Elysium Journal of Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

SURVEY AND ANALYSIS ON DATA SECURITY ISSUES FOR USERS EXERCISING CLOUD

R.Nagaraja Prabu[1], S.Christina Magneta[2]

[1]Department of Computer science, Christian College of Engineering and Technology, Dindugal, Tamil Nadu, India. Email: nagarajaprabu.r@gmail.com

[2]Assistant Professor, Christian College of Engineering and Technology Oddanchatram, Dindigul.

Abstract— Iaas provides access to computing resource over virtualized environment, "the Cloud", across a public connection, usually the internet. Computing resources means the virtual server space, network connections, bandwidth, IP addresses and load balancers. Large scale services which make use of these IaaS will assert the impulse of this model. Many organizations that hold on sensitive data eschew making use of this Iaas platform, due to much security concern. In this paper a scheme of data and security for performing operations over those data were described, IaaS endures protocols for ingrained launch of virtual machine and as well protection for storage, that's based on domain. An encompassing theoretical analysis along with the proof about the protocol resistance on subject to attacks performed over the concrete threat model is performed. Beforehand to introducing tenant virtual machine, the host platform configurations were attested remotely by the protocols and ensure the seclusion for the data stored in the third party cloud by making use of the key that is encrypted. This key is maintained outside the IaaS domain. The experimental result portrays the protocols validity and how efficiently it could be used and integrated into the existing third party cloud environment throughout the process.

Keywords- Cloud Computing, Storage Protection, Security, Encryption.

1. INTRODUCTION

Cloud computing has become an important part of every once life. Since it offer a massive storage for the users at very less cost as well free of cost sometimes. It also provides various services like IaaS (Infrastructure as a Service),PaaS (Platform as a Service),SaaS (Software as a Service).The main threat here about the cloud computing is the threat for the security. Since the entire user data were dumped into the third party cloud so that any users could access it at any time. There lies many risks and challenges. Intensive investigation over the threats and the extenuation techniques for those threats were carried out recent years [11],[7],[10],[8] ,many solutions for security as well various practicing techniques are also been recommended [4].There are huge security problems correlated by the cloud computing. They usually fall in the two categories one is issues regarding security face by the cloud providers and the second one is the security issues being faced by the cloud users. Providers who provide the cloud for the users must assure the users that their data and documents will be stored safely as well they do make use of secured infrastructure in the cloud. At the same time the users who make use of the cloud must protect their own data by making use of strong passwords and required authentication measures as well [6].When organizations host application into the third party server, it's not necessary that every organization or clients do need to have physical contact with the cloud where they do uploaded their data or applications, the major rick here is the insider attack over those data or application that a client uploads. Insider attack is the sixth major risk in the field of cloud computing. In order to overcome this issue the provider who provide the cloud for the user must ensure a thorough background check is made for the users or clients who have the direct access to the cloud server .And frequent monitor check has to be carried out in order to prevent the malfunctions and intruders. Platform integrated verification is carried out for the application host [6]. Many cloud vendors do follow this practice in order to protect their cloud data from the insider attack and other persistent threats. There are two major measures that the vendors take up in order to promote their cloud usage and also to make up many customers. First, they do never expose the solution for the above problems that they have used to protect cloud, so that no other vendors can make use for their technique and their platform will remain the best of all. Second, none of the cloud tenants will be known about the proofs regarding the integrity of computers that do support the cloud infrastructure. To overcome this set of protocols were proposed to launch the Virtual Machine (VM) in IaaS, which provides the tenants proof about the VM instance which were launched with the set of software stack.

The virtual disk volume is encrypted and implemented and sanctioned at the host level. All these are performed by the provider who provides the cloud for the users for data at rest and now the tenants could configure it with their Virtual Machine (VM) instance functionalities and migration capabilities are restricted. The details about the encryption and the decryption are being stored by the provider. This further increase the migration complexity between the cloud providers for the tenants disadvantages them with new vendor lock- in. So the tenants can encrypt key at the Os level within their Virtual Machine (VM) environment and manage themselves.

2. RELATED WORK

Samee Ullah Khan et al., [14] put forward the comparison and analysis of ten heuristics to solve fine-grained data replication problem over the Internet. The problem here is the data objects those are accessed frequently are made into replication of set of selected sights; this is done in order to minimize the time consumed by the end users for accessing the data objects. Though it saves the memory space in the server and just relocates only those objects that are in urge to be displaced and concentrates upon the balance in load, they do even face the drawbacks like they do not capture the exact idea of replication of single object over the determined number of hosts. This could be overcome in the proposed system.

Vaibhav Jain .Mr et al., [17] emphasize that though there are many approaches to improve the security in cloud they do not opt for all the issues and risks face in the cloud environment. Hence service level agreements and various strong schemes for enforcing security have to be undertaken in future to protect the cloud. The flaw here is the outcome of the study does not deal up with the physical access of the hardware in the system. This study could be very efficient for the primary resources like storage, network etc. basic services to the end users. This drawback finds out a solution by making use of end to end cryptographic techniques in the proposed study.

Sheetal.S et al., [16] describes the authentic users who use the third party cloud as a storage will make use of their digital credentials like passcode and digital certificates in consequence of the fact that their data should be protected from the intruders who do try to get an illegal access and might invade the important stuffs that the users backup in the cloud. The methodology can be more useful, users dynamically update their credentials, and this could be successful only if there exists a proper communication between the cloud and the user as in the proposed system.

Monjur Ahmed et al., [9] portrays about the concept of cloud and the series of security issues that are faced in both cloud computing and the cloud infrastructure. Security issues do differ from cloud to cloud they may depend on the infrastructure of the cloud and they vary time to time as the technology increases here comes an equal hacking competitor accordingly. Different amalgamations are being used in the computing kingdom. The deficiency of the study here is the client's personal data are hoarded to third party storage which is not owned by client. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) methodology is used in the proposed system to overcome this deficiency.

Sebastian Graf et al., [15] illustrates that reserving data in the third party cloud infrastructure provides infinite scalability and anywhere-any time availability. The user can share and access the data, whenever required at enormous speed. They do demand trust and confidence. The approach not only makes use of the related data since it uses distributed architecture but also the different types of data are handled here. Key-graph approach paves way for this act. The client encrypts the data and stores them, for decryption the trial and error techniques which is not much successful is preferred. In the suggested study AES and DDDS algorithms as well as the Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) methodology over comes the above defect.

N. Santos et al., [11] marks out that hazard to the integrity and confidentiality of the users data in the third party cloud server might occure, either by corpicious or designed mismanagement of the uderlyimg software. Hence trusted computing might is the way to over come the above threats. The goal suggested is to afford premitive sealed data by making use of Trusted Platform Module (TPM). The hindrance faced here is that only the cloud nodes will be disclosed about the premitive, but not the clients at the other end. A recover procedure followed in the suggested system is fragmentation and replication of data, so even if successfull attack happens only the meaningless data will be releaved.

Sadeghi.A.R et al., [1] detailed about the Trusted Computing Group (TCG) and Next-Generation Secure Computing Base (NGSCB) that offers various services, that verifies the probity of the platform in order to render the security for the users. Many hardware infrastructures were also used to improvise the security for the sake of the clients. The impediment is the managing the great number of possible agreeableness as well as the quality of data lacks here. The fragmentation and the replication across various nodes strategy limits the fault discussed above in the proposed system.

Mell.P et al., [13] imparts NIST definition to coincide with approaches of cloud computing and deals with the wide comparisons of various cloud services and deployment strategies. Gives guideline from what is the cloud computing to how to make use of those in a best way. The short come is both public and the private cloud could not remain in the same cloud composition at a stretch.

Blanchet.B et al., [3] elucidates an automatic cryptographic protocol verifier based on prolong rules and new efficient algorithms. Using this protocol verifier the author determines whether the fact can be proven by making use the prolog rules or not. The secrecies regarding the properties of the protocol can also be verified. The deficiency about the protocol is that it's secure all the time, possibilities for attacks. This finds a solution in the proposed system by making use of Transport Layer Protocol, and User Datagram Protocol.

Dolev.D et al., [5] delineates the methodology of making use of the public key encryption technique which is most popular presently. Even though it has gathered the fame, it has also got an eye of eavesdropping, who can decipher the ciphered text. To overcome this during encryption the sender name is included along with the plain text and then encryption operation is carried on. The opportunity to fail never fails. Better Cryptographic algorithms paved way in the advised system to overcome the discussed fault.

Allice et al., [2] from various experts report study author chronicles the significant threats to security in the cloud and he spotlights the reason for threat is all because of contribution of common resources. The data dumped in the cloud might suffer from either stolen by the hackers, lost due to some hardware problems, unconscious deletion or deteriorate from natural disasters. Somehow or other there occurs some risks but the cloud model proposed by the Cloud Security Alliance (CSA) paves major thoroughfare to hazardousness. The recommended system avoids the limitation discussed above by making use of, Data in the Cloud for Optimal Performance and Security (DROPS) methodology.

3. CONCLUSION

From the detailed survey the main common drawback that the cloud society is well studied and the recovery solutions that is being used in the suggested is Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) methodology. The Symmetric encryption technique supports the proposed system to handle the bulk data at a time. The fragmentation and the replication procedure implemented wise by distributed strategy gives hand to overcome the most discussed eavesdropping problem. By making use of the various papers survey has given a new path for the proposed architecture.

REFERENCE

[1] Ahmad –Reza Sadeghi and Christian Stuble," Prosperity-based attestation for Computing Platforms: Caring about properties, not mechanisms," Proceedings in ACM 2004.

[2] Allice ," The Notorious Nine Cloud Computing Top Threats in 2013," Proceedings in Cloud Security Alliance, Feb 2013.

[3] Bruno Blanchet," An Efficient Cryptographic Protocol Verifier Based on Prolog Rules," Published in 2001.

[4] Cloud Security Alliance, "The notorious nine cloud computing top threats 2013," February 2013.

[5] D.Dolev and A.C.Yao," On the Security of Public Key Protocols," Proceedings in *IEEE Transactions on Information Theory,* IT-29:198-208.

[6]https://en.wikipedia.org/wiki/Cloud_computing_security.

[7] J. Schiffman, T. Moyer, H. Vijayakumar, T.Jaeger, and P. McDaniel, " Seeding Clouds With Trust Anchors," in Proceedings of the 2010 ACM Workshop on Cloud Computing Security, CCSW '10, (New York, NY, USA), pp. 43–46, ACM, 2010.

[8] M. Jordon, "Cleaning up dirty disks in the cloud," Network Security, vol. 2012, no. 10, pp. 12–15, 2012.

[9] Monjur Ahmed and Mohammad Ashraf Hossain," Cloud Computing And Security Issues In Cloud," Proceedings in Internet Journal of Network Security & Its Applications (IJNSA), Vol.6,No.1,Jan 2014.

[10] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in Proceedings of the 2014 International Workshop on Security in Cloud Computing, ASIACCS '14, (New York, NY, USA), ACM, 2014.

[11] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot

[12] Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[13] Nuno Santos, Rodrigo Rodrigues, Krishna P.Gummadi, Stefan Sarious," Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services," Proceedings in MPI-SWS ,Microsoft Research,2012.

[14] Peter Mell and Timothy Grace," The NIST definition of Cloud Computing," Proceedings in National Instuite of Standards and Technology special Publication 800-145,7 pages, Sep 2011.

[15] Samee Ullah Khan and Ishfaq Ahamad," Comparison and analysis of ten static heuristic-based Internet data replication techniques," in Proceedings in the Journal of Parallel and Distributed Computing. 68(2008) 113-136.

[16] Sebastian Graf, Patrick Lang, Stefan A.Hohenadel and Marcel Waldvogel," Versatile Key Management for Secure Cloud Storage," Proceedings in Konstanzer Online-Publickation-System (KOPS) *URL:http://nbn-resolving.de/urn:nbn:de:bsz:352-200971.*

[17] Sheetal S. Dharwadkar and Rashmi M.Jogdand," A User Identity Management Protocol Using Efficient Dynamic Credentials," Proceedings in International Journal of Science Engineering and Research (IJSER) ,ISSN:2347-3878,Vol.2,Issue 6 Jun 2014.

[18] Vaibhav Jain and Varun Sharma," Surveying and Analyzing Security Challenges and Privacy in Cloud Computing," Proceeding in IRACST-International Journal

of Computer Science and Information Technology & Security (IJCSITS), ISSN:2249-9555, vol 3, No.5, October2013.