DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4350

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

STUDY ON SECURITY MODEL IN CLOUD COMPUTING

R.K.Bunkar
Research Scholar, MGCGV Chitrakoot,
Satna, M.P., India.

Dr.P.K.Rai
Department of Computer Application, APS University,
Rewa, M.P., India.

Abstract: Cloud computing is new and latest trend in Information Technology for dynamic provisioning of IT capabilities. Cloud services require addressing the security during the transmission of sensitive data and critical applications to shared public cloud environments. In cloud computing there is no standard security model and framework. According to the study of various cloud security models as CSA model, Jerico forum's model, NIST Cloud Reference architecture, cloud multi-tenancy model, and NIST formal model, we have proposed a new cloud security model which has authentication through verification and validation, security components such as OTP, 2FA, and security policies- through guidelines, procedures and security controls- through privilege control.

Keywords: Security services; Security model; Verification and validation; Security Policies; Privilege Control; Data Protection; Data Security Services; Threats/Attacks detections;

INTRODUCTION

Cloud services permit individuals and industry to utilize software and hardware that are managed by third parties at remote location. According to NIST, Cloud computing representation promote ease of use and is collection of five important features three service models as IaaS, PaaS, SaaS; and four release models private cloud, community cloud, public cloud and hybrid cloud. In virtualization, by extrication the coherent from into the physical, resolves some of the challenges faced by grid computing [12]. Virtualization enables to the sharing of computing resource as processor, memory, storage space, and input/output amongst dissimilar clients and improves the utilization of cloud property [18]. The various industry standard development organizations who have contributed to the standardization of cloud computing industry includes National Institute of Standards and Technology, The Open Group, Open Cloud Consortium, and Open Grid Forum. Security is very essential at different levels to manage and realization of cloud such as: physical security, OS security, network level security, virtual machine security, application security, and information level security. Security model of cloud computing represent a basic, advanced architecture and is intended to make possible the thoughtful of the requirements, uses, characteristics and standards of cloud computing. Security on demand for cloud computing. The presented framework for threats model for virtual machine in cloud computing, which forms the basis for understanding and analysing cloud security from the customer's perspective. The model builds a detailed mapping of various hardware and software safety architecture's property to cloud security features anticipated by customers [9]. Security is the major obstacle of the extensive dreamed visualization of cloud computing. The advancement of cloud computing upward many user, protection, and separation are continuously increasing to protect private and sensitive information which are possessed in data centres, the cloud user needs to verify the real exists of the cloud computing atmosphere in the world, the protection of information in the cloud. In cloud computing atmosphere security analysis and evaluation of privacy, security and trust issues by a quantifiable approach are the prime concerns of security.

CLOUD COMPUTING SECURITY SERVICES

The cloud computing services leverage the equipment which uses the internet and essential inaccessible server to maintain records and application. It allows to customers and business to using applications without installing them and accesses their

Personal files at any computer with help of internet access [19]. The categories of cloud computing security services are shown in the Fig.1.

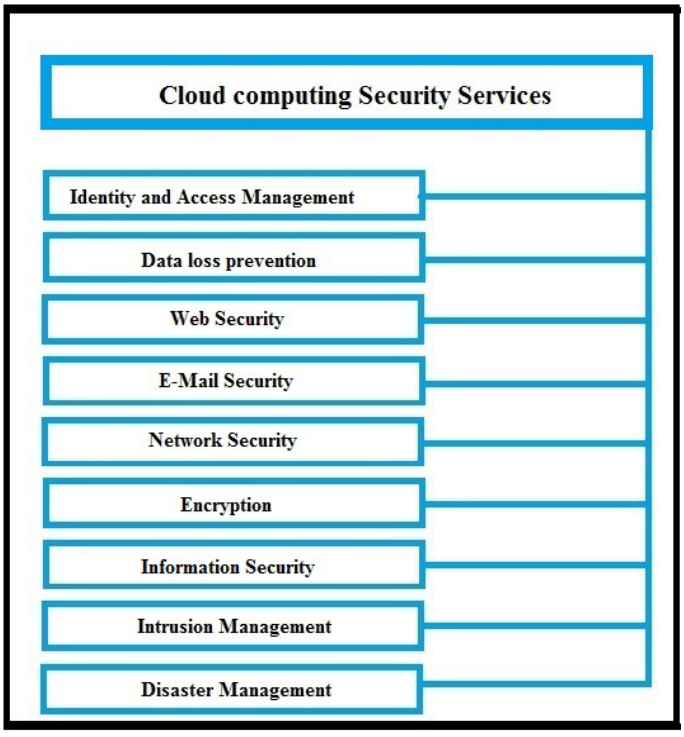

Fig 1: Cloud security services [19]

***Identity and Access Management*:** Cloud provider provide with control for secured management of identities and access. It includes nation, process and systems used for supervision access to enterprise resources. It is managed to make sure that the identity of the consumer is verified and the access rights are provided at the correct level.
***Data loss prevention*:** This service suggests protection of data by pre-installed data loss prevention software along with set of rules deployed.
***Web Security*:** Web security provides an additional protection against malware from entering the enterprise through web browsing and other activities.
Cloud service provided either by installing software or an appliance through the cloud by redirecting web traffic over to the cloud provider.
***E-Mail Security*:** It manage over the in-bound and out-bound e-mail to defend our organization from malicious attachments and phishing. This service helps to implement commercial policies such as satisfactory use, spam and providing business stability options.
***Network Security*:** The network security provide deal with security control which in a cloud environment is generally provided through virtual devices.
***Encryption*:** In encryption there are distinctive algorithms that are computationally difficult or almost impracticable to break.
***Information Security*:** Our system gathers information related to log and events. This information is used in correlating and analysing, to provide with real time reporting and alerts on events that require investigation.
Intrusion Management: It is the process which uses pattern recognition for exposure and response to procedures which statically unusual and unexpected. It may also require reconfiguration of our system components in real time so as to prevent an intrusion.
***Disaster Management*:** This cloud service helps in continuing our business and managing disasters by providing elasticity and consistent fail-over for services which are required in casing of service interruptions.

RELATED WORK

The cloud security alliance support the utilization of most excellent practice to enable security assurance in the field of cloud computing. This alliance considers itself to be a standards incubator rather than standards developing organization, having published the security related best practices, and guide [4]. Jerico forum's cloud model [10] is a figuration explanation of security aspect information indirect in the overhaul and deployment models of clouds computing and the location, manager and owner of computing resources [11]. Considerate the interaction and dependencies among cloud computing models is critical to identify with cloud computing protection risks.

IaaS is the basis of all cloud services, with PaaS building upon IaaS, and SaaS in circle structure upon PaaS as described in the cloud computing reference model. An organization's security carriage is characterized by the maturity, usefulness, and fullness of the risk-adjusted security controls implement. Cloud security controls are implemented in many layers from the facilities (physical security), to the network infrastructure (network security), and the IT systems (system security), and all the way to the information and applications (application security). Multiple-tenancy model [3] is an important utility feature of cloud computing that allows various applications of cloud service providers at present running in a physical server to offer cloud service for customers.

Virtualization possesses capabilities of distribution and separation of computing resources, and is a core machinery of cloud computing by running various virtual equipment [21] in a physical machine. The mapping model of cloud, security and observance of cloud ontology, security control and compliance check; presents a good method to explore the gap among cloud structural design and conformity framework and the corresponding security control strategies must be provided by cloud overhaul provider, consumers or third parties, the cloud model to the security control & compliance suggested by CSA [3].

For the security of cloud environment, we should firstly analyse the security, and then find out the gap surrounding substance to cloud structural design and its observance structure, and finally adopt some relevant security controls. The security reference architecture of NIST, formal model indicates that each of the architectural mechanism acknowledged in the NIST reference architecture be supposed to be protected by implementing the suitable SRA security components and associated NIST SP 800-53 [17]. Virtualization at all system level, storage level and network level became important method to get better system security, trustworthiness and ease of use, to reduce costs and provide greater flexibility. Shengmei *et.al* [16] has addressed the requirements and solutions for the security of virtualization in cloud computing situation.

PROPOSED SECURITY MODEL OF CLOUD COMPUTING

Based on the study of various security models we have to proposed a security model of cloud computing. The steps in the proposed security model are : first the user creates a local user agent, and establish a temporary security certificate, and then user's agent use this certificate for secure authentication in an effective period of time. With this certificate, which includes the host name, user name, user id, start time, end time and security attributes etc; the user's security access and authorization is completed. When the user's task is to use the resource on the cloud service provider, mutual authentication take place between user agent and specific application, while the application checks if the user agents certificate is expired, a local security policy is mapped. According to user's requirements, cloud application will generate a list of service resources and then pass it to the user agent. Through security API user agent connects specific cloud services. The proposed security model is given in Fig.2.

The model consists the following security components: (i) Verification and validation (ii) security policies (iii) privilege control (iv) data protection (v) data security services and (vi) threats/attacks detections.
Verification and Validation: This unit is required in cloud computing not only to authenticate users but also to ensure the accuracy of data and services on the cloud. The significance of security module is that cloud computing position is reachable by several customers and providers which want to use or provide many services and applications. Cloud service providers need to prove to the users that the services and data

are valid, for example, appropriate signature algorithms. Consequently, user will be able to verify the authenticity of facts and services made available to them through digital signature. This protection part can also provide work for techniques such as One Time Password [13] and 2FA [1] [22].

Security Policies: Security policies are the basis of a resonance safety completion. Frequently organizations implement technical security solutions without creating foundation of policies, standards and security policies on firewall.

Standards, procedures, and guidelines referred to as policy in the superior sense of a worldwide information security policy [14].

Privilege Control: This security component is necessary to control cloud usage by different individuals and organizations. It protects user's privacy and ensures data integrity and secrecy by applying an anthology of rules and policies. Cloud users are granted different levels of access permissions and resource ownerships based on their account type. Only authorized users can access the authorized parts of the encrypted data through identity-based decryption algorithm. For example, in a healthcare cloud, not all practitioners have the same privileges to access patient's data, this may depend on the degree to which a practitioner is involved/specialized in treatment; patients can also allow or deny sharing their information with other healthcare practitioners or hospitals [24]. Encryption/Decryption algorithms [23] such as AES [5] [7] and RC4 [6] can be employed by this component to achieve confidentiality of information [22].

Data Protection : Data stored in the cloud storage resources may be very sensitive and critical, for example, clouds may host electronic healthcare records (EHR) which contain patients' private information and their health history [15]. They may also store critical banking information (e.g., clients account numbers, balances and transactions) or national security information. Cloud security model must protect data loss or injure by provide safe storage servers. These servers should also secure data retrieval and removal from the cloud. Securing data storage and processing is important since cloud users have no idea about data location. Techniques for data protection for example truncation, redaction, obfuscation, and others are able to be used in this security component. Encryption techniques can also be employed for data security. Hash functions and Message Authentication Code (MAC) can be employed in this unit to provide data integrity [22].

Security Services: The additional factors that directly affect cloud software assurance include authentication, authorization, auditing, and accountability, are used in cloud security services [14]. Security-as-a- service is an industry form which a service contributor integrates security services into a commercial infrastructure on a subscription basis. Security-as-a-service has applications such as anti-virus software delivered over the internet however the term can in addition pass on to security administration provided in-house by an external organization [8].

Threats/Attacks Detections: Clouds are vulnerable to many attacks and malicious behaviors that threaten both data and physical and virtual computing resources of the cloud. Basically, any set of actions that threaten the cloud security requirements (e.g., integrity, confidentiality and availability) are considered to be attacks. Attacks detection and prevention components are installed within the cloud security system to protect cloud resources from various anomalies. For example, denial-of-service attacks should be reduced to the minimum to guarantee the maximum availability of business, governmental, health and other critical information and services. This can be achieved by deploying technologies that provide high availability such as dynamic server load balancing and active/deactivate clustering [20]. Standard Distributed Denial of Services (DDoS) mitigation techniques such as synchronous cookies and connection limiting can also be used.

There are provisions for the next generation of intrusion detection systems and firewalls in order to protect the resources from intruders, viruses and malware [2].

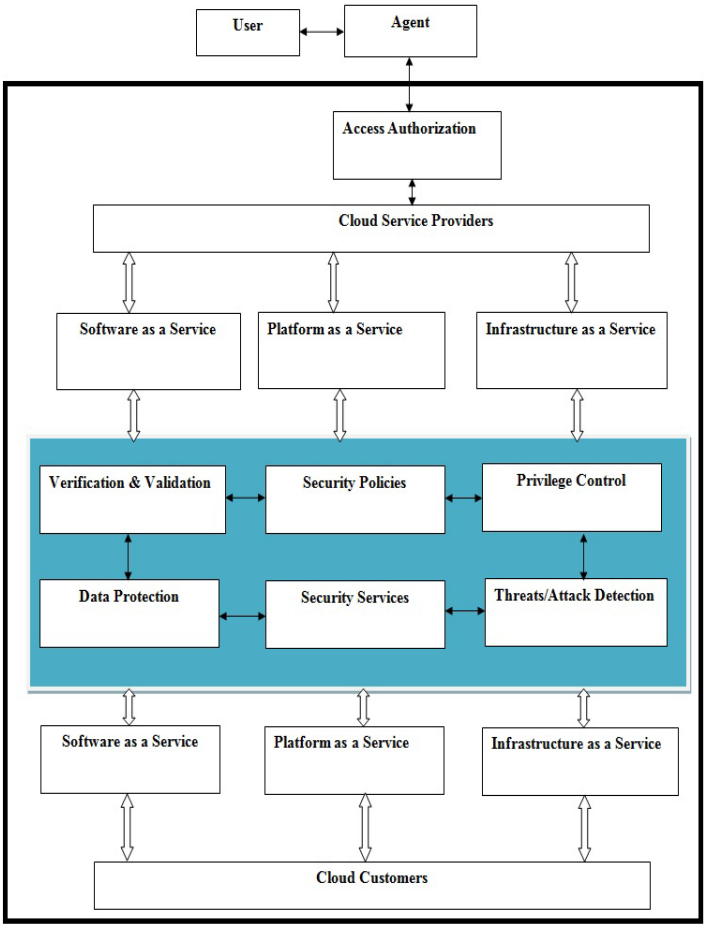

Fig. 2: Proposed Security Model of Cloud Computing

CONCLUSION AND FUTURE WORK

As discussed in the proposed model we have suggested authentication through verification and validation and we have used security components such as One Time Password (OTP), Two Factor Authentication (2FA), security policies- through standards, guidelines, and procedures, security controls- through privilege control. The proposed model protects user's privacy and ensures data integrity and confidentiality by applying a collection of rules and policies that control the authority to the cloud. Cloud security model protect data from loss or damage by providing secure storage servers, Security-as-a-Service (SECaaS), threats/attacks detections to control coming threats and attacks, involves applications such as anti-virus software delivered above the internet and pass on to security administration provided in-house by an external organization. Some prominent research

challenges are opportunities in the cloud computing are : open interoperation across (proprietary) CLOUD solutions at IaaS, PaaS and SaaS levels, managing multitenancy at large scale and heterogeneous environment, dynamic and faultless, elasticity from in house CLOUD to public CLOUDs for unusual (scale, complexity) and/or infrequent requirements, data management in a CLOUD environment and severe problems with trust, security and privacy (which has legal as well as technical aspects).

REFERENCES

[1]. Abraham Dave (2009) "Why 2FA in the cloud", Network Security, vol. 2009, issue 9, pp. 4-5.

[2]. Ahmed Mohiuddin et.al.(2012) "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, vol. 9, issue 1, No 1.

[3]. Cloud Security Alliance (2009) Security guidance for critical areas of focus in cloud computing (v2.1).

[4] Erl Thomas, Mahmood Zaigham, and Puttini Ricardo (2014) "Cloud Computing Concepts, Technology & Architecture, PEARSON, ISBN: 978-93325-3592-3.

[5]. Federal Information Processing Standards Publication (2001),"Specification for the Advanced Encryption Standards (AES)".

[6] Fluhrer S., Mantin I., and Shamir A.(2001) "Weakness in the Key scheduling algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK.

[7] http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html.

[8]. http://mti.com/managed-services/portfolio/security-as-a-service-secaas

[9]. Jamkhedkar Pramod et.al.(2013) "A Framework for Realizing Security on Demand in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science.

[10]. Jericho Formu. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. April, 2009 http://www.opengroup.org/jericho/ cloud_cube_model_v1.0.pdf.

[11]. Jianhua Che et.al.(2011) "Study on the security models and strategies of cloud computing", 2011 International Conference on Power Electronics and Engineering Application, Procedia Engineering 23 (2011) 586 – 593.

[12]. Jianhua Chea, Yamin Duanb, Tao Zhanga(201), "Study on the security models and strategies of cloud computing" Jie Fanaa 2011 International Conference on Power Electronics and Engineering Application.

[13]. Johnsson M. and Azam A.(2011) "Mobile One Time Passwords and RC4 Encryption for Cloud Computing", Technical report,IDE1108.

[14] Krutz L. Ronald et.al.(2013) "CLOUD SECURITY Comprehensive Guide to Secure Cloud Computing", Chapter 2 : Cloud Computing Architecture, WILEY-INDIA, ISBN : 978-81-265-2809-7.

[15] Leonard D.C. et.al.(2009) "Realization of Universal Patient Identifier for Electronic Records through Biometric Technology", IEEE Trans on Information Technology in Biomedicine, Vol. 13, No. 14.

[16]. Luo Shengmei et.al. (2011) "Virtualization security for cloud computing service", IEEE, International Conference on Cloud and Service Computing.

[17.] NIST Cloud Computing Security Reference Architecture (2012) NIST Special Publication 500-299,http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[18]. P.Vidya Durga et.al. (2015) "Security Models and Issues in Cloud Computing", International Journal of Advances in Engineering, 141 – 145, ISSN: 2394-9260 (printed version); ISSN: 2394-9279 (online version); url:http://www.ijae.in.

[19]. Pawan thakur and Roohi ali "Cloud computing", Satiya parmesan publication, ISBN: 81-7684-816-6.

[20]. Tripathi A. and Mishra A.(2011) "Cloud computing security considerations", IEEE International conference on signal processing, communication and computing (ICSPCC).

[21]. VMware Inc (2007) "Understanding full virtualization, Para-virtualization and hardware assist", Technical report.

[22]. Yourself E. Ahmed et.al.(2012) "A Framework for Secure Cloud Computing", IJCSI International Journal of Computer Science, Vol. 9, issue 4, No 3, ISSN (Online): 1694-0814, July 2012.

[23]. Yu Shucheng et.al.(2010) "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing".

[24]. Zhang Rui and Liu Ling (2010) "Security Models and Requirements for Healthcare Application Clouds", IEEE 3rd International Conference on Cloud Computing.