# Data Outsourcing Security Issues and Introduction of DOSaaS in Cloud Computing

Mohammad Asadullah
Sri Venkateshwara University
Meerut, India

R. K. Choudhary, Ph.D
Asia-Pacific Inst. Of Information Technology
Sonipat, India

## ABSTRACT

In the last couple of years, Cloud computing has evolved as an important paradigm for IT industry with reduced costs, pay-as-you-use, scalability, easy accessibility and improved flexibility. More and more small and large scale companies are moving towards cloud computing as it eliminates setting up of high-investment on IT infrastructure and other services like SaaS, Paas and NaaS. In cloud environment, the client data can reside in any corner of the world and maintained and controlled outside their reach. So, there can be security and privacy issues with the client data. The cloud provider needs to satisfy their client by ensuring and providing data security. This survey paper presents and analyze different security and privacy issues involved in cloud computing service. We also highlight different security models of few of the top cloud service providers. This research paper introduces new service model called Data Outsourcing Security as a Service (DOSaaS).

## Keywords

Cloud Computing, IaaS, PaaS, SaaS, Virtual Machines, Multi-tenancy

## 1. INTRODUCTION

Cloud computing is one of the most emerging IT paradigm in recent times. This technology has made Everything-as-a-service enterprise model. This is a latest state of the art technique which works on pay-as-you-use model for all IT operations like providing platform services, infrastructure services, software application services etc [1]. The cloud computing is a blending of Business enterprise applications, data storage, Internet, management and networking and solutions. This technology provide enormous benefits like 1) scalable data solutions as per your business requirement, 2) reduced cost on infrastructure to put your money at another areas, 3) high accessibility because of accessing everything through internet, 4) backup and recovery of the your data becomes easier than earlier and 5) it also provides a quick deployment of the technology you need [2] [3]. Cloud Computing has been defined by US National Institute of Standards and Technology (NIST, http://nist.gov/itl/cloud) as follows:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.

## 2. CLOUD COMPUTING SERVICE MODELS

Cloud computing offers different types of services depending on business requirement, but mainly three layers constitute the service model which are described as follows:

**2.1** *Infrastructure as a service (Iaas):* This forms a bottom layer of the service model which provides a basic hardware and network support services. It also provides platform for aggregating and maintaining the resources and which can also be scaled up or scaled down dynamically on-demand. There can be many users using the resources parallel which is managed by a billing depending upon the usage of the resources allocated [4]. The virtualisation should be potentially superior so that the accessing thousands of virtual machines at a time with fast speed could be made possible. e.g. Amazon EC2, Google FS, Open Flow, Hadoop MapReduce, Google Bigtable, Rightscale etc. [6].

**2.2** *Platform as a Service (PaaS):* This middle layer consists of the operating systems and middleware applications. This mainly offers developers a software development management platform to work on the lifecycle of application development with all the steps like designing, developing, testing to deploying [5]. Eventually, it offers an application development and execution environment for developers. e.g. Google App Engine, Django, Microsoft Azure, Amazon SSS etc [6] [7].

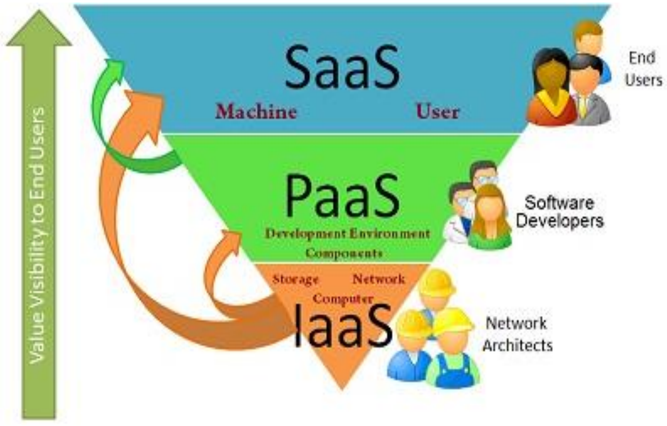

**Fig 1: Cloud Computing Service Models**

**2.3** *Software as a Service (SaaS):* This is a top layer of the cloud computing service model which provides pay-per-use model for users on the internet without bothering about the software deployment and maintenance as it is not installed on user's local computer. There is still a security concerns over the enterprises data the way they are stored and secured. e.g. Google docs, Salesforce.com, Opensocial, net suite [6][8].

## 3. CLOUD SERVICES DEPLOYMENT MODEL

There are different types of deployment model depending on the customer's requirement like some customers mainly concentrates about security, some prefer low infrastructure cost:

*3.1 Public Cloud:* In this model, User is not bothered about investing on infrastructure as it is availed by Third-party cloud service provider [9]. They need to bill as per use of the services. So many users use the infrastructure provided at the same time. Cloud Services are basically accessed through web browser on internet.

**3.2** *Private Cloud:* This cloud is provided to specific customer and it can be managed either by the customer itself or third-party service provider [10]. This provides more security and reliability because it is availed and managed by the organization internally whereas public cloud is made available for so many customers.

**3.3** *Hybrid Cloud:* This deployment model is a combination of private and public or other cloud where different services from them are shared. This cloud provides more flexibility and security than public and private cloud. Services are linked with each other that data transfer takes place without overlapping on each other [7].

**3.4** *Community Cloud:* This deployment model can be shared by group of organizations which have same requirements. It can also be said that it is a generalized form of private cloud. It can be managed by either by them or third party service provider.eg. Hospitals, government services etc.

## 4. SECURITY ISSUES OF CLOUD COMPUTING

Security issues of cloud computing can be divided at three different levels:

### 4.1 Security Issues in IaaS

#### *4.1.1 Impact of Cloud deployment model:*

The IaaS layer is also vulnerable due to network and internet connectivity associated with it. It is more prone in public cloud compared to private cloud. Physical security of infrastructure is also required for any disaster happening. The data transmission path is also needed to secure as the intruders can easily attack the data communicating between sources to destination [11]. The data flowing over the internet is a major concern as the client and service providers are placed at two different locations which are connected through internet only. Therefore, it needs high encryption techniques and strong secure protocols to safeguard data transmission.

#### *4.1.2 Virtualization:*

Virtualization provides many features to the users to create, share, migrate, copy, rollback virtual machines which helps in running many applications on them [12, 13]. But, it also becomes prone to get attacked because it opens more entry for the attackers and interconnected virtual machines complexity [14]. Virtual machines should also be considered as important as any other physical device security.

#### *4.1.3 Hypervisor:*

This is also called as Virtual Machine Monitor (VMM). This software is responsible for monitoring and controlling its virtual machines, so it cloud also produces some security flaws [14]. Security risks can be reduced by keeping Hypervisors simple and less complex to easily trace and resolve security issues.

#### *4.1.4 Shared storage resources:*

Virtual machines are connected with same server. So, there is strong chance that if one virtual machine gets affected by malicious virus, it can be used to monitor other Virtual machines shared resources. So, the attacker can easily track the information or data about other Virtual machines [15].

#### *4.1.5 Virtual Networks:*

Virtual machines are connected with virtual networks which are shared by multiple tenants across the network. It gives attacker a way to get into the virtual network [16]. Most of the Virtual Machine Monitors use virtual network to communicate with each other directly [15]. There can be possibility of spoofing and sniffing attacks in most of the virtualization platforms [14].

#### *4.1.6 Network and Internet connectivity issues:*

Cloud Infrastructure is connected through internet and maintained at different locations so that it can be recovered and managed at the time of any unpredicted disasters. Usually, the local virtual machines are more prone to internal attacks compared to external attacks as the data is shared by locally connected VMs and the different malicious software can be run and installed by the administrator privileges. So, the IaaS environment is more vulnerable to internet or network attacks compared to any other cloud layer.

### 4.2 Security Issues in PaaS:

#### *4.2.1 Application development life cycle:*

It is also a big challenge to secure a software application development because software developers face quite difficult to secure the application taking place in cloud environment. The application need to be upgraded by applying new patches or versions to keep them up-to-date and secure [16]. Developer should also aware of the legal issues of the data storage or the source code storage so that it could not be compromised [15].

#### *4.2.2 Underlying Infrastructure security:*

Cloud providers are responsible for underlying infrastructure security and the services running for applications [17]. So, the application developers have no privilege to access underlying infrastructure. SaaS and PaaS user can share the same applications because the software developed are delivered and used in SaaS while in PaaS, the development tool is used to develop and test the same application to be used by the SaaS users. So, there can be security concern about the user data and its storage [15].

#### *4.2.3 Third-party Relationship:*

Third-party also plays a important role in PaaS as the some third-party components are required in web services like Mashups which helps in integrating more than one source component into a single unit [18]. PaaS users and developers also need to depend on the services provided by third-party and the web-based development tools.

## 4.3 Security Issues in SaaS

### *4.3.1 Network Security*

In SaaS service model, different kind of data is flowing from client to cloud provider and also stored at the provider side. So, the data flowing over the internet needs to be secured to prevent the data hacking. Some strong encryption techniques are used to control using Transport layer Security (TLS) and Secure socket Layer (SSL) [5]. There are different types of attacks in network layer such as packet scanning, IP spoofing, Man in the Middle attacks (MITM) etc. There are strong risks that malicious attackers can exploit network security loopholes to sniff IP data packets.

### *4.3.2 Data Accessibility*

Application or data accessing over the network makes the life easier for cloud users. But, it also opens a gateway for security issues. The specific policies must be defined by the organization to access the data to avoid any intrusion within the network. Multi-tenant deployment can expose the issue on the managing data access within the single cloud environment [5]. So, the provider must adhere with the policies set for such scenario.

### *4.3.3 Availability*

Cloud vendor should ensure that users will have a regular access of data and their application services as well as hardware resources around the clock. Any malicious attack can make whole application or services unavailable to the users. Some proper action plan needs to be defined for unpredictable incidents in order to recover from the disaster and for up and running business. Amazan's EC2 faced a big blackout in 2011 due to some network defect in its one of the cloud zone [20]. Many of its clients like Reddit and Netflix had an adverse impact due to this network breakdown [19].

### *4.3.4 Data Integrity:*

Data integrity is one of most critical element in terms of cloud security. It deals with unauthorized modification of data. In cloud computing, the transaction management security using web services because HTTP doesn't provide proper support to transaction delivery. Data encryption is a better option to secure data on different levels: Rowl level, table level and database level. Database level encryption comes under software level encryption which is quite secure because user provides the key to encrypt and decrypted using key. So, if the data is hacked even though it cannot be deciphered without availability of the key. Row level encryption is done with hardware level encryption [21].

### *4.3.5 Multi-tenancy:*

In SaaS service model, multi-tenants share a same database. The tenant information can be at risk if any misconfigured software application source code or data leakage takes place. Based on specific security policies, the authentication should be given to the users so that only data will be modified or accessed into or from database for the particular tenant. The data of one client should be isolated from another client.

## 5. CURRENT CLOUD SECURITY SOLUTIONS

A research on cloud security is constantly going all over the world. Major cloud providers are also involved in working on the security solutions. Cloud security Alliance (CSA) is actively involving all the cloud providers and other individual people to participate and come up with some sound solutions. Tsai et al. brings a fourth-tier framework specifically for web-based development environment, provides some security at some extent [22]. In [23], Ristenpart et al. suggested that risks could be the attacks, so the cloud service providers should implement web-based co-residence check to control the attackers. Krugel et al. suggested the amount of packet-snifering output filtering for specific application services is a good approach to control security issues for specific services and network ports [24]. Kong et al. also suggested a good solution stated as "Partition-locked cache (PLcache) and random permutation cache (RPcache) to defeat cache-based side channel attacks" [25]. Raj et al. also suggested data security during processing using resource isolation method, by isolating the processor cache within the VMs and then isolating virtual cache from VMM cache [26]. The cloud security can also be enhanced by providing proper safeguard to operating systems and the virtual machines used for cloud network [27]. An cloud security has been introduced by the association with trusted third-party to ensure the security in terms of communication, integrity and confidentiality [28]. Milne et al. point out a simple solution to just use private cloud [29]. Jyoti et al. suggest that the virtualization would be the best option to shield with the security which provides less investment on hardware and multiple machines are managed centrally with high-end security [30].

## 6. DATA OUTSOURCING SECURITY AS A SERVICE (DOSAAS)

Nowadays, Cloud customer negotiates their data control to the cloud provider, so there is a risk when the data is another compound. This research work introduces a new service called Data Outsourcing Security as a service to achieve robust technical security solution. We have mentioned following important aspects which helps to understand the flow of the DOSaaS and resolve this issue:

## 6.1 Confidentiality

It prevents confidential data accessed by wrong people, making sure that the right person can only reach it. There are various methods through which we can apply confidentiality like Data encryption is a common method used widely in industries, User IDs and passwords are also one of the common ways of ensuring confidentiality.

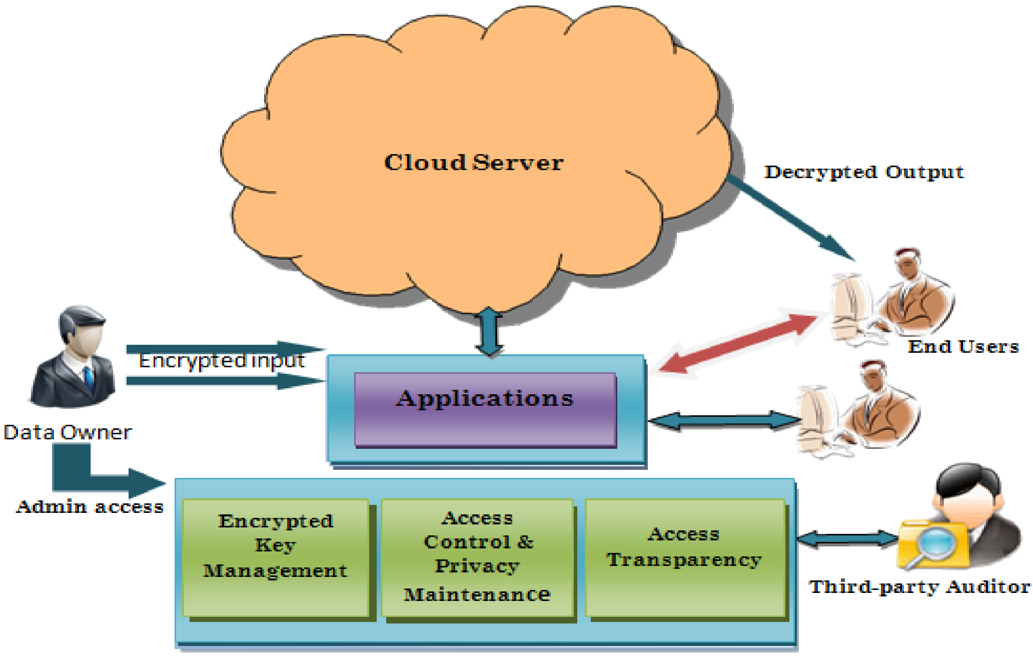

**Fig 1. Architecture sample for Data Outsourcing Security as a Service illustrates to manage the application, enryption management, access control, privacy maintenance, logging and information flow between various technologiesto understand DOSaaS.**

Captcha is also one of the current used techniques avoiding from non-human access.

## 6.2 High Availability

High availability is also one of the important aspects of cloud computing security. There can be different reasons of non-availability like network vulnerability, data storage failure etc. But the main thing which is bigger loophole is IP failover. Alternate IP addresses can be assigned to the virtual machines to avoid IP failures.

## 6.3 Integrity

Integrity helps to maintain the accuracy and trustworthiness of information of the entire product life cycle. There are risks that the data can be manipulated in transit by unprivileged people, and we need to make sure the user's stored data won't be corrupted. The outsourcing data needs to be kept protected by keeping the backups of data if any unexpected error occurs. The client needs to make clear and maintain the records what data is hosted on the cloud, the origin and control of data must be maintained to prevent data tampering or access of confidential data beyond the agreed territories.

## 6.4 Encrypted Key Management

There can be data compromised if the poor key management and insecure data storage happens, especially when any company having cloud infrastructure access managed by third-party company. At that time, the encryption keys security becomes a big issue. There can be many reasons behind the key access like key storage, weak key generation etc. Strong password also plays a vital role in securing key access. An unauthorized user or corrupt employee can come to know about your key or they can access machines where confidential data can be accessed. Data backup also highlights another problem as data archiving managed by cloud data storage provider. So, It can be better encrypted first and then send it back to cloud storage provider to avoid any risk. Crypto-shredding is also an important method of reducing risks.

## 6.5 Access Control

Cloud service provider needs to follow many accessing levels for the cloud computing by applying various access control lists. Encryption also helps in enabling access control to the cloud data. There could be a different level of access to the user data of the cloud. To prevent the unauthorized access of the cloud, the cloud provider creates access list. Microsoft uses Rule based Authorization for access control, Amazon web services provides SSL encrypted endpoints using secure HTTP web protocol [31].

## 6.6 Privacy Maintenance

The confidential information used to travel through the whole cloud network. So, there are strong chances of data being an easy prey by the attackers. They can misuse the services provided to the specific user or the data can also be manipulated. Security of private data needs to be taken care by protecting confidential information. Companies need to implement defined data privacy policy, on demand encrypted data transformation and data masking services [32].

## 6.7 Access transparency via logging

Access transparency is also an important aspect of tracking and managing the access logs which user is doing with sensitive data. Data logs will clearly provide the record who and what accessed any data. It can also be used for audit compliances. Pushing log management and correlation could solve most of the log issues to provide transparent access.

## 6.8 Identity Management

Specific user only need to allow to access the application; the client should be given privilege to create, update and delete the new or existing users in order to keep the user access transparent and under client's control. There should be an add-ins or tool for password maintenance.

## 6.9 Service level agreements (SLAs)

SLA is a kind of contract blueprint between the customer and provider. Cloud data provider has the legal responsibility to prevent of data loss. If data is breached or lost, the blaming often goes to service providers. As with many legal documents, Cloud SLAs are more often written to the benefit of the cloud service provider, not to the cloud customer. Cloud service providers used to offer various levels of data protection, but it's still difficult to provide proper liability of customer data.

Cloud SLA is documented that contains statements protecting the cloud service provider if data is lost or scrambled. In fact this agreement also helps to suggest that a cloud customer make "frequent archives" of their data and "encrypt" while transmission. The responsibility for managing the integrity of data, whether in a private cloud, hybrid cloud or public cloud or in a data centre, always goes to the company that owns data.

## 6.9 Compliance Audit

A compliance audit is a review of a regulatory guidelines and policies by an organization. Many parameters are defined to examine the compliance audit like type of data it handles or it transfers or stores the private or financial information. Audit trail is handled by the data produced by event log management application installed in the company. Auditors used to ask many questions to the IT administrators, CTO etc. About the policies and regulation guidelines followed by the company on periodic basis. There is software available for user access tracking and documentation authentication of the data transmitted to the client.

## 7. CONCLUSION

There are lots of advantages associated with the use of cloud-computing. But, it also has some security concerns which slow down the open acceptance of this technology. Cloud providers need to ensure the customer about the confidential data security. This paper has discussed on different security issues on services model level: IaaS, PaaS and SaaS. Network, shared resources, storage and virtualization are the main issues which are still immature and need to be looked ahead. This research work has introduced DOSaaS to illustrate the specific implications of this service model and the solutions. This research paper has also discussed current available solutions to overcome some common and major issues. There is need to have better encryption techniques and integrated cloud security framework to make it more dynamic with scalability.

## 8. REFERENCES

[1] Cloud Computing, http://www.cisco.com/web/solutions/trends/cloud/index.html

[2] Charlie Williams, Advantages of Cloud Computing, "http://www.2x.com/blog/2013/02/news/advantages-of-cloud-computing/"

[3] Priya Viswanathan, Cloud Computing – Is it really all that beneficial? , "http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm"

[4] Ms. Disha H. Parekh, Dr. R. Sridaran," An Analysis of Security Challenges in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013

[5] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2010), doi:10.1016/j.jnca.2010.07.006

[6]. Zhifeng Xiao, Yang Xiao, "Security and Privacy in Cloud Computing", IEEE COMMUNICATIONS SURVEYS & TUTORIALS

[7]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing"

[8]. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing (2009), DOI 10.1109/SCC.2009.84

[9]. Qi Zhang, Lu Cheng, Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", J Internet Serv Appl (2010), vol. 1: pp. 7–18.

[10]. R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[11]. Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270–4.

[12]. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41.

[13]. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa.

[14]. Reuben JS (2007) A survey on virtual machine Security Seminar on Network Security http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final..pdf. Technical report, Helsinki University of Technology October 2007.

[15]. An analysis of security issues for cloud computing, Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, Journal of Internet Services and Applications 2013, 4:5.

[16]. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42.

[17]. Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25.

[18]. Keene C (2009) The Keene View on Cloud Computing. Online available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. Accessed: 16-Jul-2011.

[19]. Sanjay P. Ahuja and Deepa Komathukattil, A Survey of the State of Cloud Security, Network and Communication Technologies; Vol. 1, No. 2; 2012, ISSN 1927-064X.

[20]. Thibodeau, P. (2011). Amazon outage sparks frustration, doubts about cloud. Retrieved from http://www.computerworld.com/s/article/9216098.

[21]. Hacigumus, H., Iyer, B., & Mehrotra, S. (2002). Providing database as a service. Data Engineering, 2002. Proceedings. 18th International Conference on, pp. 29-38, 07.

[22]. Tsai W, Jin Z, Bai X. Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware. Beijing, China: ACM; 2009. p. 1–10.

[23]. Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270–4.

[24]. Krugel C, Toth T, Kirda E. Service specific anomaly detection for network intrusion detection. In: Proceedings of the 2002 ACM symposium on applied computing, 2002, p. 201–8.

[25]. Kong J, O. Aciicmez, J.P. Siefert and H. Zhou, Deconstructing new cache designs for thwarting software cache-based side channel attacks, Proceedings of the 2nd ACM workshop on Computer security architectures, ACM, New York, USA, 2008, pp 25-34.

[26]. Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009, p. 77–84.

[27]. Santos N., K.P. Gummadi and R. Rodrigues, Towards trusted cloud computing. Proceeding of the conference on hot topics in cloud computing, (Hot Cloud'09), Berkeley, CA, USA.

[28]. Zissis D. and D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst.,2012, 28:583-592.

[29]. Milne J.Privatecloudprojectsdwarfpublicinitiatives,2010, http://www.cbronline.com/news/private_cloud_projects_dwarf_public_initiatives_281009S [accessed:19June2010].

[30]. Jyoti S., S. manish and G. Rupali, Virtualization as an engine to drive cloud computing security. Proceeding of the High Performance Architecture and Grid Computing, July 19-20, 2011, Chandigarh, India, pp: 62-66

[31] Dr. Arockiam L, Parthasarathy G and Monikandan S, Privacy in Cloud Computing: A Survey, CS & IT-CSCP 2012, pp. 321–330.

[32] Protect Data Privacy, http://www-01.ibm.com/software/data/optim/protect-data-privacy/.