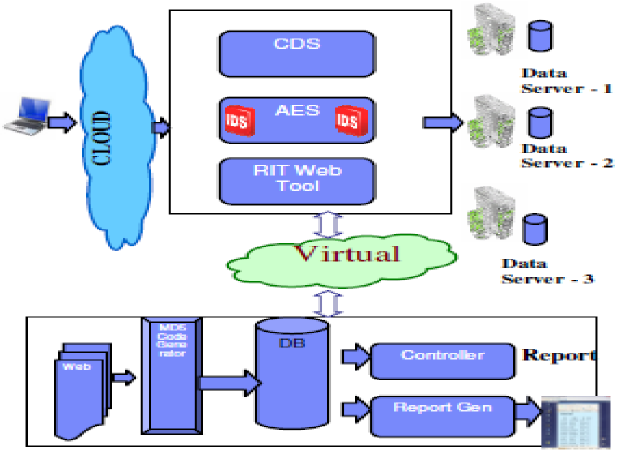

Fig 3.4: An overview of cloud data server [8]

Rituik et al [9] have focused on the metering issue or verification of job,wherein the users of cloud services can verify the cost charged by the service providers with respect to services they availed. Different types of security attacks are discussed and solutions are proposed for each type of attack. Numerous serious security problems faced by users of cloud services are reviewed in depth specially the metering issue and backup of user data. These issues are addressed in attacker model and solutions for each problem are also proposed. A simulation program is developed for eBay model. The results of simulation showed that proposed solutions attain sensible detection rate with inexpensive operating cost. The simulation software developed was deployed on a normal Intel core 2duo machine having 1GB ram. The simulation

program is coded in JAVA programming language. The program is able to simulate 1000 online shops, using different parameters deeds of the cloud computing server and online merchants are simulated. During the process of simulation It was observed that the cloud computing server misses few inventory parts.
The strength of their work is the framework proposed to address metering issue. Their proposed tool enables users to verify billing details by service provider and prevention of security attacks. The weakness is that it is only applicable to sales applications.

As per Sherif El-etriby and Eman M. Mohamed [10] the complexity of cloud computing create many issues related to security. Since Clouds typically have single security architecture but has many customers with different demands. They mainly focused on the data storage security in the cloud and the desktop. Modern Encryption algorithms mainly used for data security of cloud computing namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-Fish are evaluated at two independent platforms namely; desktop computer and Amazon EC2 Micro Instance cloud computing environment. The evaluation has been performed for those encryption algorithms according to randomness testing by using NIST statistical testing in cloud computing environment. This evaluation uses Pseudo Random Number Generator (PRNG) to determine the most suitable technique and analysis the performance of selected modern encryption techniques. Cryptography algorithms are implemented using Java Cryptography Extensions (JCE). Simulation results are shown to demonstrate the effectiveness of each algorithm.

Table 3: An overview of Evaluation modern encryption algorithms in Amazon EC2

Amazon EC2	**1**	**2**	**3**	**4**
P-Value	RC6	AES	Blow-Fish	DES/RC4
Rejection-Rate	DES	AES	Blow-Fish	RC6/Rc4
Time consuming	Blow-Fish	DES	AES	RC4

The strength of their work is the statics they provided in the tabular form. The weakness is it is just evalution not a standalone solution.

4. COMPARISON AND ANALYSIS

We have studied various research papers with respect to security and privacy threats in cloud computing. Wherein some papers have proposed different tools while other have proposed architecture to address security and privacy concerns in cloud computing . Whereas other papers have just identified some more security and privacy issues. After proper study we have summarized in the following compare and contrast table

Table 4: Critical analysis of Ten selected research papers based on providing data security in cloud computing services.

Lit Ref	**Context of Research**	**Problem Specified**	**Technique used**	**Solution proposed**
1	Enhance Data Security	Data integrity assurance	Digital signature with RSA Algorithm	Yes
2	Implementation of Data Security	security and confidentiality for their business critical application	Combination of SSL through key generation, certificate (BIN file) and AES algorithm	Yes
3	Security Architecture for Cloud Networking	security requirements in the cloud networking infrastructure.	A proposed security architecture	yes
4	Data Security Model	Data security issues at three different levels	Cloud Computing Multi-dimension Date Security CCM DSM	Yes
5.	Ensure Secure Data Communication	User authentication and data confidentiality	Data Protection framework	Yes
6.	Enhanced Data Security Model	Data security	Data security model and its testing in Amazon EC2 Micro instance	Yes
7.	Data Security and Privacy Protection	data security and privacy	Discussed some current solution like airavat, homomorphic encryption scheme developed	No

			by IBM etc	
8.	cloud data server(CDs) for providing secure service	Data security and different types of cyber attacks	Cloud Data Server along with AES algorithm	Yes
9.	Addressing security issues in cloud computing.	Metering problem, Proof of work, Attack scenarios & data Backups	A simulation program that is coded JAVA, the program is able to simulate 1000 online shops, using different parameters deeds of the cloud computing server and online merchants are simulated. During the process of simulation It was observed that the cloud	Yes
10.	Evaluation of various encryption algorithm	Data security	-	No

5. PROPOSED ARCHITECTURE

In our proposed architecture, we are also trying to interrogate the problem of data security using three ways protection scheme. Three ways protection means we are using diffie hellman algorithm for encryption keys exchange, digital signature for authentication and finally AES for encryption of user's data.

To upload a file, first key are exchanged using some encryption algorithm then the client is authenticated using digital signature. Finally user's data file is encrypted using AES and uploaded to the cloud server. Now when client is need of same file, it is to be downloaded from cloud server. For that purpose, when user login ,first encryption keys are exchanged, file to be downloaded is selected, authentication takes place using digital signature then, AES is used to decrypt the saved file and client can access the file.

6. CONCLUSION

After doing literature survey on several papers, we come up to a conclusion that some more techniques are to be blended with encryption algorithms and digital signature. Until now only privacy and authentication are the problems mentioned and tackled with.

It is clear that every paper along with its proposed solution has some advantages and disadvantages. Hence today we are in need of a full proof solution to provide data security and assure integrity of data stored in cloud. Our architecture tries to fulfill the requirement upto a certain extent.

7. FUTURE SCOPE

Verification is also an important issue to be consider for data security in cloud computing. Therefore it is advisable to develop a architecture which will be capable of preventing and or detecting various cyber attacks as well. For this a suitable combination of encryption algorithm, authentication techniques attack proof technology and verification technique is needed. Even trusted computing can be used for the same.

8. REFERENCES

[1] Uma Somani , Kanika Lakhani and Manish Mundra presented "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" at IEEE 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010)

[2] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom presented " Implementation of Data Security in Cloud Computing" at International Journal of P2P Network Trends and Technology- Volume1Issue1- 2011

[3] Volker Fusenig and Ayush Sharma Security ,"Architecture for Cloud Networking" presented at IEEE 2012 International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium .

[4] Zhang Xin Lai Song-qing and Liu Nai-wen presented Research on Cloud Computing Data Security Model Based on Multi-dimension 2012 IEEE Internatinal symposium on information technology in medical and education .

[5] M. Sudha, Dr.Bandaru Rama Krishna Rao and M. Monica published "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" at International Journal of Computer Applications (0975 – 8887)

[6] Eman M.Mohamed and Hatem S. Abdelkader presented "Enhanced Data Security Model for Cloud Computing" at The 8th International Conference on INFOrmatics and Systems (INFOS2012).

[7] Deyan Chen and Hong Zhao presented "Data Security and Privacy Protection Issues in Cloud Computing" at IEEE 2012 International Conference on Computer Science and Electronics Engineering.

[8] D.Kesavaraja, R.Balasubramanian and D.Sasireka published " Implementation of cloud data server(CDs) for providing secure service in E business" in International journal of Database Management System (IJDMS) vol-2, no-2 2010.

[9] Dan Lin & Anna Squicciarini, presented "Data Protection Models for Service Provisioning in the Cloud" at SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA

[10] Sherif El-etriby and Eman M. Mohamed presented "Modern Encryption Techniques for Cloud Computing" at ICCIT 2012.

[11] Farzad Sabahi, "Cloud computing security threats and responses" presented at Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference

[12] Jianfeng Yang and Zhibin Chen "Cloud Computing Research and Security Issues", presented at Computational Intelligence and Software Engineering (CiSE), 2010 International Conference.