Cloud Computing Security Threats

Arif Mohammad
System Analyst
Distance Education
University of Kashmir, Srinagar
arifmohammad.001@gmail.com

Tawseef Ahmed
Assist. Professor
Department of Computer Applications
Amar Singh College
Srinagar
mtawseef805@gmail.com

ABSTRACT

The IT industry has seen tremendous extended capabilities due to the fast growing development in the cloud computing. It is no longer just a business concept. It has revolutionized the enterprise fundamentals and businesses have bloomed. Cloud computing does not encompass a single technology. It is an amalgamation of many different technologies, models and tools to provide services at different levels. Cloud computing has scaled up to many heights but one of the most important concern is the security issues in cloud environment. The market has shown reluctance towards the full adaptation of cloud computing due to the issues of data privacy and security. In this paper we study different security and privacy issues in the cloud networks and the possible solutions to cope with each issue.

Keywords: *Cloud computing, business, privacy, security, network*

Introduction

Cloud computing is the latest technology in the modern world [1-3]. Cloud computing is the present technology in the field of distributed computing. The adoption of this technology is growing day by day because it facilitates the users to utilize the services through the use of shared pool of resources without the installation of any software. It provides various services to the user at lower cost and extended capabilities, Figure 1.

Figure 1. The Cloud Environment

Cloud computing offers a vast number of services with massively scalable resources [4-5] which are provided to the customers as a service over the internet. Cloud provides services at three different levels Figure 2. Infrastructure as a service (IaaS) is used when the basic infrastructure for computing is provided like cpu power, memory, storage etc. Cloud can also be used to provide the services of deploying dynamically scalable java or python based web applications and this type of service is known as Platform-as-a-Service (PaaS). Software-as-a-service (SaaS) lets users use the readily available applications anytime anywhere over the internet. Amazon's Elastic Cloud (EC2) is an example of IaaS while as Google App Engine is an example of PaaS. The services at all three layers Figure 2., have brought down the expenses of businesses significantly.

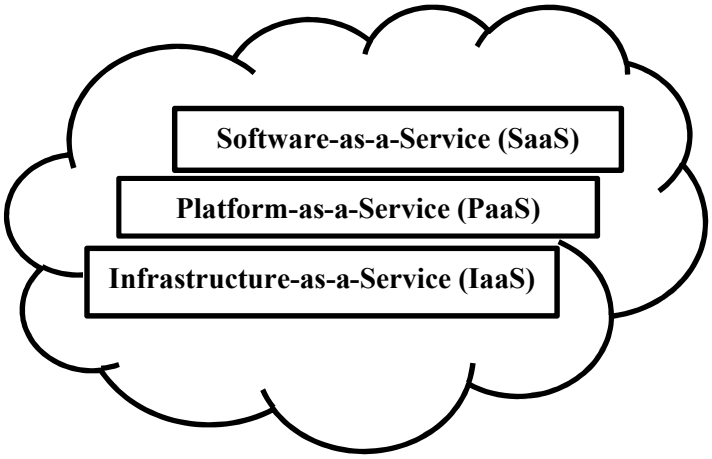

Figure 2. The Cloud Layers

The low hardware costs and reduced licensing costs have helped many small and medium sized businesses to bloom. Cloud computing is defined as a platform where the services to the customers are presented as a service using the current internet technologies as defined in [6-10]. It is the responsibility of the service providers to ensure that the customer data is protected and secure on the cloud. The cost effectiveness of the services provided by the cloud has made many SMB (Small and Medium Businesses) companies to incline toward the cloud computing infrastructure. Cloud computing necessarily puts data outside of the control of the data owner which inevitably introduces security issues too. Cloud computing security necessarily involves making all the aspects of cloud computing environment secure, Figure 3. Many of these aspects are not unique to the cloud setting: data is vulnerable to attack irrespective of where it is stored. Therefore, cloud computing security encompasses all the topics of computing security, including the design of security architectures, minimization of attack surfaces, protection from malware, and enforcement of access control.

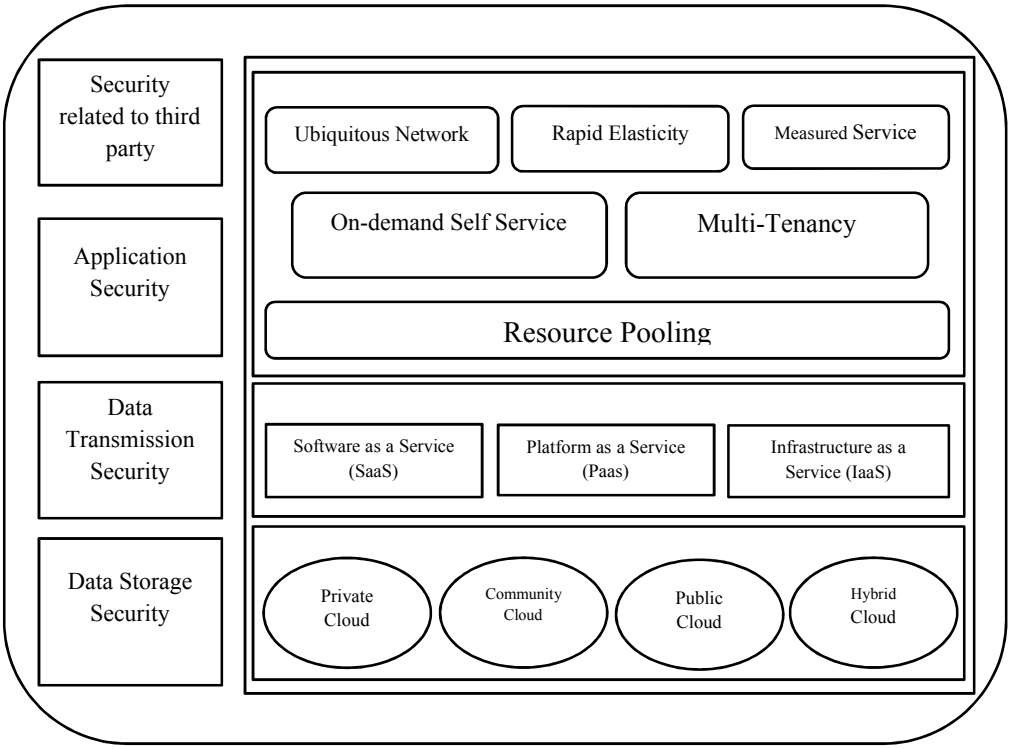

Figure 3. The Complete Cloud Model with All Security Aspects

Apart from being one of the cost effective ways to deploy business, the cloud offers many other advantages and benefits to the customers including; scalability, ease of use, easy access, cost effective data recovery and storage, real time intrusion detection and protection against network attacks etc. In spite of all these benefits, many big fishes have been on the back foot in adopting the cloud services and again the reason being the security issues [11]. One survey depicts that 74% of the executives consider security issues in cloud as a single most important concern for not submitting to use the cloud services [12]. The security issues include [13] accessibility and virtualization vulnerabilities, web application vulnerabilities like SQL (Structured Query Language) injection and cross-site scripting, physical access and privacy and control issues arising from third parties having physical control of data, the issues of identification and credential management, issues concerning to data verification, tampering, integrity, confidentiality, data loss and theft, issues related to authentication of devices and IP spoofing.

Security Issues

Cloud computing provides services using three different models; IaaS, PaaS and SaaS. The basic foundation of a cloud computing environment is IaaS on which PaaS resides and then the SaaS on it in a hierarchy as shown in Figure 2. All three layers form an inheritance ladder and like any other properties, issues of security from one layer to another are also inherited. Let us look at the security issues [14] at all three layers. The security threats in one level may not be exclusive and may overlap between levels.

1. Security threats and issues in SaaS:

a. Data security:

In SaaS, the data of a customer is not within the boundary of the customer and remains at the vendor site. This model requires the use of strong data security and a comprehensive authorization process to access the data. The data can be tampered while a user is trying to access the data, upload the data and user authentication. Many cryptographic techniques must be implemented to secure the issues.

b. Network security:

The data access is done over the internet and all the data flows on the public network which can be accessed by anybody over the internet. In order to prevent the data leakage and attacks by malicious users, the encryption techniques at Secure Socket Layer (SSL) and Transport Layer (TL) must be strong.

c. Data locality:

The users use services on the SaaS model to use and process the business data. The inherent notion of cloud computing and SaaS is not to reveal the location of the data storage. The location of data is of significant importance in many enterprises [15]. In many European countries the data cannot leave the country or travel through certain countries. Also, the location of data storage may enforce the question of who can investigate what data.

d. Data integrity:

Data integrity is easy in standalone systems where we only need to enforce ACID (atomicity, consistency, isolation and Durability) properties. In a distributed system like cloud computing it is very hard to achieve data integrity due to the presence of multiple databases and the transactions about multiple databases. It is an issue of much concern in a cloud computing environment because the applications in SaaS are exposed as a service and expose their functionality via APIs.

e. Data segregation and Data access:

The clear definition of boundaries of user data is very important [16-18]. Multiple users store their data at the same place and access their data using the same SaaS services. Since the users have access to the location where data of many users is stored, a user can exploit some of the

vulnerabilities and access other users' data. A simple code block can be executed within the application to access all the data stored within a location. Hence there should be a proper segregation of data of different users. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment.

f. Data confidentiality:

Cloud computing involves the sharing of data storage by users to store their personal information on remote servers owned and operated by a service provider and the information can be accessed using the internet. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites and many more. The entire contents of a user's storage device may be stored with a single cloud provider or with many cloud providers. Whenever an individual, a business, a government agency, or any other entity shares information in the cloud, privacy or confidentiality questions arise.

g. Web application security:

One of the important requirements for using a SaaS application is that a web browser is needed to access and manage it [19]. SaaS model with its key characteristics defines the network based access and management. The web based access and management and the security loopholes in the web applications add some sort of vulnerability to a SaaS application. Therefore, the concerns in SaaS security is the same as any other web application technology. Also, the traditional network security solutions which include network firewalls, network intrusion detection and prevention systems (IDS & IPS), do not substantially address the problem.

h. Data breaches:

In a cloud environment we have the data from multiple business organizations residing on the same place and breaching a cloud might give access to all the data in the cloud. This makes cloud vulnerable to attacks and a big target for sensitive information [20-21]. It has been stated that in the Verizon Business breach report blog [22], the external criminals pose the greatest threat (73%), but achieve the least impact (30,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Insiders pose the least threat (18%), and achieve the greatest impact (375,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Partners are middle in both (73.39% and 187,500) resulting in a Pseudo Risk Score of 73,125. The SaaS service providers claim to provide a better security on the breaches from the outside but inside people still have got access to the database. It is the single weakest link in the security breaches because a single insider job could expose all the information in the cloud.

i. Availability:

The SaaS model must provide some flexibility for making architectural modifications in order to adhere to scalability and high availability. In SaaS a resilience mechanism for both hardware/hardware failures should be implemented. A proper resistance against DoS attacks must also be implemented. For example, Amazon uses synchronous cookies and connection limiting to reduce the effect of DDoS attacks.

j. Backup:

In SaaS, the regular data backup facilitates recovery in case of failures and disasters. This backup facility calls for a strong encryption techniques to protect the data from leaking. The tests and security checks done during the data backup and recovery can be exploited to hack into the cloud and access sensitive information.

k. Interception:

In a cloud computing environment, the public network is used to access the data and the traffic is vulnerable to being read and modified. A third party may act as a session endpoint and read or rectify data. This is called hijacking. An attacker monitors the network data for sensitive data. Usually he/she looks for password in plaintext or some other sensitive information which can be easily read. An attacker sits in the background passively and waits for the right information

which he can use to gain access or steal. An attacker can also play an active role and modify the data stream before sending it back on its way.

l. Modification of data at rest and in transit:

In a cloud computing environment, data needs to travel from one location (vendor site) to other location (user site) through the network. This is the data in motion or moving data. The data at the vendor site can be stored on storage devices such as hard disks, flash drives etc. This is known as the data at rest. The data at rest is considered less susceptible to attacks than the moving data and attackers try to sniff over moving data all the time in search of sensitive information. The data in cloud environment whether at rest or moving should be protected from any attacks and different measures should be used to inhibit an attacker to compromise or steal sensitive information.

m. Privacy breach:

Privacy breach means the unauthorized access to sensitive data or personal information. In cloud computing, vulnerabilities can be exploited to steal sensitive information. The vulnerabilities can be as a result of faulty procedures or breakdowns.

n. Impersonation:

Impersonation is yet another threat that has its implications in cloud environment. It is used to gain access to resources as elevation of privilege from a lower context to higher context. A high privileged access can give the access to sensitive information.

o. Session hijacking:

In this type of attack, the attacker makes the server into accepting and receiving the data and treats the attacker as a legitimate host. Session hijacking is a method of taking over a web user session by secretly obtaining the session ID and pretending as the authorized user. Once the user's session ID has been accessed, the attacker can masquerade as that user and do anything the user is authorized to do on the network. In session hijacking, a cookie stored on the client's web browser is stolen to gain unauthorized access.

p. Traffic flow analysis

In traffic flow analysis, the frequency and the timing of network packets is continuously monitored to gain important information. An attacker can use a timing attack on the SSH protocol and use the timing information to reveal sensitive information.

2. Security threats and issues in PaaS:

In PaaS, the vendor provides services of designing and building applications to the customers on top of the platform. The security beneath the application level is still under the domain of the vendor and it is the responsibility of vendor to provide data protection and inhibit data access between different applications. Since PaaS enables the development of applications on the top of the platform and has extended capabilities than SaaS, these flexibility features come at the expense of low security. Hence an additional layer of security must be included. Enterprise Service Bus (ESB) based applications must assure the security of ESB directly. There must be some sort of metrics used to evaluate the effectiveness of the security in the application programs. Some of the metrics used in direct applications are vulnerability scores and patch coverage. An attacker can try and exploit the vulnerabilities in the infrastructure of the cloud application architectures. The vulnerabilities in PaaS are not limited to web applications only but are associated with Services Oriented Architectures (SOA) applications too. An attacker can exploit any programming flaws in the development platform such as boundary condition violation, exploitable logic errors and inadequate identification and authentication.

3. Security threats and issues in IaaS:

Virtualization has made the services of IaaS possible. Virtualization completely hides the hardware beneath IaaS platform and gives users an ability to utilize infrastructure/hardware as a service without indulging into the underlying complexities. Virtualization poses a definite security threat in cloud computing. There are many security problems in VMs as explained in [23-24]. Virtualization tries that different instances running on a single machine be separated from each other. The whole process of virtualization does not completely solve this problem. Many loopholes in the code of VMs have lead hackers to try and exploit these vulnerabilities and gain access to the system and hence all the information. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege. Another example would be the vulnerability in Xen caused due to an input validation error in tools/pygrub/src/GrubConf.py. This can be exploited by 'root' users of a guest domain to execute arbitrary commands in domain 0 via specially crafted entries in grub.conf when the guest system is booted. The other issues at this level include misuse of infrastructure and damage from natural disasters.

Secure cloud environment

We have three layer based architecture in cloud computing; SaaS (Software as a service) layer, PaaS (Platform as a service) layer and Iaas (Infrastructure as a service). It is very essential to organize the security based on the perception of these three layers which operate in a top down manner. The top layer should trust the layer beneath it and vice-versa while interfacing with each other. The security is needed at operational, technical, procedural and legal levels to facilitate a secure and smooth communication between the layers. There must always be a certificate, a trusted certificate which would serve as a passport that authenticates an individual's identity or credentials and its role. The certification process guarantees the chain of trust from an end user to application owner and the infrastructure vendor. In a distributed environment like a cloud computing environment, TTP serves as a good security facilitator in which different entities from different domains establish secure interactions with no background knowledge of each others existence. During the data communication between the user and the cloud, a combination of two different certificates is used for a secure connection. A personal digital certificate of the end user is used to authenticate him/her with a cloud service and validate his privileges to access any resource from the cloud. Another certificate from the service provider at PaaS or IaaS level is used for a secure SSL connection and hence the encryption of exchanged data. All personal data on the cloud is encrypted to fight the confidentiality risks. At hardware infrastructure, digital certificates are used to communicate between devices and virtual servers securely and for the authentication as well. Certificates are not only used for the authentication purpose by the application provider but they are also used to encrypt and decrypt the application data. The virtualization not only abstracts every underlying detail and complexity but also obscures the physical key storage location and hence makes key exchange and management a critical issue in cloud infrastructure. There must be fool-proof techniques and devices with hardware security for key protection. In this environment, cryptography can be seen as a solution to ensure the authentication and integrity of the data used during the communications between the end user and the cloud. Especially public key cryptography, single-sign-on technology and LDAP directories can be used to securely identify and authenticate the end users.

Most of the security problems in cloud infrastructure can be managed by the public key cryptography which is then transformed into the key management issues. The whole idea of key management revolves around controlling access to the private keys. The efficiency could be deteriorated as additional encryption processes are done in host-to-host communication. The frequent encryption and decryption of data could degrade the performance and may adhere to more processing overhead. Thus, key management issues directly affect quality of service and performance. Some recent researches have shown that data could be searched without it being decrypted first. This could enhance the performance and thus improve the availability and quality of services provided in the cloud infrastructure. Using standard encryption techniques in cloud environment the data is encrypted before sending it and the data is decrypted every time we need to perform an operation. The user is required to provide the private key to the service provider to perform the operations on data which is a threat to privacy and confidentiality of data. Homomorphic Encryption systems can be used to overcome this problem. In these systems, operations on the data can be performed without the need of private key of the user. Table 1. depicts the characteristics of some of the Homomorphic Encryption algorithms used in cloud computing. The other issues like low and high level confidentiality, client and server authentication, cryptographic separation of data and certificate based authorization can be outsourced to a trusted third party. There are different encryption techniques which can be used in cloud computing to allow the users to store their data on the cloud infrastructure with minimum risk. Amit et al [25]

described a bidirectional DNA encryption algorithm for improving the security in cloud computing. P Subhasri et al. [26] proposed a multilevel encryption algorithm which will be more secure than the other encryption techniques.

	Homomorphic Encryption Cryptosystems					
Characteristics	**RSA**	**Pailler**	**El Gamal**	**Goldwasser-Micali**	**Boneh-Goh-Nissim**	**Gentry**
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Encryption Type	Multiplicative	Additive	Multiplicative	Additive, but it can encrypt only single bit	Unlimited Number of additions but only one multiplication	Fully
Data Privacy	Is ensured in Communication and storage processes	Is ensured in Communication and storage processes	Is ensured in Communication and storage processes	Is ensured in Communication and storage processes	Is ensured in Communication and storage processes	Is ensured in Communication and storage processes
Security applied	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server	Cloud Provider Server
Keys	The Client (Different keys for Encryption and Decryption)	The Client (Different keys for Encryption and Decryption)	The Client (Different keys for Encryption and Decryption)	The Client (Different keys for Encryption and Decryption)	The Client (Different keys for Encryption and Decryption)	The Client (Different keys for Encryption and Decryption)

Table 1. Homomorphic Encryption systems and their characteristics

They have described two types of encryption method to make the clod data more secure. The first method is the Rail fence cipher algorithm that will use Transposition and the other one is the Caeser cipher for substitution. In this method it is difficult to understand the cipher text compared with the other techniques. Hey have used a combination of three different algorithms to improve the security in [27]. Dimpi Rani et al. [28] depicted that the combination of RSA and Blowfish will be more secure when it is used with the digital signature. They have explained various vulnerabilities and the threats that can affect cloud computing environment [29]. The study defined elaborates the various issues of security that are seriously affecting the cloud infrastructure [30]. There are many other encryption based solutions given by [31-33].

Conclusion

Cloud computing is relatively a new technology that provides a number of benefits to the users. Cloud computing has huge applications in business but the security hazards in cloud environment directly affect the benefits that it offers. Cloud computing serves as a backbone for every small and medium sized business (SMB). Security is an inflexible requirement for cloud computing environment. We have presented the various cloud computing security issues and threats and the possible silver lining to cope with these issues. In this study, we also presented various encryption techniques which can help make the data secure on cloud. The Homomorphic Encryption systems offer good performance enhancements in performing the operations on the data without decrypting it first. It has also been established that encryption techniques could be enhanced to provide better performance and security in the cloud with focus on Public Key encryption and Key management.

References

[1] K. Stanoevska-Slabeva, T. Wozniak, Grid and Cloud Computing-A Business Perspective on Technology and Applications, Springer-Verlag, Berlin, Heidelberg, 2010.

[2] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.

[3] E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009

[4] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice, O'Reilly Media, 2009.

[5] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009).

[6] Stanojevi R, Shorten R. Fully decentralized emulation of best-effort and processor sharing queues. ACM SIGMETRICS international conference on the measurement and modeling of computer systems. New York: ACM Press; 2008ACM SIGMETRICS international conference on the measurement and modeling of computer systems. New York: ACM Press; 2008. p. 383–94.

[7] Vaquero LM, Rodero-Merino L, Caceres J, Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5.

[8] Weiss A. Computing in the clouds. In: ACM networker, December 2007, 2007, p. 16–25.

[9] Whyman B. Cloud computing. Information Security and Privacy Advisory Board; 2008. 11–3.

[10] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009.

[11] Viega J. Cloud computing and the common man. Computer 2009;42(8):106–8

[12] Clavister. Security in the cloud, Clavister White Paper /http://www.it-wire.nu/ members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf

[13] Wang C, Wang Q, Ren K. Ensuring data storage security in cloud computing, Cryptology ePrint Archive, Report, 2009/http://eprint.iacr.org/

[14] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing,"Gartner Report, 2009. [Online]. Available: http://www.gartner.com/DisplayDocument?id=685308.

[15] Softlayer. Service Level Agreement and Master Service Agreement, 2009/http:// www.softlayer.com/sla.html.

[16] Blaze M, Feigenbaum J, loannidis J, Keromytis AD. The role of trust management in distributed systems security, secure Internet programming, issues for mobile and distributed objects. Berlin: Springer-Verlag; 1999. p. 185–210.

[17] Kormann D, Rubin A. Risks of the passport single signon protocol. Computer Networks 2000;33(1–6):51–8.

[18] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology ePrint Archive, Report 2008/489, 2008/http://eprint.iacr. org.

[19] Zalewski M. Browser security handbook, 2009/http://code.google.com/p/browsersec.

[20] Bernard Golden. Defining private clouds, 2009 /http://www.cio.com/article/ 492695/Defining_Private_Clouds_Part_One.

[21] Kaufman LM. Data security in the world of cloud computing, security and privacy. IEEE 2009;7(4):61–4.

[22] Cooper R. Verizon Business Data Breach security blog, 2008/http://securityblog. verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report.

[23] Attanasio CR. Virtual machines and data security. In: Proceedings of the workshop on virtual computer systems. New York, NY, USA: ACM; 1973. p. 206–9.

[24] Gajek S, Liao L, Schwenk J. Breaking and fixing the inline approach. In: SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37–43.

[25] Amit et al. "Enhancing Security in Cloud Computing Using Bi-Directional DNA Encryption Algorithm" Springer 2015.

[26] P.Subhasri et al. "Multilevel Encryption for Ensuring Public Cloud", IJARCSSE, Volume 3, Issue 7, July 2013.

[27] Aman et al. "Comparative Analysis between DES and RSA Algorithm‟s", IJARCSSE, Volume 2, Issue 7, July 2012.

[28] Dimpi et al "Enhance data security of private cloud using encryption scheme with RBAC", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014.

[29] Keiko et al. "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013.

[30] Monjur et al. "Cloud Computing and Security Issues in the Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[31] Aized et al. [2] "Encryption Techniques For Cloud Data Confidentiality", International Journal of Grid Distribution Computing Vol.7, No.4 (2014).

[32] Rachna et al. [3] "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4.

[33] Dr .A.Padmapriyaet al. [4] "Cloud Computing: Security Challenges & Encryption Practices", Volume 3, Issue 3, March 2013.