Secure cloud computing based on mutual intrusion detection system

Sanjay Ram M[#]

Department of MCA,
Adhiyamaan College of Engineering (Autonomous), Hosur, India.
sanjayramm@gmail.com

Abstract

Cloud computing allows people the way to sharing distributed resources and services that belong to various organizations and sites. The cloud computing has its own concept, technical, economic and user experience characteristics are: service oriented, loose coupling, strong fault tolerant, and ease use are main characteristics of cloud computing. In this paper, proposed a method to build a mutual and reliable computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system and pay attention to the security requirements in cloud computing environment. Some important concepts, including denial-of-service, intrusion detection system and distributed intrusion detection systems in cloud computing system will be discussed in this paper.

Keywords- *cloud computing, Mutual IDS, reliable computing platform, reliable computing, reliable service, denial-of-service, mutual intrusion detection system, Grid Computing*

[#]Corresponding Author

1.1 Introduction

Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast micro processor, huge memory, high-speed network and reliable system architecture. Without the standard inter-connect protocols and mature of assembling data centre technologies, cloud computing would not become reality too.

This paper tries to summarize basic characteristics, mutual and reliable security of cloud computing which will help the development and adoption of this rapidly evolving technology. Cloud computing security issues such as confidentiality, integrity and availability are the most important security considerations. Denial-of-service attack, distributed denial-of-service attacks cause the targeted system or network unusable. If the cloud computing system suffers from these kinds of attacks, the service providers and end users could not use the services. The intrusion detection system (IDS) will mutually with each other by exchanging alerts to reduce the impact of the denial-of-service attack. The Snort based intrusion detection system implemented into three modules is: block, mutual and communication modules.

A mutual agent is used to receive alert messages from other intrusion detection systems. By collecting these alerts and implementing majority vote on them, the accuracy of these alerts could be judged by the agent. If the agent accepts these alerts, the system adds new blocking rule into the block table against this type of packet attacks on the cloud computing regions. Therefore, by this new blocking rule the cloud computing regions except the victim one can avoid this kind of attack.

In this paper described in section 2 Characteristics of cloud computing like service oriented, loose coupling, strong fault tolerance and section 3 mutual intrusion detection system for

reliable security of cloud computing - Authentication cloud computing environment with TCP, Role Based Access Control Model, Data Security in cloud based on TCP, The Trace of the User's Behaviour, Numerous representative based distributed Intrusion Detection System and Mutual Intrusion Detection System, and conclusion.

2.1 Characteristics of Cloud Computing

The comparable characteristics of cloud computing and grid computing are listed in Table I. The "yes" and "no" stand for cloud computing or grid computing has the special characteristic or not. The "half" means not owning the whole characteristic to a certain extent. This paper doesn't pay much attention on the similarities and difference between them and focuses on the essential characteristics of cloud computing [6].
The cloud computing, grid computing, High performance computing (HPC) or supercomputing and data centre computing all belong to parallel computing. HPC focuses on scientific computing which is computing intensive and delay sensitive. So high processing performance and low delay are the most important criteria in HPC. Grid computing is based on HPC centre. Many connected HPC centres form a large grid which owns a powerful underlying concept – service oriented architectures (SOA). Some other creative and impressive concepts like utility computing and autonomic computing do not come into reality.

Table 1 Cloud Computing Vs. Grid Computing

Characteristics	Cloud Computing	Grid Computing
Service Oriented	Yes	Yes
Strong Fault Tolerant	Yes	Half
TCP/IP Based	Yes	Half
High Security	Half	Half
Loose Coupling	Yes	Half
Virtualization	Yes	Half
Ease Use	Yes	Half
Commercial Pattern	Yes	No

The cloud computing which is based on data centre is much more widely accepted than grid computing. Data centre which doesn't only pursue powerful processing performance and low delay is more balanced than HPC centre.

2.1.1 Service oriented

The service oriented concept is similar to but more practical than the concept of SOA in grid computing. Abstraction and accessibility are two keys to achieve the service oriented conception. Through virtualization and other technologies, the underlying architecture is abstracted without exposing much to user. So it is opacity to cloud user. Abstraction reduces both the need for cloud user to learn the detail of cloud architecture and the threshold of application development. At the same time, the key elements of underlying architecture can be simply accessed by cloud user.
Cloud user can consume all the capacity easily by exploring system parameters such as processing performance and storage capacity. In general, according to the type of provided capability, the services of cloud computing is broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [5, 6].

Apple's App store [19] is a creative and famous cloud computing in wireless area. Software services are sold in pay-per-use style. But running on terminals such as 3G phones instead of huge data centres is different from SaaS. The electric books resources in Amazon [20] are also services in cloud computing. These services hardly have substitution and building another EC2 is much easier than owning so many electric resources. In online game area, powerful game servers supply the interactions of millions game players. Game players use the capability of cloud computing without much waking up to this technology.

2.1.2 Loose coupling

The loose coupling is the technical fundamental of cloud computing and goes beyond the loose coupling method of application interaction. Through virtualization or other technologies, the infrastructures are separated in logic or physic. The behaviour of one part hardly affects other parts. The independent cloud users can induce many other features such as stateless, scalability and strong fault tolerant. Software services are sold in pay-per-use style. But running on terminals such as 3G phones instead of huge data centres is different from SaaS. All these services are as important an opposite example is the tight coupling of HPC systems which focus on solving scientific problems. Usually, there are too many data dependences or global synchronizations in different iterations to bear the high delay among computing nodes. This kind of systems use high speed network e.g. InfiniBand instead of industrial standard Ethernet which is much cheaper and widely supported. It is hard to imagine spending tens of minutes to achieve a global synchronization in HPC. But in cloud computing one time of global data synchronization may cost several hours or even several days.

2.1.3 Strong fault tolerant

There are many fault tolerant methods in parallel computing. At low-level, there always exist some fault correction mechanisms with specific hardware. At high-level, many specific applications are studied with methods aiming at algorithms. Checking point is one of the most effective methods at middle-level. In large scale parallel computer systems, the interval of two failures may be shorter than application execution time. The fault tolerant technology becomes critical in this condition. Otherwise it has only less chance to complete the time consuming computing tasks. Because a minimum error is unacceptable and redoing costs too much time in many scientific applications, so the whole computation states which are saved periodically on stable storage will roll back to a special checking point if an error occurs. It is unnecessary to keep the whole states of cloud computing systems. There is almost no dependence between two transactions. The failure of one transaction does not affect the other one and partly failure of system will not cause chain reaction.
There are mainly four places where faults maybe occur in cloud computing: provider-inner, provider-across, provider-user and user-across. If a fault occurs in provider, the backup or redundancy of provider will substitute for the failed part. Stop services and restart are another common method if the services are not on time or urgent. If a fault occurs among providers, the provider-across transaction will be cancelled and return with an error hint. Redirecting to other providers is a universal method which involves load balance of whole cloud system. Fortunately, there are only fewer transactions, which are caused by background management in the main, involving more than one provider. It needs only to run background management one time per day or even per week.

3.1 Mutual IDS for Reliable security of Cloud Computing

The reliable computing mechanism can provide a way that can help to establish a security environment. The model of reliable computing is originally designed to provide the privacy and trust in the personal platform and the reliable computing platform is the base of the reliable computing. Since the internet computing or network computing has been the main computing from the end of the last century, the model of reliable computing is being developed to the network computing, especially the distributed systems environment.
Web service technology have developed as quickly and have been used broadly, cloud computing system could evolve to cloud computing service, which integrates the cloud computing with web service technology. So we could extend the trusted computing mechanism to cloud computing service systems by integrating the TCP into cloud computing system.
The network computing environment, trust will go on to envision a connected, digital world in which trusted entities would interact with one another in much the same way individuals and businesses interact in traditional commercial relationships. "The digital universe requires that parties to a common transaction be able to trust that their mutually agreed upon intents will be fulfilled and their rights protected. For true commerce automation to exist, trading partners must know what to expect from each other's systems."[3]. Reliable computing, therefore, must provide the basis for trusted transactions to occur, and reliable computing technologies must allow stakeholders to express policies and have those policies negotiated and enforced in any execution environment.
Distributed intrusion detection system (DIDS) is a kind IDS designed to discover attacks on individual hosts as well as the network which connects them. A great deal of research has been devoted to providing reasonable solutions to support this system. The idea of DIDS is to aggregate data generated by individual intrusion detection systems. In DIDS, messages sent by the agents are based on IDMEF (Intrusion Detection Message Format) [2]. It is an XML document type definition for the exchange of messages between intrusion detection systems. The benefit of this kind of system is to gather the resources from intrusion detection system in the network to with stand denial-of-service or distributed denial-of-service attack.

3.1.1 Authentication cloud computing environment with TCP

The cloud computing environment, different entities can appeal to join the CLOUD. First step to prove their identities to the cloud computing system administration. Because cloud computing should involve a large amount of entities, such as users and resources from different sources, the authentication is important and complicated. Considering these, we use the TCP to aid to process the authentication in cloud computing.
The TCP is based on the TPM. The TPM is a logic independent hardware. It can resist the attack from software, and even the hardware attack. The TPM contain a private master key which can provide protect for other information store in cloud computing system. Because the hardware certificate can store in TPM, it is hard to attack it. So TPM can provide the trust root for users. Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user’s identity is proved by user’s personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information.
Each site in the cloud computing system will record the visitor’s information. So by using the TCP mechanism in cloud computing, the trace of participants can be known by the cloud computing trace mechanism.

3.1.2 Role Based Access Control Model

A role hierarchy is introduced to reflect inheritance of authority and responsibility among the roles. If a user has a user-role certificate showing membership in role R, and a cloud computing service requires role r, the user should be able to get permission. On the other hand, the resource owners should also use this mechanism to express their identities, and get the rights to provide their resources to other users.

The cloud computing service should present which role it will give the permission, when the cloud computing service notifies itself to the cloud computing environment. So the user will able to know whether he could make access to that cloud computing service before his action.

The encryption is another major mechanism in our design. This function lets data be encrypted in such a way that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration. This service is built by a combination of hardware and software application. The hardware maintains a "master secret key" for each machine, and it uses the master secret to generate a unique sub-key for every possible configuration of that machine.

As a result, data encrypted for a particular configuration cannot be decrypted when the machine is in a different configuration. When one machine wants to join the cloud computing, it will show its certificate and generate session key with other co-operators buy using the unique sub-key. If the configuration in the local machine is changed, the session-key will also be not useful. The distributed environment, we can use this function to transmit data to remote machine and this data can be decrypted when the remote machine has certain configuration.

The user login the CLOUD from the TCP, which is based on the Trust Platform Module (TPM), and get the certificate from the CA, which is trusted by the cloud. When the participant wants to communicate with remote entity, it will carry all the information, including the personal ID, certificate and role information. And the information between them is protected buy their session key.

3.1.3 Data Security in cloud based on TCP

With the TCP, the different entities can communicate in a security way. The TCP generate random numbers and then create session keys. The random keys created by physical hardware have the security characteristics better than those generated just by software programs. The security communication protocols use the system in cloud to call TSS to use the TPM. Then TPM provides the encryption key and session key to the communicators in cloud computing. With its computing capacity, TPM can burden few computation works from CPU and improve the performance.

The important data stored in the computer can be encrypted with keys generated by the TPM. When accessing to these data, the users or applications should pass firstly the authentication with TPM, and encryption keys are stored in the TPM, which makes it hard to attack these keys. To prevent the attack for integrity of data, the hash function in TPM is used. The TPM will check the critical data in a certain interval to protect the integrity of data. The processes of encryption and integrity check use TSS to call the function of TPM.

3.1.4 The Trace of the User's Behaviour

Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware,

such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Before the distributed machine cooperates to do something, they should attest their local information to the remote site.
When the user login the cloud computing system, his identity information should be recorded and verified at first. Each site in the cloud computing system will record the visitor's information. So if the TCP mechanism is integrated into the cloud computing, the trace of the participants, including the users and other resources, can be knew by the cloud computing trace mechanism. Then if the participants do some malicious behaviour, they will be tracked and be punished. In order to achieve the reliable computing in the cloud computing system, we should have the mechanism to know not only what the participants can do, but also what the participant have done. So the monitoring function should be integrated into the cloud computing system to supervise the participants' behaviour. In fact, reference monitors have been used in the operation system for more than several decades, and it will be useful in cloud computing too.

3.1.5 Numerous representative based distributed Intrusion Detection System

3.1.5.1 Advantages

- Numerous-representative expertise has a strong flexibility, good independent and scalability in distributed IDS. It uses representative's autonomy and system structure to ensure Intrusion Detection System scale extensible. Intrusion Detection Module is designed by a unified framework and its rules can be extended.
- It uses a top-down control mechanism which can work layer by layer to prevent the spread of damage. Upper entity can control lower entity. Entities in the same layer can send transaction information with each other.
- Toughness of the system is very strong. Each representative has a System image inspection system to ensure its safety. Once a representative lost its function, it will send an initiative message to the upper, and the upper representative will do restoration work.
- It uses the analysis of representative for application software to protect a number of important applications. It uses data integrity analysis technology to make detection more accurate.

3.1.5.2 Framework

The system consists of a number of agents that have different functions in the network to form a Uniform level of system. These agents can either work independently or work together. Data collection agent has three categories [24, 25]: data collection agent based on host, data collection agent based on network, data collection agent based on applications. The main job of data collection agent is to collect raw data [24, 25]. These raw data includes the State and behaviour of system, network and user activity. Data collection agent filters and re-organizes the raw data collected, then transmitters to data analysis agent.
Data analysis agent has three categories [24, 25]: data analysis agent based on host, data analysis agent based on network, data analysis agent based on applications. Data analysis agent's main job is to do a comprehensive analysis with the data that data collection agent sent to. Data analysis agent can detect the intrusion involving multiple hosts, networks and applications. Data analysis agent is the key to the whole

Intrusion Detection System [24, 25]. The accuracy of Data analysis agent directly affects the performance of whole system.

Communication agent's main task is in charge of related agent's communications. Communication agent can not detect and control. Communication agent is responsible for transmission of all information flow [24, 25]. Centre agent monitors in the high-level the whole system's operation. System administrator use centre agent to manage the entire Distributed Intrusion Detection System.

3.1.5.3 Functioning standard

Distributed Intrusion Detection System based on numerous-representative expertise uses the architecture of Distributed Intrusion Detection System and uses a variety of advanced intrusion analysis and detection technology comprehensively. These intrusion analysis and detection technologies include pattern matching, Protocol analysis, anomaly detection, key surveillance, content resume, network audit and so on[24, 25]. Intrusion Detection System based on numerous-representative expertise can monitor and analysis of network communication and provide real-time intrusion detection and the corresponding preventive methods. It can create comprehensive network security protection.

In specific deployment Data collection agent should be flexible configured according to actual situation, such as network rate, the data encryption, network for switching and so on[24, 25]. Data analysis agent uses misuse detection technology based on the expert system ,State analysis and attacking tree analysis to make the proper response to attack[24, 25]. Data analysis agent can achieve high detection rate, low false alarm and timely response [24, 25].

Communication agent is a numerous-representative based Distributed Intrusion Detection System's key parts. Communication agent can not detect and control attack, so communication agent must set reliable security mechanism. Centre agent can determine the condition that data analysis agent can't judge, unity allocate and manage the entire Agent in the system, display the alarm information and respond to treatment.

3.1.6 Mutual Intrusion Detection System

The idea of mutual defence by intrusion detection systems in the cloud computing environments is a kind of distributed denial-of-service. Within this system, IDS is deployed in each cloud computing region. Any IDS will send out the alert to other IDS while they are suffering from a severe attack defined in this block table. Each intrusion detection system exchanges their alerts and has a judgment category to evaluate the reliable of these alerts. After evaluation, the new blocking rule is added into the block table if the alerts are regarded as a new kind of attack. Therefore, by early detection and prevention from a victim IDS, IDS in the cloud computing regions could resist this type of attack.

In this IDS system implemented four components are: intrusion detection, alert clustering, threshold computation, response and blocking. Each intrusion detection system has three modules: block, communication and mutual modules. The block is used to drop bad packets sent out from the source node; the communication is used to send warning messages about some specific attack detected by itself to other IDS; and the mutual is used to gather alert messages and has to decide these alert messages are either true of false alerts. The system architecture can be described in fig. 1

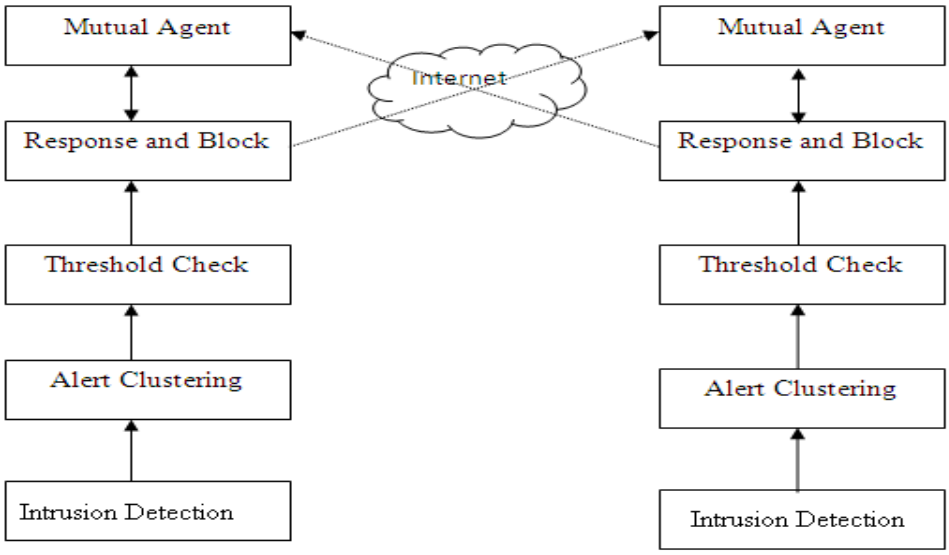

Fig. 1 The Mutual Intrusion Detection system architecture

3.1.6.1 Intrusion Detection System

In the proposed system the intrusion detection systems component is used to gather network packets and analyse these packets. In case type of the packet is corresponds with one of the block table, then the system drops this packet immediately. It would reduce time required for the signature comparison about this packet and improve the system performance, other hand type of the packet is not block table but belongs to type of strange packet defined in the signature comparison rules then the intrusion detection component forwards to the next component. Otherwise the system accepts this packet.

The proposed system modifies Snort system to realize the proposed mutual IDS system. The proposed mutual IDS system is a kind of network based with signature comparison IDS system.

3.1.6.2 Alert Clustering and Threshold Check

The component used to identify the level of spacious packet delivered from intrusion detection component. The level of alerts includes low, medium and high. The following table refers various levels of alerts.

Table 2 Levels of alert process

Level of alert	Type of alert	Process
1	High	Drops the packets and sends an alert notification to other IDS
2	Medium	Threshold check is used to make a decision on whether to drop the packet and send an alert message to other IDS or not
3	Low	Don't care about the packets

The alert level 1, system identifies the packet as a bad one (severe attacks) and drops the packet immediately in the intrusion detection process and then sends an alert message to other IDS by communication module. So that all the packets belongs to first level are blocked without executing signature comparison.
The alert level 2, system executes threshold check by data clustering method to find outlier. The purpose of threshold check is to reduce the possibility of generating false alert. If the number of same type packets is larger than the threshold, then the system changes the alert level medium to high. The reliability of system will be improved.
The alert level 3, the system not cares about this level packet. The proposed system easily identifies the possible packets trying to attack the cloud computing services.

3.1.6.3 Response and Block

The main function of this component is blocking bad packets and sends an alert message to other IDS. This intrusion response and blocking component is built in each intrusion detection systems. The two modules of this component are communication and block. Communication module used to send an alert message to other IDS. The level of alert about the packet is either high or medium level but over threshold, then block module is triggered to block or drop this bad packet.

3.1.6.4 Mutual operations

In this component used to receive alert messages delivered from other IDS. After receiving alerts, the mutual agent makes a decision according to executing majority vote and use the following definition:
If (number of repeated alert messages sends from IDSs) / (Number of IDSs in the cloud computing) > 1/2, then IDS accepts this alert message and regards this type of packets as a bad packet. If any one of the cloud computing regions suffers from denial-of-service attack, other IDS in the cloud computing regions except this one will receive alert message. Majority vote method is used to deciding the responsibility of an alert. The early detection and prevention might be implemented. The malicious IDS might be found if they send false alerts habitually. To end with IDS would have a chance to block this type of attack in advance. The proposed system is compared with pure Snort based IDS with respect to two performance metrics. They are computation time and detection rate. From the metric analysis the proposed mutual IDS system gives better result compare with Snort. The proposed mutual IDS are preventing the system from single point of failure attack.

4.1 Conclusion

The Understanding a technical area as complex as cloud computing is not easy and requires identifying its fundamental characteristics. Clear concepts and terminology into cloud computing help but do not entirely solve the problem of how to design, develop and adopt a cloud computing system.
This paper discusses the characteristics, mutual and reliable security in of cloud computing. The conception service oriented characteristic abstracts the details of cloud computing implementation. The loose coupling and strong fault tolerant stand for the main technical characteristics. The ease use user experience characteristic helps cloud computing being widely accepted by non computer experts. We believe that these characteristics expose the

essential of cloud computing and the development and adoption of this evolving technology will benefit from our work.

The analysed reliable computing in the cloud computing environment and the function of reliable computing platform in cloud computing. The advantages of proposed approach are to extend the mutual and reliable computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfil the reliable cloud computing. TCP is used as the hardware base for the cloud computing system. In this design, TCP provides cloud computing system some important security functions, such authentication, communication security and data protection. The TCP provides cloud computing a secure base for achieve reliable computing. The proposed concept is a mutual intrusion detection system for cloud computing network to reduce the impact of denial-of-service attacks.

The security protection based on firewalls and encryption technology is very important and we must develop Distributed intrusion detection technology in order to improve the system's security status. A Mutual Distributed Intrusion Detection System can improve the detection accuracy and detection speed, and enhance the system's own security. The proposed mutual IDS only increases little computation effort compared with pure snort based IDS but the probability of survival of IDS is improved under denial-of-service attack.

Emphasize the new and important aspects of the study and conclusions that follow from them, do not repeat in detail data given in the results section. Include in the conclusion implications of the findings and their limitations and relate the observations to other relevant studies. Link the conclusion with the goals of the study but avoid unqualified statements and conclusions not completely supported by your data. Avoid claiming priority and alluding to work that has not been completed.

References

[1] IBM, "Google and IBM Announced University Initiative to *Address Internet Scale ComputingChallenges*,"http://www-3.ibm.com/press/us/en/pressrelease/22414.wss.

[2] D. Cury and H.Debar, "*Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition*" draft-ietf-idwg-idmef-xml-06.txt, Feb'2002.

[3] Trusted Computing Group (TCG), "TCG Specification Architecture Overview Specification Revision 1.2", April 28, 2004.

[4] Techsmith, "*UX 2.0: Any User, Any Time, Any Channel*," http://www.techsmith.com/morae/whitepaper/ux20.asp.

[5] searchcloudcomputing.com, "*What is cloud computing?*" http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html.

[6] M. Vaquero, L.R. Merino, J. Caceres, and M. Lindner, "*A break in the clouds: towards a cloud definition*," ACM SIGCOMM Computer Communication Review, v.39 n.1, 2009.

[7] Wikipedia,"*Cloud computing*," http://en.wikipedia.org/wiki/Cloud_computing.

[8] J. Geelan, "*Twenty one experts define cloud computing. Virtualization*", Electronic Magazine, http://virtualization.sys-con.com/node/612375.

[9] D.Farber,"*Oracle's Ellison nails cloud computing*," http://news.cnet.com/ 8301-13953_3-10052188-80.html.

[10] The Economist, "*Cloud computing: Clash of the clouds*," http://www.economist.com/displaystory.cfm?story_id=14637206#top

[11] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "*Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*," Future Generation Computer Systems, 25 (6), pp. 599-616, 2009.
[12] D. Malcolm, "*The five defining characteristics of cloud computing*," http://news.zdnet.com/2100-9595_22-287001.html.
[13] P. Sharma, "*What kinda apps are best suited for 'Cloud deployment': 4 Solutions*," http://www.techpluto.com/cloud-computingcharacteristics/.
[14] D.Amrhein,"*Forget Defining Cloud Computing*," http://ibm.ulitzer.com/ node/1018801.
[15] Microsoft, "*Windows Azure*," http://www.microsoft.com/windowsazure/windowsazure/.
[16] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D.Zagorodnov, "*Eucalyptus open source cloud computing system*" In CCA08: Cloud Computing and Its Applications, 2008.
[17] P. Watson, P. Lord, F. Gibson, P. Periorellis, and G. Pitsilis, "*Cloud computing for e-science with carmen*," IBERGRID, pp.1-5, 2008.
[18] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, L. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. C´aceres, M. Ben-Yehuda, W. Emmerich, and F. Gal´an, "*The RESERVOIR Model and Architecture for Open Federated Cloud Computing*," IBM Systems Journal, 2009, in press.
[19] Techsimth, "*UX 2.0: Any User, Any Time, Any Channel*," http://www.techsmith.com/morae/whitepaper/ux20.asp.
[20] Amazon, "*Kindle*," http://www.amazon.com/Kindle-Wireless-Reading- Device-Display/dp/B00154JDAI.
[21] M.Castro , and B. Liskov, "*Practical Byzantine fault tolerance*," Proceedings of the third symposium on Operating systems design and implementation, pp.173-186, 1999.
[22] P. Morville, "*User Experience Design*," http://semanticstudios.com/publications/semantics/000029.php.
[23] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D.Patterson, A. Rabkin, I. Stoica, M. Zaharia. Above the Clouds: A Berkeley View of Cloud computing.Technical Report No.UCB/EECS-2009-28, University of California at Berkley, USA, Feb.10, 2009.
[24] Ming Tan,Xiaolong Hu,Liancheng Liu, Based on multi-examination technology invasion examination system model, Computer project and design, 2008.
[25] Ming Xiao, Distributed Intrusion Detection System Design, Electronic Science and Technology University, 2002.