ISSN:2320-0790

An International Journal of Advanced Computer Technology

Secure Co-processor and Billboard Manager Based Architecture Help to Protect & Store the Citrix Xenserver Based Virtual Data.

Debabrata Sarddar[1], Rajesh Bose[2]

[1]Department of Computer Science & Engineering University of Kalyani Nadia, West Bengal
[2]Simplex Infrastructures Ltd. Kolkata

Abstract: Any discussion of Cloud computing typically begins with virtualization. Virtualization is critical to cloud computing because it simplifies the delivery of services by providing a platform for optimizing complex IT resources in a scalable manner, which is what makes cloud computing so cost effective. Desktop virtualization, often called client virtualization, is a virtualization technology used to separate a computer desktop environment from the physical computer. Desktop virtualization is considered a type of client-server computing model because the "virtualized" desktop is stored on a centralized, or remote, server and not the physical machine being virtualized. Desktop virtualization "virtualizes desktop computers" and these virtual desktop environments are "served" to users on the network. In this paper, we proposed a secure cloud data center architecture that made by an application virtualization product like citrix xenapp/citrix xen desktop and with a proposed model that help us to encrypt and store the data like virtualized desktop or virtualized application in a suitable storage area.

Keywords: Cloud computing, virtualization, citrix xenapp/citrix xendesktop, storage, cloud data center.

I. INTRODUCTION

Virtualization is a key enabling technology for cloud computing environments. Virtualization is used in the cloud to allow cloud vendors to maximize their resources, a business need not know this is being used at all, and it is not part of the decision making process to leverage the cloud. We can classify Virtualization in three main categories as follows:

A. Hardware Virtualization:

This is the most common type of Virtualization prevalent in corporations and IT companies. In this case, Virtualization software is typically run on an actual physical server to capture its "image" and port it to being a "Virtual Server" with all the same settings intact. This image is then run from a part of your current existing virtual server farm on whatever technology you are implementing (such as VMware or Hyper-v). Consolidating your physical server to a virtual one gives you many advantages such as:

- Making server upgrades easy as you can add RAM and CPU on the fly to a virtual server.
- We can re task our old physical server.
- Never have to worry about physical component failure or not being able to find outdated hardware
- Smaller carbon foot print due to more efficient power distribution and utilization in a virtual environment.

B. Desktop/Application Virtualization:

Desktop virtualization (or Virtual Desktop Infrastructure) is a server-centric computing model that borrows from the traditional thin-client model but is designed to give administrators and end users the best of both worlds: the ability to host and centrally manage desktop virtual machines in the data center while giving end users a full PC desktop experience [4]. Desktop virtualization is emerging as an alternative to traditional desktop delivery. The main

concept of desktop virtualization is based on moving OS and application execution from local (to the user) device to a remote data center. End user device becomes a lightweight computer that handles only keyboard, mouse and monitor, as well as locally attached devices such as scanners and printers. Connectivity between end-user device and desktop OS executing in the data center is handled using remote protocols such as those in [2], [3]. The virtual desktop paradigm has several advantages over the typical "fat-desktop" approach. Management costs of the solutions are significantly lower because operating system images, applications, and data are no longer installed on a large number of distributed systems but in a well-controlled data center, which improves manageability of the system as well as data and application security. Moreover, since the local device is stateless, it is very easy to troubleshoot and replace, thus on site labor is significantly reduced [1].Benefits of desktop virtualization include most of those with application virtualization as well as:

High Availability–

Downtime can be minimized with replication and fault tolerant hosted configurations.

Extended Refresh Cycles–

Larger capacity servers as well as limited demands on the client PCs can extend their lifespan.

Multiple Desktops–

Users can access multiple desktops suited for various tasks from the same client PC. Currently, most of the proposed desktop virtualization systems [5], [6], [7] are based on the technologies to provide the whole desktop. They pay more attention to supply high quality display effects in clients, improve the interaction experiences between users and machines, or reduce the transmission delay in which desktops are propelled to clients. However, all these protocols do not lay emphasis on decreasing the propelled desktop's granularity and optimize the protocol utilized between clients and servers, which are important to the flexibility and extendibility of the whole system.

Application virtualization is an umbrella term that describes software technologies that improve manageability and compatibility of legacy applications by encapsulating applications from the underlying operating system on which they are executed. A fully virtualized application is not installed in the traditional sense, although it is still executed as if it is. Application virtualization differs from operating system virtualization in that in the latter case, the whole operating system is virtualized rather than only specific applications[4].With streamed and local application virtualization an application can be installed on demand as needed. If streaming is enabled then the portions of the application needed for startup are sent first optimizing startup time. Locally virtualized applications also frequently make use of virtual registries and file systems to maintain separation and cleanness from the user's physical machine. Examples of local application virtualization solutions include Citrix Presentation Server and Microsoft Soft Grid. One could also include virtual appliances into this category such as those frequently distributed via VMware's VMware Player. Benefits of application virtualization include:

1. **Security**– Virtual applications often run in user mode isolating them from OS level functions.
2. **Management**– Virtual applications can be managed and patched from a central location.
3. **Legacy Support**– Through virtualization technologies legacy applications can be run on modern operating systems they were not originally designed for.
4. **Access**– Virtual applications can be installed on demand from central locations that provide failover and replication.

C. Network Virtualization-

In computing, network virtualization is the process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Network virtualization involves platform virtualization, often combined with resource virtualization. Network virtualization is categorized as either external, combining many networks, or parts of networks, into a virtual unit, or internal, providing network-like functionality to the software containers on a single system [4].

Using the internal definition of the term, desktop and server virtualization solutions provide networking access between both the host and guest as well as between many guests. On the server side virtual switches are gaining acceptance as a part of the virtualization stack. The external definition of network virtualization is probably the more used version of the term however. Virtual Private Networks (VPNs) have been a common component of the network administrators' toolbox for years with most companies allowing VPN use. Virtual LANs (VLANs) are another commonly used network virtualization concept. With network advances such as 10 gigabit Ethernet, networks no long need to be structured purely along geographical lines. Companies with products in the space include Cisco and 3Leaf. In general benefits of network virtualization include:

1. **Customization of Access**– Administrators can quickly customize access and network options such as bandwidth throttling and quality of service.
2. **Consolidation**– Physical networks can be combined into one virtual network for overall simplification of management.

Similar to server virtualization, network virtualization can bring increased complexity, some performance overhead, and the need for administrators to have a larger skill set.

D. Storage Virtualization-

Storage virtualization refers to the process of abstracting logical storage from physical storage. [4]

While RAID at the basic level provides this functionality, the term storage virtualization typically includes additional concepts such as data migration and caching. Storage virtualization is hard to define in a fixed manner due to the variety of ways that the functionality can be provided. Typically, it is provided as a feature of:

- Host Based with Special Device Drivers
- Array Controllers
- Network Switch
- Stand Alone Network Appliances

Each vendor has a different approach in this regard. Another primary way that storage virtualization is classified is whether it is in-band or out-of-band. In-band (often called symmetric) virtualization sits between the host and the storage device allowing caching. Out-of-band (often called asymmetric) virtualization makes use of special host based device drivers that first lookup the Meta data (indicating where a file resides) and then allows the host to directly retrieve the file from the storage location. Caching at the virtualization level is not possible with this approach.

General benefits of storage virtualization include:

1. **Migration**– Data can be easily migrated between storage locations without interrupting live access to the virtual partition with most technologies.

2. **Utilization**– Similar to server virtualization, utilization of storage devices can be balanced to address over and underutilization.

3. **Management**– Many hosts can leverage storage on one physical device that can be centrally managed.

The rest of the paper is organized as follows security issues for cloud is introduced in Section II. The encrypted data storage is described in Section III and Section IV describe the related work and the proposed system architecture is presented in Section V. Finally, conclusion part is drawn in Section VI.

II. SECURITY ISSUES FOR CLOUD

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, con-currency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

A. 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 [8]. These are required to be collocated 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.

B. *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[9].

C. *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[10]. 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.

D. 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 [9].

E. 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[11]. This is one of the most complicated problems in cloud computing as it has many customers using various virtual machines.

III. ENCRYPTED DATA STORAGE

Since data in the cloud will be placed anywhere, it is important that the data is encrypted. We are using secure co-processor as part of the 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. First, Open Cirrus provides limited access based on their economic model (e.g., Virtual cash). Furthermore, Open Cirrus does not provide the hardware support we need (e.g., secure co-processors). By embedding a secure co-processor (SCP) into the cloud infrastructure, the system can handle encrypted data efficiently (see Figure 5). Basically, SCP is a tamper-resistant hard-ware capable of limited general-purpose computation. For example, IBM 4758 Crypto-graphic Coprocessor (IBM) 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 tampering is detected, then the secure coprocessor 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. 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 (Smith, 1999).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 (i.e., a master key that encrypts all other keys). 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, SCP scan be used for privacy preserving information integration which is important for assured information sharing [12].

IV. RELATED WORKS

In industry and academia there have been significant advances in the delivery of desktop and application environments to users, mainly through the use of virtualization and thin clients. At the data center there are various virtualization technologies, (at both OS and application level) that have been used to abstract desktop execution from underlying hardware. Examples of those include [14], [15], [16] etc. Many researchers have invented different techniques in the field of secured cryptographic co-processor and data security, Network security in the cloud. A complete outline on various researches and trends in cloud computing has been presented in [17].The authors discuss a scheme for secure third party publications of documents in a cloud. Next, the paper will converse secure federated query processing with map Reduce and Hadoop, and discuss the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing [18]. A good report has been presented in [19]. Another good report on various architectural strategy used by cloud computing in oracle white paper [20]. Many researches on providing privacy to user data in cloud have been presented in [24, 25, 21, 22, and 23].

V. PROPOSED WORK

In a method which we now propose, we shall be introducing a secure network architecture for a cloud data center using equipment consisting of hardware (hard disks,

processors, memory modules, solid state disks, secured co-processors, etc.), and software which would include the Billboard Manager[26]. The architecture would be tailored to (a) support efficient storage of encrypted and sensitive data; (b) store, manage and query massive amounts of data; (c) support fine-grained access control; and (d) support strong authentication features.

In this suggested methodology, an end-user would be able to obtain and establish through secure links, remote desktop sessions, wherein applications, designed and marketed as ready for deployment and hosting on virtual platforms, e.g., Auto CAD, is running. A secure link, over the web, would be extended to the user by the appropriate credential and cloud service provider.

Using this secure link and armed with a designated user ID and password so provided by the credential and cloud service provider, the user would be able to connect to the cloud data center through a secure connection via the SSL VPN. The link to the Citrix XenApp server hosting the remote desktop session and the virtualized application is displayed on a page following successful authentication.

To access the remote desktop, and any of the applications running, thereon, the user would then have to click on the link and supply the corresponding user ID and password.

Data would be channeled through the secure co-processor for encryption. The Billboard Manager [26] would then position the encrypted data in locations which it calculates to be optimum considering the parameters within which it has been designed to operate.

Cryptographic co-processors help in defining the security protocols and implement them. A dedicated set of hardware forms a Cryptographic co-processor which can only take care of either encryption or decryption [13].The Billboard Manager helps to choose the appropriate storage location to store the encrypted data. A major part of our system is Billboard Manager which is to handle a large number of storage nodes. Billboard Manager knows the available blank space of cloud storage. Necessary collected encrypted data sends different suitable cloud storage.Fig1 shows this proposed architecture.

Billboard Manager follows this algorithm[26].

1) BM stores all information about Cloud storage Nodes like capacity, IP address, and shortest node distance and any kinds of information about the nodes.

2) All Cloud nodes send periodic information to BM.

a) Channel capacity

b) Storage space

Both of the information varies time to time and also area to area.

3) Now for t=0, storage capacity if the storage capacity >0

Continue;

Else stop.

4) Compare storage capacity, choose the maximum one.

5) If the storage capacity of the two Cloud nodes to handover is same.

6) Compare the data rate. Choose the highest data rate.

Else go back to 4

7) Repeat 4-6 every time while choosing a new cloud storage node to handover.

8) Make a list of the available cloud storage node and store it to BM

9) Now BM again makes a list of available cloud storage node based on free space.

10) Now comparing the best cloud storage node to send the data.

11) Now the connection is established.

VI. CONCLUSION

Although cloud computing has many advantages, there are still many actual problems that need to be solved. Security is considered one of the most critical aspects in everyday computing, and it is no different for cloud computing due to the sensitivity and importance of data stored in the cloud. Cloud computing infrastructures use new technologies and services, most which haven't been fully evaluated with respect to security.

There is several security challenges including security aspects .There are many security issues for cloud. These issues include storage security, middle ware security, data security, network security and application security. In our paper, the main goal is to securely store and manage data with a secure connection or proper authentication. Next, we discussed how secure coprocessors and Billboard Manager may be used to enhance the security.

Our proposed datacenter architecture is given below.

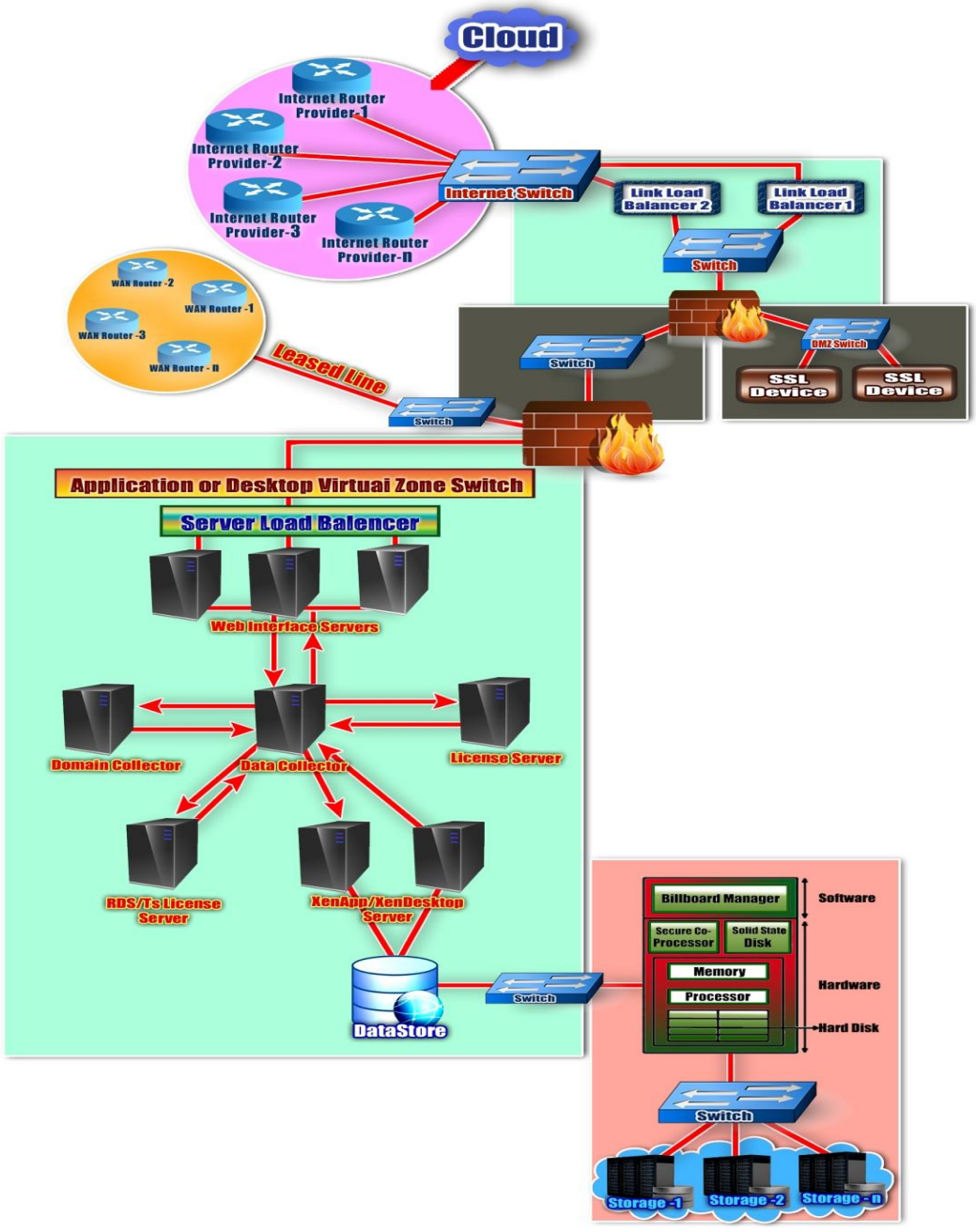

Fig1:- A Secure Cloud Datacenter Architecture

REFERENCES

[1]Guangda Lai, Hua Song, Xiaola Lin,A Service Based Lightweight Desktop Virtualization System,© 2010 IEEE DOI 10.1109/ICSS.2010.44

[2] Real VNC, "Vnc," http://www.realvnc.com/.

[3] Microsoft Corporation, "Remote Desktop Protocol," http://msdn2.microsoft.com/en-us/library/aa383015.aspx.

[4]Wikipedia

[5] Citrix Corporation, "Citrix Application Delivery Infrastructure."

[6] "Kernel Virtual Machines," http://sourceforge.net/projects/kvm.

[7] Desktone, "Desktop as a Service," http://desktone.com/, 2008.

[8][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 Languagesand Analysis for Security(PLAS). June 2009

[9] Mr. D. Kishore Kumar, Dr.G.Venkatewara Rao , Dr.G.Srinivasa Rao,Cloud Computing: An Analysis of Its Challenges & Security Issues,International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012.

[10]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.

[11]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.

[12] C.Kishor Kumar Reddy, P.R Anisha, K.Srinivasulu Reddy, S.Surender Reddy, Third Party Data Protection Applied To Cloud and Xacml Implementation in the Hadoop Environment With Sparql, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 2, Issue 1 (July-Aug. 2012), PP 39-46.

[13] Praveen Ram C, Sreenivaasan G,Security as a Service (SasS),Securing User Data by Coprocessor and Distributing the Data,978-1-4244-9008-0/10/$26.00 ©2010 IEEE

[14] Citrix Corporation, "Citrix Application Delivery Infrastructure."

[15] Microsoft Corporation, "Windows Terminal Services."

[16] VMWare EMC, http://www.vmware.com.

[17] Mr. D. Kishore Kumar, Dr.G.Venkatewara Rao , Dr.G.Srinivasa Rao,Cloud Computing: An Analysis of Its Challenges & Security Issues,International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012.

[18]Kevin Hamlen,Murat Kantarcioglu,Latifur Khan,Bhavani Thuraisingham,Security Issues for Cloud Computing,International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[19] Robert Gellman, ―WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, February 23, 2009.

[20]Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing.

[21]Robert Gellman, ―WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing‖, February 23, 2009.

[22] A. Cavoukian, ―Privacy in the clouds‖, in Springer Identity in the Information Society, Published online: 18 December 2008.

[23] Pearson, ―Taking Account of Privacy when Designing Cloud Computing Services, in Proceedings of ICSE-Cloud'09, Vancouver, 2009.

[24] C.Kishor Kumar Reddy, P.R Anisha, K.Srinivasulu Reddy, S.Surender Reddy, Third Party Data Protection Applied To Cloud and Xacml Implementation in the Hadoop Environment With Sparql, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 2, Issue 1 (July-Aug. 2012), PP 39-46.

[25]Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing.

[26] Debabrata Sarddar, Rajesh Bose, Creating a Secured Cloud Based Data Center Using Billboard Manager (BM) and Secuare Co-Processor, International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013.

AUTHORS PROFILE

Debabrata Sarddar, Assistant Professor in the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, INDIA. He has done PhD at Jadavpur University. He completed his M. Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.E in Computer Science & Engineering from NIT, Durgapur in 2001. He has published more than 75 research papers in different journals and conferences. His research interest includes wireless and mobile system and WSN, cloud computing.

Rajesh Bose is a project engineer employed by Simplex Infrastructures Limited at the company's Data Center located in Kolkata. He received his M. Tech. Degree in Mobile Communication and Networking from WBUT in 2007. He had also received his B.E. Degree in Computer Science and Engineering from BPUT in 2004. His research interests include cloud computing, wireless communication and networking.