Research Challenges for Adoption of Cloud Environment

Nitin Nagar

Assistant Professor, IIPS, DAVV, Indore

Abstract: ***Cloud computing is one of the important research aspects of distributed computing in the emergence of information technology. Cloud computing refers to services, applications, and data storage delivered online through powerful file servers. Deployment of cloud computing depends on whether the cloud is a private, community, public, or hybrid one. Private clouds are operated for a particular organization, whereas community clouds are mutual by a number of organizations. Public clouds are available to the common public or large groups of Industries, while hybrid clouds combine public and private elements in the same data center. The proposed work focuses on a solution to the threats that are the major issues in the cloud adoption.***

Keywords: VM, Cloud Computing, Kerbores, Authentication, Authorization, Security

1. Introduction

Cloud computing is divided into several categories such as outage (availability), security, performance, compliance, private cloud, public cloud, hybrid cloud, integration and environment is an on premises cloud [7][8]. Cloud securities issues have recently gain lots of attention from research community, with much of the focus on securing the OS and VM on which the services are deployed [5]. The data centric view of security provides a way to secure data sharing between applications hosted in the cloud. There is a file system that provides a secure file storage service for Web 2.0 applications. Currently each web application stores its own user data, which is not only burdens the applications with storing, managing, and securing user data but also dispossess users from controlling their own data [6]. For improvement in security, analyst have their different view as privacy is an important issues in cloud computing in terms of user trust and need to be consider at every phase of design [2]. Sometime it happens that without awareness of company's detail user record their data; companies may send user's sensitive information to other companies for economical reason, from transformation of data cyber criminal may steal the user email and bank's detail etc. The awareness is also increases for the need of design privacy from both companies and government organization [3].

Authentication may the required user name or password or any of the authentication techniques include hardware token, software token, digital certificates on smart cards and USB tokens, out-of-band authentication and biometric [1]. It is observed that everyday new security advisors are published [4] [5]. Thus, a secure architecture to avoid abuse and nefarious use of cloud computing which will cover the designing of a framework to secure insecure interfaces and API, accounting on service hijacking and malicious insider. Cloud computing is the recent research area in the field of distributed computing. The rest of the literature review is organized as follows. The section 2 presents literature survey on various cloud computing aspects and its related issues. In section 3, we state our research challenges for improvement of cloud computing application. Finally, the references of all the literature review.

2. Literature Review

B. et al. explores cloud computing security issues and highlights the key research challenges that include such as availability and performance, malicious insiders, outside attacks and service disruptions [10]. M. et al identifies that the major issues pertaining to data security in the cloud computing environment are data location and data transmission, data availability and data security [9]. P. et al. indicate security issues of cloud computing systems by highlighted the problems of cloud computing, particularly, the security management models based on security standards and the security issues pertaining to security standards such as the information technology infrastructure library (ITIL) and open virtualization format (OVF). The service providers can follow these guidelines to secure their cloud services. It is imperative to address the security issues aptly, as otherwise they could possibly result in unauthorized access to the systems that ultimately lead towards potential data corruption and compromising the confidential data [11].

C.et al. discusses cloud computing data security and data privacy protection issues. The security architecture is defined at three levels: software security (identity authentication, identity management, and access control), platform security (framework security, component security and interface security) and infrastructure security (virtual environment security, shared storage security). Data privacy protection issues of the data lifecycle in cloud computing include transfer, use, share, storage, archival and demolition [12]. S.et al. highlights the major problems in large-scale acceptance of cloud computing, mostly due to service security and privacy issues. Based on the discussed scenarios, it is recommended that sensitive information should be minimized when data is processed on cloud and privacy to the end-user must be assured. A client based generic privacy manager tool has been proposed for this purpose that not only reduces security issues but also provides added privacy features [13].

H. et al. highlights the regulatory and legal concerns associated with security issues. To avoid unauthorized access and to ensure data integrity, confidentiality and availability, the storage provider should offer encryption schema, strict access control mechanism and scheduled data backups. Adoption of a universal standard is also recommended to ensure interoperability among service providers [14]. Shen et al. analyses the security component of the trusted cloud computing systems through role-based access control model. It is stressed that the trusted cloud not only comprises of data security elements but also entails availability, reliability, integrity and safety. Security aspects have further been described as data confidentiality, the trust among the participant and dynamically building trust domains. For this purpose, a software middleware has been designed named as the Trusted Platform Software Stack (TSS) which makes use of security functions of Trusted Platform Model (TPM). TSS has two layers namely, the TSS service provider (TSP) and TSS core services (TCS). Application calls TSP function which sends a call to TCS and in response, TCS authenticates the request in TPM order and returns the results to the upper layer. The proposed middleware provides hardware level authentication with the help of TPM, which makes the solution more secure from unauthorized access [15].

G. et al. identified the potential hurdles for cloud usage as the lack of consumer trust and complexity of compliance to make the cloud trustworthy. They ascertain the components of trust as security, privacy, accountability and auditability. To achieve the trust components in the cloud, the system controls are identified as preventive, detective and corrective. Further, a model is proposed to achieve trust in the cloud by applying preventive control on data requests. If the request is faulty, as ascertained through detective control, then the model makes a vulnerability log and generates the report accordingly; and if the request is not faulty then it is forwarded to service provider through the corrective control. Response is also validated through this model. However, the proposed model is not capable to support security and privacy components of trust [16].

3. Research Challenges

The research challenges of the literature reviewed on cloud computing security issues are provided as follows.

- Cloud computing emphasizes on various service oriented architectures with the help of tools, which reduces the infrastructure cost of users. There are varying range of cloud tools and technology such as Eucalyptus, OpenNebula, Nimbus and OpenStack etc. The comparative study of different cloud tools and technology on the basis of certain cloud parameters for the deployment of clouds [28].
- Investigation of major and various adoption issues of cloud computing. Different security aspects in cloud computing are discussed that can serve as a quick reference guide [9].
- The cloud security challenges like availability of data, performance, malicious insiders, outside attacks and service disruptions. Security strategy model is proposed to overcome the challenges. The same security model is equally implementable for complex and dynamic cloud infrastructure [10].
- Data protection and data privacy issues are the biggest challenges in the cloud computing. Data security and protection issues covers all the data lifecycle components i.e., transfer, use, share, storage, archival and destruction of data [11].
- The unavailability of good secure framework is always a biggest concern in the area of cloud computing. A security framework is designed comprising multiple components that include services integrator, security management, service management and trust management. However, proposed framework is only for the consumption of service providers **[**20].
- Trust management systems are always useful for the computing environment. Standard trust management system is evaluated and proposed solution is only meant for service users to identify trustworthy service providers [21].
- In a cloud computing environment client based privacy manager tool must require. The privacy manager tool for user has been proposed that not only reduces security issues but also provides added privacy features. However, the proposed tool is not generic and is limited to specific scenarios [13].

4. Conclusion

Authentication and authorization are the two major concern of cloud computing. Various worked had already done in this area. Kerberos is model for securing authentication service in a network. Kerberos model is having no provision of host security. Each network service which requires a different host name will need its own set of Kerberos keys. It creates complication in virtual hosting and clusters. Kerberos model is running with a strict time requirements, which means the clocks of the involved in hosts must be synchronized within configured limits [29] [30]. In our research review we found that Kerberos and LDAP together make for a great combination in cloud computing environment. Kerberos is used to manage credential securely (authentication) while LDAP is used for hold authoritative information about the account such as what they are allowed to access (authorization) (current proposed work) [33].

References

[1] Entire Deniz Sarier, “A new approach for Biometric Templates storage and Remote Authentication”, *ICB’09:Proceeding of the 3rd International workshop on Advances in Biometrics*, Volume 5558/2009, June 2009, pp 909-918.

[2] Harold C. Lim et al, “Automated Control in Cloud Computing: Challenges and Opportunities”, *ACDC’09*, June 19, 2009, Barcelona, Spain, pp 13-18.

[3] Siani Pearson, “Taking Account of privacy when designing Cloud Computing”, *Cloud 09*, May 23, 2009, pp.44-52.

[4] D. Kesavaroja, R.Balasubramaniam et al, “Implementation of Cloud Data Server (CDS) for providing secure services in E-Business”, *IJDMS*, 2005, pp. 18-21.

[5] Wenchao Zhou et al., “Toward-a Data Centric View of Security”, *CloudDB 2010*, October 30, 2010, Ontario, Canada, pp. 25-32.

[6] Francis Hsu and Hao Chen, “Secure File System Services for Web 2.0 Application”, *CCSW’09*,

November 13, 2009, Chicago, Illinois, USA, pp. 11-17.

[7] John Foley, Private Cloud Take Shape, *Information Week Analysis*, Aug 9, 2009.

[8] Alan Radding, Private Cloud on Horizon, *Information Week Analysis*, April 13, 2009.

[9] M. et al., "Data Location and Security Issues in Cloud Computing", *IEEE International Conference on Emerging intelligent Data and Web Technologies*, 2011.

[10] B. et al., "Emerging Security Challenges in Cloud Computing", *IEEE international Conference Information and Communication Technologies (WICT)*, 2011.

[11] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", *IEEE International conference on Computer Science and Electronics Engineering*, 2012.

[12] P.et al., Cloud Computing security issues and challenges, *MIPRO, Proceedings of the 33rd International Convention*, 2010.

[13] S. et al., "Security Threats in Cloud Computing", *6th international Conference on Internet Technologies and Secure Transactions*, 2011.

[14] J. Harauz et al., "Data Security in the World of Cloud Computing Security & Privacy", *IEEE* 7 (4), pp 61-64.

[15] Z. Shen et al., "Cloud Computing System based on Trusted Computing Platform", *International Conference on Intelligent Computation technology and Automation*, 2010.

[16] K.G.Kumar et al., "To Achieve Trust in the Cloud", *Second International Conference on Advanced Computing & Communication Technologies*, 2012.

[17] B. Zou and H. Zhang, "Toward Enhancing Trust in Cloud Computing Environment", *2nd International Conference on Control, Instrumentation and Automation*, 2011.

[18] K. M. Khan et al., "Establishing Trust in Cloud Computing", *Cloud Computing*, pp. 20-27, 2010.

[19] W. Li, L. Ping and X. Pan, "Use Trust management module to achieve effective security mechanisms in cloud environment", *International Conference on Electronics and Information Engineering*, 2010.

[20] H. Takabi, D Joshi and G. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environment", *34th Annual IEEE Computer Software and Applications Conference Workshops*, 2010.

[21] S. M. Habib, et al., "Towards Trust Management System for Cloud Computing", *IEEE Computer Society*, Washington DC, USA, 2011.

[22] H. Sato et al., "A Cloud Trust Model in a Security Aware Cloud", *10th Annual International Symposium on Applications and the Internet*, 2010.

[23] S. Nivetha et al.,"Assessing the Risks and Opportunities of Cloud Computing - Defining Identity Management Systems and Maturity Models", in *International Conference on Computing and Control Engineering*, 2012.

[24] B. Clifford et al., "Kerberos: An Authentication Service for Computer Networks", *IEEE Communications*, September 1994.

[25] John T. et al., "The Evolution of the Kerberos Authentication System", *Distributed open systems. IEEE Computer Society Press*, Washington, pp. 78–94, 1994.

[26] Revar, A.G.; Bhavsar, M.D., "Securing User Authentication using Single Sign-on in Cloud Computing", *Engineering (NUiCONE), 2011 Nirma University International Conference on* , vol., no., pp.1-4, 8-10 Dec. 2011.

[27] C. Leckie, K. Ramamohanarao T. Peng, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", *ACM Computer Survey, 39 (1) (2007), p. 3.*

[28] Nitin Nagar and Ugrasen Suman, "Architectural Comparison and Implementation of Cloud Tools and Technologies," in *4th International Conference on Electronics Computer Technology (ICECT 2012)*, KanyaKumari,INDIA, 2012, pp. 581-585