ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Three Stage Secured Cloud Proffering Environment with Privilege Performance Results Using Hardware Security Model

Anbazhagan .S[1], Karthick .B[1], Naveen .R[1], G. Pushpa Antanet Sheeba[2]

Dept. of C.S.E, GTEC, Vellore, Tamil Nadu, India[1]

Assistant Professor, Dept. of C.S.E, GTEC, Vellore, Tamil Nadu, India[2]

ABSTRACT: Increase in the usage of Cloud computing, the security alarms in the form of confidentiality of user data by the domain and administrator is high. Within the secured environment, the hardware security module provides essential security functionality with automatic generated keys for data in storage. Such restrictions prevent the cloud administrator from affecting the security of the Guest users. This system not only defends against wide attacks but also for the small TCB. The software implementation of the proposed Proffering approach with safety unit is done. Analysis of the security is performed and the performance results are calibrated. This system provides the three methods of cloud security.

KEYWORDS: Iaas, Security, Trusted computing, Trusted virtual machine launch, Cloud Computing, Scalability, Infrastructure, Confidentiality, Integrity, Trusted cloud computing platform.

I. INTRODUCTION

The proposed trusted cloud system provides restricted interfaces to cloud administrators. The system provides a secure connection scheme between a user and an allocated VM. The proposed system provides a secure storage scheme. To protect VM guest images from cloud administrators, the cloud system should isolate the cryptographic environment as well as a cryptographic key and integrity data.The system provides a secure management scheme. The management operation is triggered by a cloud user, and the result of the operation is reported to the user. When a communication protocol is not designed correctly, a malicious entity can compromise the protocol and take control of communication. The protocols are correctly designed with an automatic verification tool.

II. INFRASTRUCTURE AS A SERVICE

In Infrastructure as a Service (IaaS) cloud services such as Amazon’s EC2, the provider hosts virtual machines (VMs) on behalf of its customers, who can do arbitrary computations. In these systems, anyone with privileged access to the host can read or manipulate a customer’s data. Consequently, customers cannot protect their VMs on their own.

A hypervisor, such as Xen, Oracle Virtual Box, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. Customers can use either the Internet or carrier clouds (dedicated virtual private networks). To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure.

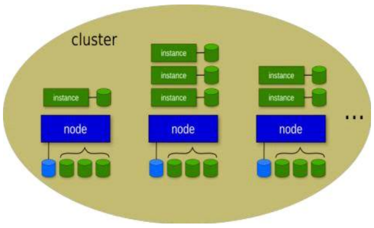

Fig.1. Simplified architecture of IaaS

III. PURPOSE OF THE PAPER

Nowadays the business people can store the data in cloud technology only. In this online proffering scheme the bid is secured and encrypted. The key will automatically generate for the authentication and it avoids the security breach in the cloud and also in the communication between the admin and user. Security is a primary consideration for cloud users. Even though security threats by cloud administrators are feasible and critical, cloud service providers are mainly concerned with security threats from external attacks rather than internal attacks. This viewpoint hinders the proliferation of cloud computing. By providing the security module supporting special storage which is accessible to cloud administrators security critical data in the hardware isolated which prevent the malicious admin. The proposed system provides a secure connection between the a cloud administrator and cloud provider the connection between an allocated VM is secured by exchanging the keys

IV. TRUSTED VIRTUAL MACHINE MONITOR

Trusted Virtual Machine Monitor is a security enhanced VMM isolating several data for guest VMs from cloud administrators. TVMM encrypt the guest VM images with cryptographic keys delivered by a TCM and it enables the secure connection between cloud user and cloud administrators .TVMM also validates the management operation triggered by a cloud user.

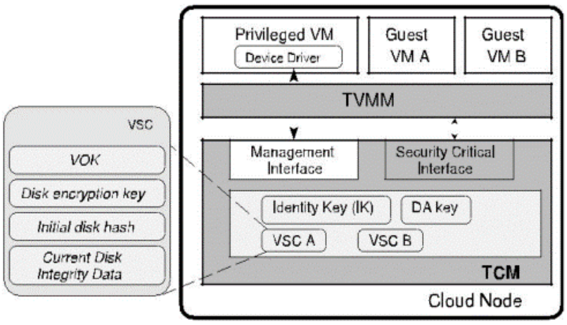

Fig 2: TVMM environment

V. DATA ENCRYPTION STANDARD

In existing system, using I/O model of hypervisor with management tool they performed the cloud storage allocation for the cloud administrators. In this module the physical machines shared by multiple admin so they can easily access the others data. By I/O scheduler they perform the bidding operations based on the storage space required by a cloud administrator. The digital signature based on only the conventional system (i.e) using the DES algorithm while digital signature proposed which provides encryption function on more completing function it will be more complex for users and easily attacked by malicious admin. In previous methods they used DES –Data Encryption Standard which uses 62 bit encrypt all data Self-service cloud computing method is efficient but in this method they cloud user and cloud admin have equal authority to change the data so it is insecure for the data. Anybody can access the data which is stored in the database

VI. CONSIGNMENT PROCESS

Admin should upload the full details about the bidding offers Admin should commerce the auction once the auction is started then users who are all interested in the bidding can bid in the particular time period. Clients who are all interested in the bidding they can apply for the bidding. The client have to login into their valid account a then update the rate what they wish for the current offer.

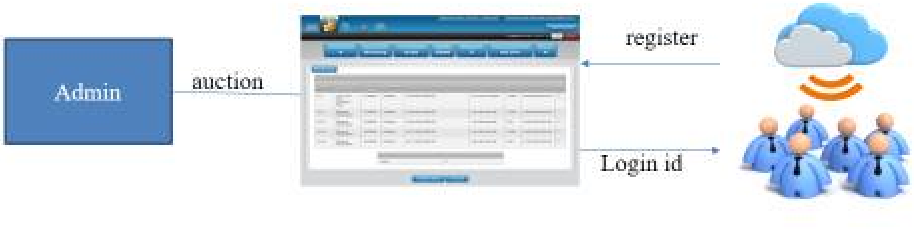

FIG 3:CONSIGNMENT PROCESS

VII. CONFIRMATORY PROCESS

Once the client updates the offers their details should be encrypted for the secure bidding this should prevent the bidding. To know this for each client separate private key is generated and stored in the cloud storage people who are all applied for the bid details is encrypted using AES algorithm this algorithm used to encrypt the data in 128 bit which is most efficient way for the security purpose. Once the client entered their details the data will be encrypted and the private key is generated and send to the admin via email. We will be using AES algorithm here.

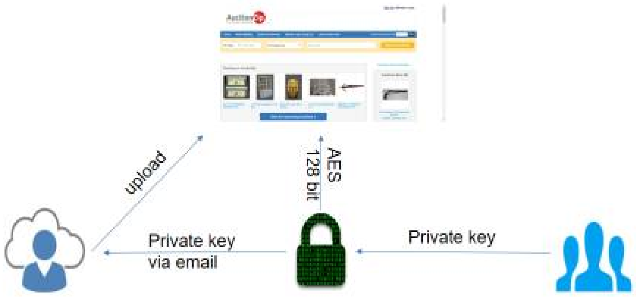

Fig 4:Confirmatory process

VIII. ADVANCE ENCRYPTION STANDARD

To prevent the data from the malicious admin we are providing keys for the secure isolated path for the cloud administrators. The keys are stored in separately in cloud, the keys are automatically generated. The data are stored in encrypted form protected with security key. In the proposed system we used AES-Advanced Encryption Standard which encrypts the data on more efficient way. For each process there will be an attestation using security key this will prevent the data from malicious admin. There will be a hash values for the every data to prevent the forgery and is verified by the device authority this will increase more secure connection between cloud administrator and cloud provider. Using the entrusted attestation, management and reporting and managing VSC.

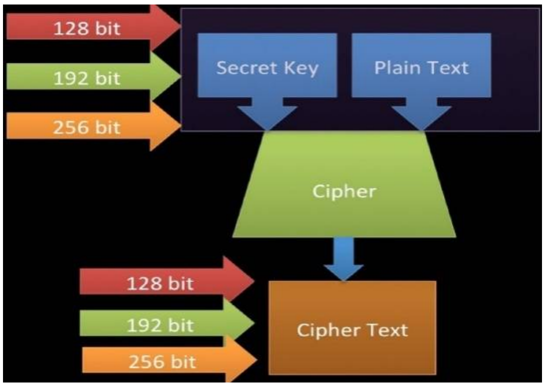

Fig 5:AES design

AES parameters

Nb – Number of columns in the State
- For AES, Nb = 4e

Nk – Number of 32-bit words in the Key
- For AES, Nk = 4, 6, or 8

Nr – Number of rounds (function of Nb and Nk)
- For AES, Nr = 10, 12, or 14

AES methods

- AddRoundKey
- SubBytes
- ShiftRows
- MixColumns

IX. DECIPHERMENT PROCESS

Once the bid time is completed the every clients details in storage in encrypted format. To view this admin must have the private key with them using private key they have to decrypt the details of the client if the private key is matched then the details of the client who claimed the offer for higher rate will be decrypted. Then showed to the admin who uploaded the particular bidding offers other admin can’t see the details of the client who bagged the offers.

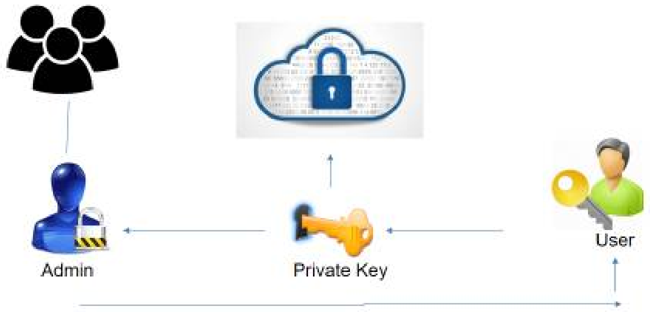

Fig 6:Decipherment process

X. PERFORMANCE ANALYSIS PROCESS

Performance may be limited by cloud resource controls rather than physical limits Hardware virtualization complicates things – as a guest you can't analyze down to metal directly hopefully the cloud provider provides an API for accessing physical statistics, or does the analysis your behalf.

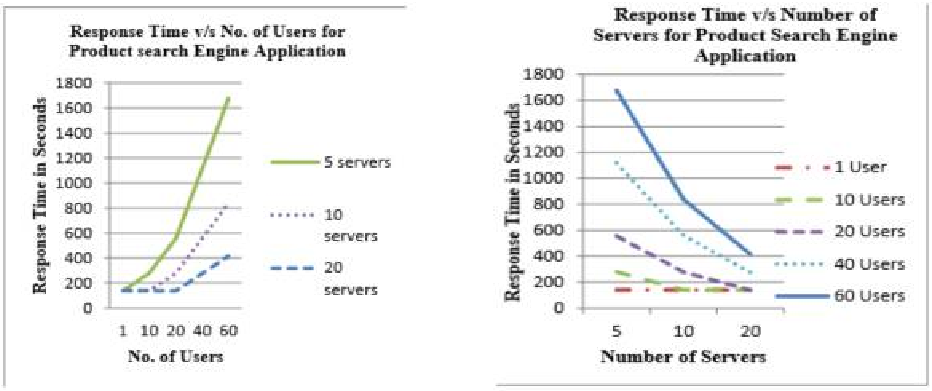

Fig 7: Performance analysis

XI. CONCLUSION

There have been many prior studies that aimed to enhance the security of cloud architecture. We discuss several studies focused on hardening virtualization environments, security of guest VMs. VMs on a verified platform. To enable virtualization. To solve this problem, AES encryption schemes on the client side. So VMM and a privileged domain are essential components. Hardening such components is a stepping stone toward the security of virtualization. To enhance the security of guest VMs, VMM was modified to support various security features for guest VMs. Even if an OS in a guest VM is compromised, the OS cannot compromise VMM or other VMs because VMM has a higher privilege than guest VMs. On the occasion that guest VMs launch on an impaired VMM, the confidentiality and integrity of guest VMs cannot be guaranteed. The proposed system provides security functionality against malicious attacks and achieves a small TCB. It also shows reasonable I/O performance analysis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

XII. FUTURE WORK

In the proposed system the automatic generated keys are stored in a particular storage and the third party user can easily retrieve the document or application. But in the future work the random keys are generated and the other user cannot identify the keys which are multiple in count and complexly combined.

REFERENCES

1) A Trusted IaaS Environment with Hardware Security ModuleJinho Seol, Student Member, IEEE, Seongwook Jin, Student Member, IEEE.
2) Daewoo Lee, Jaehyuk Huh, Member, IEEE, and Seungryoul Maeng, D. G. Murray, G. Milos, and S. Hand, “Improving xen securitythrough disaggregation,” in Proc. 4th ACM SIGPLAN/SIGOPS Int.Conf. Virtual Execution Environ., 2008, pp. 151–160.
3) L. Chunxiao, A. Raghunathan, and N. Jha, “Secure virtualmachine execution under an untrusted management OS,” in Proc.IEEE 3rd Int. Conf. Cloud Comput., 2010, pp. 172–179.
4) S. Butt, H. A. Lagar-Cavilla, A. Srivastava, and V. Ganapathy,“Self-service cloud computing,” in Proc. ACM Conf. Comput. Commun.Security, 2012, pp. 253–264.
5) J. Kong, “Protecting the confidentiality of virtual machines against untrusted host,” in Proc. Int. Symp. Intell. Inf. Process. Trusted Com-put., 2010, pp. 364–368.
6) TCG architecture overview, version 1.4. [Online]. Available: http://www.trustedcomputinggroup.org/resources/
7) B. D. Payne, M. D. de Carbone, and W. Lee, “Secure and flexible monitoring of virtual machines,” in Proc. 23rd Annu. Comput. Security Appl. Conf., 2007, pp. 385–397.
8) C. Li, A. Raghunathan, and N. K. Jha, “A trusted virtual machine in an untrusted management environment,” IEEE Trans. Serv. Comput., vol. 5, no. 4, pp. 472–483, Fourth Quarter 2012.
9) Y. Xia, Y. Liu, H. Chen, and B. Zang, “Defending against VM roll-back attack,” in Proc. 42nd IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops, 2012, pp. 1–5.
10) Amazon elastic compute cloud (EC2). [Online]. Available: http:// aws.amazon.com/ec2/
11) J. Choi, J. Park, J. Seol, and S. Maeng, “Isolated mini-domain for trusted cloud computing,” in Proc. 13th IEEE/ACM Int. Symp. Clus-ter, Cloud Grid Comput., 2013, pp. 194–195.
12) A.Baldwin, C. Dalton, S. Shiu, K. Kostienko, and Q. Rajpoot, “Providing secure services for a virtual infrastructure,” ACM SIGOPS Oper. Syst. Rev., vol. 43, no. 1, pp. 44–51, Jan. 2009.