Volume 5, Issue 3, July 2018 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Enhanced Security Techniques Implementation to Provide Security to Cloud

Vangari Mounika
M.Tech Research Scholar
Department of Computer Science & Engineering
Dhruva Institute of Engineering & Technology,
Hyderabad (T.S) [INDIA]
Email: mounika.vangari1996@gmail.com

K.V. Naganjaneyulu
Professor & Principal,
Department of Computer Science & Engineering
Dhruva Institute of Engineering & Technology,
Hyderabad (T.S) [INDIA]
Email: kvnaganjaneyulu75@gmail.com

ABSTRACT

Cloud computing has fashioned the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is quickly moving towards cloud primarily based design. Whereas it's necessary to take benefits of might primarily based computing by suggests that of deploying it in heterogeneous sectors, the protection aspects during a cloud primarily based computing surroundings remains at the core of interest. Cloud primarily based services and service providers are being evolved that has resulted during a new business trend supported cloud technology. With the introduction of diverse cloud primarily based services and geographically distributed cloud service providers, sensitive info of various entities square measure ordinarily keep in remote servers and locations with the probabilities of being exposed to unwanted parties in things wherever the cloud servers storing those info square measure compromised. If security isn't sturdy and consistent, the pliability and benefits that cloud computing must supply can have very little quality.

Keywords *:— Cloud computing, cloud service, cloud security, computer network, distributed computing, security.*

I. INTRODUCTION

Recent developments within the field of may computing have vastly modified the manner of computing moreover because the construct of computing resources. during a cloud based mostly computing infrastructure, the resources ar usually in somebody else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & jangwal, 2012). Processing is finished remotely implying the actual fact that the info and alternative parts from someone would like to be transmitted to the cloud infrastructure or server for processing; and also the output is came back upon completion of needed process. In some cases, it'd be needed or a minimum of attainable for someone to store knowledge on remote cloud servers. These offers the subsequent 3 sensitive states or situations that are of specific concern at intervals the operational context of cloud computing:

1. The transmission of non-public sensitive knowledge to the cloud server,
2. The transmission of information from the cloud server to clients' computers and

3. The storage of clients' personal knowledge in cloud servers that ar remote server not owned by the purchasers.

All the on top of 3 states of cloud computing are severely liable to security breach that creates the research and investigation at intervals the protection aspects of cloud computing observe an essential one. There are variety of various blends that are getting used in cloud computing realm, but the core construct stay same – the infrastructure, or roughly speaking, the resources stay somewhere else with somebody else's possession and also the users 'rent' it for the time they use the infrastructure (Bisong & Rahman, 2011; Rashmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012). In some cases, keep sensitive knowledge at remote cloud servers are to be counted. Security has been at the core of safe computing practices. once it's attainable for any unwanted party to 'sneak' on any non-public computers by means that of various ways that of 'hacking'; the availability of widening the scope to access someone's personal knowledge by means that of cloud computing eventually raises any security issues. Cloud computing cannot eliminate this widened scope thanks to its nature and approach.

As a result, security has continuously been a difficulty with cloud computing practices. strength of security and a secured computing infrastructure isn't a happening effort, it is rather in progress – this makes it essential to analyze and understand the progressive of the cloud computing security as a compulsory observe. Cloud is principally classified as non-public cloud, community cloud, public cloud and hybrid cloud (Ogigau-Neamtiu, 2012; Singh & jangwal, 2012; Rashmi et al., 2013; Qaisar & Khawaja, 2012; Kuyoro, Ibikunle & Awodele, 2011; Suresh & Prasad, 2012; Youssef, 2012) - the discussion during this paper assumes only 1 class of cloud exists that is public cloud; as this assumption can well satisfy all the characteristics of any other sort of cloud. thanks to its heterogeneous potentiality, the approach to cloud computing is being thought to be because the fifth utility to affix the league of existing utilities water, electricity, gas and telephony (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009) instead of being simply another service. The study bestowed during this paper is organized with a read to debate and indentify the approach to cloud computing moreover because the security problems and issues that has to be taken under consideration in the preparation towards a cloud based mostly computing infrastructure. Discussion on the technological concepts and approaches to cloud computing together with the branch of knowledge illustration has been taken into thought at intervals the context of debate during this paper. Security problems inherent in cloud computing approach are mentioned after. The exploration within the technological and security issues of cloud computing has LED to the terminal realization on the aspects of cloud computing. The approaches to counter security problems inherent in cloud computing ar varied with heterogeneous sides and applications that has been unbroken out of scope. A discussion on the authentication of cloud computing has been self-addressed because it forms the holistic basis to imbed integrity within the context of cloud computing security.

II. CLOUD SECURITY

Cloud computing security is a fast-growing service that provides many of the same functionalities as traditional IT security. This includes protecting critical information from theft, data leakage and

deletion. One of the benefits of cloud services is that you can operate at scale and still remain secure. It is similar to how you currently manage security, but now you have new ways of delivering security solutions that address new areas of concern. Cloud security does not change the approach on how to manage security from preventing to detective and corrective actions. but it does however give you the ability to perform these activities in a more agile manner. Your data is secured within data centers and where some countries require data to be stored in their country, choosing a provider that has multiple data centers across the world can help to achieve this. Data storage often includes certain compliance requirements especially when storing credit card numbers or health information. Many cloud providers offer independent third party audit reports to attest that their internal process exist and are effective in managing the security within their facilities where you store your data.

2.1 Security techniques:

Following are the security techniques used to provide security to cloud

1. Authentication and Identity:
2. Data Encryption: Information integrity and Privacy
3. Availability of Information (SLA)
4. Secure Information Management
5. Malware-injection attack solution
6. Flooding Attack Solution

III. AUTHENTICATION IN CLOUD

Security is that the most prioritized side for any variety of computing, creating it a clear expectation that security problems ar crucial for cloud setting similarly. because the cloud computing approach can be related to having users' sensitive knowledge hold on each at clients' finish similarly as in cloud servers, identity management and authentication are terribly crucial in cloud computing (Kim & Hong, 2012; Emam, 2013; Han, Susilo, 2013; Yassin, Jin, Ibrahim, Tibeto-Burman & Zou, 2012). Verification of eligible users' credentials and protective such credentials are a part of main security problems within the cloud - violation in these areas could lead on to unseen security breach (Kumar, 2012) a minimum of to some extent for a few amount. Security issues Cloud computing comes with varied potentialities and challenges at the same time. Of the challenges, security is taken into account to be a important barrier for cloud computing in its path to success (Khorshed, Ali & Wasimi, 2012). the safety challenges for cloud computing approach square measure somewhat dynamic knowledge location may be a crucial consider cloud computing security (Teneyuca, 2011). Location transparency is one amongst the distinguished flexibilities for cloud computing, that may be a security threat at an equivalent time – while not knowing the precise location of data storage, the supply of knowledge protection act for a few region could be severely affected and violated. Cloud users' personal knowledge security is therefore an important concern during a cloud computing environment (Joint, Baker, 2009; Ismail, 2011; King & Raja, 2012). In terms of customers' personal or business knowledge security, the strategic policies of the cloud suppliers square measure of highest significance (Joint & Baker, 2011) because the technical security exclusively isn't equal to address the matter. Trust is another downside that raises security issues to use cloud service (Ryan & Falvy, 2012) for the explanation that it's directly associated with the

credibleness and believability of the cloud service suppliers. Trust institution may become the key to determine a triple-crown cloud computing setting. the supply of trust model is crucial in cloud computing as this is a standard interest space for all stakeholders for any given cloud computing situation. Trust in cloud could be addicted to variety of things among that some square measure automation management, human factors, processes and policies (Abbadi & Martin, 2011). Trust in cloud is not a technical security issue, however it's the foremost important soft issue that's driven by security issues inherent in cloud computing to a good extent. all types of attacks that square measure applicable to a computer network and therefore the knowledge in transit equally applies to cloud primarily based services – some threats in this class square measure man-in-the-middle attack, phishing, eavesdropping, sniffing and alternative similar attacks. DDoS (Distributed Denial of Service) attack is one common however major attack for cloud computing infrastructure. The standard DDoS attack will be a potential downside for cloud computing, although not with any exception of getting no choice to mitigate this. the safety of virtual machine can outline the integrity and level of security of a cloud setting to bigger extent (Rakhmi, Sahoo & Mehfuz, 2013; Agarwal & Agarwal, 2011). Accounting & authentication likewise as victimisation encoding falls among the apply of safe computing - they will be thought-about as a part of security issues for cloud computing (Lee, 2012; Ogigau-Neamtiu, 2012; Singh & Jangwal, 2012). However, it's necessary to differentiate between risk and security issues during this regard. as an example, seller lock-in could be considered collectively of the attainable risks in cloud primarily based services that don't primarily ought to be related to security aspects. On the contrary, using specific form of software package (e.g. open source vs. proprietary) may create security threat and issues that, of course, may be a security risk. Other samples of business risks of cloud computing can be licensing problems, service unavailability, provider's business separation that don't fall among the safety issues from a technical viewpoint. Thus, in cloud computing context, a security concern is usually some sort of risk however any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties concerned during a cloud computing infrastructure may end in experiencing inconsistency which could eventually result in a scenario with security vulnerabilities. like all alternative network situation, the supply of insider-attack remains as a legitimate threat for cloud computing (Ogigau-Neamtiu, 2012). Any security tools or other forms of software package

IV. CONCLUSION

Cloud computing has enormous prospects; however the safety threats embedded in cloud computing approach are directly proportional to its offered blessings. Cloud computing could be a nice opportunity and moneymaking choice each to the companies and also the attackers – either parties will have their own blessings from cloud computing. The huge potentialities of cloud computing can't be ignored entirely for the safety problems reason – the continuing investigation and analysis for sturdy, consistent and integrated security models for cloud computing can be the sole path of motivation. The safety problems may severely have an effect on may infrastructures. Security itself is conceptualized in cloud computing infrastructure as a definite layer (Dukaric & Juric, 2013). Security for cloud computing surroundings could be a non-

compromising demand. Cloud computing is inevitable to become the best (and presumably the ultimate) approach to business computing though the safety barriers together with different problems have to be compelled to be resolved for cloud computing to create it additional viable (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011).

REFERENCES:

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

[2] 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), 257-259.

[3] 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

[4] 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), 546-552.

[5] 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), 30-45. doi:10.5121/ijnsa.2011.3103

[6] 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, 599–616. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 34

[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008

[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021

[9] Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551

[10] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193

[11] Dou, W., Chen, Q. and Chen, J. (2013). A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 29, 1838–1850. doi:10.1016/j.future.2012.12.011

[12] Dukaric, R. and Juric, M.B. (2013).

Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/j.future.2012.09.006

[13] Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3 (2), 110-113.

[14] Fernando, N., Loke, S.W. and Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29, 84 – 106. doi:10.1016/ j.future.2012.05.023

[15] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(11), 1-18.

[16] Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51. doi: 10.4018/jisp.2010040103

[17] Han, J., Susilo, W. and Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems, 29, 673–681. doi:10.1016/j.future.2012.07.010

[18] Hashizume et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), 1-13.

[19] Ismail, N. (2011).Cursing the Cloud (or) Controlling the Cloud? Computer Law & Security Review, 27, 250 – 257. doi:10.1016/j.clsr.2011.03.005

[20] Joint, A. and Baker, E. (2011). Knowing the past to understand the present 1 e issues in the contracting for cloud based services. Computer Law & Security Review, 27, 407 - 415. doi:10.1016/j.clsr.2011.05.002

[21] Joint, A., Baker, E. and Eccles, E. (2009). Hey, you, get off of that cloud? Computer Law & Security Review, 25, 270–274. doi:10.1016/ j.clsr.2009.03.001

[22] Jorissen, K., Villa, F.D. and Rehr, J.J. (2012). A high performance scientific cloud computing environment for materials simulations. Computer Physics Communications, 183, 1911–1919. doi:10.1016/j.cpc.2012.04.010

[23] Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28, 833–851. doi:10.1016/ j.future.2012.01.006

[24] Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.

[25] Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology, 8(1), 65-72.

[26] King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[27] Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

[28] Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255.

[29] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

[30] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176–189. doi:10.1016/j.dss.2010.12.006

[31] Mason, S. and George, E. (2011). Digital evidence and 'cloud' computing. Computer Law & Security Review, 27, 524-528. doi:10.1016/j.clsr.2011.07.005 International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 35

[32] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

[33] Mosher, R, (2011). Cloud Computing Risks. ISSA Journal, July Issue, 34-38.

[34] Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. Journal of Defense Resource Management, 3 (2), 141-148.

[35] Okuhara, M., Shiozaki, T. and Suzuki, T. (2010). Security Architectures for Cloud Computing. FUJITSU Science Technology Journal, 46(4), 397–402.

[36] Petcu, D., Macariu, G., Panica, S. and Craciun, C. (2013). Portable Cloud applications—From theory to practice. Future Generation Computer Systems, 29, 1417–1430. doi:10.1016/j.future.2012.01.009

[37] Petre, R. (2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.

[38] Qaisar, S. and Khawaja, K.F. (2012). Cloud Computing: Network/Security Threats and Countermeasures. Interdisciplinary Journal of Contemporary Research in Business, 3(9), 1323-1329.

[39] Rashmi, Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401

[40] Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513-521. http://dx.doi.org/10.1016/j.clsr.2012.07.002

[41] Sharma, S. And Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. International Journal of Innovative Research in Science, Engineering and Technology, 2(4), 994-998.

[42] Singh, S. and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer

Science & Information Technology, 4 (2), 17-31.

[43] Svantesson, D. And Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26, 391-397. doi:10.1016/j.clsr.2010.05.005

[44] Suresh, K.S. and Prasad, K.V. (2012). Security Issues and Security Algorithms in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 110-114.

[45] Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107. doi:10.1016/ j.istr.2011.08.005

[46] Westphall, C.B., Westphall, C.M., Koch, F.L., Rolim, C.O., Vieira, K.M., Schulter, A., Chaves, S.A., Werner, J., Mendes, R.S., Brinhosa, R.B., Geronimo, G.A. and Freitas, R.R. (2011). Management and Security for Grid, Cloud and Cognitive Networks. Revista de Sistemas de Informação da FSMA, 8, 8-21.

[47] Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient Password-based Two Factors Authentication in Cloud Computing. International Journal of Security and Its Applications, 6(2), 143-148.

[48] Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.

[49] Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583–592. doi:10.1016/ j.future.2010.12.006

* * * * *