International Journal of Computing and Network Technology

http://dx.doi.org/10.12785/ijcnt/010303

Ten Security Concerns to be Kept in Mind While Accessing Cloud

Anisha P R[1], Kishor Kumar Reddy C[2], Prashanth S K[3]

Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India
[1]Email Address: anishanaidu.pushpala@gmail.com
[2]Email Address: kishoar23@gmail.com
[3]Email Address: sk_p21@yahoo.co.in

Received: 12 Jul. 2013, Revised: 8 Aug. 2013; Accepted: 15 Aug. 2013
Published online: 1 Sep. 2013

Abstract: Cloud computing is a promising development, deployment and delivery model in information technology sector across the globe. The burgeoning cloud computing model attempts to tackle the hotheaded growth of web-connected devices and handles gigantic amount of data. Security factor plays a key role in cloud computing. There is a critical need to securely store, manage, share and analyze huge amounts of complex data to resolve patterns and trends in order to improve the quality of realistic applications. Because of the critical nature of the applications, it is vital that clouds be secure. The major security confront with cloud computing is that the end user may not have control over the data and doesn’t know where the data is actually stored. Providing security is quite complex in cloud because it comprises of various technologies, storage devices, platforms and so on. In this paper we discuss the major security issues for the data stored in cloud and its concerns, services and finally solutions for the security

Keywords: Cloud computing; DOS attacks; Side channel attacks; Security issues;

I. INTRODUCTION

Cloud computing is an emerging development, deployment and delivery model in the information technology sector and enables real time delivery of IT products, services and solutions [1]. Cloud computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition. 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 name cloud computing is retrieved from the drawings that are basically used to indicate the internet. The entire process is transmitted over the networks commonly known as internet, which follows the IPSec protocol. Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers that are connected through a real-time communication network The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location.

Cloud computing comes forward only when someone thinks about what exactly IT really and always needs. Cloud computing is the most intellectual idea, ever conceived in IT field. Cloud relies on sharing of resources to achieve coherence and economies of scale similar to a utility over a network. The cloud also focuses on maximizing the efficacy of the shared resources [2]. Cloud resources are usually not only shared by multiple users but also it is dynamically re-allocated as per demand to different users in different time

© 2013 UOB, SPC, University of Bahrain

zones. This approach should maximize the use of computing powers thus reducing environmental damages less power, air conditioning, rack space, and so on, that are usually required for the same functions.

In cloud computing, end-users need not be familiar with the details of a specific technology as one can access the services based on On-Demand service by paying charges to service provider, usually follows pay per use methodology. End user can share computing resources rather than possessing his/her own local servers, storage devices, networks and so on, in order to handle various applications.

Many of the companies, organizations, users and so on are placing their sensitive, bulk and valuable data over the cloud in order to decrease the cost factor and are gradually getting addicted towards cloud computing because of the ease it works [9]. The bulk of data is stored at the service provider end which is basically located at provider physical location, but the end user/client do not have any idea about where exactly the data is stored and would remain with a dilemma thinking if his/her data is secured or not. Further, the service provider need to take the whole and soul responsibility of providing full fledged security to the client’s data. Though the service provider tries to provide the maximum security at times it is quite important to discuss how far and how efficient and secure is the data [13]. At times if the security provided by the service provider fails and the data gets insecure it becomes quite important to discuss on how to overcome the security issues in cloud computing and finally how to handle intruder activities while preventing the hacking of end user data from the cloud server. These factors are to be discussed as there is a great need for security in cloud computing. This motivates us to do a research in this domain.

Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re-provision technological infrastructure resources.

Application programming 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 [4]. Cloud computing systems typically use Representational State Transfer -based APIs.

Cost is claimed to be reduced, as in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's [5] state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Virtualization technology allows servers and storage devices to be shared thus increasing their utilization. This technology helps the applications to migrate easily from one physical server to another.

Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford [13]. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

The rest of the paper is organized as follows. Section 2 describes the history on cloud computing. Section 3 illustrates security issues with cloud computing. Section 4 illustrates cloud computing attacks. Finally section 5 provides the conclusion.

II. History of Cloud Computing

The underlying concept of cloud computing dates back to the 1950s, when large-scale mainframe computers became available in academia and corporations, accessible via thin clients/terminal computers, often referred to as "dumb terminals", because they were used for communications but had no internal computational capacities [6]. To make more efficient use of costly mainframes, a practice evolved that allowed multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time. This eliminated periods of inactivity on the mainframe and allowed for a greater return on the investment. The practice of sharing CPU time on a mainframe became known in the industry as time-sharing.

John McCarthy opined in the 1960s that "computation may someday be organized as a public utility."Almost all the modern-day characteristics of cloud computing (elastic provision, provided as a utility, online, illusion of infinite supply), the comparison to the electricity industry and the use of public, private, government, and community forms, were thoroughly explored in Douglas Parkhill's 1966 book, The Challenge of the Computer Utility. Other scholars have shown that cloud computing's roots go all the way back to the 1950s when scientist Herb Grosch (the author of Grosch's law) postulated that the entire world would operate on dumb terminals powered by about 15 large data centers.Due to the expense of these powerful computers, many corporations and other entities could avail themselves of computing capability through time sharing and several organizations, such as GE's GEISCO, IBM subsidiary The Service Bureau Corporation (SBC, founded in 1957), Tymshare (founded in 1966), National CSS (founded in 1967 and bought by Dun & Bradstreet in 1979), Dial Data (bought by Tymshare in 1968), and Bolt, Beranek and Newman (BBN) marketed time sharing as a commercial venture.

In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service, but at a lower cost. By switching traffic as they saw fit to balance server use, they could use overall network bandwidth more effectively. They began to use the cloud symbol to denote the demarcation point between what the providers was responsible for and what users were responsible for. Cloud computing extends this boundary to cover servers as well as the network infrastructure.

As computers became more prevalent, scientists and technologists explored ways to make large-scale computing power available to more users through time sharing, experimenting with algorithms to provide the optimal use of the infrastructure, platform and applications with prioritized access to the CPU and efficiency for the end users.

After the dot-com bubble, Amazon played a key role in all the development of cloud computing by modernizing their data centers, which, like most computer networks, were using as little as 10% of their capacity at any one time, just to leave room for occasional spikes. Having found that the new cloud architecture resulted in significant internal efficiency improvements whereby small, fast-moving "two-pizza teams" (teams small enough to feed with two pizzas) could add new features faster and more easily, Amazon initiated a new product development effort to provide cloud computing to external customers, and launched Amazon Web Services (AWS) on a utility computing basis in 2006.

In early 2008, Eucalyptus became the first open-source, AWS API-compatible platform for deploying private clouds. In early 2008, Open Nebula, enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid clouds, and for the federation of clouds. In the same year, efforts were focused on providing quality of service guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting to a **real-time cloud environment**. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them" and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing ... will result in dramatic growth in IT products in some areas and significant reductions in other areas." On March 1 2011, IBM announced the IBM Smart Cloud framework to support Smarter Planet. Among the various components of the Smarter Computing foundation, cloud computing is a critical piece.

III. SECURITY ISSUES WITH CLOUD COMPUTING

The major benefits with the cloud computing are cost and ease. When considering moving critical real time applications and sensitive data to public and shared cloud environments, security concerns are to be addressed. To address various security concerns, the cloud service provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used.

Cloud computing [13] encompasses many technologies, including networks databases, operating systems, virtualization, resource scheduling transaction managementt, load balancing concurrency control and memory management. As cloud computing encompasses various technologies, security issues grow in a linear manner. For example, the network commonly preferable is internet which interconnects the system in a cloud that has to be secure [11]. If the network is secured then the data transmission over the network is also securable to some extent. The major concerns that are to be kept in mind when accessing cloud are lined below.

3.1 Data storage

The end user does not know where the data is actually stored because the provider maintains number of servers in order to provide the transactions in a faster manner. Different nations have different requirements, rules and controls placed on access. Initially the end user requests to service provider in order to store the data. Once service provider accepts end user proposal then end user stores data at the provider end. Once the data is sent to provider end, here onwards the complete responsibility regarding security issues is to be handled by cloud service provider.[12] Most of the time data is going to be replaced leads to data leakage, a major security threat with cloud computing.

3.2 Accessibility

Access control plays a vital role in cloud computing and it is a key concern. Once the data is stored at the provider end, any employ of the provider can access the data in order to make further transactions. This is to be limited and can be done by making a service level agreement during the initial stages itself.

3.3 Regulatory Requirements

Before approaching with the provider, make sure that the particular provider is providing all the regulatory requirements. Many organizations operate in US, Canada, Europe and other countries and may have many regulatory requirements that they must abide by. So it’s better to check for regulatory requirements.

3.4 Audition

The client may withdraw the data in the middle inorder to make changes to his/her data. Make sure that whether the client is having the right for audition or not, and make agreement with the provider in a written agreement form regarding the terms of audit.

3.5 Training to employees

Before showing the data, know how that particular provider trains their employees because people will always be the weakest link in security. The major challenging problem in cloud computing is security. The trainers should be more effective while providing training to employees and always to be in a position that they need to provide maximum security because everything is transmitting over the internet which indirectly provides a way to intruders.

3.6 Data Separation

As cloud is an on demand service, number of clients can access cloud and stores their data at the cloud. Data is to be separated from other users otherwise it may be mixed and leads to breakage of data. Many of the encryption techniques are to be used. Make an agreement with the provider regarding the type of encryption mechanism that you desire.

3.7 SLA terms

The service level Agreement serves as a contracted level of guaranteed services between the customer and the cloud provider that specifies what levels of services will be provided. Once SLA is completed and during that particular time if the provider breaks the terms mentioned in SLA, then customer can approach to court for justice.

3.8 Provider background

Before approaching to a particular provider, discuss that how long the cloud provider has been in business and also know the track records of that provider. In the middle, if the provider goes out of business, what happens to your data is returned? All these things should be discussed in order to protect the data.

3.9 Security breach

Suppose the data stored over the provider and is hacked then what support will you receive from the cloud providers to be mainly discussed. Security breach is to be clearly discussed during the initial stages service level agreement.

3.10 Disaster recovery

The client may not know where the data is stored in fact the data is stored at provider physical servers and is located at somewhere. All physical locations face threats such as fire, storms, natural disasters, any loss of power. In case of these disasters how the cloud service provider responds will, and what guarantee of continued services are they promising?

IV. SECURITY ATTACKS IN CLOUD COMPUTING

Cost and ease of use are the two major benefits with cloud computing [11], leads to more companies to move towards cloud computing, look for hackers to follow. Some of the major attacks include side channel attacks, man in the middle attacks, and denial of service attacks and so on. The major reasons for attacks in cloud computing are providers lack security visibility and security awareness.

4.1 Side channel attacks

An intruder could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launches a side channel attacks. If the provider maintains security to the virtual machine by making use of encryption and decryption techniques [9], this can be overcome to some extent. Whenever the cloud service provider uses virtual machine, the following steps are to be followed. By making use of Figure 1 side channel attacks can be minimized to greater effects.

Initially cloud service provider requests to virtual machine in an encrypt format in order to provide services requested by end user. Virtual machine decrypts the encrypted format received from cloud service provider and provides necessary response to cloud service provider in encrypted format. Finally cloud service provider decrypts in order to visible the message and the procedure is shown in Figure 1.

4.2. Man in the middle attacks

The intruder is in between the client and provider and tries to attack and succeeds in modifying the communication and is shown in Figure 2. Intruder tries to attack in between client and provider as the data is transmitted through a network i.e. internet. In between client and provider, always intruder tries breaking the internet. This can be overcome by using standard protocols i.e. using a URL “https” while connecting to provider to browser and is shown in Figure 3.

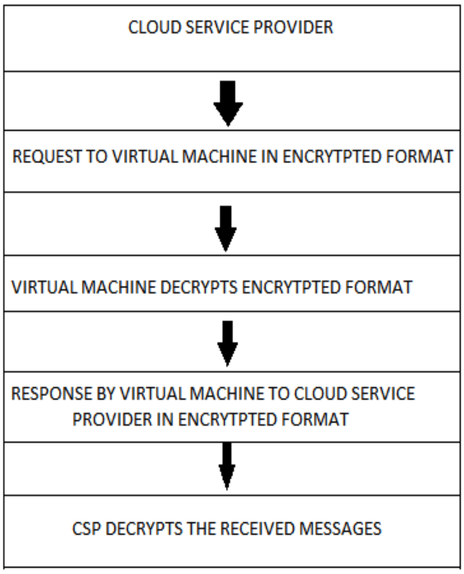
CLOUD SERVICE PROVIDER
REQUEST TO VIRTUAL MACHINE IN ENCRYTPTED FORMAT
VIRTUAL MACHINE DECRYPTS ENCRYTPTED FORMAT
RESPONSE BY VIRTUAL MACHINE TO CLOUD SERVICE PROVIDER IN ENCRYTPTED FORMAT
CSP DECRYPTS THE RECEIVED MESSAGES

Figure 1. Side channel attacks.

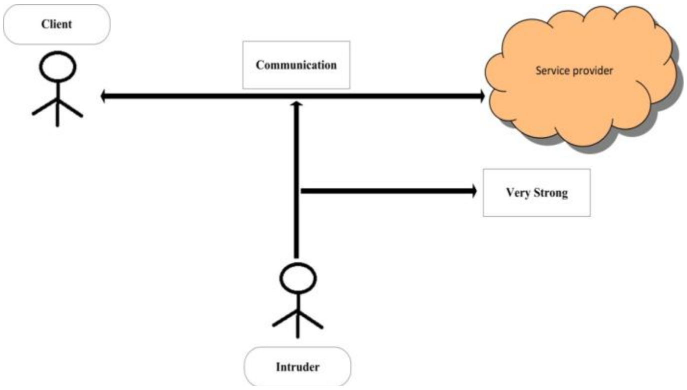

Figure 2. Man in the middle attacks.

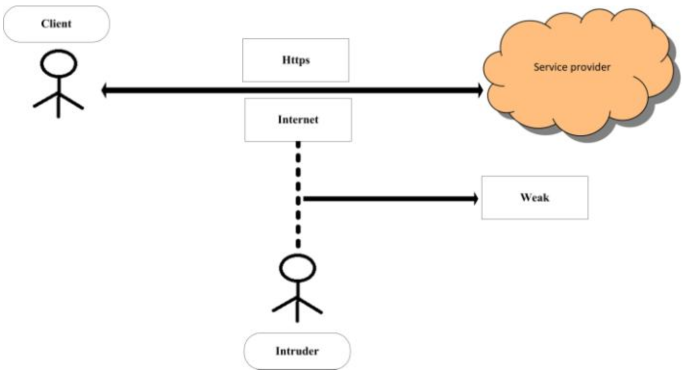

Figure 3. Overcome of man in the middle attacks.

4.3 Denial of service attacks

Cloud is a place for storing the data and is applicable to number of end users. Each end user stores his/her data at the provider end. The duty of service provider is to separate the data [10]. If the provider fails in separating the data, then data leads to leakage and it is to be overcome, which is the main security threat with clouds computing, shown in Figure 4.

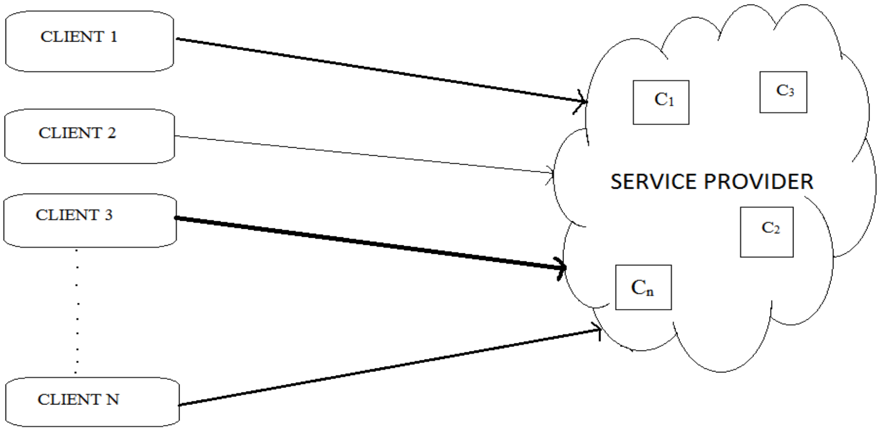

Figure 4. Denial of service attacks.

Fig. 4 shows that whenever client stores data immediately cloud service provider allocates space required for that request and stores separately. As the data is stored separately, overcomes the denial of service attacks. Client 1 stores data at the provider end. In the Figure 4 at the service provider end it is clearly visible that there is a separate block for client 1 and the data belongs to client 1 are stored in that block. In a similar manner all the clients stores their data in a separate block shown in Figure. 4. Some times at a physical location of server there may be more than one client storing his/her data. Client 1, client 2, client 3 are storing their data at the provider end and it is shown in Figure 5.

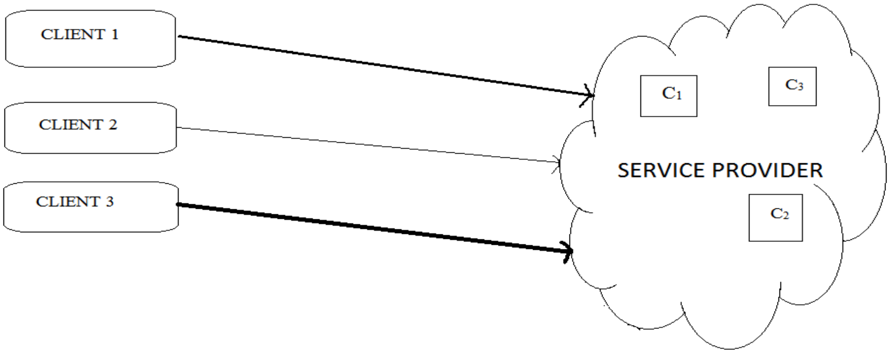

Figure 5. Data separation in cloud.

If c1 completes its work and doesn’t want any access from cloud then the duty of service provider is to delete all the data belonging to C1. If provider fails to delete then it leads to data leakage [9]. Suppose C4 request for data storage, then there is a chance that the provider may allocate same C1 place to C4. In fact if the provider previously deletes the data of C1 then there will be no problem if not leads to data leakage shown in Figure 6.

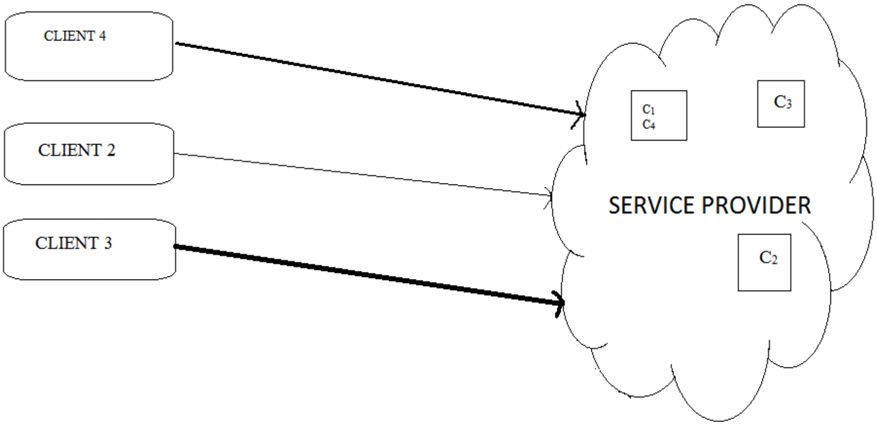

Figure 6. Data leakage in cloud.

CONCLUSION

Cloud computing offers tremendous promise for IT organizations to transform their architecture and their relationships with their business partners and also provides benefits to companies seeking a competitive edge in today's economy. Major concern in the cloud computing implementation is security and reliability of this paradigm in satisfying stringent requirements. This paper highlights security issues, security concerns in cloud computing and finally provided with how to overcome various attacks.

In this paper, denial of service attacks in cloud computing is explained and in further paper we will explain how to overcome accessibility problem in cloud, discussed in section 4.3.

References

[1] C. Bienia, S. Kumar, J. P. Singh, and K. Li. The PARSEC benchmark suite: Characterization and architectural implications. *In Proceedings of the 17th international conference on Parallel architectures and compilation techniques PACT*, (2008), pp. 1-10.

[2] S. Boyd-Wickizer, H. Chen, R. Chen, Y. Mao, F. Kaashoek, R. Morris, A. Pesterev, L. Stein, M. Wu, Y. Dai, Y. Zhang, and Z. Zhang. Corey: An operating system for many cores. *In OSDI*, (2008), pp. 1-23.

[3] R. Buyya, D. Abramson, J. Giddy, and H. Stockinger. Economic models for resource management and scheduling in grid computing. *Concurrency and Computation: Practice and Experience*, **14**(13-15), (2002), pp. 1507-1542. Published in special issue: Grid Computing Environments.

[4] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good. The cost of doing science on the cloud: the Montage example. *In Proceedings of the 2008 ACM/IEEE conference on Supercomputing*, (2008), pp. 1-12.

[5] S. L. Garfinkel. An evaluation of Amazon's grid computing services: EC2, S3 and SQS. *Technical Report TR-08-07, Harvard Univ.*, (2007), pp. 1-15.

[6] B. He, W. Fang, Q. Luo, N. K. Govindaraju, and T. Wang. Mars: a mapreduce framework on graphics processors. *In Proceedings of the 17th international conference on Parallel architectures and compilation techniques*, (2008), pp. 260-269.

[7] Y. Li, B. He, Q. Luo, and Y. Ke. Tree indexing on solid state drives. *In Proceedings of VLDB Endowment*, **3**(1-2), (2010), pp. 1195-1206.

[8] R. Mason. Simple competitive Internet pricing. *European Economic Review*, **44**(4-6), (2000), pp. 1045-1056.

[9] C. Molina-Jimenez, N. Cook, and S. Shrivastava. On the feasibility of bilaterally agreed accounting of resource consumption. *In Proceedings of Service-Oriented Computing-ICSOC 2008 Workshop*, **5742**, (2009), pp.270-283.

[10] C. Kishor Kumar Reddy, et al., Cloud specific issues and vunerabilities solutions, *International journal of scientific and engineering research*, **3**(7), (2012), pp.1-6.

[11] C. Kishor Kumar Reddy, et al., Third party data protection applied to cloud and XACML implementation in the hadoop environment with sparql, IOSR, **2**(1), (2012), pp. 39-46.

[12] C. Kishor Kumar Reddy, et al., Distributed systems and economics related to pricing in cloud computing, *International journal on advanced computer theory and engineering* , **1**(1), (2012), pp. 47-53.

[13] Armbrust, et al., Berkeley view of cloud computing, *UCB/EECS-2009-28*, 1-25.