International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420

Cloud Computing: An Analysis of Its Challenges & Security Issues

[1] Mr. D. Kishore Kumar, [2] Dr.G.Venkatewara Rao , [3] Dr.G.Srinivasa Rao

[1,2,3]Department of Information Technology, GIT, GITAM University, Visakhapatnam, AP, India

Abstract

Cloud computing is one of the most significant milestones in recent times in the history of computers. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. The basic concept of cloud computing is to provide a platform for sharing of resources which includes software and infrastructure with the help of virtualization. In order to provide quality of service, this environment makes every effort to be dynamic and reliable. As in most other streams of computers, security is a major obstacle for cloud computing. There are various opinions on the security of cloud computing which deal with the positives and negatives of it. This paper is an attempt to investigate the crucial security threats with respect to cloud computing. It further focuses on the available security measures which can be used for the effective implementation of cloud computing.

Keywords: *SaaS, IaaS, PaaS, Cloud Architecture, DDOS, IP Spoofing, Port Scanning, Flooding Attacks.*

1. INTRODUCTION

Cloud computing is a model for allocating compute and storage resources on demand. Cloud computing offers new ways to provide services while, significantly altering the cost structure underlying those services[1]. These new technical and pricing opportunities drive changes in the way businesses operate. Cloud computing is a unique combination of capabilities which include:

- A massively scalable, dynamic infrastructure
- Universal access
- Fine-grained usage controls and pricing
- Standardized platforms
- Management support services

Cloud computing services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (Paas) and Software-as-a-Service (SaaS).

Platform-based cloud services deliver higher-level services than the infrastructure-based model offers. Platform-based services include tools for designing, developing, and deploying applications using a set of supported application components, such as relational databases and application security services that span multiple layers of the application stack[2].

Software as a Service provides network-based access to commercially available software. It is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS represents the potential for a lower-cost model for businesses to use software—using it on demand rather than buying a license for every computer. In this model, the administration process and collaboration will be easier and will have global accessibility. Infrastructure services deliver computing and storage services .Infrastructure-as-a-Service (IaaS represents a new consumption model for the use of IT resources. An IaaS provider offers customers - bandwidth, storage and compute power on an elastic, on-demand basis, over the Internet[2]. The environment of IaaS differs depending on the size of the organization and the nature of the business.
For Small and Medium Businesses (SMBs) with a limited capital budget, IaaS shifts the capital requirement to an operational expense that tracks with the growth of the business.

2. COMMON ATTRIBUTES OF CLOUD SERVICE MODELS

The three defining characteristics of clouds: massive scalability, easy to allocate resources and a service management platform to describe key architectural elements of computing and storage clouds[3]. A consumer of cloud services may see a different set of attributes depending on their own unique needs and perspective:
- On demand self service—the ability to allocate, use, and manage computing, storage, application, and other business services at will without depending on IT support staff,
- Ubiquitous network access—the ability to work with cloud resources from any point with Internet access; cloud service consumers are not dependent on being in corporate

headquarters or in a data center to have access to an enterprise cloud,

• Location independent resource pools—compute and storage resources may be located anywhere that is network accessible; resource pools enable redundancy and reduce the risks of single points of failure,

• Elastic scalability—cloud consumers decide how much of any resource they utilize at any time; allocation is driven by immediate demand not the need to maintain capacity for peak demand,

• Flexible pricing—cloud providers typically charge with a "pay as you go" model.

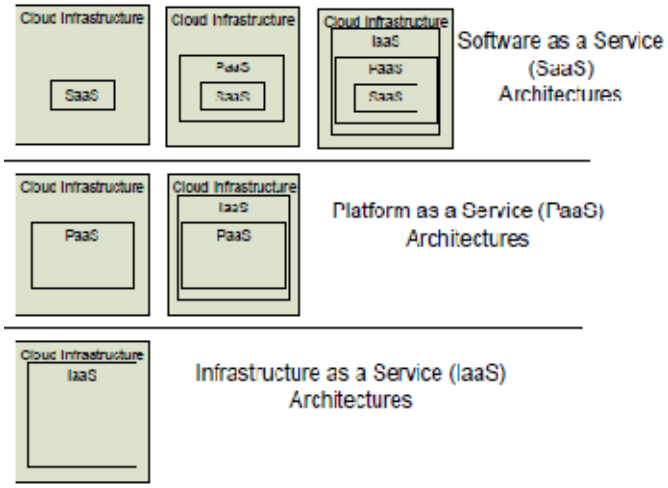

Fig 1: Cloud Computing Service Model Architectures

3.CLOUD COMPUTING ARCHITECTURE

The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue[4]. Elastic provisioning implies intelligence in the use of tight or loose coupling of cloud resources, services, middleware, and software components. In the area of cloud computing, protection depends on having the right architecture for the right application. Organizations must understand the individual requirements of their applications, and if already using a cloud platform, understand the corresponding cloud architecture.

A cloud computing architecture consists of a front end and a back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or what the client, sees. The back end is the "cloud" section of the system.

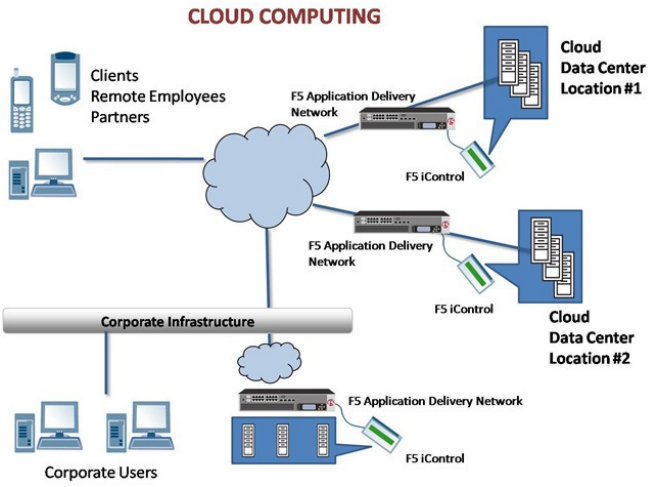

Fig 2: Architecture of Cloud Computing

The front end of the cloud computing system comprises of the client's devices (or it may be a computer network) and some applications are needed for accessing the cloud computing system. All cloud computing systems do not give the same interface to users[6]. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

Back end refers to some physical peripherals. In cloud computing, the back end is cloud itself which may encompass various computer machines, data storage systems and servers. Groups of these clouds make a whole cloud computing system. Theoretically, a cloud computing system can include practically any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services. A central server is established which is used for administering the whole system. It is also used for monitoring client's demand as well as traffic to ensure that every component of the system runs without any problem. There are some set of rules, generally refered to as protocols which are followed by this server and it uses a special type of software known as middleware[5]. Middleware allows computers that are connected on networks to communicate with each other. If a given cloud computing service provider has many customers, then will be high demand for huge storage space. Many companies that are service providers need hundreds of storage devices. The cloud computing system must have a copy of all the

data of its client's. Having a copy of data is called redundancy.

4. CHALLENGES IN CLOUD COMPUTING

Computing is always in a state of constant change and it is witnessed by the breakthroughs taking place in the field of computers. However, business transactions being done with the help of computers are still at stake. The impeccable usage of computers, security and storage access, manipulation, and transmission of data is always of high importance and it must be safeguarded by technology that enforces particular information control policies[6]. With respect to security, there are many issues which show an adverse impact on cloud computing. In this paper, we have given a brief analysis of the major security concerns of cloud computing.

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring that the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is, for the client to own and manage the data encryption keys.

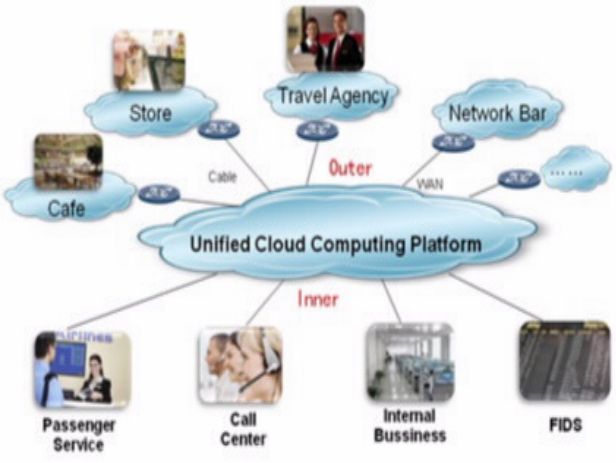

Fig 3: Cloud Computing Risks to consider as a Challenge in different sectors

Confidentiality of data must be ensured by the system as the large business doing companies like banks would not prefer to do the data transactions through clouds which involves the interaction of another system. Many business scenarios involve trade secrets, proprietary information about products and processes, competitive analyses, as well as marketing and sales plans[3]. Privacy for governments involves the collection and analysis of demographic information and the ability to keep secrets that affect the country's interests. While doing various actions with cloud computing which is based on a virtualization process, the privacy of communications would be at the edge of vulnerability.

Keeping valid data and protecting it from deletion and corruption is what is meant by integrity. It ensures that only authorized users can have access to and change data. It does not allow an intruder to change or delete the data at will. There is no universal customary practice which ensures data integrity and eventually it leads to a deficit of trust among the users[4]. In fact, there is a common assumption that trust is the biggest concern facing cloud computing.

Data resting in the cloud needs to be accessible only to those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

Compatibility is another major issue in cloud computing. Different vendors provide different storage services and all these services may not be compatible with one another[1]. Due to this, it will be difficult for the end user to transform from one vendor to another vendor.

Another setback in Cloud computing is the constant changes. Frequent improvements take place in cloud computing and users must keep themselves abreast of those developments to ensure data security. These changes will have their impact on both software development life cycle and security.

5. CLOUD COMPUTING AND NETWORK SECURITY

Network security is a combination of activities which protect your network usability, reliability, integrity and safety of data. Network security measures are implemented to get protection from various threats and prevent these threats from entering or spreading on our network.

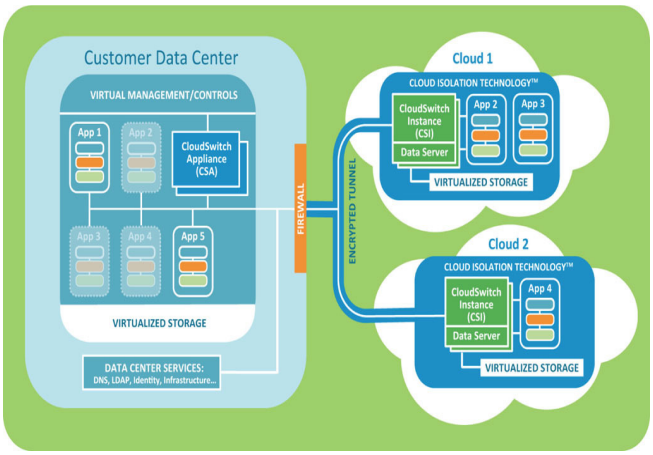

Fig 4: Example Data Center Switch Network Architecture

5.1 DDOS: In DDOS , the attacks will be in the form of requests. More number of requests will be sent to make the server busy and it can't respond to its genuine requests. In a typical DDoS attack, a hacker begins by exploiting vulnerability in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple - sometimes thousands of - compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service[5]. Even in cloud computing, the hackers attack the server in the same manner by sending more requests so that the server will be busy and this makes the job easier for an attacker as he attacks the third party server which holds the requests of many other parties.

Man in the Middle Attack: In cloud computing, the improper configuration of SSL (Secure Socket Layer) which is a commonly-used protocol for managing the security of a message transmission on the Internet will create a security problem known as "Man in the Middle Attack". If there is a problem with SSL, it gives a chance to the hacker to launch an attack on the data of both the parties and in an environment like cloud computing it can create disasters.

5.2 IP Spoofing: IP spoofing is one of the very well-known hacking techniques in which the intruder sends messages to a computer indicating that the message has come from a trusted system. In the process of IP Spoofing, the hacker first determines the IP of a trusted system and modifies the packet headers to appear as if they are originating from a trusted system.

5.3 Port Scanning: Port scanning is the act of scanning a computer's ports systematically. Port scanning identifies open doors to a computer since it is a place where information goes into and out of a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer. The security groups are usually configured to allow traffic from any source to a specific port of the computer and then the port responds to the signal[6]. Both TCP and UDP employ *port numbers* to identify the higher layer applications at the hosts that are communicating with each other. End-to-end data communications on the Internet, in fact, are uniquely identified by the source and destination host IP addresses and the source and destination TCP/UDP port numbers. In cloud computing, where there will be interaction of third party servers and systems, the port scanners may provide an opportunity for the attackers when the subscriber configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan.

5.4 Packet Sniffing: Packet sniffing is used for monitoring and analyzing the network. It is used legitimately by the network or system administrators to monitor or troubleshoot network traffic. Packet sniffing helps the administrators in maintaining efficient network data transmission. In virtual machine environment, it is not possible to capture the right packet that is intended for a specific machine. It is easy for an attacker to hack the systems as the two virtual instances which are located on the same host and owned by the same customer will not be able to listen to each other's traffic.

6.SECURITY ISSUES

When it comes to cloud computing, the focus should be on two different environments in terms of its security issues. Both physical and virtual machine security has to be taken into consideration as there is a dependency between these two servers. None of the servers security should be compromised as it could show a catastrophic impact on other virtual machines of the same host.

6.1 Data Isolation: There will be various instances running on the same physical machine and all these instances are isolated from one another. There are certain techniques like Instance Relocation, Server Farming, Address Relocation, Failover and Sandboxing, which are used for instance isolation. Multiple organizations have multiple virtualization systems[7]. These are required to be co-located on the same physical resource. Even after implementing the basic required data security measures in the physical environment, there is no assurance of complete

protection for the virtual machines as the physical segregation and hard-ware based security cannot protect against these attacks. Due to the reason that administrative access is done through internet, rigorous inspection for changes in system control is required.

6.2 Browser Security: SSL is used to encrypt the request that has been received from the client in web browser as SSL supports point to point communication means. Because of the presence of the third party in cloud, there is a possibility that the date can be decrypted by the intermediary host. If any of the sniffing packages are installed on the intermediary host, it will be an easier task for the hacker to get the credentials of the user and those credentials can be used as a valid user ones.

6.3 Cloud Malware Injection Attack: It is one of the most spreading of attacks. The attack is done via a compromised FTP, and many believe that the virus can actually "sniff out" FTP passwords and send it back to the hacker. The hacker then uses your FTP password to access your website and add malicious i-frame coding to infect other visitors who browse your website. In this attack, attempts which are adversary are used to inject vicious service or code[5]. Eavesdropping ensures the success of an attacker in cloud computing. If the user has to wait for a few actions to be completed which are actually not requested by him/her, then it is a sure sign that the malware has been injected. Attackers target either IaaS or SaaS of the cloud servers and take steps which disturb the functionality of these servers.

6.4 Flooding Attacks*:* Cloud system repeatedly increases its size when it has further requests from clients and the initialization of a new service request is also done to satisfy client requirements. Here all the computational servers work in a service specific manner maintaining internal communication among them. In flood attacks, the attacker tries to send more number of requests and makes the server busy and incapable to supply service to normal requests and then he attacks the service server.

6.5 Protection of DATA: Data is the most significant part of any company and utmost priority is given to protect it. Data protection is very important in cloud computing as in any system. It is the responsibility of the cloud supplier that he is protecting the data and supplying to the customer in a very secure and legal way[2]. This is one of the most complicated problems in cloud computing as it has many customers using various virtual machines.

7.SECURITY MEASURES IN THE CLOUD

Cloud computing has numerous security issues as it encompasses many technologies. We have focused on only some of the secure aspects of cloud computing like efficient storage of the data, encryption of data and hadoop distributed file system for virtualization.

7.1 THIRD PARTY SECURE DATA PUBLICATION APPLIED TO CLOUD:

Cloud Computing facilitates storage of data at a remote site to maximize resource utilization. As a result, it I critical that this data be protected and only given to authorized individual. This essentially amounts to secure third party publication of data that is necessary for data outsourcing as well as external publications. We have developed techniques for third party publication of data in a secure manner. We assume that the data is represented as an XML document[7]. This is a valid assumption as many of the documents on the web are now represented as XML documents. First we discuss the access control framework proposed in [BERT02] and then discuss secure third party publication discussed in [BERT04].

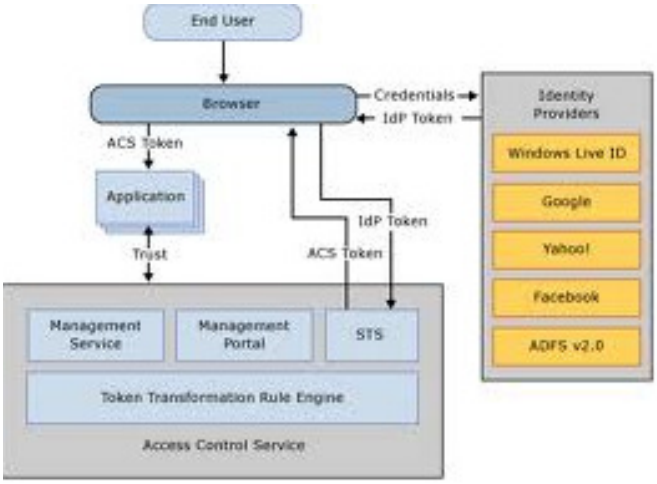

Fig 6: Access Control Framework

In the access control framework proposed in [BERT02], security policy is specified depending on user roles and credentials(see fig 1). Users must possess the credentials to access XML documents. The credentials depend on their roles. For example, a professor has access to all of the details of students while a secretary only has access to administrative information. XML specifications are used to specify the security policies[7]. Access is granted for an entire XML document or portions of the document. Under certain conditions, access control may be propogated down the XML tree.

For example, if access is granted to the root, it does not necessarily mean access is granted to all the children. One may grant access to the DTD's and not to the document instances. One may grant access to certain portions of the document. For example, a professor does not have access to the medical information of students while he has access to

student grade and academic information. Design of a system for enforcing access control policies are also described in [BERT02]. Essentially the goal is to use a form of view modification so that the user is authorized to see the XML views as specified by the policies. More research needs to be done on role-based access control for XML and the semantic web. In [BERT02] we discuss the secure publication of XML documents(see fig 2). The idea is to have untrusted third party publishers[8]. The owner of a document specifies access control policies for the subjects. Subjects get the policies from the owner when they subscribe to a document. The owner sends the documents to the publisher.

Fig 7: Secure third party Publication

When the subject requests a document, the publisher will apply the policies relevant to the subject an give protions of the documents to the subject. Now, since the publisher is untrusted, it may give false information to the subject. Therefore, the owner will encrypt various combinations of documents and policies with his/her private key. Using Merkle signature and the encryption techniques, the subject and verify the authenticity and completeness of the document (see fig 2 for secure publishing of XML documents).

In the cloud environment, the third party publisher is the machine that stored the sensitive data in the cloud. This data has to be protected and the techniques we have discussed above have to be applied to the authenticity and completeness can be maintained.

7.2 Encrypted Data Storage For Cloud:

Since data in the cloud will be placed anywhere, it is important that the data is encrypted. We are using secure co-processor parts cloud infrastructure to enable efficient encrypted storage of sensitive data. One could ask us the question; why not implement your software on hardware provided by current cloud computing systems such as Open Cirrus? We have explored this option[8]. First, Open Cirrus provides limited access based on their economic model (eg., virtual cash). Furthermore, Open Cirrus does not provide the hardware support we need (eg., secure co-processors). By embedding a secure co-processor (SCP) into the cloud infrastructure, the system can handle encrypted data efficiently (see Fig 3).

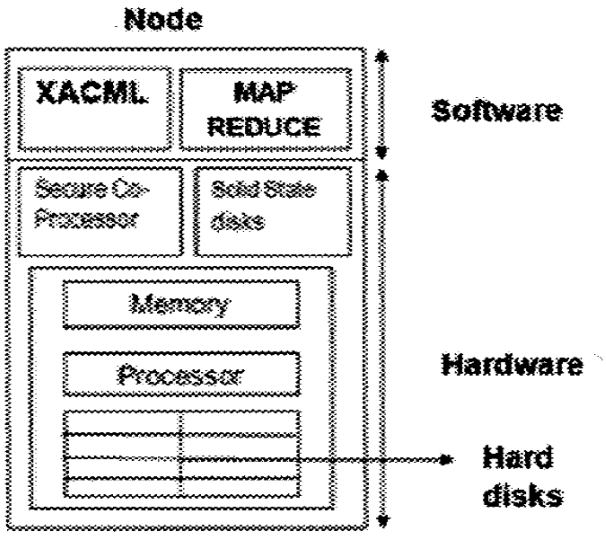

Fig 8: Parts in a Proposed System

Basically, SCP is a tamper-resistant hardware capable of limited general-purpose computation. For example, IBM 4758 Cryptographic Coprocessor[IBM04] is a single-board computer consisting of a CPU, memory and special-purpose cryptographic hardware contained in a tamper-resistant shell; certified to level 4 under FIPS PUB 140-1. When installed on the server, it is capable of performing local computations that are completely hidden from the server. If the tampering is detected then the secure co-processor clears the internal memory. Since the secure coprocessor is tamper-resistant, one could be tempted to run the entire sensitive data storage server on the secure co-processor[8]. Pushing the entire data storage functionality into a secure co-processor is not feasible due to many reasons.

First of all, due to the tamper-resistant shell, secure co-processors have usually limited memory (only a few megabytes of RAM and a few kilobytes of non volatile memory) and computational power [SW99]. Performance will improve over time, but problems such as heat dissipation/power use (which must be controlled to avoid disclosing processing) will force a gap between general purposes and secure computing. Another issue is that the software running on the SCP must be totally trusted and verified. This security requirement implies that the software running on the SCP should be kept as simple as possible. So how does this hardware help in storing large sensitive data sets? We can encrypt the sensitive data sets using random private keys and to alleviate the risk of key disclosure, we can use tamper-resistant hardware to store some of the encryption/decryption keys. (ie., a master key that encrypts

all other keys)[7]. Since the keys will not reside in memory unencrypted at any time, an attacker cannot learn the keys by taking the snapshot of the system. Also, any attempt by the attacker to take control of (or tamper with) the co-processor, either through software or physically, will clear the co-processor, thus eliminating a way to decrypt any sensitive information. This framework will facilitate (a) secure data storage and (b) assured information sharing. For example, SCPs can be used for privacy preserving information integration which is important for assured information sharing [AAK06].

We have conducted research on querying encrypted data as well as secure multipart computation (SMC). With SMC protocols, one knows about his own data but not his partner's data since the data is encrypted. However, operations can be performed on the encrypted data and the results of the operations are available for everyone, say, in the coalition to see. One drawback of SMC is the high computation costs[8]. However, we are investigating more efficient ways to develop SMC algorithms and how these mechanisms can be applied to a cloud.

8. CONCLUSION

Cloud computing has been showing its impact on the industry for the past few years and it has heralded a revolutionary change giving new directions to how information technology resources can be best utilized and by reducing the cost and complexity for customers. In this paper, we have given a brief analysis of various security concerns of cloud computing. We will try to come forward with more innovative ideas and security measure in future.

In this paper, we have made an attempt to analyze the various security concerns of cloud computing and has provided some security measures. Even though Cloud Computing offers a wide range of benefits and newer services, people express different opinions about the security aspects of it. Because of these security concerns, it is still not gaining its full momentum. Most of the organizations are stepping back as they don't want to take the security risk. It is essential to have more standard security measures for cloud computing in order to gain complete acceptance from all levels of organizations.

REFERENCES

[1] D. Wentzlaff, C. Gruenwald III, N. Beckmann, K. Modzelewski, A. Belay, L. Touseff, J. Miller, and A. Agarwal. Fos: A Unified Operating System for Clouds and Manycore. *Computer Science and Artificial Intelligence Laboratory TR*, Nov. 20, 2009.

[2] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni. *Cloud Security is not (just) Virtualization Security*, CCSW'09, Nov. 13, 2009, Chicago, Illinois, USA.

[3] Anderson, C. 2009. *Free: The Future of a Radical Price*. New York: Hyperion.
Brunette, G. and R. Mogull (ed). 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. Cloud Security Alliance, December 2009.Cloud Computing: The Evolution of Software-as-a-Science.

[4] Catteddu, D; Hogben, G eds. (2009), 'Cloud Computing - Benefits, risks and recommendations for information security', European Network and Information Security Agency (ENISA) –available at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment/at_download/fullReport

[5] Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, H. Raghav Rao, ―The Information Assurance Practices of Cloud Computing Vendors‖, IT Pro July/August 2010, InIEEE Computer Society, p. 29-37.

[6] D. Oliveira, F. Baião, and M. Mattoso, 2010, "Towards Taxonomy for Cloud Computing from an e-Science Perspective", *Cloud Computing: Principles, Systems and Applications (to be published)*, Heidelberg: Springer-Verlag

[7] [DGH09] B. W. DeVries, G. Gupta, K. W. Hamlen, S. Moore, and M. Sridhar. Action Script Bytecode verification with Co-Logic Programming. In Proc., of the ACM SIGOPLAM workshop on Programming Languages and Analysis for Security(PLAS). June 2009.

[8] S. Ramanujam, A. Gupta, L. Khan, S. Seida, B. Thuraisingham, "R2D: A Bridge between the Semantic Web and Relational Visualization Tools", to appear in "Third IEEE International Conference on Semantic Computing, Berkeley, CA, USA- September 14-16,2009.

[9] Chang, Y-S., Yang, C-T, & Luo, Y-C., (2011). An Ontology based Agent Generation for Information Retrieval on Cloud Environment. Journal of Universal Computer Science, Vol. 17, No. 8, Pages: 1135-1160. Retrieved October 25, 2011 from http://jucs.org/jucs_17_8/an_ontology_based_agent/jucs_17_08_1135_1160_chang.pdf

[10] AlZain, M.A., Pardede, E., Soh, B. & Thom, J.A. (2012). Cloud Computing Security: From Single to Multi-clouds, 45th Hawaii International Conference on System Sciences. *IEEE ComputerSociety*, 5490-5499. Available from

http://www.computer.org/plugins/d1/pdf/proceedings/hicss/2012/4525/00/4525f490.pdf

[11] Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing*, 16(1), 69-73.

[12] World Economic Forum, *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology Driven Transformation* (WEF 2010). As of 22 November: http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010. pdf