International Journal of Science Engineering and Advance Technology

Challenges and Issues of Data Security in Cloud Computing

Anil Kumar Dudla[1], Ashok Kote[2], VijayaRaju Motru[3]
[1,2]Dept of CSE, College,
[3] Dept of Information Technology,
QIS Institute of Technology.
[2] Nova College of Engineering & Technology, Vijayawada.
3 UshaRama College of Engineering & Technology, Vijayawada

anil.dudla@gmail.com, kote.ashok@gmail.com, vijayaraju.m@gmail.com

Abstract-- Cloud computing is still in its infancy in spite of gaining tremendous momentum recently, high security is one of the major obstacles for opening up the new era of the long dreamed vision of computing as a utility. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security challenges. It might be difficult to track the security issue in cloud computing environments. So this paper primarily aims to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses, which includes: (a) surveying the most relevant security, privacy and trust issues that pose threats in current existing cloud computing environments; and (b) analyzing the way that may be addressed to eliminate these potential privacy, security and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment. In the near future, we will further analysis and evaluate privacy; security and trust issues in cloud computing environment by a quantifiable approach, further develop and deploy a complete security, privacy trust evaluation, management framework on really cloud computing environments.

Keywords: Privacy, security, trust, secure, tangible.

1. INTRODUCTION

"Cloud computing alludes to both the applications conveyed as administrations over the Internet and the equipment and frameworks programming in the datacenters that give those administrations" [1]. As to cloud benefits, the Cloud computing sorts can be separated into two gatherings: Service Models: Service model alludes to the administrations sort that gave by cloud suppliers, for example, Amazon EC2 and Microsoft Azure and so forth. Programming as a Service (SaaS) alludes to conveyance of programming applications or administrations that keep running in cloud supplier framework. The customer does not control or deal with the assets like servers, working framework and stockpiles. Stage as a Service (PaaS) alludes to conveyance of sending administrations onto cloud supplier framework though the shopper can convey certain applications with restrictions on control on administration of the assets [2,3]. Framework as a Service (IaaS) alludes to conveyance of base provisioning administrations to the customer where the buyer can procurement servers, working framework, stockpiling and others central assets 11-12. Organization Models: Deployment Model alludes to how cloud base proprietor host and offer the Cloud computing administrations. These are open, private and half and half cloud models10 [4,5]. Open Cloud model alludes to buyer utilization of an association's cloud foundation on a pay for every utilization premise. Private Cloud model alludes to interior arrangement, administration and operation of an association's own particular cloud foundation. Half breed Cloud: model alludes to reconciliation on both open and private cloud models inside of an association[6].

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud [7]. There are four types of issues raise while discussing security of a cloud.

1. Security issues

2. Data Issues
3. Privacy issues
4. Infected Application

This paper essentially expects to highlight the significant security, protection and trust issues in current existing Cloud computing situations and offer clients some assistance with recognizing the substantial and elusive dangers connected with their employments. Our commitments can be condensed as: (a) studying the most pertinent protection, security and trust issues that stance dangers in current existing Cloud computing situations; and (b) breaking down the way that may be tended to wipe out these potential security, security and trust dangers, and giving a high secure, reliable, and tried and true Cloud computing environment[8,9]. The rest of this paper is composed as takes after. Segment 2 presents security issues and tending to in Cloud computing situations. Area 3 presents security issues and tending to in Cloud computing situations. Area 4 presents trust issues and tending to in Cloud computing situations. At last, determinations and a course for future work are given in area 5.

2. SECURITY ISSUES

Security is seen as a composite thought, in particular "the mix of privacy, the counteractive action of the unapproved revelation of data, trustworthiness, the avoidance of the unapproved revision or erasure of data, and accessibility, the aversion of the unapproved withholding of data" [13]. Security is the nonappearance of unapproved access to, or treatment of, the framework state. The primary measurements of security are accessibility, secrecy and respectability. Security is a standout amongst the most deterrents for opening up the new time of the since a long time ago imagined vision of registering as an utility.

Security issues in Cloud computing situations can be partitioned into six sub-classifications [5] [6] [7] [11] [14], which include: (a) how to give wellbeing components, so that to screen or follow the cloud server, (b) how to keep information privacy for all the individual and delicate data, (c) how to evade noxious insiders illicit operation under the general absence of straightforwardness into supplier procedure and system situations, (d) how to maintain a strategic distance from administration commandeering, where phishing, extortion and misuse are understood issues in IT, (e) how to administration multi-occurrence in multi-occupancy virtual situations, which expect all case are totally detached from one another. On the other hand, this suspicion can at some point separate, permitting assailants to cross virtual machines side channel, get away from the limits of the sandboxed environment and have full access to the host, and (f) how to create fitting law and actualize legitimate ward, with the goal that clients have a chain against their suppliers if need.

3. DATA ISSUES

sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accessesable to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

4. PRIVACY ISSUES

Privacy is the capacity of an individual or gathering to disconnect themselves or data about themselves and along these lines uncover themselves specifically, and it is incorporate [15]: (a) when: a subject may be more worried about her present or future data being uncovered than data from the past, (b) how: a client may be agreeable if companions can physically ask for his data, yet may not need cautions sent naturally, (c) degree: a client might rather have her data reported as an uncertain area as opposed to an exact point. In the business, shopper setting and privacy needs the assurance and fitting utilization of the data about clients and meeting the desires of clients about its utilization. In the associations, privacy involves the use of laws, components, guidelines and procedures by which by and by identifiable data is overseen [8]. The protection issues contrast as per distinctive cloud situation, and can be partitioned into four subcategories [5] [6] [8], which include: (a) how to make clients remain control over

their information when it is put away and prepared in cloud, and dodge robbery, odious use and unapproved resale, (b) how to ensure information replications in a purview and predictable state, where repeating client information to various suitable areas is a generally decision, and maintain a strategic distance from information misfortune, spillage and unapproved change or creation, (c) which gathering is in charge of guaranteeing legitimate necessities for individual data, and (d) what degree cloud sub-temporary workers included in handling can be appropriately recognized, checked and learned.

5. TRUST ISSUES

Trust is seen as a quantifiable conviction that uses experience, to settle on reliable choices. It is initially utilized as a part of sociology in building individuals' relationship and is presently a key substitute for framing security component in Cloud registering situations, as trust has numerous delicate protection traits, for example, unwavering quality, trustworthiness, certainty, legitimate, conviction, trustfulness, security, skill, and suchlike. Truth be told, trust is the most complex relationship among substances on the grounds that it is to a great degree subjective, setting subordinate, non-symmetric, questionable, and somewhat transitive [9] [10]. Trust assessment is a multi-faceted and multi-staged marvel taking into account multi-dimensional elements and trust assessment cycle, and it is utilized to discover the response to the inquiry "With which node(s) if I connect and with which I ought not?" A quantifiable trust perspective is adjusted by [16], "Trust of a gathering A to a gathering B for an administration X is the quantifiable conviction of An in that B acts constantly for a predetermined period inside of a predefined setting (in connection to administration X)." Another scientific trust perspective is given in [17], "Trust (or, symmetrically, doubt) is a specific level of the subjective likelihood with which a specialists surveys that another operators or gathering of specialists will perform a specific activity, both before he can screen such activity (or autonomously or his ability ever have the capacity to screen it) and in a setting in which it influences his own particular activity." To ensure mists, conventional hard security strategies, for example, encryption and approval give a strong establishment, however they fall flat while coordinating elements act vindictively because of scale and makeshift nature of joint efforts. Trust as a delicate social security restricting so as to reason can battle against such protection dangers malevolent elements from partaking in associations and hence offers a high dependability Cloud computing environment. Trust issues in Cloud computing situations can be isolated into four sub-classifications [5] [6] [8] [12], which include: (a) how to definition and assessment trust as indicated by the special trait of Cloud computing situations, (b) how to handle vindictive suggest data, which is essential in Cloud computing situations, as trust relationship in mists is makeshift and element, (c) how to consider and give contrast protection level of administration as indicated by the trust degree, (d) how to oversee trust degree change with association time and connection, and to screen, modify, and truly reflect trust relationship element change with time and space.

6. SOLUTIONS TO CLOUD SECURITY ISSUES

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing environment. It consists of four layers as shown in Figure 1.

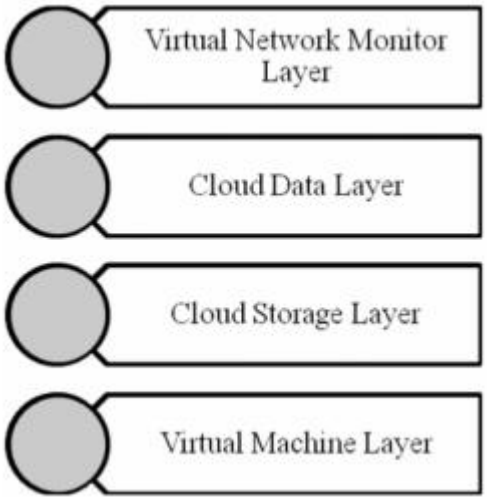

Fig 1: Layered framework for cloud

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN [8]. However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and

future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers. There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

Verify the access controls: Set up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data.

Control the consumer access devices: Be sure the consumer's access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features [15,16].

Monitor the Data Access: cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc.

Share demanded records and Verify the data deletion: If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract [6].

Security check events: Ensure that the cloud service provider gives enough details about fulfillment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider.

7. CONCLUSIONS AND FUTURE WORK

K High protection is one of the significant deterrents for opening up the new period of the since quite a while ago imagined vision of figuring as an utility. As the touchy applications and information are moved into the cloud server farms, keep running on virtual figuring assets as virtual machine. This one of a kind characteristics, be that as it may, postures numerous novel protection difficulties, for example, availability vulnerabilities, virtualization vulnerabilities, and web application vulnerabilities. With headway of Cloud computing and expanding number of cloud client, security, and protection and trust measurements will consistently increment[17]. To ensure private and touchy information that are handled in server farms, the cloud client needs to confirm (a) the genuine exists of the Cloud computing environment on the planet; (c) the security of data in the cloud; and (b) the reliability of the frameworks in Cloud computing environment. In this paper, we fundamentally expects to highlight the real security, protection and trust issues in current existing Cloud computing situations and offer clients some assistance with recognizing the substantial and immaterial dangers connected with their employments. We cover two principle parts of protection, security and trust issues, which include: (a) looking over the most applicable security, security and trust issues that stance dangers in current existing Cloud computing situations, and (b) breaking down the way that may be tended to kill these potential protection, protection and trust dangers, and giving a high secure, reliable, and tried and true Cloud computing environment. Future works will concentrate on the accompanying: (a) dissecting and assessing protection, security and trust issues in Cloud computing environment by a quantifiable methodology, the reviewing and breaking down methodology technique proposed in this paper is an initial move toward investigating protection, protection and trust issues, (b) adding to a complete protection, protection trust assessment, administration system as a piece of Cloud computing administrations to fulfill the security requests; and (c) sending the structure on truly Cloud computing situations.

6. REFERENCES

[1] Foster I, Zhao Y, Raicu I, Lu, S. Cloud Computing and Grid Computing 360-degree compared. Proceedings of the Grid Computing Environments Workshop, GCE 2008; IEEE Press, Nov. 2008, 1-10.

[2] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009;25(6):599–616.

[3] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM; 2010;53(4):50–58.
[4] Mell P, Grance T. The NIST Definition of Cloud Computing. Communications of the ACM; 2010;53(6):50.
[5] Paquette S, Jaeger P T, Wilson S C. Identifying the privacy risks associated with governmental use of cloud computing. Government Information Quarterly; 2010;27(3):245–253. [6] Subashini S, Kavitha V. A survey on privacy issues in service delivery models of cloud computing. Journal of Network and Computer Applications; 2011;34(1):1–11.
[7] Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: A survey on IaaS cloud privacy. Computing; 2011;91(1):93– 118.
[8] Pearson S, Benameur A. Privacy, privacy and trust issues arising from cloud computing. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010; IEEE Press, Nov. 2010, 693-702.
[9] Ahamed S I, Haque M M, EndadulHoque M, Rahman F, Talukder N. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments. Journal of Systems and Software; 2010;83(2):253– 270.
[10] Karaoglanoglou K, Karatza H. Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values. Journal of Systems and Software; 2011;84(3):465–478.
[11] Takabi H, Joshi J B D, Ahn G. Privacy and privacy challenges in cloud computing environments. IEEE Privacy & Privacy; 2010;8(6):24–31.
[12] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data privacy risks in cloud computing environments. Communications in Computer and Information Science; 2010;54:255–265.
[13] Algirdas A, Jean-Claude L, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing; 2004;1(1):11–33.
[14] Tchifilionova V. Privacy and privacy implications of cloud computing - Lost in the cloud. Proceedings of the IFIP WG 11.4 International Workshop on Open Research Problems in Network Privacy, iNetSec 2010; Springer Verlag Press, Mar. 2010, 149-158.
[15] Krumm J. A survey of computational location privacy. Personal and Ubiquitous Computing; 2009;13(6):291–399.
[16] Shekarpour S, Katebi S D. Modeling and evaluation of trust with an extension in semantic web. Journal of Web Semantics; 2010;8(1):26–36.
[17] Iltaf N, Hussain M, Kamran F. A mathematical approach towards trust based privacy in pervasive computing environment. Proceedings of the Third International Conference and Workshops, ISA 2009; IEEE Press, Jun. 2009, 702-711.