ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

A Critical Review on Risk of Cloud Computing in Commercial

Bharatratna P. Gaikwad[1]

Department of Computer Science and IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad , India[1]

ABSTRACT*:* This paper explores Cloud computing is a powerful innovative technology that is broadly used in the business world. The cloud computing is a systems architecture model for Internet-based computing. This paper presents a study about the risk issues involved in cloud computing. It highlights the different types of risks and how their existence can affect the cloud users. It also discusses the different circumstances in which the risks occur while the business software and data are stored on servers at a remote location. The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security controls involved in a particular cloud environment. The risks will vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud vendor also referred to as a cloud service provider has implemented their specific cloud services. The level of risk availability of data and business functionality, protecting data from unauthorized access and handling security incidents.

KEYWORDS: Cloud Computing, Security, architecture, risk of cloud computing.

I. INTRODUCTION

Cloud computing has served the ever growing storage and data processing needs, however it has also given rise to a number of risks. The risks arise due to the various factors such as the location of the data centres, data segregation, data integrity, infrastructure and lack of knowledge about the governing policies. In a cloud computing environment, the resources are used when required and this is expected to translate into reduced costs of maintenance and elastic scalability. For example, in order to process a user request, the service provider decides upon the resources to be utilized for the particular task and when these resources needs to be released. Since the entire process is carried out by the service provider and not by the user, the security and integrity of the user's data becomes a significant concern. This paper analyses three major risks associated with cloud computing namely, 1) Security risks 2) Privacy risks 3) Consumer risks [1].

Cloud computing has caused a marketing fog as competing IT solution vendors redefine this seemingly simple term in their own image a practice called cloud washing making it difficult for business executives, cloud computing is a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to multiple external customers using internet technologies, Cloud computing enables businesses of all sizes to quickly procure and use a wide range of enterprises-class IT systems on a pay-per-use basis from anywhere at any time [2]. The availability of infrastructure as a service and platform as a service environments provided a fundamental base for building cloud computing based applications. It also motivated the research and development of technologies to support new applications. Since the adoption of the cloud computing paradigm by IBM Corporation around the end of 2007, other companies such as Google (Google App Engine), Amazon (Amazon Web Services (AWS), EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service)), Apple (iCloud) and Microsoft (Azure Services Platform) have progressively embraced it and introduced their own new products based on cloud computing technology [3]. However, cloud computing still poses risks related to data security in its different aspects (integrity, confidentiality and authenticity). In this paper, we review the main cloud computing architecture patterns and identify the main issues related to business issue in order to risk issues; we present a high level architecture models in cloud computing environments. This paper is organized as follows. In Section II, we present an overview of cloud computing, presenting a summary of its main features, architectures and deployment models. In Section III, we present related works. In Section IV, we introduce the risk of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

cloud computing in business. Finally, in Section IV, we conclude with a summary of risk of cloud computing in business.

II. CLOUD COMPUTING

The out of the cloud will come massive computing resources at prices that seem to defy economics—information and services that stream to the end user as if from some beneficent power. Like a river flowing from the mountains, the Internet "cloud" provides resources to distant points without incurring any extra charge. For example, you might get access to software that will help you design a sailboat to the latest principles of streamlined hull shapes. You might find advice and interactive guidance on how to cope with problems as you start a company. You might go through an interactive process, using video to show what your firm is doing, with venture capitalists that are looking for a worthy candidate in which to invest. Once you've tapped into the cloud, you cease to be an isolated individual and you become part of a larger digital cosmos, where everything is linked to everything. These data centers on the network foster new kinds of software that in themselves are marvels of recent engineering. With the Hadoop cloud-based data engine, data is lifted off hundreds or thousands of disk drives in parallel without "thrashing" the drive spindles—that is, forcing the drive heads to move this way and that in the struggle to collect data from a spinning disk. Other systems can't do it, but the cloud can map to the ends of the earth [4]. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service [5]. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers. [6]Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location; in other cases, entire business applications have been coded using web-based technologies such as AJAX.Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies [7][8].

A. Characteristics of Cloud Computing

The five essential characteristics of cloud computing and goes on to explain what they are in technical terms (Mell and Grance, 2009), On-demand self-service consumers can log on to a website or use web services to access additional computing resources on demand, that is, access additional computing resources on demand, that is, whenever they want them, without talking to a sales representative or technical support staff. Broad network access we can access cloud computing services from any internet connected device [11].

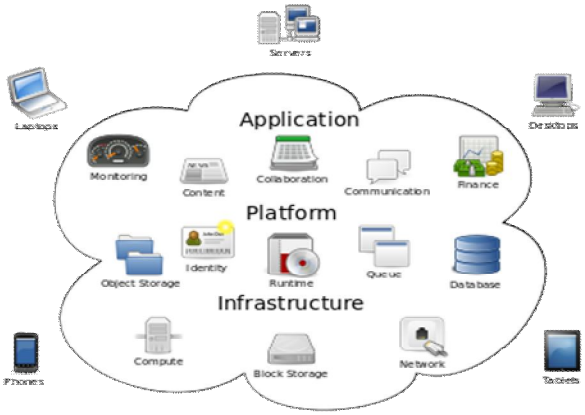

Fig.1. Cloud computing sample architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

B. Cloud Computing Architectures

Address key difficulties surrounding large-scale data processing. In traditional data processing it is difficult to get as many machines as an application needs. Second, it is difficult to get the machines when one needs them. Third, it is difficult to distribute and co-ordinate a large-scale job on different machines, run processes on them, and provision another machine to recover if one machine fails. Fourth, it is difficult to auto-scale up and down based on dynamic workloads. Fifth, it is difficult to get rid of all those machines when the job is done. Cloud Architectures solve such difficulties. Applications built on Cloud Architectures run in-the-cloud where the physical location of the infrastructure is determined by the provider.[10].

C. Layers of Cloud Computing

Once an internet protocol connection is established among several computers, it is possible to share services within any one of the following layers.

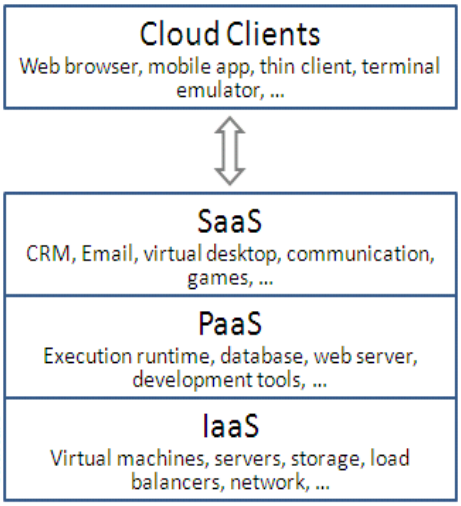

Fig.2. Layers of Cloud Computing.

A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery and that is in essence useless without it. Examples include some computers, phones and other devices, operating systems, and browsers. Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support. Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates Deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment [14]

D. Software as a Service (SaaS)

Software as a Service (SaaS) provides complete business applications delivered over the web. Advances in web technology such as Ajax, along with ubiquitous internet access, have made it possible to deliver the rich features and functionality of desktop applications in web browser. SaaS applications also make use of standards for web services, and these standards enable them to easily 'call on services' of other applications somewhere else on the web in order to exchange, include or 'mash up' data. The time savings that come with on-demand software, where nothing needs to be installed on a PC and new users can be added easily along with the pay-per –use business model have made SaaS success [11]. SaaS systems reduce costs since no software licenses are required to access the applications. Instead, users access services on demand. Since the software is mostly Web based, SaaS allows better integration among the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

business units of a given organization or even among different software services. Examples of SaaS include [3]: Google Docs and Customer Relationship Management (CRM) services.

E. Platform as a Service (PaaS)

Platform as a Service provides consumers with a stable online environment where they can quickly create test and deploy web applications using browser-based software development tools. There is less work involved in creating an application using PaaS than the traditional approach, which involves procuring and managing one or more servers for development, testing and production, and installing and configuring server software [11].PaaS provides an operating system, programming languages and application programming environments. Therefore, it enables more efficient software systems implementation, as it includes tools for development and collaboration among developers. From a business standpoint, PaaS allows users to take advantage of third party services, increasing the use of a support model in which users subscribe to IT services or receive problem resolution instructions through the Web. In such scenarios, the work and the responsibilities of company IT teams can be better managed. Examples of SaaS [4] include: Azure Services Platform (Azure), Force.com, Engine Yard and Google App Engine.

F. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) that caused the fire to take hold. LaaS provides consumers with administrative, web-based access to fundamental computing resources such as processing power, storage and networks. All cloud infrastructures depend on virtualization. By abstracting server software from the underlying hardware, multiple virtual machines, including operating systems, storage and installed software, can run on a single physical computer and share its processing power. In cloud computing, server virtualization is extended further, going beyond the more efficient use of a single physical machine or cluser to the aggregation and portioning of computing resources across multiple data centers. This enables cloud providers to efficiently manage and offer on-demand storage, servers and software resources for many different customers simultaneously [11].The term IaaS refers to a computing infrastructure, based on virtualization techniques that can scale dynamically, increasing or educing resources according to the needs of applications. The main benefit provided by IaaS is the payper-use business model [13]. Examples of IaaS [2] include: Amazon Elastic Cloud Computing (EC2) and Elastic Utility Computing Architecture Linking Your Programs to Useful Systems (Eucalyptus) [8].

G. Cloud computing Deployment

According to the intended access methods and availability of cloud computing environments, there are different models of deployment [4].Many industry experts dispute the validity of the four deployment models in the NIST (National Institute of Standards and Technology) definition framework, which are public clouds, community clouds, private clouds and hybrid clouds. Only public clouds are true clouds, but when the user experience and functional capabilities are the same, and there is the possibility of moving seamlessly across cloud boundaries [9].

Public: In this model, Infrastructure is made available to the public at large and can be accessed by any user that knows the service location. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used [8]. The cloud computing services are provided off-premise by third-party providers to the general public and the computing resources are shared with the provider's other customers [11].

Community: Several organizations may share the cloud services. These services are supported by a specific community with similar interests such as mission, security requirements and policies, or considerations about flexibility. A cloud environment operating according to this model may exist locally or remotely and is normally managed by a commission that represents the community or by a third party [8].Community clouds are used by distinct groups (or 'communities') benefits from public cloud capabilities but they also know who their neighbors are so they have fewer fears about security and data protection [11].

Private: The cloud may be local or remote, and managed by the company itself or by a third party. There are policies for accessing cloud services. The techniques employed to enforce such private model may be implemented by means of network management, service provider configuration, authorization and authentication technologies or a combination of these [8].Many large organizations prefer, or are legally obligated, to keep their servers, software and data within their own data centers; and private clouds enable them to achieve some of the efficiencies of cloud computing while

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

taking responsibility for the security of their own data. By implementing cloud computing technologies behind their firewall, enterprises can enable pooling and sharing of computing resources across different applications, departments or business units [12].

Hybrid: Involves the composition of two or more clouds. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds[9].Many enterprises take the 'hybrid cloud' approach by using public clouds for general computing while customer data is kept within a private cloud, community cloud or a more traditional infrastructure[11].

III. RELATED WORKS

In this section, we present related works in the fields of security, risks of cloud computing, a number of risks that should take account of before moving any business data or systems into public cloud. These risks include internal security breaches; cloud security breaches; data protection risks; data loss; vendor lock-in and vendor failure, risk vary from business to business and industry to industry. Every cloud service provider has installed various security measures depending on its cloud offering and the architecture. Their security model largely depends upon the customer section being served, type of cloud offering they provide as following comparative analysis [18]

TABLE I. COMPARATIVE ANALYSIS FOR STRENGTHS AND LIMITATIONS OF SOME OF THE EXISTING SECURITY SCHEMES

Security Scheme	Suggested Approach	Strengths	Limitations
Data Storage security	Uses homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data Modification and server colluding attacks as well as against byzantine failures.	The security in case of dynamic data storage has been considered. However, the issues with fine-grained data error location remain to be addressed.
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing.	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his requests.
Trust model for interoperability and security in cross cloud	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and transaction factors are taken into account for trust assignment.	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid cooperating/serving malicious users.	Security in a very large scale cross cloud environment is an active issue. This present scheme is able to handle only a limited number of security threats in a fairly small environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds.	The proposed model is in its early developmental stage and needs further simulations to verify the performance.
Secure virtualization	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files.	A virtualized network is prone to different types of security attacks that can be launched by a guest VM. An ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud environment	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the chances of information leakage.	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.

A. Internal Security Risks

If our business replaces its desktop software with web-based application, or its internal firewall-protected servers with externally hosted systems, then they becomes more easily accessible over the internet, but there are associated internal security risks whether they are cloud-based or not. There are ways to minimize the likelihood of internal security breaches, including internal processes, two-factor authentication and single sign-on.

1) Internal processes-Most businesses have checklists they use and processes they follow when employees take up or leave their Employment; but the deployment of new IT systems in public clouds can outpace the development of internal security processes , especially when they can set up by non-IT staff. Thus, whenever a new cloud-based system is introduced, checklists must be modified immediately and existing user account management processes must be followed, to ensure though good internal processes that all ex-employees and ex-contractors user accounts are deactivated immediately to reduce the risk of these accounts being misused or confidential data passed on to competitors.

2) Two-factor authentication- User names and passwords can be guessed or stolen, along with other personal information such as users mother's name maiden name or users place of birth, and so on. Thus if we really want to secure access to our cloud-based systems then two-factor authentication is a good solution.

3) Single sign-on- Employees may end up with user accounts on multiple cloud-based systems so password management becomes a problem, and the temptation is there to use the same password on different systems, which is a security risk. To deal with this issue of 'cloud proliferation' there are a number of commercially available federated identity services that enable users to log on to multiple clouds and internal IT systems though a single website [17].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

B. External Security Risks

Data stored in public clouds can be compromised as a result of failure in a provider's security technology or its operational security practices and this is a major risk in a multi-tenanted system where business competitors share the same IT infrastructure.

1) Security technology failures- An example of a Security technology failure in public cloud was the bug found in Google Docs (a Software as a Service system) in March 2009 that led to a small percentage of documents being inadvertently shared with unauthorized users.

2) Operational security failures- An example of an operational security failure in another software as a service system was the twitter hack of January 2009 where a hacker gained access to system support tools and look temporary control of the Twitter user accounts of user. But cloud are well aware that the most common fear about cloud computing, particularly in public clouds, is over security and a number of them have joined forces to form the cloud security alliance[15].

C. Data Protection Risks

If a security breach results in sensitive customer details being stolen our business may be prosecuted by national authorities, Penalized by standards bodies or sued by our customers. In the financial industry, regulations and standards are being imposed on organizations compelling them to use effective security controls, and in some cases specifying the type of controls to use. For example, the Payment Card Industry Data Security Standards (PCI DSS) specify two-factor authentication 'for remote access for all employees, administrators, and third parties'.

D. Data Loss

A public cloud is to remove a troublesome burden for our business and let someone else worry about data back-ups and failover systems. But cloud computing provider has completely redundant systems in multiple geographical locations and exactly how they recover from disasters, with evidence of successful test recoveries [16].

E. Risk Calculator

The appetite for risk varies from business to business and from industry to industry, but there is perhaps one golden rule when considering a cloud service: it is responsibility to ensure that the service provider can look after data and systems .With a particular service we must first attempt to calculate the risk associated with that service before making a decision about using it for a particular project[10].

IV. CONCLUSIONS

In this paper review the cloud computing is an Internet-based technology through which information is stored in servers and provided as a service and on-demand to clients. Cloud computing constructs on eras of research in virtualization, scattered computing, service computing, and, more recently, networking, web and software services. They may fear losing control of key systems and they may even fear for their jobs. It supervise to work more on front-end applications where there is potentially more business value to be gleaned .The security risk within public clouds, business is probably more likely to lose a laptop containing company data than to have data stolen from the cloud. The users should be aware of the risks and weaknesses present in the current cloud computing environment before being a part of the environment. A proper risk investigation approach will be of great help to both the service providers and the customers.

REFERENCES

1. Sneha Prabha Chandran and Mridula Angepat "Cloud Computing: Analysing the risks involved in cloud computing environments" School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden Sept 2007.
2. Mell,P and Grance,T(2009)[accessesed 12December 2009]'The NIST Definition of Cloud Computing', Version 15,10-7-09,National Institute of Standards and Technology Information Technology Laboratory, http://csrc.nist.gov/group/SNS/cloud-computing/cloud-def-v15.doc.
3. Xue Jing and Zhang Jian-jun, "A Brief Survey on the Security Model of Cloud Computing," 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), Hong Kong IEEE, pp. 475 – 478. Aug 2010.
4. "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. http://www.economist.com Retrieved 2009-11-03.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

5. Charles Babcock Management strategies for The Cloud Revolution: The Cloud revolution topics, The McGraw-Hill Companies, United States, 2010.
6. Minqi Zhou, Rong Zhang, Dadan Zeng, and Weining Qian, "Services in the cloud computing era: a survey," Software Engineering Institute. Universal Communication. Symposium (IUCS), 4th International. IEEE Shanghai, pp. 40-46. China. 978-1-4244-7821-7 (2010).
7. P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft). National Institute of Standards and Technology. ttp://csrc.nist.gov/groups/SNS/cloudcomputing. 2009. 30 may 2011.
8. Buyya, Rajkumar; Chee Shin Yeo, Srikumar Venugopal (PDF).Market-Oriented cloud Computing Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Department of Computer Science and Software Engineering, University of Melbourne, Australia. p. 9.
9. http://www.irishtimes.com/business-services/cloud-computing-ireland/getting-clear-about- computing.
10. Edna Dias Canedo and Robson de Oliveira Albuquerque "Review of Trust-based File Sharing in Cloud Computing" 2011The Fourth International Conference on Advances in Mesh Networks.
11. Jinesh Varia, "Cloud Architectures " june 2008.
12. Dr. Mark I Williams "A Quick Start Guide To Cloud Computing"2010.
13. P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft). National Institute of Standards and Technology. http://csrc.nist.gov/groups/SNS/cloudcomputing. 2009. 30 may 2011.
14. http://www.Wikipedia.com/cloud-Computing/cloud -Computing.html.
15. Zetter, K (2009) 'Weak Password Brings Happiness to Twitter Hacker', http://www.wired.com/thredtlevel/2009/01/professed-twitt/
16. Boggs,R et al (2009) 'Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology', IDC http://www.hp.com/hpinfo/newsroom/press_kits/2009/CompetitiveEdge/ReducingDowntime.pdf.
17. ITRC '2008 Data Breach Totals Soar', Identity Theft Resource Center,http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Souar.html.
18. Rohit Bhadauria, Sugata Sanyal ," Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", International Journal of Computer Applications (0975 – 888) Volume 47– No.18, June 2012.