Creating a Secured Cloud Based Data Center Using Billboard Manager (BM) and Secuare Co-Processor

Debabrata Sarddar, Rajesh Bose

Abstract— Cloud computing is fast becoming a reality, combining IT on-demand with pay-per-use flexibility. But cloud computing not only cuts costs – it also provides increased resilience for critical applications. Cloud computing has become one of the most significant issues in recently. Those associative applications and services based on cloud computing are dramatically emerging. However, in order to enjoy the widely utilization of cloud computing through wired/wireless networking, providing sufficient assurance of information security such as confidentiality, authentication, non-repudiation, and integrity is the critical factor of success . As in most other streams of computers, security is a major obstacle for cloud computing. In this paper, we proposed secure cloud data center architecture. We discuss a secure cloud data center architecture where end users can connect over a secure channel and store their encrypted data in suitable storage area with the help of secure co-processor and Billboard Manager. Billboard Manager [21] helps to choose the appropriate location of storage.

Key woard— cloud data center, Authentication,secure channel, secure co-processor, Billboard Manager,storage,

1. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

Cloud Computing has now been defined by the National Institute of Standards and Technology (NIST) as [6];"A model for enabling convenient, on demand network access to a shared pool of configurable computing resources (E.g. networks, servers, storage, applications and services). That can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud Computing has now been defined by the National Institute of Standards and Technology (NIST) as [6];
"A model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
Some advantages of Cloud Computing could be defined as [5]; having an inexpensive secures and managed hosting. Having off site server backup in the event of the business server failure full support of server providers removing the need to purchase new software as the business grows.
Some disadvantages of Cloud Computing could be [5]; Loss of control of servers, software and security. The business's private data is under the control of a Third party (Trust issues arise) the logistics of migrating large amounts of data from the provider. A possible extra cost of data transfer fees.
The primary models for delivering cloud services:
Software as a Service (SaaS) [2] is described as 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.
Platform as a Service (PaaS) [3] is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.
Infrastructure as a Service (IaaS) [4] is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the

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, WSN and 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.

equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

There are currently four deployment models for Cloud. The services as follows: Public cloud, Community cloud, Hybrid cloud and Private cloud.

A. **Private Cloud:** the infrastructure is operated solely for an organization; it may be managed by the organization or a third party and may exist on or off the premises of the organization.
B. **Community Cloud:** the infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.
C. **Public Cloud:** the infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
D. **Hybrid Cloud :** the infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

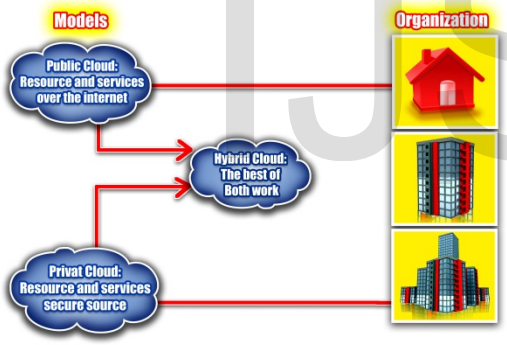

Fig1 - Three cloud Models

Security Concerns

Key security concerns can be summed up by using the five W's; Who, What, Why, When and Where [7].

Who? Who will have access to the Data? As well as the organizations own employees who outside of the organization and in particular within the Cloud providers organization will have access to this information?

What? What data is to be stored? What types of data will be stored in the Cloud? Is the data sensitive, personal, confidential or secret?

Why? Why do they need access? (Is the access appropriate?) Why does anybody outside of the organization need access to the data that is to be stored in the Cloud?

When? When does the data require encryption? When should the data be encrypted? Before leaving the organization or will it be encrypted at the Cloud providers end?

Where? Where will the data be stored?

Will the data storage location meet with the compliance regulations? For example will the Cloud servers be located within Europe or will they be passed on to USA held servers? All of the questions above should not only be matters of security they should all be part of the compliance requirements of the business.

There is a critical need to securely store, manage, share and analyze massive amounts of complex (e.g.,semi-structured and unstructured) data to determine patterns and trends in order to improve the quality of healthcare, better safe-guard the nation and explore alternative energy. Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore, we need to safeguard the data in the midst of untrusted processes. The emerging cloud computing model attempts to address the explosive growth of web-connected devices, and handle massive amounts of data. Google has now introduced the Map Reduce framework for processing large amounts of data on commodity hard-ware. Apache's Hardtop distributed file system (HDFS) is emerging as a superior software component for cloud computing combined with integrated parts such as Map Reduce. The need to augment human reasoning, interpreting, and decision-making abilities has resulted in the emergence of the Semantic Web, which is an initiative that attempts to transform the web from its current,merely human-readable form, to a machine-processable form. This in turn has resulted in numerous social networking sites with massive amounts of data to be shared and managed.

Therefore, we urgently need a system that can scale to handle a large number of sites and process massive amounts of data. However, state of the art systems utilizing HDFS and Map Reduce are not sufficient due to the fact that they do not provide adequate security mechanisms to protect sensitive data. We are conducting research on secure cloud computing. Due to the extensive complexity of the cloud, we contend that it will be difficult to provide a holistic solution to securing the cloud, at present.

Therefore, our goal is to make increment enhancements to securing the cloud that will ultimately result in a secure cloud. In particular, we are developing a secure cloud consisting of hardware , software (includes Billboard Manager [21]).Our cloud system will: (a) support efficient storage of encrypted sensitive data, (b) store, manage and query massive amounts of data, (c) support fine-grained access control and (d) support strong authentication. This paper describes our approach to securing the cloud. The organization of this paper is as follows: In section 2, we will give an overview of security issues for cloud. In section 3, we will discuss about encrypted data storage.n section 4, we will discuss about related works. In section 5, we will discuss about proposed work, in section 6, we will discuss about coclusion.

2. 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.

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, Fail over and Sand boxing, which are used for instance isolation. Multiple organizations have multiple virtualization systems [9]. 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.

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[12].

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.

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 [12].

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.

3. 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 Cryptographic 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 [1].

4. RELATED WORKS

A lot of research has been done 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 [12].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 thei beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing [8]. A good report has been presented in [13]. Another good report on various architectural strategy used by cloud computing in oracle white paper [14], Many researches on providing privacy to user data in cloud have been presented in [1, 14, 15, 16, and 17].In the paper [19] authors says the various issues with cloud and it has also provided some guidelines on minimizing personal information stored and sent to the cloud, and this paper also enhancing g the security to the user data. IBM has discussed about the secure coprocessor in [19, 20].

5. PRPPOSED WORK

In our proposed method we are introduce a secure network architecture for cloud data cen ter with proposed equipment that consisting hardware (Hard Disks, Processor, Memory, solid state disk,secure co-processor), software (includes Billboard Manager).this architecture will (a) support efficient storage of encrypted sensitive data, (b) store, manage and query massive amounts of data, (c) support fine-grained access control and (d) support strong authentication. In our proposed work an end user have to access a secure link which is eventually publish in SSL VPN gateway and have to log in with necessary credential .Once a user has logged in via an encrypted connection to resource server will be established through SSL VPN device in our proposed architecture. After the secure connection is established the end users can access the desire server as well as database, we discuss a secure cloud data center architecture where end users can connect over a secure channel and store their encrypted data in suitable storage area with the help of secure co-processor and Billboard Manager [21].Co-processors are secondary processors that help in accelerating system performance by taking hold of processor intensive applications and tasks. It has to be noted that, Unlike Processors, co-processors cannot fetch instructions from Memory. 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 [22]. 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.

Billboard Manager follows this algorithm.

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, compare 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 Cloud nodes 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.

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.

Now the connection is established.

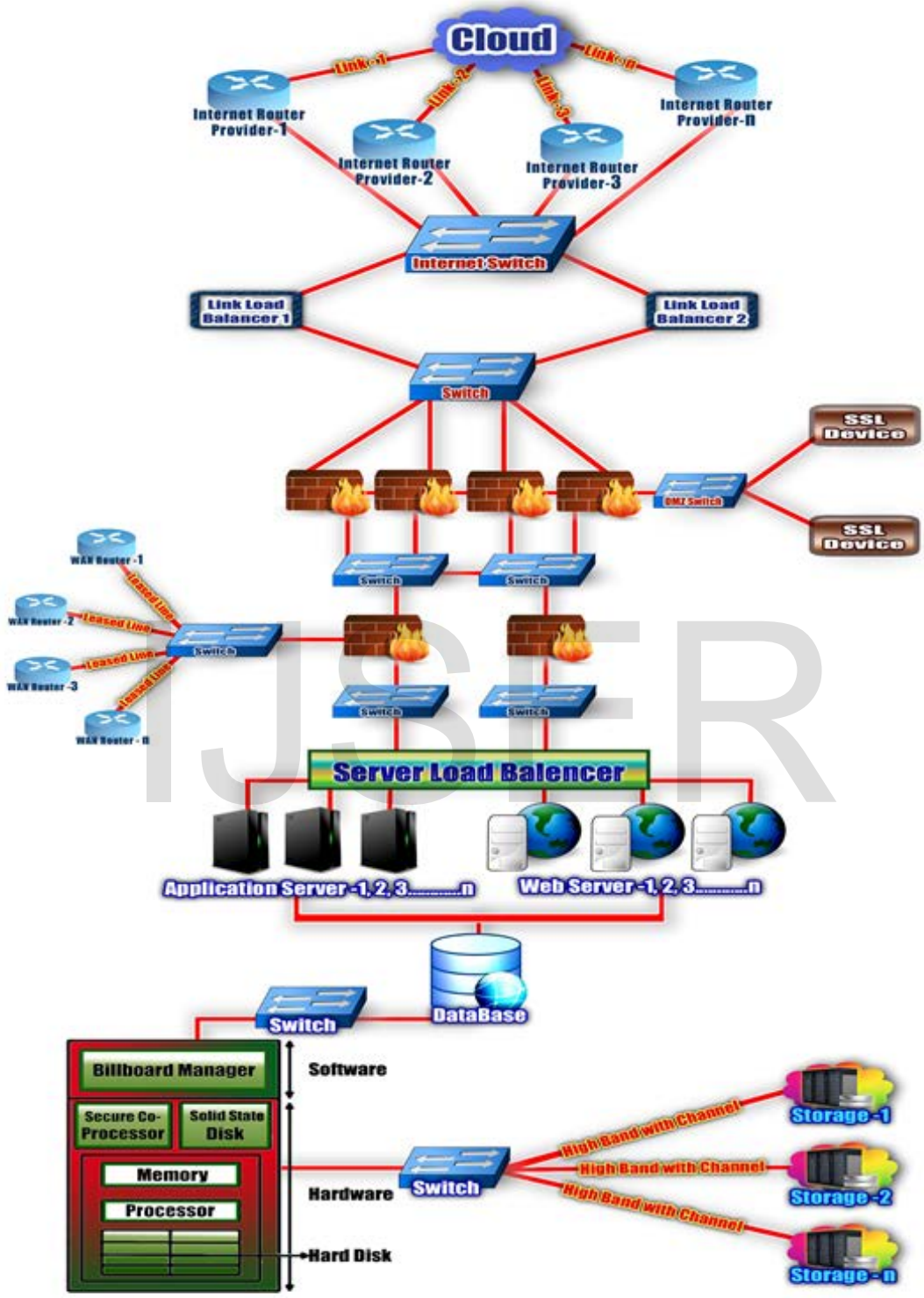

Fig2 - A Secure Cloud Datacenter Architecture

6. 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 compu-

ting, 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 are 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.

REFERENCES

[1] 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.*

[2] TechTarget (2006) Definition Software as a Service (SaaS) [Online].Available:http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

[3] TechTarget (2006) Definition Platform as a Service (PaaS) [Online].Available:http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

[4] TechTarget (2006) Definition Infrastructure as a Service (IaaS) [Online]. Available: http://searchcloudcomputing. Techtarget.com/definition /Infrastructureas-a-Service-IaaS

[5] Kenneth Aspinall, Stewart Blakeway, Security Practices in Cloud Computing and the Implications to SMEs, ISBN: 978-1-902560-25-0 © 2011 PGNet.

[6] P. Mell and T. Grance (2009) The NIST Definition of Cloud Computing [Online].Available:http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html.

[7] P. Cox. (2010) "A Guide to Securing Data in the Cloud and Meeting Cloud Security Regulations [Online] Available: http://viewer.media.bitpipe.com/1103740304_372/1280167431_218/CA_sCompliance_SO-O31222-E-Guide_7-22.pdf

[8]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*

[9] 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.

[10]Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S.Raghu,H.Raghav Rao, ―The Information Assurance Practices of Cloud Computing Vendors‖, *IT Pro July/August 2010, In IEEE Computer Society, p. 2937.*

[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] 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.*

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

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

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

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

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

[18] S. Pearson and A. Charlesworth, ―Accountability as a 5 Way Forward for Privacy Protection in the Cloud, HP Labs Technical Report, HPL-2009-178, http://www.hpl.hp.com/ techreports/2009/HPL-2009-178.pdf (2009).

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

[20]S. Weingart, ―Building the IBM 4758 secure coprocessor‖, IEEE Computer, 34:57–66, October 2001.

[21] Debabrata Sarddar, Rajesh Bose, Reducing Carbon Emission Rate Using Billboard Manager (BM), *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013.*

[22] 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*