International Journal of Information Technology and Management
Vol. XI, Issue No. XVII, November-2016, ISSN 2249-4510

Security Architecture for Cloud Computing

Prof. (Dr.) S.S. Sarangdevot[1]* Dr. Neeraj Bhargava[2] Dr. Pooran Singh[3] Mandeep Kaur[4]

[1]Vice Chancellor, Janardan Rain Agar Rajasthan Vidyapeeth, University, Udaipur, Rajasthan, India

[2]Professor & Head Department of Computer Science, School of Engineering & System Sciences MDS University, Ajmer, Rajasthan, India

[3]Department of Computer Science, Kuchaman College Kuchaman City MDS University, Rajasthan, India

[4]Computer Science, Maharaj Vinayak Global University, Jaipur (India)

Abstract – Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. In this chapter, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss critical challenges: regulatory, security and privacy issues in cloud computing. Cloud computing continues to increase in popularity. 'It's a long-running trend with a far-out horizon. But among big meta trends, cloud computing is the hardest. According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment.

Keywords- Cloud Computing, Cloud Service, Cloud Security, Computer Network.

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

Recent developments in the field of cloud computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & Jangwal, 2012). Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The cloud computing landscape continues to realize explosive growth. The worldwide public cloud services market was projected to grow nearly 20 percent in 2012, to a total of $109 billion, with 45.6 percent growth for Infrastructure as a Service (IaaS), which is the fastest growing market segment. Yet for security professionals, the cloud presents a huge dilemma: How do you embrace the benefits of the cloud while maintaining security controls over your organizations' assets? It becomes a question of balance to determine whether the increased risks are truly worth the agility and economic benefits.

Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

This shift in control is the number one reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can you be assured that business or regulatory data remains private and secure, and that your organization is protected from damaging data breaches—and feel you can still completely satisfy the full range of reporting, compliance, and regulatory requirements? This white paper describes:

* Cloud Computing Security Challenges

* Techniques for Protecting Data in the Cloud

* Strategies for Secure Transition to the Cloud

Enterprises increasingly recognize cloud computing's compelling economic and operational benefits.

Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerates deployment of new applications. However, those valuable business benefits cannot be unlocked without addressing new data security challenges posed by cloud computing. Deploying confidential information and critical IT resources in the cloud raises concerns about vulnerability to attack, especially because of the anonymous, multi-tenant nature of cloud computing. Applications and storage volumes often reside next to potentially hostile virtual environments, leaving information at risk to theft, unauthorized exposure or malicious manipulation. Moreover, it's possible for remnant data to persist when consumers vacate cloud volumes but vendors do not recycle storage devices securely. Governmental regulation of data privacy and location presents the additional concern of significant legal and financial consequences if data confidentiality is breached, or if cloud providers inadvertently move regulated data across national borders.

As a global leader in content security, Trend Micro has pioneered Secure Cloud – a next-generation advancement that enables enterprises and other organizations to operate safely and securely in the cloud. Secure Cloud represents a patented security infrastructure specifically engineered to control the security and privacy of data deployed to any cloud computing environment.

CLOUD COMPUTING DEFINED

Cloud computing is the latest extension of an evolution in distributed computing that takes advantage of technology advances. The cloud's roots date back to early mainframe processing, when users connected to a shared computing resource through terminals to solve their computing needs. The advent of faster and cheaper microprocessors, RAM and storage brought computing into the client-server model, which grouped sets of users into networks sharing computing power on decentralized commodity servers. As bandwidth became more ubiquitous, speedier, and less costly, these networks interconnected to form the Internet. IT departments typically provisioned their datacenters in house, protected inside a firewall. Eventually, enterprises took advantage of higher throughputs to reexamine the need for monolithic onsite data centers.

Accessing servers virtually through a browser window presented substantial advantages in software and hardware maintenance. Software vendors began capitalizing on the concept that a scaled datacenter could also deliver remote content to customers almost immediately at a reduced cost, giving rise to on-demand Software-as-as-Service. Today's mature virtualization platforms now enable contemporary cloud computing: a new model of rapid, on-demand, low-cost, al-a-carte computing Like its predecessors, present-day cloud computing features a multitude of users connected to remote computing resources over the Internet. Cloud computing delivers software and services over networked connections, relying on a steady flow of throughput to and from the virtualized datacenter in order to maintain high service levels. Thanks to scalable virtualization technology, cloud computing gives users access to a set of pooled computing resources that share the following attributes:

- Multi-tenancy
- Highly scalable and elastic
- Self-provisioned
- Pay-per-use price model

In contrast to the significant capital expenditures it takes to purchase and provision the launch of a traditional in- house operational site, as well as the months of lead time that effort involves, cloud computing lets administrators spin up virtual servers at will. They can provision necessary storage and launch an operational site within minutes or hours and for a fraction of historical costs.

OVERVIEW OF CLOUD ARCHITECTURE:

We provide an architectural view of the security issues to be addressed in cloud computing environment for providing security for the customer. We have defined four layers based on cloud computing services. The cloud computing categorization based on services as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). This section elaborates the four layers shown in figure 1 and mapping the different security issues in each layer. Some of the important components of User layer are Cloud Applications, Programming, Tools and Environments. Some of the popular examples for these applications are B2B, Facebook, My Space, Enterprise, ISV, CDNs, Web 2.0 Interfaces, Aneka, Map Reduce, Dryad, Workflows and libraries. Some of the security issues related to the user layer are Security as a Service, Browser security, and Authentication are elaborated in the next sections.

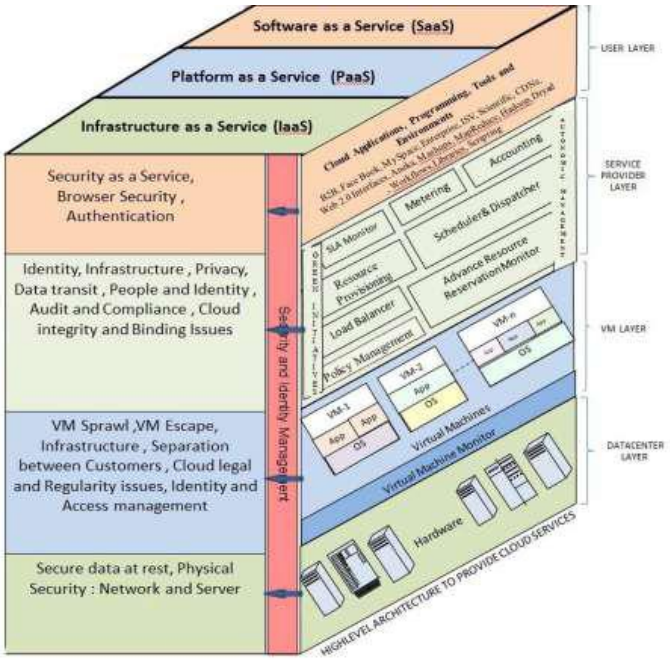

Figure 1: Security Architecture of Cloud Computing

THERE ARE FOUR MAIN TYPES OF CLOUD:

Private cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud - The cloud 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 premise or off premise.

Public cloud - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud - The cloud 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).

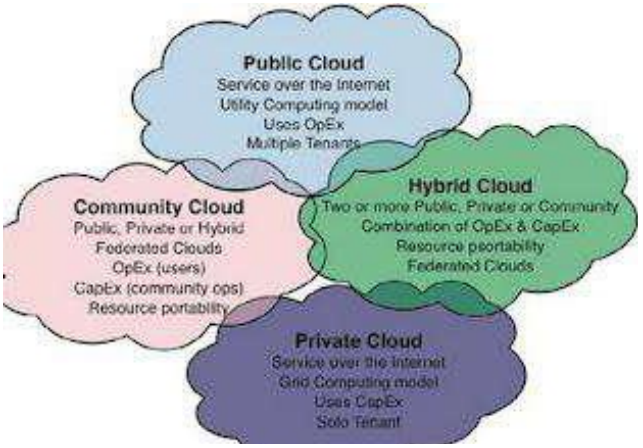

Figure 2: Deployment models operated by Cloud Computing

CLOUD COMPUTING SECURITY CHALLENGES

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2012 Computerworld "Cloud Computing" study, which measured cloud computing trends among technology decision makers. When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data. Derek Tumulak, vice president of product management at Vormetric, explains, "Everyone wants to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play. In traditional datacenters, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves. In the private and public cloud, however, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers.

There are complex data security challenges in the cloud:

DATA MOBILITY AND CONTROL

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or

replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries. Further, legislation such as the US Patriot Act allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners' consent.

DATA REMANENCE

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

DATA PRIVACY

The public nature of cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

* The need to protect confidential business, government, or regulatory data
* Cloud service models with multiple tenants sharing the same infrastructure
* Lack of standards about how cloud service providers securely recycle disk space and erase existing data
* Auditing, reporting, and compliance concerns
* Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
* A new type of insider who does not even work for your company, but may have control and visibility into your data

Such issues give rise to tremendous anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud, and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data. There's also ongoing concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another cloud service provider.

Specific security challenges pertain to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

- SaaS --- Deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.
- **PaaS** --- Is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.
- Iaas---lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the

consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.

SECURITY ASPECTS HAVE TO BE PROTECTION

A user's information and access rights must be protected against abuse by unauthorized users and intruders. Due to the fact that information and applications are based in the cloud, security measures such as door locks or uniformed security personnel no longer work. The storage, transmission, and use of information must be digitally protected. This can be done using technologies such as PGP, SSL, FTPS, and HTTPS. However, cloud providers choose to go further. Most supplement the existing security measures with specific measures to dispel the cloud user's fears and un-familiarity with cloud data centers. Data in cloud environments must be protected to an even greater extent than in your own operating environment.

Privacy---Privacy measures protect personal information in such a way that others cannot access it. Various identity and access management systems support cloud services with a wide range of privacy and security measures. These include low security level with password-based authentication, to high security level with attribute-based authentication systems. The latter systems use state-of-the-art privacy-supporting certificates. Efficient process organization is also important in the event that the authorities raise any questions. For example, what does the provider do if a public prosecutor asks for data? How can the government demonstrate to its citizens and businesses that the provisions of the relevant laws will be up held .

Recoverability---Data stored in the cloud is subjected to regular integrity tests to guarantee its recoverability. Most cloud service providers replicate data three of four times instead of making real backups. This means they can recover from disk crashes and major disasters. However, most service providers do not guarantee the backup and recovery of data which is "accidentally" deleted by the end-users themselves. A government body must therefore make or arrange its own backups, for example by taking snapshots and downloading and storing these on its own premises or with another cloud provider.

Access and reliability - Access to information and the processing of data items must comply with the privileges granted to the user requesting access. Unauthorized access must be prevented. Every user claiming a unique identity when gaining access to data will be subject to a process to investigate whether he is indeed the authentic owner of the claimed identity. After verification, the user may only carry out those actions for which he has been granted permission. Cloud providers have set up facilities for this. There are even providers who offer the possibility, for example, of linking such facilities to an active directory of their customers. An active directory of this kind establishes the authenticity and access rights.

Connectivity - Managing the process of access to cloud services through identity authentication and authorization is critical, but there are also other steps once connected to the network. Extract net-work security may be needed beyond SSL, TLS secure messaging and data transport layers to ensure the actual security of this network.

ACCOUNTABILITY AND CONTROLLABILITY

A full log must be maintained for accountability in respect of data operations. This must record all actions carried out within a user session to allow controllability. What precisely has to be logged must be agreed within your organization. This is technically feasible, but (comparable to the storage and logging of telecom data) can be very expensive. Most cloud providers offer logging and monitoring tools, although some are rather rudimentary. Market participants are responding to this by offering additional logging and monitoring tools.

Integrity and irrefutability- Cloud providers must ensure that the integrity of data is protected and that it cannot be modified, duplicated or deleted without authorization, just as in the client's own ICT organization. The long-term irrefutability of digitally signed data is an important aspect of PKI-related standards in clouds. Cloud providers use various mechanisms among themselves to deal with routine events. These could include the expiry of a public-key certificate and the expiry of a time-dependent trusted-authority certificate.

Compliance with regulations – Legal, regulatory, and contractual requirements must be defined for all parts of the information system. Monitoring activities must be planned and laid down in advance in joint consultation between the parties concerned. It is also necessary to conduct regular independent reviews and assessments. Cloud providers must comply with all internal and external regulations,

laws, contracts, policy and mandatory standards. Many public cloud providers use the compliance and legislative frameworks of the country in which the respective cloud data center is located.

Insurable - The risks relating to the system must be controlled. Few parties other than the cloud service providers themselves currently offer such financial insurance for cloud services.

Migratable and up gradable - A migration path must exist that is feasible, controllable, and acceptable to users in order to move from an old to a new cloud provider or to a subsequent version. The cloud infrastructure must be easily up gradable to new releases of hardware and software. This may pose a problem for the use of some business functionality, as some business functions are currently available from only one cloud provider.

SOLVING THE CLOUD SECURITY CHALLENGE:

TREND MICRO SECURE CLOUD--Secure Cloud alleviates data security and privacy risks associated with deploying information into any cloud computing environment. Secure Cloud's patented key-management technology combined with industry standard encryption allows businesses to control access to sensitive data stores and operate safely in public, private and hybrid clouds.

EASY DEPLOYMENT - With a simple agent installed on the virtual machine image, Secure Cloud is able to ensure that data in the cloud environment is tamper proof, protected through encryption at the kernel level. Communication between the agent and Secure Cloud management server is secure, thus avoiding the risk of any man-in the- middle attacks to gain access to the encryption keys.

SECURE KEY MANAGEMENT - With Secure Cloud, cloud consumers have exclusive control of the encryption keys, and therefore control of their own data. The encryption key management is not hosted by the cloud service provider, but rather by Trend Micro or by the cloud consumers themselves. This provides the cloud consumers the ability to take advantage of the cloud services, but still maintain full control of the encryption keys within their environments. Secure Cloud uses VM-level encryption, which provides the ability to encrypt data in the working storage, while using different keys for each cloud consumer's information. This feature mitigates the risk of compromise between cloud consumers if one were to obtain recycled disk blocks from another cloud consumer or fall victim to a configuration error that would otherwise compromise data privacy.

INDUSTRY STANDARD ENCRYPTION

Secure Cloud uses industry standard AES encryption to make data unreadable and unusable to those without the encryption key. Rendering the data useless greatly reduces the risks associated with data theft, exposure to unauthorized parties or data seizure through judicial subpoena. Secure Cloud's ability to encrypt data adds additional benefits to the cloud consumer when changing vendors or terminating storage agreements. Any encrypted data remaining on vendor storage devices is unrecognizable and secure.

GRANULAR CONTROL - Secure Cloud's unique policy-based approach to key management and data access allows users to determine exactly which server gets access to secure data. Virtual servers spinning up in the cloud consumer's environment must first authenticate to the Secure Cloud key server with credentials that have been encrypted in the virtual machine's kernel. Based on the defined policies, information provided back to the key management server is then vetted, ensuring the cloud environment is safe to release the keys into. Along with detailed key management policies, Secure Cloud offers role-based access to the administrators, with specific permission levels ranging from full access, key approval, to audit logging only.

CUSTODY OF ENCRYPTION KEYS - Secure Cloud helps users control data access with the option of isolating the physical storage of keys away from the cloud infrastructure provider. This stops infrastructure administrators from accessing data or keys and gives customers the freedom to move data from one provider to another without the fear of vendor lock in. Secure Cloud's on-premise solution gives customers even more control by keeping keys within their trusted environment and controlling custody at all times. Further, if a regulatory agency presents vendors with subpoenas and seizes data without informing or getting consent from data owners, the encrypted volumes remain useless without the encryption keys.

REPORTING - Secure cloud accommodates the frequent need to view system configuration settings by providing a full audit trail of key approvals occurring on the management server. Secure cloud also offers detailed logging and reporting for any actions performed within the system and any key approvals. All events and changes, whether they come from an administrator or the system itself, are logged and can be called upon for a full detailed audit trail.

For Protecting Data in the Cloud - Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not

provide sufficient protection against APTs, privileged users, or other insidious types of security attacks. Many enterprises use database audit and protection (DAP) and Security Information and Event Management (SIEM) solutions to gather together information about what is happening. But monitoring and event correlation alone do not translate into data security.

"It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities:

* Data lockdown

* Access policies

* Security intelligence

First, make sure that data is not readable and that the solution offers strong key management. Second, implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information. Third, incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when us.

CONCLUSION:

Cloud computing in its various forms - Cloud computing is an important trend in the field of information provision and related ICT. It turns com-puter processing power and data storage into a utility for collective use, as has long been the case of gas, water, and electricity. The rise of cloud computing has been particularly strong, is set to continue, and is irreversible. In view of the advantages for government organizations, cloud computing should also be trusted and supported within the public sector, both at central and local government levels and within executive agencies are performing actions outside of the norm.

Trend Micro Secure Cloud empowers businesses to operate securely in the cloud through the use of encryption and patented key management that protects and manages data in virtualized environments. By giving enterprises control over how and where data is accessed, it allows them the flexibility to move between cloud vendors without being tied to any one provider's encryption system. Secure Cloud defends information against manipulation or theft, helps ensure compliance with encryption requirements and automatically facilitates the delegation of encryption keys. Delivered as an on-premise console or a Software-as-a-Service, Secure Cloud represents a complete solution for safeguarding information in private clouds and public Infrastructure-as-a-Service environments.

REFERENCES:

Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, pp. 108-114. doi:10.1016/j.istr.2011.08.006

Abdul Ghafoor, Sead Muftic (2010). "*Crypto NET: Security Management Protocols*", published in the Proceeding of the 9th WSEAS International Conference on Data Networks, Communication, Computers (DNCOCO! 2010), Faro, Portugal, pp. 15-20.

Abdul Ghafoor, Sead Muftic "*Crypto NET: Software Protection and Secure Execution Environment*", published in the International Journal of Computer Science and Network Security (IJCSNS), pp. 19!26, Vol. 10, February, 2010.

Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), pp. 257-259.

Arshad, J, Townsend, P. and Xu, J. (2013). A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009

Atayero, A. A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), pp. 546-552.

Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), pp. 30-45. doi:10.5121/ijnsa.2011.3103

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, pp. 599–616.

Chen, Y., Paxson, V., & Katz, R.H. (2010). What's New About Cloud Computing Security?

Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, 2010. Available Online at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html (Accessed on: November 29, 2012).

Chor, B., Kushilevitz, E., Goldreich, O., & Sudan, M. (1998). Private Information Retrieval. *Journal of ACM* (*JACM*), Vol 45, No 9, pp. 965-981, November 1998.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In *Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09)*, Chicago, Illinois, USA, November, 2009, pp 85-90, ACM Press, New York, USA.

Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009. Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessed on: November 29, 2012).

Cloud Security Alliance. Home page URL: https://cloudsecurityalliance.org.

Muftic, S., Zhang, F., DeZoysa, K. (2009) "*SAFE System: Secure Applications for Financial Environments using Mobile Phones*", Proceedings of the IADIS International Conference e–Society, Barcelona, Spain.

Zhang, F., Muftic, S., Schmölzer, G., "*Secure Service-Oriented Architecture for Mobile Transactions*".

Corresponding Author

Prof. (Dr.) S.S. Sarangdevot*

Vice Chancellor, Janardan Rain Agar Rajasthan Vidyapeeth, University, Udaipur, Rajasthan, India

E-Mail – prof.sarangdevot@gmail.com