International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 279 – 282

Threats –Solutions in Cloud security

Ranjit Kumar[1],
[1] Department of Computer Science & Engineering,
Rayalaseema university,kurnool, Andhra Pradesh, India
ranjithphdd@gmail.com

L.Venkateswar Reddy[2]
[2] Department of Information and Technology
Sree vidyaniketan Engineering college,chittor, Andhra Pradesh, India
lakkireddy.v@gmail.com

Abstract: Distributed computing frameworks speak to a standout amongst the most complex processing frameworks as of now in presence. Current uses of Cloud include broad utilization of disseminated frameworks with shifting level of network and use. With a late concentrate on huge scale expansion of Cloud processing, personality administration in Cloud based frameworks is a basic issue for the maintainability of any Cloud-based administration. This zone has additionally gotten extensive consideration from the exploration group and also the IT business. Diverse calculations and methodology are utilized by the specialists. Still distributed computing security is in its center stage. A few IT organizations are concentrating on cloud security and cloud information security. This paper gives a thought regarding security dangers and arrangements.

Keywords: *Cloud computing, security, attacks, distributed computing*

*****

I. Introduction

Distributed computing develops this pattern through mechanization. As opposed to arranging with an IT association for assets on which to convey an application, a register cloud could be a self-administration recommendation wherever a MasterCard can purchase process cycles, and an online interface or API is utilized to make virtual machines and set up system connections between them. Instead of requiring a long haul contract for administrations with an IT association or an administration supplier, mists chip away at pay-by-use show wherever an application may exist to run business for various minutes orhours, or it will exist to supply administrations to clients on a long haul premise. It almost abandons expression that distributed computing amplifies the present pattern of making administrations accessible over the system. For all intents and purposes every undertaking has perceived the value of Web-based interfaces to their applications, regardless of whether they are inward applications that are made out there to the staff, accomplices, suppliers, experts. The estimation of basically based administration conveyance is that applications will be made out there wherever, and whenever. Though ventures are mindful of the adaptability to secure interchanges the quality Secure Socket Layer (SSL) encoding adjacent to durable confirmation, bootstrapping trust in an extremely distributed computing environment needs painstakingly considering the varieties between big business figuring and distributed computing. Once legitimately architected, web administration conveyance will offer the flexibleness and security required by endeavors of all sizes. Distributed computing and matrix figuring are versatile. Quantifiability is refined by utilizing load adjusting of utilization cases running on an individual premise on a spread of agent frameworks and associated through net administrations. Electronic hardware and system data measure is dispensed and dis-assigned on interest. The framework stockpiling ability will goes here and there relying on the measure of clients, examples, furthermore the amount of data exchanged at a given time. Both figuring assortments include multi-tenure, which implies that a great deal of clients will perform entirely unexpected assignments, getting to one or numerous application occurrences. Sharing assets among a larger than usual pool of clients helps with lessening foundation costs and top burden capacity. Cloud and lattice processing give administration level understandings (SLAs) for secure timeframe administration; the purchaser can get administration kudos for accepting data late. The Amazon S3 gives an online administrations interface to the capacity and recovery of data inside the cloud. Setting a most confines the amount of articles we will store in S3. We can store an item as one byte and as vast as 5 GB or perhaps numerous terabytes.

II. Threats and solutions

Security danger is one of the wellsprings of the specialized danger that clients perceive and in this way can be said as the danger of being not able fulfill the security prerequisites among clients amidst or in the wake of utilizing cloud administration [1]. Besides, since cloud server farms are putting away data on numerous organizations and people, it is likely that they are harmed by programmers and that insider's information spillage dependably exists. Indeed, cloud administration has numerous security dangers in cloud execution situations or in the earth helpless against strict detachment in nature. The security dangers of cloud

administration are more lethal than those of the general one in light of the fact that in the event that one's security has openings (data spillage including hacking), it may influence corporate intensity and the harm itself fatal. The utilization of cloud administration may contrarily influence the utilization and spread of cloud administration since it is more intentional than the other data administration situations. Specifically, all things considered a perceived danger is high in an Internet space, generally negative impacts have a tendency to be high [2,3]. Also, arrange based frameworks like cloud administration see specialized components as vital wellsprings of danger including security defenselessness not at all like alternate frameworks [4]. On the off chance that we expect that the level of client's acknowledgment of security danger in cloud administration is high, it might influence the utilization and spread of the framework. In spite of the universalized utilization of cloud administration, numerous clients have questions about the wellbeing in security of cloud administration and such an impression of security danger may lower client's expectation to utilize cloud benefit ceaselessly [5]. Hexin and Ahn utilized brand impact, equipment environment, administration content, straightforwardness, ease of use, and dependability as compelling components to the nonstop utilize goal of individual cloud administration clients in China and played out an investigation [6]. Jun, et al. led an investigation with an extended TAM model so as to recognize the effect on the ceaseless use goal of the distributed storage administration. Accordingly, an individual's imaginativeness, self-adequacy, practical attribute, and mental changing over expense affected the nonstop utilize aim of the distributed storage administration [7]. Seo examined with an extended TAM model to break down the effect on the cloud administration reception goal. Therefore, ease of use, social impact, effectiveness, and dependability affected appropriation goal [8]. Park inspected different significant issues brought about by distributed computing environment including security, distinguished the dangers to the distributed computing, and proposed inexact countermeasures to lessen the security hazard [9]. Distributed computing is bringing about impediments in light of the fact that different suppliers are giving clients benefit and putting away individual data, lastly creating security issues. New qualities showing up in distributed computing make the conventional security idea connected in the current Internet administration hard to be utilized and this highlights the need to modify the customary security idea proper for distributed computing. The studies on the security hazard variables of distributed computing are as per the following: Siani and Azzedine talked about that control over information lifecycle, accessibility and reinforcement, absence of institutionalization, multitenancy and review are the critical issues in managing distributed computing securities [10]. Advantaged client access, administrative consistence, information area, information isolation, recuperation, investigative backing, longterm practicality are the seven security-related issues proposed [11]. Almond included multi-occupancy, always creating hazard, unwinding of security, administration supplier levels, temporary worker access, fiascos, outside physical, outer intelligent, episodes, application bugs, information spillage as danger elements in distributed computing [12]. Zissis and Lekkas isolated programming as an administration (Sass) into four administration levels, stage as an administration (PaaS)/base as an administration (IaaS) into seven administration levels, and Physical Data focus into five variables [13]. Foster et al. break the danger components into advantaged client access, information isolation, protection, bug abuse and recuperation, responsibility [14], while Tarrant et al. break it into accessibility administration, access control, weakness administration, patch administration, design administration, episode reaction, framework utilize and get to checking [15]. There are several studies in the literature that have identified security threats in the cloud computing paradigm. Some such studies [16]–[23] ranging from 2009 to 2016 have been selected to get the gist of the security concerns. The study of [13] have tried to categories these issues on the basis of cloud service models (SaaS, PaaS and IaaS). Similarly [17] has classified the security concerns on the basis of technology (communication and architecture) and business issues (conceptual and legal aspects). Whereas the study of [18] has presented threats in various general dimension of cloud computing. The study of [19] presents the security issues to be handled in service level agreements. And also emphasize upon the security threats to be addressed at various access points such as Server, Internet and Database. In addition to maintaining Data Privacy and Program access Security.

As given investigation report in [23] Cloud Computing credits which are dangers to Cloud Computing. They are Confidentiality, Integrity, Availability, Security, Accountability, Usability, Reliability and Audit capacity. The records of the most undermine properties are in fig1. It demonstrates that Confidentiality 31% and Integrity 24% recorded most debilitate, while contrasting and ease of use, unwavering quality, responsibility and review capacity which recorded not exactly the 10%.

Fig 1: List of Compromised attributes [23]

Looking at the importance of cloud computing various organizations such as NIST has put forth the guidelines for adopting cloud computing. It has categorized cloud security issues into 9 categories [20]. Similarly another important organization European Union Agency for Network and Information Security (ENISA) provides insights to SMEs on issues related to network and information security risks before they adopt cloud computing [21]. Last but not least, Cloud Security Alliance (CSA)'s Top Threat Working Group has recently published 12 most treacherous cloud threats based on survey from industry experts [22]. As the Web services and SOA are integral parts of cloud orchestration, the security in this domain is of paramount importance. The open web application security project (OWASP) has been issuing ten most critical web application security risks since 2003. In its present release of 2013 it has consolidated the top 10 list from over 500,000 vulnerabilities across hundreds of organizations and thousands of applications [20]. The review of these studies shows the cloud computing security issues range from physical ICT resources, internet, web applications, and data access and privacy, data centers on one hand to virtualization and cloud architecture, cloud deployment and service models, and service level agreements on the other hand. In essence first category is more pertinent to the traditional ICT infrastructure and second category is more concerned with the Cloud Computing domain. There exits huge literature to deliberate and advocate the concept of security-as-a-service. But there are clear negative connotations to this idea that are very detrimental to the proliferation of the cloud computing. Firstly, it means that one has to pay directly for the security a major deterrent in time of scarce competitive resources. Secondly it implies the security is the luxury of effluents hurting the efforts to bridge the digital divide. Or the worst implications is that it sends the signal that without security-as-a- service subscription your resources are not safe, a very serious restraint for the potential adopters. The correct approach would be to integrate the security features in all of the cloud offerings SaaS, PaaS or IaaS. And various levels of it can be defined such as normal, High or critical.

Similarly security control APIs can be developed to enforce these levels. At the time of service subscription user must define the desired level based on the domain specific requirement. And during service configurations these can be enforced through the implementation of the various security control APIs. The cost of these endeavors can be first tried to be realized from the extra utilization of computing, storage and bandwidth or the increase in customer base. The other option, the less desirable, is through the direct billing on the subscription of these APIs. In either case security will remain the integrated concept in the cloud. Similarly the push security model should be followed from CSP1, CSP2 to CSC. Where almost all onus of security embedding should fall upon CSP1 and CSP2 in that order. And the CSC level users should be encouraged or enforced to security standard operating procedures through push models.

Table1: Review of different attacks and solutions

Attack Type	Solution
Eavesdropping	Authentication Protocols that protect secrets, ensures user anonymity and Password Authenticated Key exchange (PAKE) protocols are much preferred in a multi-tenant Cloud environment.
Shoulder Surfing Attack	This attack results in information disclosure and in a Cloud scenario it can be mitigated by using secure two factor authentication and out-of band authentication mechanisms.
Cookie Poisoning	It can be handled by attaching the hash values of the data stored in the cookies and recalculating the same at the destination
Replay Attack	The integrity of the nonce value send by the legal user can be ensured by attaching the plain nonce value with the hash of the nonce XORed with the message value.
Session Hijacking	A key exchange mechanism, that involves the calculation of session key separately by the Client and server, resulting in the same key value, can be adopted in a Cloud environment
Flooding Attack	This attack can be controlled by data transfer throttling, fool proof authentication mechanisms and mechanisms that filter out bogus requests
Browser Attack	The web browser has to use SSL/TLS to encrypt the credentials and use SSL/TLS 4-way handshake process in order to authenticate the client
Weak Authentication	**:** Strong authentication mechanisms such as 2-factor authentication without password tables are recommended in a Cloud environment

All these attacks included in the category of password discovery attacks, focuses on obtaining the passwords of a legal user which in turn is used to illegally impersonate the user to a verifier. Such attacks will result in a successful authentication, if and only if the authentication process is solely based on password. In a Cloud scenario, this can be handled by protecting secrets, avoiding the storage of passwords, Zero Knowledge Proof (ZKP) mechanisms, privacy enhanced protocols implementing 2-factor authentication mechanisms without password tables etc.Different attacks and solutions are reviewed in table1.

III. Conclusion

Distributed computing can be considered as an administration, like the way that power is viewed as an administration in urban territories. A cloud client can use distinctive processing assets (e.g. system, stockpiling, programming application), at whatever point required, without being worried with the complex basic innovation and framework engineering. The most essential component is that the figuring assets are accessible at whatever point they are required. Also, clients pay just for the asset they really utilize. Subsequently, cloud clients can without much of a stretch scale their data innovation foundation, taking into account their business strategy and prerequisites. This adaptability makes the business procedure more agile.This paper talks about a few dangers that are connected with the cloud security.

References

[1] Ratansingham, P., Kumer, K.: Trading partner trust in electronic commerce participation. In: Proceeding of the 22nd International Conference on Information systems, pp. 544–552 (2000)

[2] Kim, K.K., Lee, J.W., Kim, H.S.: Impact of trust and risk on internet banking adoption. Korean Manag. Rev. **32**(6), 1771–1797 (2003)

[3] Jarvenpaa, S.L., Knoll, K., Leidner, D.E.: Is anybody out there? Antecedents of trust in global virtual teams. J. Manag. Inf. Syst.**14**(4), 29–64 (1998)

[4] Lim, N.: Consumer's Perceived Risk: Sources versus Consequences. Electron. Commer. Res. Appl. **2**(3), 216–228 (2003)

[5] Ahn, J.H.,Choi,K.C., Sung, K.M., Lee, J.H.:Astudy on the impact of security risk on the usage of knowledge management system: focus on parameter of trust. In: International Conference on Information systems, vol.15

[6] Hexin, Y., Ahn, J.C.: An empirical analysis on the persistent usage of personal cloud service: a cast study of China. Proc. Korean Soc. Internet Inf. Conf. **15**(2), 149–150 (2014)

[7] Jun, C.J., Lee, J.H., Jeon, I.S.: Research about factor affecting the continuous use of cloud storage service: user factor, system factor, psychological switching cost factor. J. Soc. e-Bus. Stud. **19**(1), 15–42 (2014)

[8] Seo, K.K.: Factor analysis of the cloud service adoption intension of Korean firms: applying the TAM and VAM. J. Digit PolicyManag.**11**(12), 155–160 (2013)

[9] Park, C.S.: Study on security considerations in the cloud computing. J Korea Acad.-Ind. Co-op. Soc. **12**(3), 1408–1416 (2011)

[10] Siani, P., Azzedine, B.: Privacy, security and trust issues arising from cloud computing. In: 2nd IEEE International Conference on Cloud Computing Technology and Science, pp. 693–702 (2010)

[11] Heiser, J., Nicolett, M.: Assessing the Security Risks of Cloud Computing. Gartner (2008)

[12] Almond, C.: A Practical Guide to Cloud Computing Security What You Need to Know Now About Your Business and Cloud Security, pp. 6–27. Avanade Inc. (2009)

[13] Zissis, D., Lekkas, D.:Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**(3), 583–592 (2012)

[14] Foster, T., Zhao,Y., Lu, S.: Cloud computing resource management through a grid middleware: a case study with diet and eucalyptus. Cloud computing. In: IEEE International Conference, pp. 151–154(2009). Accessed 25 August (2015)

[15] Tarrant, D., Brody, T., Carr, L.: From the desktop to the cloud: leveraging hybrid storage architectures in your repository. In: International Conference on Open Repositories. http://eprints.soton.ac.uk/267084/1/or09.pdf (2009). Accessed 25 August (2015)

[16] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[17] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015.

[18] M. Jouini and L. B. A. Rabai, "A Security Framework for Secure Cloud Computing Environments," *Int. J. Cloud Appl. Comput.*, vol. 6, no. 3, pp. 32–44, 2016.

[19] B. R. Kandukari, R. Paturi V, and A. Rakshit, "Cloud Security Issues," in *2009 Ieee International Conference on Services Computing*, 2009, pp.517–520.

[20] W. Jansen and T. Grance, "Guidelines on Security and Privacy in PublicCloud Computing," *National Institute of Standards and Technology Draft (NIST) Draft Special Publication 800-144*, 2011

[21] M. A. C. Dekker and L. Dimitra, "Cloud Security Guide for SMEs," *European Union Agency for Network and Information Security*, 2015.

[22] OWASP Top 10, "The Ten Most Critical Web Application Security Risks," 2013.

[23] Venkata Sravan Kumar Maddineni ,ShivashankerRagi.,(2011). "Security Techniques for Protecting Data in Cloud Computing".