International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Cloud Data Security Using Filters Authentication and Encryption

Ashim Sarkar
Senior Faculty, NIIT, Ranchi Jharkhand India

ABSTRACT

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud is a technology invention. It provides the computational resources (Server, Storage, OS and Network) to user as service based on demand. Cloud computing has emerged as a popular solution to provide cheap and easy access to externalized Information Technology resources. An increasing number of organizations benefit from Cloud computing to host their applications [1]-[2]. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.Cloud computing eliminates the need of having a complete infrastructure of hardware and software to meet users requirements and applications. It can be thought of or considered as a complete or a partial outsourcing of hardware and software resources. To access cloud applications, a good Internet connection and a standard Internet browser are required. The National Institute of Standard and Technology defines cloud computing in the following way: Cloud Computing is a model for enabling convenient, on demand network access to share pool of configurable computing resources e.g. networks, services, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider interaction [6].Many vendors declared that adoption of this technology can bring many benefits to the users such as cost reduction, convenience and continuous availability, scalability and performance, quick deployment and ease of integration, yet some organization are still not feeling comfortable in adoption of this technology due to concerns of trust and security *e.g.*, data security is one of them [7, 8]. One of the best ways to ensure confidentiality of secret data in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage [10]. To protect user‘s secret data in the cloud, encryption is considered as essential tool that can be used efficiently. User can confidently utilize cloud services by knowing that their confidential data is protected by encryption.In cloud computing, Security of file or data is provided to the end user in the private cloud environment. The main concern is to provide the security to end user to protect files or data from unauthorized user. Difference is that the research is done in cloud, but security related issue can’t be resolved completely. Security is the main intention of any technology through which unauthorized users can't access your file or data in cloud. In this research work we are going to resolve cloud data security issues through Filter Authentication and Encription.In particularly, we intend to discuss cloud security requirement and data privacy issues. In this research work we are proposing three layers of security architecture using Filters as First Layer Authentication as second Layer and encryption as third Layer to provide complete data security in the cloud.

Keywords: VPN, Authentication, Security, Filtering, Encryption

I. INTRODUCTION

1.1 Essential Characteristics of Cloud Computing

1.1.1 On-demand Self Service : Cloud provides various computing capabilities to the consumers. A consumer can utilize computing resources like servers, network storage, as needed automatically without any human interaction.

1.1.2 Broad Network Access- The network provides extensive capabilities that can be accessed by thin or thick clients following the standard mechanism.

1.1.3 Resource Pooling : The service provider have a reservoir of resources for the consumers. It can serve multiple consumers using multi-tenant model. The various physical and virtual resources are dynamically allocated to the consumers according to the demand. At lower level of abstraction the consumers have no control or knowledge over the exact location of the resources (location independency) but may be able to specify location at higher level.

1.1.4 Rapid Elasticity : Capabilities can be rapidly and elastically provisioned to scale out and rapidly released to scale in. the capabilities available for provisioning appears to be unlimited to the consumers. The consumers can purchase or release in any quantity at any time.

1.1.5 Measured Services- Cloud provides proper measuring of services and resources. Resource utilization is monitored, controlled and reported to provide transparency for both consumer and service provider.

1.2 Models of Cloud Computing

1.2.1 Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

i) Public Cloud
The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

ii) Private Cloud
The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature, e.g. Microsoft private cloud;

iii) Community Cloud
The Community Cloud allows systems and services to be accessible by group of organizations.
e.g. Government community cloud by Microsoft.

iv) Hybrid Cloud
The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud. e.g. VMware hybrid cloud provider.

1.2.2 Service Models

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

There are many other service models all of which can take the form anything as a Service. This can be Network as a Service, Business as a Service, Identity as a Service, Database as a Service or Strategy as a Service. The Infrastructure as a Service (IaaS)is the most basic level of service.

Infrastructure as a Service (IAAS)
Infrastructure as a service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Platform as a Service (PAAS)
Platform as a service provides the runtime environment for applications, development & deployment tools, etc.

Software as a Service (SAAS)
Software as a service model allows to use software applications as a service to end users.

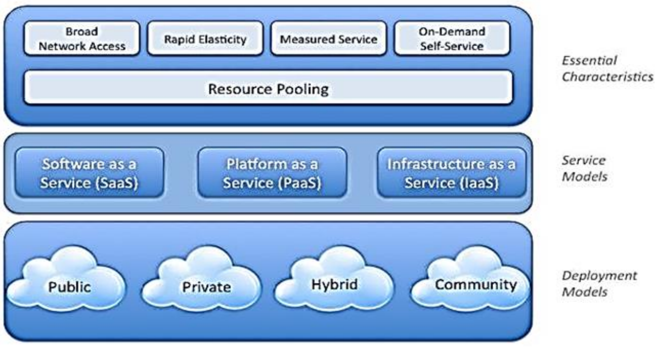


Figure 1. NIST Characteristics and deployment models of Cloud Computing

1.3 Life Cycle of Data in Cloud

The typical lifecycle of data can be described as the following stages:-

1.3.1: Data Creation/Transmission this is the initial stage, data is created by the user and then pushed to the Cloud for consumption.

1.3.2: Data Reception data is received in the Cloud before being written to storage and logs taken of activity.

1.3.3: Output Preparation data is prepared to be returned to the consumer, this involves any transformations that needs to be performed on the data prior to its return i.e. Serialisation.

1.3.4: Data Retrieval data is received by the consumer from the cloud and has now within the domain of the user.

1.3.5: Data Backup the Cloud Service Providers will replicate data for archival purposes. This may involve the transferral of a copy of the data to an external store.

1.3.6: Data Deletion data is permanently deleted from the cloud.

1.4 Encryption

Secure client authentication prevents unauthorized network access. For complete security, client data should be secured as well. Data encryption is one way to secure client information.

There are two main categories of encryptions used in cryptography to achieve data confidentiality, integrity, availability, authentication and non-repudiation. Non-repudiation means that when something has been sent from someone, there has to be a way to track back to the sender. There are symmetric and asymmetric encryption algorithms.

1.4.1 *Shared-key,* or *symmetric, encryption* systems, the same key is used both to encode and to decode the message. The secret key must somehow be communicated securely between the two parties to the communication.

1.4.2 *key-pair,* or *asymmetric, encryption* systems, each party has two keys: a *public key*, which anyone can obtain, and a *private key*, known only to the individual. Anyone can use the public key to encrypt data; only the holder of the associated private key can decrypt it.In this research work we will use Java Cryptographic Extensions (JCE) which is a set of Java API's which provides cryptographic services such as encryption, secret Key Generation, Message Authentication code and Key Agreement. The ciphers supported by JCE include symmetric, asymmetric, block and stream ciphers.

2. Problem Statement

Data security is a key feature for cloud computing, by consolidation as a robust and feasible multipurpose solution. This viewpoint is shared by many distinct groups, such as academia researchers, business decision makers and government organizations [2]. The many similarities in these perspectives indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing.

These concerns include not only existing problems, directly inherited from the adopted technologies, but also new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization [4]. Data security is the number one issue when it comes to cloud computing. Since a third party stores business data, it is never known what’s going on with the data. Along with the benefits of BPO comes an increased risk to data. If the Organization cannot protect its data, the business is at risk. However, the organization constricts the use of data too much; the restriction can paralyse the outsourcing effort and finally the business itself [6].

Today cloud computing make everything flexible and easier but there is another aspect that is what about security of user’s data? Is cloud computing in current scenario is providing confidentiality, integrity and being regulated by compliance like Data Protection Act [1]. Through cloud computing the resource are centralized, so the exposure factor proportionally increase which results in risk. So it is necessary to put a countermeasure to mitigate the potential risk. With the rapid development of modern technology, we face many security challenges in the storage of data in online especially in the cloud. The problem is to find efficient protocol which avoids unnecessary overhead to the user in checking the integrity of their own data and also it should support dynamic data operations instead of just achieve and back up the data files in the cloud.Therefore, the research questions addressed by our research are following:

Question 1: What security approaches have been used to ensure data security in cloud computing?

Question 2: How the approaches have been validated?
So only Encryption is not sufficient to solve the security issues therefore our proposed model of three layers of security is better than existing solutions, because in first layer Filters will be used to block Black listed IP address to access the cloud data. In second layer authentication is used so that only user with valid userid and password can access their data and this authentication will done by using sql server as back end. In third layer of security encryption will be used in this encryption first data is changed in cypher text and then only data will be uploaded in the cloud during uploading a key will be generated in the sql server and same key have to use by cloud user to decrypt their data , thus in third layer we will provide additional security by generating an decryption key which will store in sql server and user will able to decrypt their data by providing this key during decryption.

3. Literature Review

An extensive study of the existing work in the area of the cloud implementation has been carried out to understand the extent of the research work done in this area. The significant research papers, articles and other published work of different researchers have been studied. A detailed relevant research work in this domain has been presented below. There has been an increasing interest of researchers in the field of cloud computing to make it the best technology. That is why lot of research has been going on in this field. The biggest concern of current cloud computing system is auditing of the security controls and mechanisms in terms of user level [3].

There are various encryption algorithms used in cloud computing for user data privacy and security. One of technique of user data security is TPA (Third Party Auditor) between client and cloud service provider, which acts as external auditor to audit the user outsource data. This scheme provides secure and efficient dynamic operations (data update, delete and append) on data blocks stored in the cloud [4]. But what happen when data is transfer from user to cloud, there is no mechanism for security between user and cloud.

Data security and privacy risks are mitigated through data encryption and it is the Cloud Service Providers responsibility to handle these elementary risks [6]. To ensure data integrity, confidentiality and availability, the storage provider should offer encryption schema and scheduled data backups [7]. Cloud Service Provider is responsible to adopt added security measures to ensure data security. These security measures involve the use of strong encryption techniques for data security and fine-grained authorization to control user access to data [8]. Providers are more responsible for the privacy and security of data and application services in public than in private clouds [9]. The major problem with data encryption is the responsibility of key management. Ideally, it’s the data owners. But due to the lack of user expertise to handle the keys, they usually hand over the key management to Cloud service Provider. But again it will become more difficult for Cloud service provider to maintain keys for a large number of users [10, 11]. Cloud service Provider is the one responsible for the security of the data while is being processed, transferred and stored [12]. Cloud Service Provider does not have permission for access to the physical security system of data centres rather they must depend on the infrastructure provider to get full data security. The Cloud Service provider can only specify the security settings remotely, and don't know either they are fully implemented or not. It is major security risks for Cloud Service Provider if the security settings are not fully implemented [13].

Another technique IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages[5]. Compared with typical public key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators.

Suppose a user wants to login to a secured cloud system. To login into a system we must provide a correct combination of user name and password and it should be matched with the combination stored in the database whether in plaintext form or in encrypted form. For a secured login user provide login credentials and then to authenticate the user system encrypts the provided password up to the number of times defined to the system [6]. Above technique is only for secure user id and password but this technique is not use in user data which is stored by user in to the cloud. So our proposed algorithms provide encryption of user data by performing encryption technique and transfer user data in encrypted form from user to cloud.

Identity and Access Management improves operational efficiency, regulatory compliance by managing the major security concerns, automated provisioning, authentication and authorization services.

To avoid unauthorized access, the CSP should offer strict access control mechanism. In cloud computing administrative access is done through the internet and this increases the risk of unauthorized access to data and resources. Therefore, it is very important to control and monitor the administrative access to maintain data integrity [7]. Data in the cloud is globally distributed which brings the issue of jurisdiction and privacy [11]. According to study only 37% of cloud providers were confident about security to authenticate users before granting access, whereas 50% of cloud users considered Identity and Access Management as the cloud provider's responsibility. Therefore, achieving compliance requirements could be problematic [15]. when the data is outsourced to a cloud, enforcing secure and reliable data access between several users is very critical. The user cannot even trust the server because the user's private data can be exposed in the event of server compromise. The solution is to encrypt data in differentiated manner and disclose the corresponding decryption keys only to authorized users. This approach has a drawback of performance loss and scalability [16].Gartner list seven security issues from Cloud Service Provider perspective. The data security and privacy risks include privileged user access, which inquires about who has access to data [17].

Multi-tenancy is an essential attribute of cloud computing as it increases the use of underlying hardware resources and allowing for efficient resource provisioning.Multi-tenancy security and privacy is one of the critical challenges for the public cloud [16]. It is the responsibility of Cloud Service Provider to ensure an isolated boundary for each user's data at both physical and application levels [8]. It is possible that the customers' personal and financial data are stored by the Cloud Service provider. Therefore, Cloud service Provider is responsible to secure the customers' data. Some providers use job scheduling and resource management, but most providers employ Virtualization to maximize the use of hardware [18]. These two methods allow attackers to have full access to the host and cross- Virtual Machineside channel attacks to extract information from a target Virtual Machine on the same machine. In multi-tenancy, data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high [12]. Data is placed in a shared environment with the data from other clients which poses a great risk of multitenancy for Cloud Service Provider. There is a need for some mechanism through which Cloud Service provider must guarantee data isolation between clients and they also should be liable for ensuring this isolation [19].

No doubt, the latest innovations in cloud computing are making business applications even more mobile and collaborative. However, there are certain challenges to be addressed in this technology. The issue of vulnerability is one of them. In fact, vulnerability and security are closely related to each other. So, a vulnerable system cannot be secure [7].

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to such providers. Although the cloud computing vendors ensure more secure password protected accounts, any sign of security breach would result in loss of clients and businesses.

4. Objective of the Study

The purpose of this paper is to provide an overview of cloud computing and security of the confidential data that the data owner store on the cloud storage server, to preserve the data integrity while it is transmitted from data owner to Cloud Service Provider(CSS) and downloaded by the authorized client.So the following are the objectives of the study

4.1 Creating secure cloud architecture.
4.2 Cloud data access control and key management.
4.3 Identification and privacy in cloud.
4.4 Dynamic data operation security.
4.5 To develop a system that wills Provide Security and Privacy to Cloud Storage.
4.6 To Establish an Encryption Based System for protecting Sensitive data on the cloud.

4.7 To develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site by using a private key.

5. Research Methodology

Research methodology is the way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically.
A literature survey was carried out on the study area before the experimental work started.
Here I am using the synthetic data collection technique for security issues such as.

5.1. Open access Research papers.
5.2. Web links.
5.3. Published books.
5.4. Technical Research articles.
Relevant information is extracted after analysing the data as per our topic requirement.

6. Significance of Study in Cloud Data Security

To find out and organize the information related to cloud security and to provide complete security of data, the cloud security area group them into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues.This research paper identifies the main problem in Cloud which is data security and tries to overcome it by using three layers of data protection. The popularity of Cloud Computing is mainly due to the fact that many enterprise applications and data are moving into cloud platforms; however, lack of security is the major barrier for cloud adoption [6]. According to a recent survey by International Data Corporation (IDC), 87.5% of the masses belonging to varied levels starting from IT executives to CEOs have said that security is the top most challenge to be dealt with in every cloud service [10]. Many of the threats found in existing platforms. Out of them, the Security Threat is considered to be of High Risk [3].

7. Proposition of the Research work

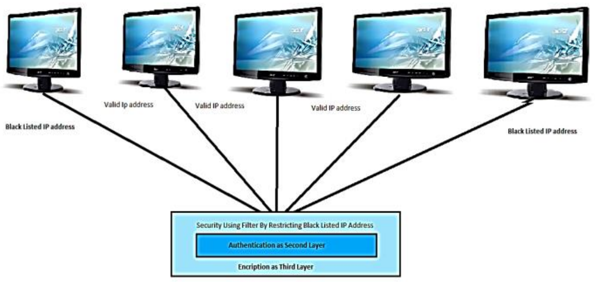

Valid Ip address
Valid IP address
Valid IP address
Black Listed IP address
Black Listed IP address
Security Using Filter By Restricting Black Listed IP Address
Authentication as Second Layer
Encription as Third Layer

Figure 2. Proposed security model by using three layers of protection

Research comprises defining and redefining problems, formulating hypothesis or suggested solution collecting organizing and evaluating data making deductions and reaching conclusions and at last carefully testing the conclusion to determine whether they fit the formulating hypothesis. After collecting analyzing and defining the cloud computing security issues the suggested solution and future related experimental work is:-

7.1 First Layer of Security by using Filter

The filter provides a basic security mechanism for a firewall to determining what traffic passes through the firewall based on IP address details. This protects the secure network from outsiders. A filter is an object that performs filtering tasks on request and response. A FilterConfig object used by a servlet container used to pass information to a filter during initialization. Filters are registered in web.xml (deployment descriptor) of a web application.

The most easiest and effective way of minimize the risk from outside attacks is to filter incoming requests based on the IP address of the client. For example, if you have few web addresses that make requests using 192.168.10.145, 192.168.10.146, 192.168.10.147 and 127.0.0.1 and if you wish to restrict the application access from 192.168.10.145, 192.168.10.146 or any other available IP then it will be possible using Filter. So in this proposed system we can restrict or block the access of resources based on a particular IP address by using filter. You can apply the filter for request, response, and forward condition not only for incoming request but also for outgoing responses. By default administrators are able to access all the data's but using filter you can restrict an administrator to accessing your confidential data, such features are not available in firewall. So here we are using filter to make our cloud data completely secure.

7.2 Second Layer of Security by using Authentication

Our authentication technique will help to more secure user data within a cloud so user can trust on their data security. In authentication technique we provide secure authentication of user data such as first user login into the cloud with user name and password and the password is stored in database in encrypted form you can't decrypt it thus making the authentication more and more secure. In the suggested system all the login and access details are save in database and only authenticated user can see all the previous login records with date and time.

7.3 Third Layer of Security by using Encryption

Our proposed encryption algorithm provide user side file encryption in that when user upload file at that time file is encrypt and then store in to the cloud. Without worrying about security issue more and more user can move their data on cloud and enjoying cloud storage service. In this encryption only authenticated user can decrypt their own data after providing valid userid and password and not any other user able to decrypt the data so it will offer maximum security of your personal and private data.

One of the most common ways the hacker hack your password is by using a trojan. Many of them inbuilt key loggers, so whenever you type anything on your keyboard, it goes to them. To enhance the security while logging into secure websites is by using virtual keyboard, so there will be also virtual key board concept during authentication mechanism thus it is completely secure against any malicious programme or hacker. Thus the proposed system will provide filter authentication, encryption and virtual keyboard concept to solve the data security risk associated with cloud computing.

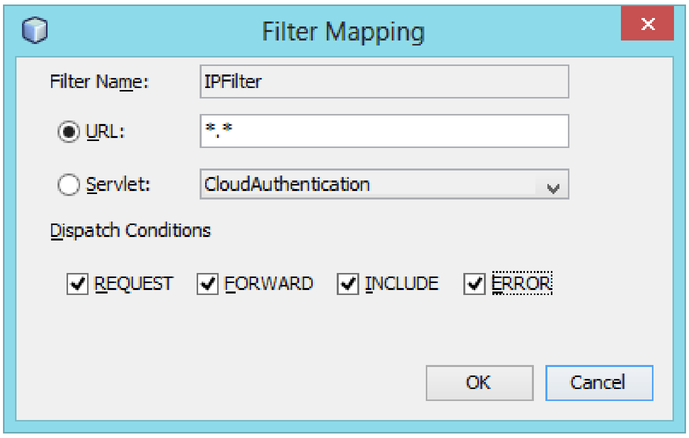
The proposed research work implementation will be done by using NetBeans IDE and Sql server as back end by using following steps:-
i) First the user interface of the proposed model will be designed.

ii) Then all the security implementations will be done by using servlet or jsp in MVC (Model-View-Controller) architecture.

iii) Finally testing will be done by deploying the system in local webserver and accessing the same through different system.

Prototype of the cloud data storage system

Step-1



Filter Mapping

Filter Name: IPFilter

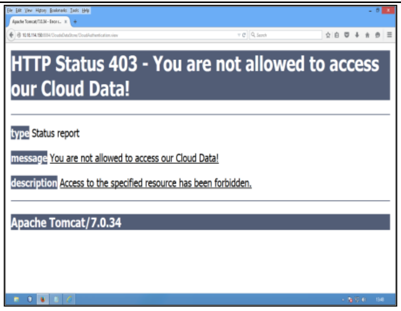
● URL: *.*

○ Servlet: CloudAuthentication

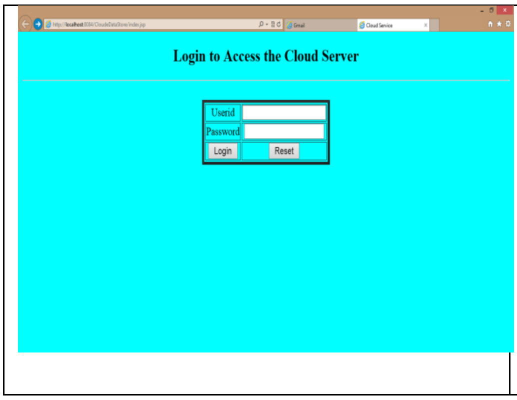
Dispatch Conditions

☑ REQUEST ☑ FORWARD ☑ INCLUDE ☑ ERROR

http://localhost:8084/CloudeDataStore/CloudAuthentication.view

 10.18.114.150:8084/CloudeDataStore/CloudAuthentication.view HTTP Status 403 - You are not allowed to access our Cloud Data! type Status report message You are not allowed to access our Cloud Data! description Access to the specified resource has been forbidden. Apache Tomcat/7.0.34	1. First layer of security using filter by blocking black listed IP address to access our Cloud Data Store and preventing further misuse of your private and confidential data.

Step-2

 http://localhost:8084/CloudeDataStore/index.jsp Login to Access the Cloud Server Userid Password Login Reset	2) In second layer user have to give their valid userid and password and after validation they can use cloud data

	storage system. in our Cloud system Administer are not allowed to access your important and private data only authenticated user can able to access their own data. so, our cloud system is fully secure against any misuse of your data.

Step-3
Authenticated User has to select the data want to upload in to the cloud data store, after that by using java cryptographic extension plain text converted into cipher text. Only cipher text will be uploaded in to the cloud making it more secure.

During uploading a private key will be generated along with the encryption key. Both the keys will be store in Sql server in encrypted format so the database administrator also unable to read your keys.

Whenever any authenticated user try to download his data he/she has to provide the encryption key along with private key and the same will be validated against the key store in the Sql server if the keys will be matched then data will be downloaded. So the data stored in the cloud is completely secure.

II. REFERENCES

[1]. J.Srinivas, K.VenkataSubba Reddy and Dr.A.MoizQyser, ”Cloud Computing Basics”, International Journal of Advanced Research in Computer and Communication EngineeringVol.1, Issue 5, pp 343-347, 2012.

[2]. Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, ”The Characteristics of Cloud Computing”, 39th International

[3]. Gartner, “What you need to know about cloud computing security and compliance”, (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013).

[4]. Z. Yandong and Z. Yongsheng, “Cloud computing and cloud security challenges in Information Technology in Medicine and Education (ITME)”, 2012 International Symposium on, (2012), pp. 1084-1088.

[5]. “Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0”, https://cloudsecurityalliance.org/research/security-guidance/

[6]. NIST Definition of cloud Computing V15 http://csrc.nest.gov/groups/SNS/cloudcomputing/clouddef- V15.doc

[7]. Harauz, J., Kauifman, M., Potter, B.: Data Security in the world of cloud computing. IEEE Security & Privacy 7(4), 61–64 (2009)

[8]. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2011)

[9]. Takabi, H., Joshi, J.B.D.: Security and Privacy Challenges in Cloud Computing Environments. Published. IEEE Security and Privacy 8(6), 24–31 (2010)

[10]. Chen, D., Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing. In: Int. Conference on Computer Science and Electronics Engineering, pp. 647–651 (2012)

[11]. Rahul, S.S., Rai, J.K.: Security & Privacy Issues In Cloud Computing. International Journal of Engineering Research & Technology (IJERT) 2(3) (March 2013)

[12]. Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications 4(5) (2013)

[13]. Reddy, V.K., Thirumala, R.B., Reddy, L.S.S., Kiran, S.: Research Issues in Cloud Computing. Global Journal of Computer Science and Technology 11(11) (July 2011)

[14]. Argall, K.: Compliance in a Cloud Computing Environment. HIPAA and PCI DSS (2010)

[15]. Ren, K., Wang, C., Wang, Q.: Security Challenges for the Public Cloud. Journal of InternetComputing IEEE 16(1) (2012)

[16]. Lovell, R.: White Paper: Introduction to cloud computing (October 2009)

[17]. Pearson, S., Benameur, A.: Privacy, Security and Trust Issues Arising from Cloud Computing. In 2nd International Conference on Cloud Computing Technology and Science (2010)

[18]. Ayala, L.C., Vega, M., Vargas, L.M.: Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing. In: Elleithy, K., Sobh, T. (eds.) Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. LNEE, vol. 152, pp. 37–52. Springer, Heidelberg (2013)

[19]. Rana, S., Joshi, P.K.: Risk Analysis in Web Applications by Using Cloud Computing. International Journal of Multidisciplinary Research 2 (January 2012)

[20]. Khajeh- Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P.: Decision Support Tools for Cloud Migration in the Enterprise. In: IEEE CLOUD 2011 (November 2011)

[21]. D. Catteddu and G. Hogben, “Cloud computing: Benefits, risks and recommendations for information security”, European Network and Information Security Agency (ENISA), pp. 1–125.

[22]. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1-11.

[23]. T. Dillon, C. Wu and E. Chang, “Cloud computing: issues and challenges”, Paper presented at the Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. (2010).

[24]. AmanBakshi and Yogesh B, “Securing cloud from DDOS Attacks using Intrusion Detection System in VM”, IEEE, 2010, pp. 260-264.