www.ioirp.com

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 10. September 2015

IMPROVING SECURITY REQUIREMENTS IN CLOUD COMPUTING

C.Radha
Department of MCA
Muthayammal Engineering College
Namakkal, Tamilnadu
radhamca7@gmail.com

P.Sakthi Priyanka
Department of MCA
Muthayammal Engineering College
Namakkal, Tamilnadu
sakthipriyanka91@gmail.com

Dr.S.Prabha
Principal
Sri Sarada Niketan College of Arts and Science for Women
Salem, Tamilnadu
s.prabhakumaravel@yahoo.co.in

***Abstract*-Cloud computing is technology where the users' can use high end services in form of software that reside on different servers and access data from all over the world. Cloud storage enables users to access and store their data anywhere. The concepts of cloud computing is based on various technologies like virtualization, grid and utility computing. The service oriented, loose coupling, strong fault tolerant, business model and ease use are main characteristics of cloud computing. Most of the IT industries today are moving onto cloud to meet their high computational requirements with reduced cost. Grid computing in the simplest case refers to cooperation of multiple processors on multiple machines and its objective is to boost the computational power in the fields which require high capacity of the CPU. In grid computing multiple servers which use common operating systems and software have interactions with each other. Grid computing is hardware and software infrastructure which offer a cheap, distributable, coordinated and reliable access to powerful computational capabilities. This paper strives to show the importance of cloud computing and its security from various angles.**

Keywords-Cloud Computing, Distributed, Grid Computing, Resources Sharing, Security,

I. INTRODUCTION

Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has become important issues to highlight. There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software -, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software NIST defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction". It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use. It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues. According to, 91 % of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment.

A. Types of Clouds

Several different configurations of cloud computing and its deployment models exist to serve the enterprise's needs. Each approach offers its own strengths, risks, and level of control it provides the cloud consumer. See fig 1 for a representation of the types and deployments models.

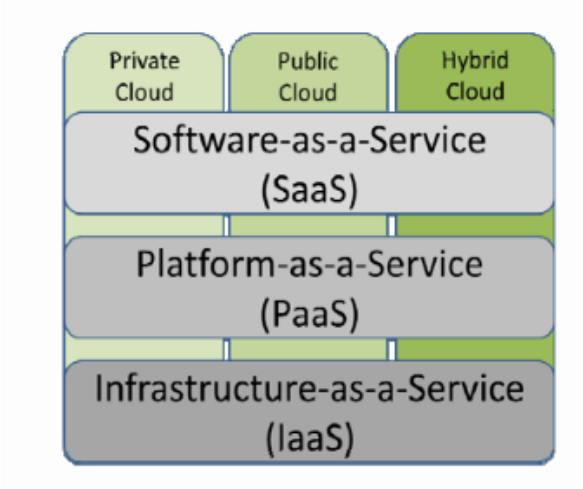

Fig. 1. Types of clouds

1) Software as a Service

In an October 2009 publication, Peter Mell and Tim Grance of the U.S. National Institutes of Standards & Technology (NIST) defined Software as a Service (SaaS) as the capability for a consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure – including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. An example of SaaS would be online tax filing.

2) Platform as a Service

Platform as a Service (PaaS) provides the cloud consumer with the capability to deploy applications onto the cloud platform using programming languages and tools that are supported by the cloud provider. The cloud consumer does not manage or control the underlying cloud infrastructure – including network, servers, operating systems, or storage, which is all fully managed by the cloud provider. However, the cloud consumer can control the deployed applications and possibly the application hosting environment configurations. Microsoft™ Azure and Google App engine are examples of PaaS.

3) Infrastructure as a Service

Infrastructure as a Service (IaaS) gives the cloud user the most control of the three types of clouds. The cloud consumer has the ability to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software such as operating systems and applications. Although the cloud consumer has control over the operating system, storage and deployed applications, the cloud provider is still responsible for the control of the underlying cloud infrastructure. However businesses using the IaaS cloud service model are typically responsible for securing their own virtual machines and the applications and data that reside on them. Amazon EC2 or vCloud are examples of IaaS.

II. EXISTING SYSTEM

A. *Grid Computing*

Grid computing is a computer network in which each computer's resources are shared with very other computer in the system. Processing power, memory and storage devices are all community resources that authorized users can tap into and leverage for specific tasks. A grid computing system can be as simple as a collection of similar computers running on the same operating system or as complex as inter-networked systems comprised of every computer platform you can think of. Grid computing is concerned with the sharing and coordinated use of diverse resources in distributed "virtual organizations." Grid computing has been a buzzword in information technology since past few years. Grid computing is an infrastructure involving collaboration of computers, databases & network resources available, to perform manipulation of intensive and large scale data set problems. The hike in the complexities of computational problems in modern era of science and technology forced the engineers and scientists to cross the organizational boundaries to get desired data manipulation. The best logical solution to this issue is distribution of the problem set over multiple computational resources/nodes. Several solutions to grid computing has been

developed and are still evolving, since the notion of Grid sprang up in mid 1990s, most of which came from the academic research projects. Selection and sharing of resources worldwide is the fundamental working logic behind grid computing which can be represented by Fig.2.

Fig. 2. Grid Computing

B) Types of Grid

•Computational grids

These type of grid are meant to provide secure access to computational resources, sufficient enough to perform processing of computational problems which otherwise would have required high computing power machines.

•Collaboration grid

With the advances in network hardware resources and internet services, demand for better collaboration has increased. Such desired collaboration is best possible with these kinds of grids.

•Utility Grid

In this type of grid not only CPU cycles are shared, also other softwares and special peripherals like sensors are also shared.

•Network grid

Even if we have computational machines with enough computational power as a part of grid but with poor network communication one can't utilize those machines optimally. Network grid provides high performance communication using data caching between nodes there by speed-up communication with each cache nodes acting as router.

•Data grid

There are two things, data and computation over that data. Data grid provides the support for data storage other data related services like data discovery, handling, publication, etc.

C) Grid Architecture

In grid computing infrastructure resources belong to and come from physically scattered administrative domains to collectively provide various resources (data, computing, and network) to the users. In a grid, computing nodes might not be placed at common physical location but can be independently operated from different locations. Each computer on the grid is a distinct computer. Collection of servers clustered together to work out a common problem forms a grid. The computers joined to form a grid may even have different hardware and operating systems. Grid consists of a layered architecture model providing protocols and service at five different layers represented by Fig.3.

1) Fabric layer

Fabric layer sits at the bottom of this layered architecture; it provides shareable resources such as network bandwidth, CPU time, memories, scientific instruments like sensors, telescope, etc. Data received by sensors at this layer can be transmitted directly to other computational nodes or can be stored in the database over grid. Standard grid protocols are responsible for resource control. Accomplishment of sophisticated sharing operation is the measure for quality of this layer. Operating system, queuing systems and processing kernels also form the part of this layer.

2) Connectivity layer

This layer specifies the protocols for secure and easy access. Protocols related to communication and authentication required for transactions are placed in this layer. These communication protocols permit the exchange of data between resource layer and fabric layer. Authentication protocols are meant to provide secure cryptographic mechanisms for identification of users and resources. E.g. GSI – Grid Security Infrastructure (built around existing TLS protocols).

3) Resource layer

This layer specifies the protocols for operating with shared resources. Resource layer build on the connectivity layer's communication and authentication protocols to define Application Program Interfaces (API) and software development kit (SDK) for secure negotiation, accounting, initiation, control, monitoring and payment of sharing resources. E.g. GRIP (Grid resource Information Protocol; based on LDAP), GRAM (Grid Resource Access and Management) for allocation and monitoring of resources.

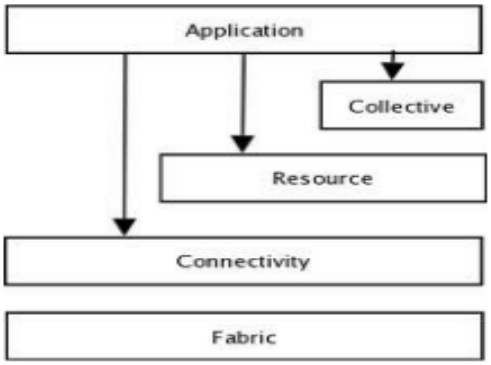

Fig. 3. Grid Architecture

4) Collective layer

This layer consists of general purpose utilities. Any collaborative operations in the Shared resources are placed in this layer and it coordinates sharing of resources like directory services, co-allocation, scheduling, brokering services, monitoring and diagnostic services, data replication services.

5) Application layer

At the top of the grid layered architecture sits the application layer. This layer consists of application which the user will implement. Moreover, this layer provides interface to the users and administrators to interact with the grid.

D) Security risks involved in Grid Computing

There are security risks in every application downloaded from the Internet. Whenever you link two or more computers together, you have to prepare yourself for certain questions. How do you keep personal information private? How do you protect the system from malicious hackers? How do you control who can access the system and use its resources? How do you make sure the user doesn't tie up all the system's resources? Thus Security requirements are fundamental to the grid design. The critical problems are resource discovery, authentication, authorization, and access mechanism. Without this functionality, the integrity and confidentiality of the data processed within the grid would be at risk.

III. PROPOSED SYSTEM

A. Cloud Computing

Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. Enterprises are rapidly adopting cloud services for their businesses, measures need to be developed so that organizations can be assured of security in their businesses and can choose a suitable vendor for their computing needs. Cloud computing depends on the internet as a medium for users to access the required services at any time on pay-per-use pattern. However this technology is still in its initial stages of development, as it suffers from threats

and vulnerabilities that prevent the users from trusting it. Various malicious activities from illegal users have threatened this technology such as data misuse, inflexible access control and limited monitoring. The occurrence of these threats may result into damaging or illegal access of critical and confidential data of users. In this paper we identify the most vulnerable security threats/attacks in cloud computing, which will enable both end users and vendors threats associated with cloud computing and propose relevant solution directives to strengthen security in the Cloud environment. We also propose secure cloud architecture for organizations to strengthen the security.

Cloud computing is current buzzword in the market. It is paradigm in which the resources can be leveraged on peruse basis thus reducing the cost and complexity of service providers. Cloud computing promises to cut operational and capital costs and more importantly let IT departments focus on strategic projects instead of keeping datacenters running. It is much more than simple internet. It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. There are numerous benefits of this construct. For instance other company hosts user application. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well.

B) Cloud Computing Security

Key references such as CSA's security guidance and top threats analysis , ENISA's security assessment and the cloud computing definitions from NIST high- light different security issues related to cloud computing that require further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption. Emphasis is given to the distinction between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification. However, no other methods are standardized or even employed to organize cloud computing security aspects apart from cloud deployment models, service types or traditional security models. Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:

1) Network security

Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks, adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process.

a) Transfer security: Distributed architectures, massive resource sharing and virtual machine(VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.

b) Firewalling: Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders. They also enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of-Service (DoS) and detection of external security assessment procedures. Efforts for developing consistent firewall and similar security measures specific for cloud environments reveal the urge for adapting existing solutions for this new computing paradigm.

c) Security configuration: Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency

2) Interfaces

Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.

a) API: Programming interfaces (essential to IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use .

b) Administrative interface: Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations).

c) User interface: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment.

d) Authentication: Mechanisms required to enable access to the cloud. Most services rely on regular accounts consequently being susceptible to a plethora of attacks whose consequences are boosted by multi-tenancy and resource sharing.

3) Data security

Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels). (a) Cryptography: Most employed practice to secure sensitive data, thoroughly required by industry, state and federal regulations. (b) Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes and, thus, mission-critical data integrity and availability must be ensured. (c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion. In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement.

4) Virtualization

Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies.

a) Isolation: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks. The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.

b) Hypervisor vulnerabilities: The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.

c) Data leakage: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.

d) VM identification: Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.

e) Cross-VM attacks: Includes attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks. One example consists in overlapping memory and storage regions initially dedicated to a single virtual machine, which also enables other isolation-related attacks.

5) Governance

Issues related to (losing) administrative and security controls in cloud computing solutions .

a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.

b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.

c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.

6) Compliance

Includes requirements related to service availability and audit capabilities.

a) Service Level Agreements (SLA):

Mechanisms to ensure the required service availability and the basic security procedures to be adopted.

b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.

c) Audit: Allows security and availability assessments to be performed by customers, providers and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions and are usually required by contracts or legal regulations. There are solutions being developed to address this problem by offering a transparent API for automated auditing and other useful functionalities.

d) Service conformity: Related to how contractual obligations and overall service requirements are respected and offered based n the SLAs predefined and basic service and customer needs.

7) Legal issues

Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

a) Data location: Customer data held in multiple jurisdictions depending on geographic location are affected, directly or indirectly, by subpoena law-enforcement measures.

b) E-discovery: As a result of a law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware. Data disclosure is critical in this case.

c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information.

d) legislation: Juridical concerns related to new concepts introduced by cloud computing.

C) Cloud Computing Security Taxonomy

Aiming to create a security model both for studying security aspects in this context and for supporting decision making, in this section we consider the risks and vulnerabilities previously presented and arrange them in hierarchical categories, thus creating a cloud security taxonomy. The architecture dimension is subdivided into network security, interfaces and virtualization issues, comprising both user and administrative interfaces to access the cloud. It also comprises security during transferences of data and virtual machines, as well as other virtualization related issues, such as isolation and cross-VM attacks. The architecture group allows a clearer division of responsibilities between providers and customers, and also an analysis of their security roles depending on the type of service offered (Software, Platform or Infrastructure). This suggests that the security mechanisms used must be clearly stated before the service is contracted, defining which role is responsible for providing firewalling capabilities, access control features and technology-specific requirements (such as those related to virtualization).The compliance dimension introduces responsibilities toward services and providers. The former includes SLA concerns, loss of service based on outages and chain failures, and auditing capabilities as well as transparency and security assessments. The latter refers to loss of control over data and security policies and configurations, and also lock-in issues resulting from lack of standards, migrations and service terminations. The privacy dimension includes data security itself (from sensitive data, regulations and data loss to disposal and redundancy) and legal issues (related to multiple jurisdictions derived from different locations where data and services are hosted). We note that the concerns in this dimension cover the complete information lifecycle (i.e., generation, use, transfer, transformation, storage, archiving, and destruction) inside the provider perimeter and in its immediate boundaries (or interfaces) to the users. A common point between all groups is the intrinsic connection to data and service lifecycles. Both privacy and compliance must be ensured through all states of data, including application information or customer assets, while security in this case is more oriented towards how the underlying elements (e.g., infrastructural hardware and software) are protected.

Fig. 4. Cloud Security Taxonomy

D) Secure Cloud Architecture

We propose cloud security architecture, which protect organization against security threats and attacks. The key points for this architecture based on our analysis of existing security technologies are:

1) Single Sign-on (SSO)

Currently, Users are having multiple accounts in various Service Providers with different usernames accompanied by different password. Therefore the vast majority of network users tend to use the same password wherever possible, posing inherent security risks. The inconvenience of multiple authentications not only causes users to lose productivity, but also imposes more administrative overhead. Enterprises today are seriously considering the use of Single Sign On (SSO) technology to address the password explosion because they promise to cut down multiple network and application passwords to one. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign- On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.

2) Defence in depth Security Approach

As enterprise networking technology has evolved, so too has enterprise security. What began simply as setting up a perimeter around the network via fairly basic security tools like firewalls and email gateways, has evolved into adding an array of virtual private networks (VPNs), virtual local area network (VLAN) segmentation, authentication, and intrusion detection systems (IDS)—necessary to handle the consistently growing number of threats to the corporate network. Virtual firewall appliances should be deployed instead of first-generation firewalls. This allows network administrators to inspect all levels of traffic, which includes basic web browser traffic, to peer-to-peer applications traffic and encrypted web traffic in the SSL tunnel .Intrusion Prevention Systems (IPS) should be installed to protect networks from internal threats from insiders.

3) Increase Availability

Availability is a reoccurring and a growing concern in software intensive systems. Cloud systems services can be turned offline due to conservation, power outages or possible denial of service invasions. Fundamentally, its role is to determine the time that the system is up and running correctly; the length of time between failures and the length of time needed to resume operation after a failure. Availability needs to be analyzed through the use of presence information, forecasting usage patterns and dynamic resource scaling. Access to cloud service should be available all the time, even during maintenance. This makes critical business data stored in the cloud to be always available to cloud users, reducing network down time, thereby increasing business profits. This can be done by implementing high availability technologies such as active/active clustering, dynamic server load balanced and ISP load balancing within the network infrastructure.

4) Data Privacy

Cloud data privacy problem will be found at every stage of the life cycle. For the data storage and use, Mow bray et al. proposed a client-based privacy management tool that provides a user-centric trust model to help users control their sensitive information during the cloud storage and use. Data loss prevention (DLP) tools can help control migration of data to the cloud and also find sensitive data leaked to the cloud. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. DLP help a network administrator control what data end users can transfer. End users do not send sensitive or critical information outside of the corporate network. DLP help a network administrator control what data end users can transfer.

5) Data Integrity

As a result of large scale data communication cost, the users don’t want to download data but verify its correctness. Therefore, users need to retrieve the little cloud data through some kinds of agreements or knowledge’s which are the probability of analytical tools with high confidence level to determine whether the remote data integrity. User can do the increase and decrease of the data capacity in the cloud server with the help of CSP (cloud service provider) in his request. This storage level must be with flexible and durability condition as far as its entire design or structure is concerned. Thus it should be claimed extra storage space concerning future process in data exchange.

6) Virtual Machine Protection

You can't just install your firewall or antivirus software on a cloud-based virtual machine. Physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running 10 virtualized servers. Because VMs can start, stop and move from hypervisor to hypervisor at the click of a button, whatever protection you've chosen has to handle these activities with ease. Plus, as the number of VMs increases in the data center, it becomes harder to account for, manage and protect them. And if unauthorized people gain access to the hypervisor, they can take advantage of the lack of controls and modify all the VMs housed there. These virtual machines are vulnerable like their physical counterparts. Hence, to adequately protect virtual machines, they should he isolated from other network segments and deep inspection at the network level should be implemented to prevent them both from internal and external threats. Illegal internal access should be restricted by implementing intrusion prevention systems and unauthorized external access should be protected by using secure remote access technologies like IPSec or SSL VPN.

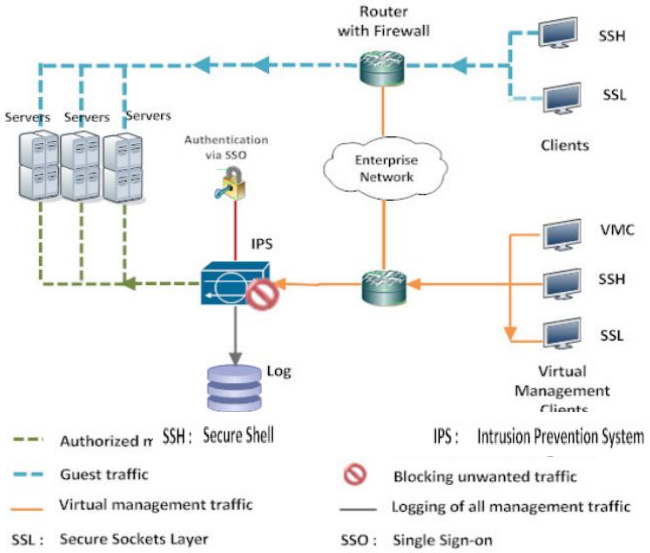

Fig. 5. Secure Cloud Architecture

IV. COMPARISON BETWEEN CLOUD AND GRID COMPUTING

There are many important features that are common to both Cloud and Grid. The first one of these features is Resource Sharing; Grids appear to be fairly sharing resources across organizations, whereas Clouds provide the resources that the Service Provider requires on demand. Another feature is Heterogeneity, both Cloud and Grid Computing support the aggregation of heterogeneous resources. Add to these, Virtualization feature that covers both, data and computing resources. Mutually, Clouds and Grids add the virtualization of hardware resources. As far as the Security feature is concerned, it has been argued by some authors that security has not been seriously explored. Grids have not dealt with end user security, however in Clouds each user has an access to its individual virtualized environment. Clouds system is facing a serious problem caused by lack of high level services; this may be as a result of the low level of maturity associated to Clouds paradigm. In contrast, Grids have a number of these high level services for instance data transfer, metadata search. Moreover, Still there are some valuable features (e.g. Scalability and Self Management, Usability, Standardization and Payment Model Quality of Service), which are summarized in the table below. There are many similarities between Grid and Cloud computing, both systems share the same basic goal : "to reduce the cost of computing, increase reliability, and increase flexibility by transforming computers from something that we buy and operate ourselves to something that is operated by a third party". However, there are some differences Grids come out from existing heterogeneous resources to add new abstraction layers, allowing the definition of new and complex services by aggregation. In contrast, Clouds are not effectively composed of homogenous components, and it is possible to be designed on top of an existing grid. The essential objective for creating the Cloud system is to provide a determined set of capabilities to the user; therefore the principle of the design is a specific goal interface. In contrast, Grids are considered to be general purpose, so they display a complete set of available system capabilities and the resulting interface available for users and applications remains low level.

V. CONCLUSION

Cloud computing as mentioned above is a new technology of computer network, providing the web services in high quality and lower cost comparing to normal technique. Using cloud computing might contribute to improvement of services in other related technologies specially the previous generations such as Grid computing. Cloud computing is almost certainly set to be developed and become an attractive option for many corporations. Cloud computing is an emerging technology which can bring revolutionary changes in the usage of internet. Cloud computing is a combination of various computing technologies and it can

play a major role in bringing significant improvement in data transfer and communication. This paper provides a basic understanding of cloud computing which includes the cloud security architecture, services and types of clouds. We believe cloud computing will become main technology in our information life. Cloud has owned all the conditions. Now the dream of grid computing will be realized by cloud computing. It will be a great event in the IT history.

References

[1] A.Rajadurai, A.Ranjeeth, J.Ilanchezhian and Varadharassu, A detailed study on cloud computing based on security and future opportunities, IEEE International Conference on Computing and Control Engineering (ICCCE 2012), April 2012.
[2] Dheeraj Rane, Pritesh Jain and Shyam Patidar, A Survey Paper on Cloud Computing, IEEE Second International Conference on Advanced Computing & Communication Technologies, 2012.
[3] Kirit Modi, Yashpalsinh Jadeja, Cloud Computing -Concepts, Architecture and Challenges, IEEE International Conference on Computing, Electronics and Electrical Technologies, 2012.
[4] I. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Proceedings of the IEEE Grid Computing Environments Workshop, pp. 1-10, 2008.
[5].Wikipedia, "Cloud computing" http://en.wikipedia.org/wiki/Cloud_computing
[6]H. Nakada, Y. Tanaka, S. Matsuoka, S. Sekiguchi. "Ninf-G: a GridRPC system on the Globus toolkit", Grid Computing: Making the Global Infrastructure a Reality, pp. 625--638, 2003.
[7]R. Buyya, K. Bubendorfer. "Market Oriented Grid and Utility Computing", Wiley Press, New York, USA, 2008
[8]J. Varia. (2008)."Cloud Architectures".
[9] jineshvaria.s3.amazonaws.com/public/cloudarchitectures-varia.pdf
[10]Andre Rigland (2010-12-17). "Cloud Computing-How it is Different from Grid Computing". Trial lecturer in conjunction with PhD thesis defence.
[11]Bart Jacob, Michael Brown, Kentaro Fukui, Nihar Trivedi First Edition (December 2005). Introduction to Grid Computing.
[12] Berman, F., Anthony J. G. H. and Geoffrey C. F. (2003).Grid Computing: Making the global infrastructure a reality, ISBN 0-12-742503-9.
[13] Joseph, J., Ernest, M. and Fellenstein, C. (2004), Evolution of Grid Computing Architecture and Grid Adoption Models, IBM Systems Journal, Vol. 43, No. 4, pp. 624- –645
[14] Douglas O. Balen, C.B.W., Westphall, C.M.: Experimental Assessment Of Routing For Grid And Cloud. The Tenth International Conference On Networks(Icn 2011) Pp. 341–346 (2011).
[15]Aman Bakshi, Yogesh B.Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks,pp. 260-264,2010,IEEEComputer Society,USA,2010.ISBN: 978-0-7695-3961-4
[16]Ronald L.Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing,Inc.,2010
[17] Sun Microsystems, Inc,, "An Overview of Grid Computing From Sun," 2002
[18] A. Tripathi and A. Mishra, "Cloud computing security considerations" IEEE Int. conference on signalprocessing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China,2011.
[19] Cloud Computing and Security –A Natural Match, Trusted Computing Group (TCG) http://www.trustedcomputinggroup.org.
[20]"A Security Analysis of Cloud Computing" http://cloudcomputing.sys- con.com/node/1203943