Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Security Issues of Inter Cloud Computing

Sharmistha Dey, Sourav Auddy, Sonali Saha
Dept. of Computer Application
Guru Nanak Institute of Technology, India

Abstract— Cloud computing, one of the most robust and disruptive technologies in the very recent era, has been proven as a buzzword in today's technological world. Along with it's so many virtues like 24 x7 availability, optimized storage capacity, better utilization and maintenance ,cloud computing has become a well accepted and highly popular technology among many industrial as well as academic organizations. Small and medium companies use cloud computing services for various reasons, either to get a faster access to their applications or to reduce their infrastructure costs. In spite of all the virtues, security and privacy are still now being the matter of concern for the cloud providers as well as cloud users. Inter cloud or multi-cloud, being a widely adapted technology of today, provides better utilization, cost and storage optimization and effective services with mutual understanding among several cloud service providers. Like single cloud service, the security and privacy issues are a matter of concern in case of inter cloud communication, where several service providers collaborate with each other for providing cloud services. In order to make the cloud system to be able to continue to satisfy demands for guaranteed quality of service availability and performance, even in such cases, it is indispensable to organize that cloud systems complement each other such as to procure resources from other cloud systems by cooperating with other cloud system (inter-cloud) connected via broadband networks. This paper discusses about a brief overview of the cloud system, its pros and cons and then gives a deeper view of the inter cloud system architecture and the security issues arises in case of inter cloud communication like distributed denial of services or effect due to a malicious code, in an analytical manner.

Keywords— Data Unavailability, Insecure API, Multi Tenancy, Cloud Broker, Cloud Exchange

I. INTRODUCTION

Cloud computing, or something being in the cloud, is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically re-allocated per demand. The name "cloud" came from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. The cloud symbol was used to represent the Internet as early as 1994.The core concept of cloud computing comes around the year of 2004-2005. In the year 2006, when Amazon Web service (AWS) was first launched on a utility computing basis, the essence of cloud computing started for the industry. The agility, multi tenancy, virtualization and better performance of a cloud has made this technology enormously growing with the time. With traditional "off-the-shelf" software packages, an application is normally installed on the company's main server, and then on each computer in the office.

A. Architecture of Cloud:

From an architectural perspective, there is much confusion surrounding how cloud is both similar to and different from existing models of computing and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices [Figure I].

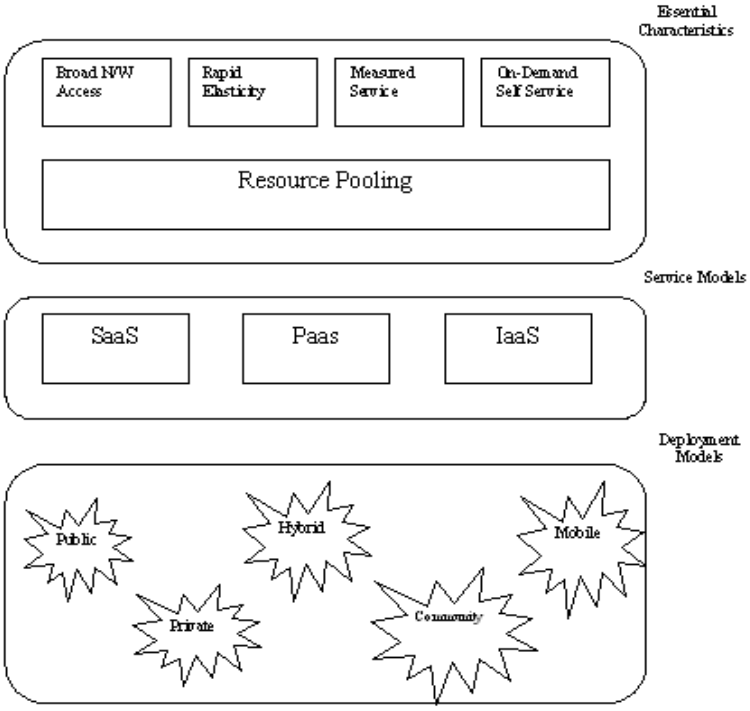

Figure I: Architecture of Cloud

B. Characteristics of Cloud:

Cloud computing exhibits the following key characteristics:

- **On-demand self-service:**

On-demand self-service allows users to obtain, configure and deploy cloud services themselves using cloud service catalogues, without requiring the assistance of IT[15]. This feature is listed by the National Institute of Standards and Technology (NIST) as a characteristic of cloud computing. The self-service requirement of cloud computing prompts infrastructure vendors to create cloud computing templates, which are obtained from cloud service catalogues.

- **Broad network access:**

Cloud capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, tablets, laptops, and workstations.

- **Resource pooling:**

The provider's computing resources are pooled together to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center).

- **Rapid elasticity:**

The cloud is elastic, meaning that resource allocation can get bigger or smaller depending on demand. Elasticity enables scalability, which means that the cloud can scale upward for peak demand and downward for lighter demand. Cloud services can be rapidly and elastically provisioned and released, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

- **Measured service:**

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service such as storage, processing, bandwidth, and active user account. Cloud computing resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

- **Multi tenancy:**

Multi tenancy is an important property of cloud which enables sharing of resources and costs across a large pool of users thus allowing for centralization of infrastructure in locations with lower costs, peak-load capacity increases, utilization and efficiency improvements. It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Cloud Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

- **Standardized interfaces:**

Application Program Interface (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs. Cloud services

should have standardized APIs, which provide instructions on how two application or data sources can communicate with each other. A standardized interface lets the customer more easily link cloud services together.

C. Cloud Service Models:

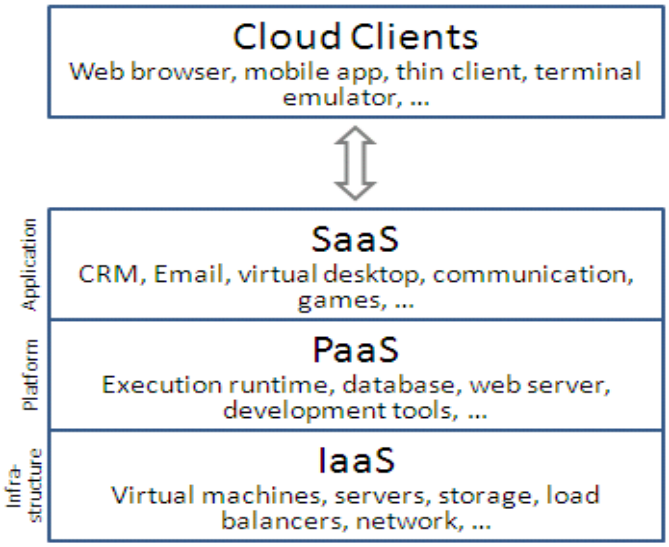

Figure II: Cloud Service Model

1) **Infrastructure-as-a-Service(IaaS):**The Infrastructure as a Service(IaaS) is a provision model in which an organization outsourcers the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it[Figure 2]

2) **Platform as a Service (PaaS) :** It is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries.

3) **Software as a Service (SaaS):** SaaS represents the capability provided to the cloud user to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin-client interface such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, but only some limited user-specific application configuration settings. SaaS allows a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider.

D. Deployment Models of cloud:

There are four primary Cloud Deployment Models – Public, Private, Mobile and Hybrid. Each of the Cloud Deployment Models provides much needed sources for different set of business needs. Surely the Cloud Computing is the next big thing that would happen to the businesses in the upcoming years.

- **Public Cloud:** Public cloud applications, storage, and other resources are made available to the general public by a service provider, using a free to all services or a pay per use model.
- **Private Cloud:** Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally .It is also known as Internal Cloud or Corporate Cloud. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service.
- **Hybrid Cloud:** Organizations may host critical applications on private clouds and applications with comparatively less security concerns on the public cloud. In case of hybrid cloud computing, both private and public type of cloud computing is combined together. This is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.
- **Mobile Cloud :** Mobile cloud computing is the usage of cloud computing in combination with mobile devices. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. In case of mobile cloud, Applications are run on a remote server and then sent to the user.

II. Inter Cloud Communication

Inter Cloud or multi cloud is a highly adapted technique for the cloud providers providing better utility and effective service to the cloud users with mutual understanding among different service providers. The Inter cloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based. The term was first used in the context of cloud computing in 2007 when Kevin Kelly opined that "eventually we'll have the inter-cloud, the cloud of clouds". It became popular in early 2009 and has also been used to describe the data center of the future[14]. Cloud hosting is largely intended to deliver on-demand services. Through careful use of scalable and highly engineered technologies, cloud providers are able to offer customers the ability to change their levels of service in many ways without waiting for physical changes to occur. Terms like rapid elasticity, resource pooling and on-demand self-service are already part of cloud hosting service designs that are set up to make sure the customer or client never has to deal with limitations or disruptions.

A. Inter Cloud Architecture:

The inter-cloud architecture shows the high level components of the service-oriented architectural framework consisting of client's brokering and coordinator services that support utility-driven federation of clouds: application scheduling, resource allocation and migration of workloads. The architecture cohesively couples the administratively and topologically distributed storage and computes capabilities of Clouds as parts of single resource leasing abstraction[Figure III].

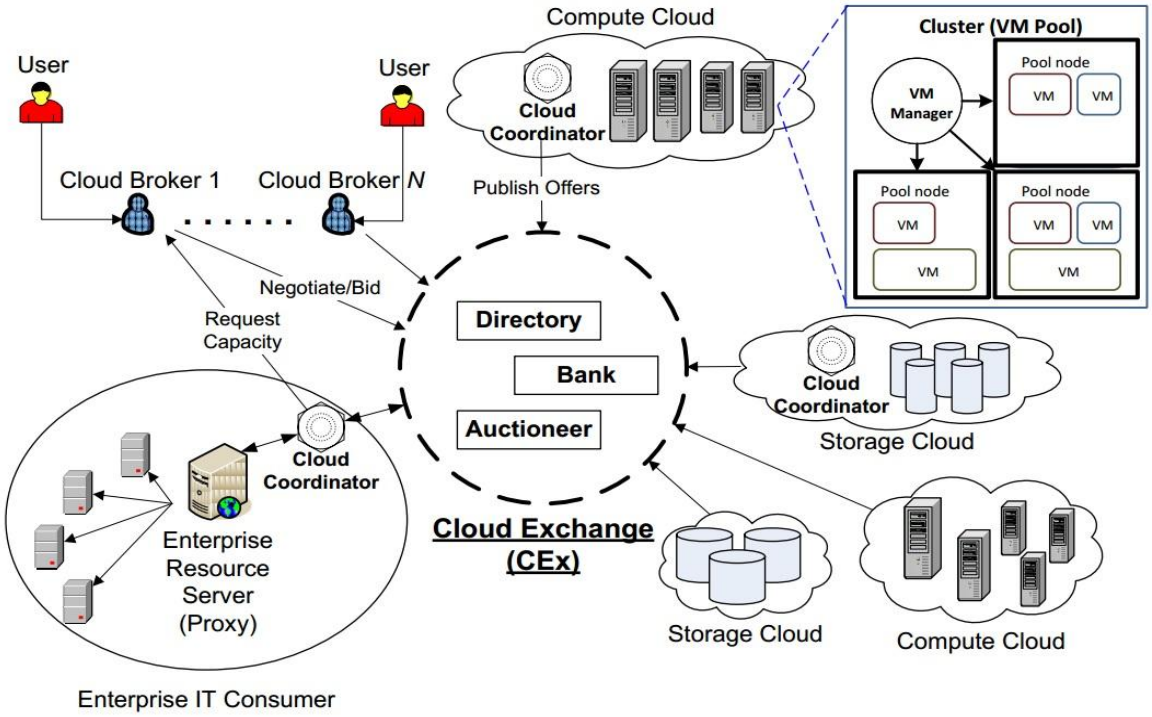

Figure III: Inter Cloud Architecture

The Cloud Exchange (CEx) acts as a market maker for bringing together service producers and consumers. It aggregates the infrastructure demands from the application brokers and evaluates them against the available supply currently published by the Cloud Coordinators. The Cloud Coordinator service is responsible for the management of domain specific enterprise Clouds and their membership to the overall federation driven by market-based trading and negotiation protocols. It provides a programming, management, and deployment environment for applications in a federation of Clouds. The Cloud Coordinator exports the services of a cloud to the federation by implementing basic functionalities for resource management such as scheduling, allocation, (workload and performance) models, market enabling, virtualization, dynamic sensing/monitoring[1].

In Inter-cloud architecture**,** the components allocate virtual machines to the Cloud nodes based on user's QoS targets and the Clouds energy management goals. The devices like VMware or sensor provides a good infrastructural support to the inter-cloud architecture increasing the power of cloud services and productivity.

B. Advantages of Using Inter-Cloud over single provider service:

There are some reasons for which Inter Cloud has been preferred now a day's [6].

- **Enhance Security:** With Inter-Cloud, no data goes through the Internet. You access your outsourced critical applications through an end-to-end private network, including the access to public Clouds
- **Benefit from commitments on performances**: Through specific agreements with the main Cloud Computing Service Providers and a network specifically designed for this purpose, Inter Cloud improves hosted applications' performance with a smooth flow and comparable to internal applications.

- **Benefit from the Flexibility of on-demand service:** Inter-Cloud designed a network that can adjust itself to any billing model of Cloud Computing, on a per-user unit basis rather than a per- bandwidth basis , but per-user or per-use.
- **Benefit from an end-to-end commitment**: Inter Cloud is committed on performance and on service continuity, from the customer site to the outsourced platform, thus filling the existing vacuum in terms of service level commitment between the Cloud and the end users.
- **Benefit from a one-stop shop:** Inter Cloud is the single contact for all outsourced applications, whether they are hosted on private or public Clouds, allowing the IT department to answer all network, security and performance related issues for its outsourced services.
- **Optimize your costs:** Inter Cloud has heavily invested in interconnection infrastructures with the main Cloud Computing Providers, and Private Cloud Providers in particular. Therefore, using the Inter Cloud network rather than your usual network operator to connect to these services is leads to substantial cost savings.
- **Rely on a trusted third party:** As a neutral intermediary between you and Cloud Service Providers , InterCloud can claim a position of privileged partner to IT departments.. Inter Cloud can objectively perform transparent audits in regards to hosted applications.

III. Security Issues and Inter Cloud

In spite of having so many virtues like better utilization capacity, flexibility of on demand service, cost optimization , inter cloud has to face many security and privacy problems like data unavailability, Insecure API or rely on a trusted third party.

A. Security Issues faced by Inter-Cloud:

1) Data Integrity: Data integrity is one amidst the foremost vital constituents in any system. Data integrity is decisively accomplished throughout a standalone scheme with one data. Data integrity in such a scheme is sustained by info constraints and transactions [13].

2) Service Unavailability: One of the most critical problems in Inter- cloud services is service accessibility or service availability. Service accessibility is most important in the cloud computing security. Amazon currently mentions in its authorizing agreement that it is possible that the service might be unavailable from time to time. The user's World Wide Web service may terminate for any cause at any time if any user's documents shatter the cloud storage principle ([1]-[4],[15]).

Some attacks in case of Inter-cloud causes serious problems with this issues. Distributed Denial of Service attack[Figure IV] is a popular attack which has been proven as a major concern for the Inter-cloud researchers. With different service providers, in case of inter-cloud the risk enhances much more than single cloud service.

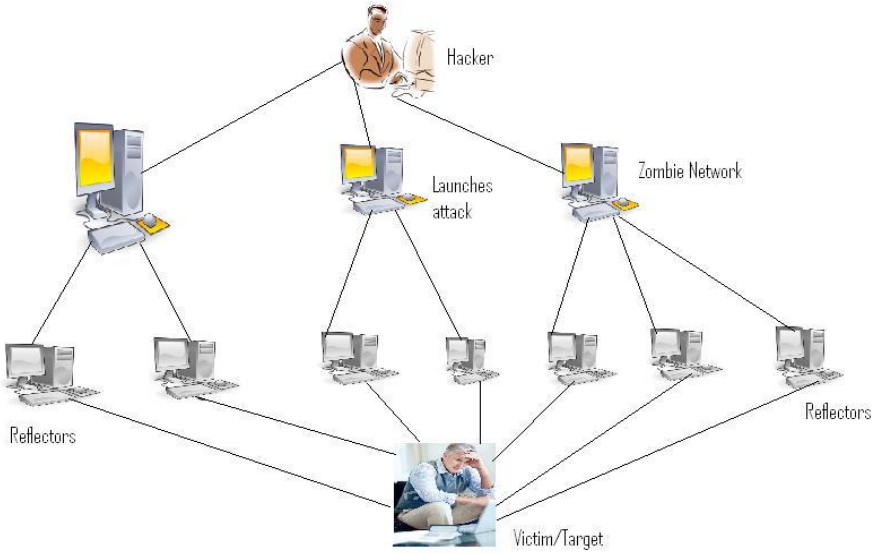

Figure IV: Distributed Denial of Service(DDOS) Attack

***D*istributed *D*enial *o*f *S*ervice** is a special type of DOS attack where multiple compromised systems are used, which are usually infected with a Trojan and used to target a single system causing a Denial of Service (DoS) attack In this attack, the eavesdropper being the master component, launches the attack on the victim, using a compromised network which is in turn divided into two separate layers . This attack is very vulnerable especially for shared environment like cloud, where sometimes even the service provider does not know from where the service has come to them and where the data has been stored. There are some other issues except those two issues which have been discussed in the table below[See Table I][12] :

Table I :Security Issues in Inter-Cloud

Security Issue	Explanation
Data Security	Encryption, fine grained authorization
Network Security	All data flow over the network needs to be secured in order to prevent leakage of sensitive information. Traditional network security issues: Man in the middle, IP spoofing ,Port scanning
Data locality	Due to compliance and data privacy laws in various countries, location of data is of utmost importance in many enterprise architecture.
Data Segregation	As a result of multi-tenancy multiple users can store their data using the applications provided by SaaS. In such a situation, data of various users will reside at the same location, so Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system.
Data Access	Data access issue is mainly related to security policies provided to the users while accessing the data.
Virtualization Vulnerability	Ensure isolation of different instances running on the same physical machine [Current VMMs (Virtual Machine Monitor) do not offer perfect isolation]. Also Controls host and guest operating system by the administrator.
Insecure Interfaces and APIs	The security and availability of general cloud services is dependent upon the security of these basic APIs .his introduces the complexity of the new layered API.

IV. Conclusion and Future Scope

The privacy and security area in cloud computing leaves an ample scope for the Inter-cloud researchers and developers. This newly emerging technology is still on the growing stage leaving a huge scope of discovering issues in the security and privacy area. This paper analytically discusses about major issues faced by inter-cloud and tries to categorize those issues. A lots of specific goals have been identified in this field. Our goal is to discuss several issues by comparing the priority among those, with a more quantitative approach.

References:

1. Rajkumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros *,"InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Service",*C.-H. Hsu et al. (Eds.): ICA3PP 2010, Part I, LNCS 6081, pp. 13–31, 2010. © Springer-Verlag Berlin Heidelberg 2010
2. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "*An analysis of security issues for cloud computing"* Hashizumeet al. Journal of Internet Services and Applications2013,4:5, http://www.jisajournal.com/content/4/1/5
3. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom,"*Cloud Computing Security: FromSingle to Multi-Cloud ",*2012 45th Hawaii International Conference on System Sciences
4. Mohemed Almorsy, John Grundy and Amani S. Ibrahim, *Collaboration-Based Cloud Computing Security Management Framework*, 2011 IEEE International Conference on Cloud Computing (CLOUD 2011), Washington DC, USA on 4 July –9 July, 2011, IEEE
5. C.Kishor Kumar Reddy, SK. Lokesh Naik, B.Suresh Kumar and S.K.Prasanth, *Cloud Specific Issues and Vulnerabilities solutions*, International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012, ISSN 2229-5518
6. https://www.intercloud.com/why/10-reasons/
7. Deepak Kumar, Amit Kumar Tyagi and Sadique Nayeem, *"Handling of Incident, Challenges, Risks, Vulnerability and Implementing Detection approaches inside the Cloud",* International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 2
8. "SANS Institute InfoSec Reading Room", a white paper publication from SANS Institute Reading Room site., June 19, 2006
9. Cloud Security Alliance(CSA), *The Notorious Nine Cloud Computing Top Threats in 2013*, February 2013
10. Manish M. Potey, C A Dhote and Deepak H. Sharma," *Cloud Computing – Understanding Risk, Threats, Vulnerability and Controls: A Survey",* , International Journal of Computer Applications (0975 – 8887) Volume 67– No.3, April 2013
11. Yanpei Chen, Vern Paxson and Randy H. Katz," *What's New About Cloud Computing Security?",* Technical Report No. UCB/EECS-2010-5, Electrical Engineering and Computer Sciences University of California at Berkeley.

12. Sahar Mohammed Abduljalil, Osman Hegazy and Ehab E. Hassanein, *A Novel Approach for Handling Security in Cloud Computing Services,* International Journal of Computer Applications (0975 – 8887) Volume 69– No.5, May 2013
13. Monali Shrawankar and Ashish Kr. Shrivastava, *Comparative Study of Security Mechanisms in Multicloud Environment,* International Journal of Computer Applications (0975 – 8887) Volume 77 – No.6, September 2013
14. http://en.wikipedia.org/wiki/Intercloud
15. http://en.wikipedia.org/wiki/Cloud_computing

Acknowledgment

Sharmistha Dey: The author is an assistant professor in Guru Nanak Institute of Technology from Computer Application Department. She has completed her M Tech from Calcutta University with research work on security metrics of cloud computing. She has also done Post Graduation diploma in Journalism and Mass Communication from Jadavpur University. Her research areas are cloud computing, Wireless Mesh Network, Intrusion detection system.

Sourav Auddy: The author is a student of Master of Computer Application from Guru Nanak Institute of Technology. He has global certification on RHCE. He has the knowledge and experience on Server Administrations and Networking. His research areas are Cloud Computing, Network Security.

Sonali Saha: The author is a student of Master of Computer Application from Guru Nanak Institute of Technology. She also received her Bachelor of Science degree in Computer Application in 2010.Her research includes Cloud computing and Inter Cloud Communications.

