Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Survey on Encryption and Improved Virtualization Security Techniques for Cloud Infrastructure

Koushik Akkinapalli[1] and R. Rajeswara Rao[2]

[1] SITAM

Received: 12 December 2013 Accepted: 3 January 2014 Published: 15 January 2014

Abstract

Cloud Computing is one of the latest developments in the IT industry which offers on-demand services without requiring to create an IT infrastructure. It provides scalability, high performance and relatively low cost feasible solution for organizations. Despite of all its advantages, security is still a critical challenge in cloud computing paradigm. This paper presents a survey on some possible techniques used for encrypting user data and also providing techniques used in improving virtualization security for the cloud infrastructure.

Index terms— cloud computing, scalability, security, virtualization.

1 Introduction

loud Computing is an upcoming model which provides on-demand access to the resources provided on the network for different users accessing the service from the cloud in an efficient manner **??**1].The main advantages of cloud computing are providing increased scalability, providing cost effective services to users, customization of applications in an efficient manner, providing better storage space for users etc [2,12].

The different service models provided by the cloud are Software as a Service (Saas), Platform as a service (Paas), Infrastructure as a service (Iaas). In Saas model CSP(cloud service provider) provides the capability of controlling the applications running on the cloud. The benefits of this model are providing better administration, compatibility, collaboration among different users. In Paas model, CSP provides an infrastructure for deploying the applications which have been developed using programming languages that are specified. The benefits of this model are costs can be reduced and up gradation of different services can be done in an optimized manner. In Iaas model, CSP provides the necessary resources for deploying the consumers systems and applications. The benefits of this model are different administrative tasks can be automated in an optimized manner and better services based on policies [1, 3,13].

There are several deployment models which are emerged as cloud came into existence. A The features of an ABE are listed below ? providing confidentiality for user's data.

? providing fine-grained access control for the user's data.

2 b) Homomorphic Encryption

It is promising research area and also cryptographic technique where complex mathematical computations are performed on encrypted data without decrypting them using user's private key. The different steps in performing Homomorphic encryption is summarized below where + and * denotes two algebraic operations.

? Let rÑ?"M be prime number chosen from M which is large and also taken as a secret key. ? Let p and q be two arbitrary integers with (p,q)<rÑ?"M.

? Encryption of p and q can be performed which is shown below. p'=p+(t1*r) where t1Ñ?"M is random large integer q'=q+(t2*r) where t2Ñ?"M is random large integer ? p'+q'=p+(t1*r)+q+(t2*r) and when performing decryption on mod r gives p+q(additive homomorphism) ? p'*q'=p+(t1*r)*q+(t2*r) and when performing decryption on mod r gives p*q(multiplicative homomorphism) iv.

3 Example Explanation of Homomorphic Encryption

Given r=7,p=2,q=3,t1=4 and t2=5 p'=p+(t1*r)=2+(4*7)=30 q'=q+(t2*r)=3+(5*7)=38 (p'+q')mod r=(30+38)mod7=68mod 7=5(p+q) (p'*q') mod r= (30*38)mod7=1140mod 7=6(p*q)[16]. v. Advantages ? provides confidentiality, integrity and data protection.

? reduces the burden to cloud providers each time in decrypting the data in cloud.

4 c) Cloud Computing Confidentiality Framework

The steps for the framework are summarized below ? Identify business goals and objectives.

? Perform impact analysis i.e., identification of system and processes in organization, Secure Virtualization using Split Visor Architecture?

Most Intel processors operate in two modes ? Virtual machine extension (VMX) root mode.

? VMX non root mode.

Split visor runs in VMX root mode where as Guest Visor and VM's runs in the VMX non root mode shown in the fig below [20].

Guest Visor VMC's (data structure maintaining the control information of VMX transition)is controlled by the split visor and VM's VMC's is controlled by Guest Visor.

5 IV. Secure Virtualization using Security and Reliability Monitors

There are two features introduced for increasing security performance in virtualization technology using security and reliability monitoring units [19] a) VSEM b) VREM.

There are two more units(hypervisor security monitor(HSEM) and hypervisor reliability monitor(HREM) available in hypervisor level). The proposed architecture is shown in fig below [19] It identifies attacks and malicious behavior of the virtual machine by helping HSEM. It is generally operated at two levels [19] ? In Level1, VSEM's monitor their own VM's. The proposed system identifies the VM as attacker if hypervisor recognizes the number of service requests more than specified threshold then VSEM notifies HSEM and switches to Level2[19] ? In Level 2, it monitors and captures the activity of each VM where hypervisor sets activity limits for types of activities until HSEM notifies that VM is not an attacker. HSEM gets the reliability status from VREM [19].

6 b) VM Reliability Monitor(VREM)

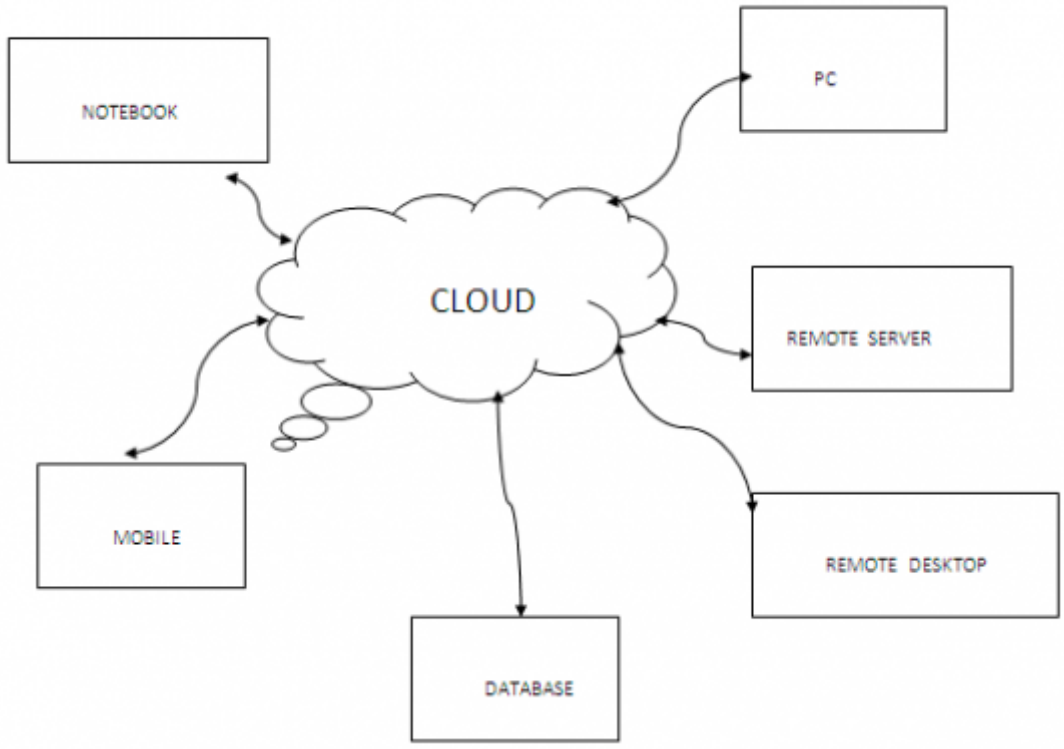
Reliability requirements such as workload have been monitored and load balancer is being notified (within the hypervisor) that sends the workload status to HREM and decides to give VM more resources or not. The proposed HREM detects the overflow attacks if any when VM requests more resources than specified value [19].

i. Advantages ? The proposed architecture safeguards each virtual machine against all the possible attacks.

7 Conclusion

Cloud computing is an emerging technology which provides on demand-resources to customers. It provides high performance, scalable nature and low cost feasible solution to all the customers. Security is still major concern in cloud computing and it has to be provided with an utmost priority to the customers. Encryption techniques have been illustrated for securing the data hosted in cloud. This paper also illustrated techniques in improving virtualization security for cloud environment. [1]

Figure 1:



1

Figure 2: Figure 1 :?

Figure 3:

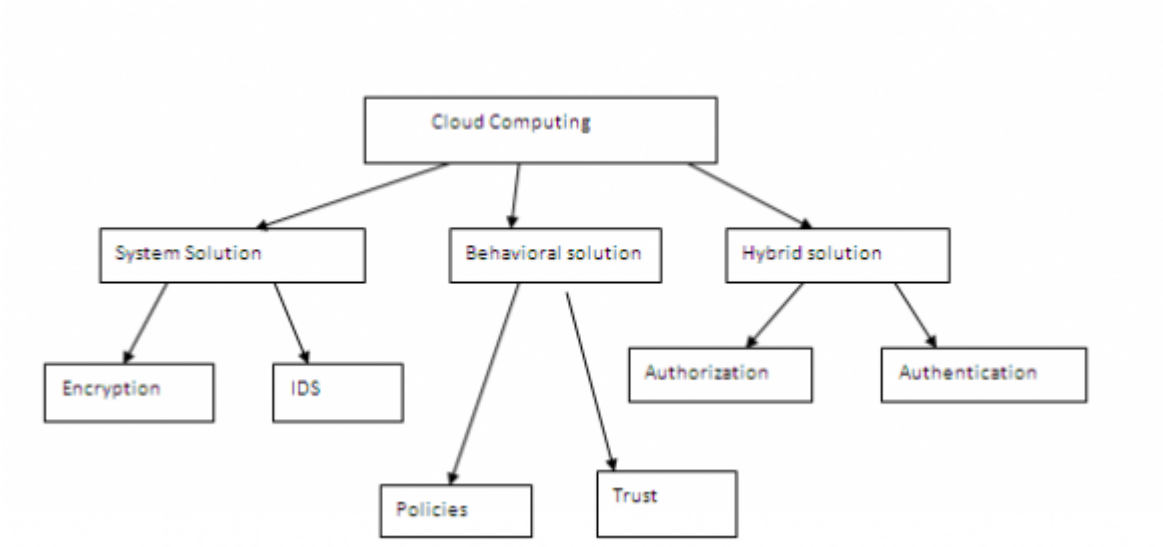
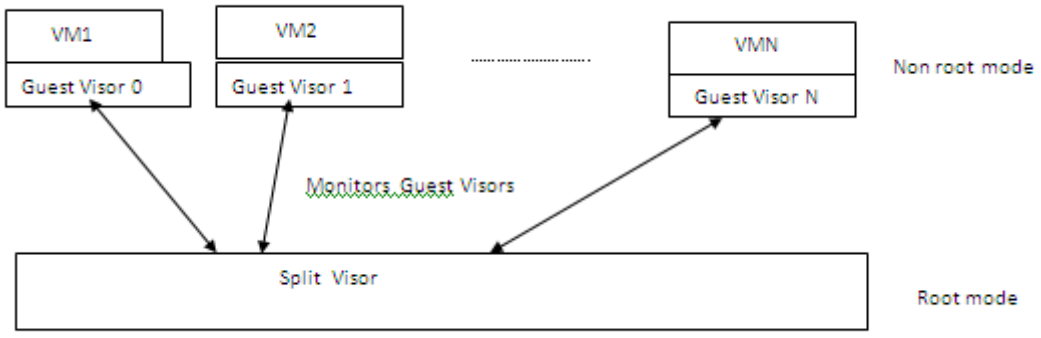
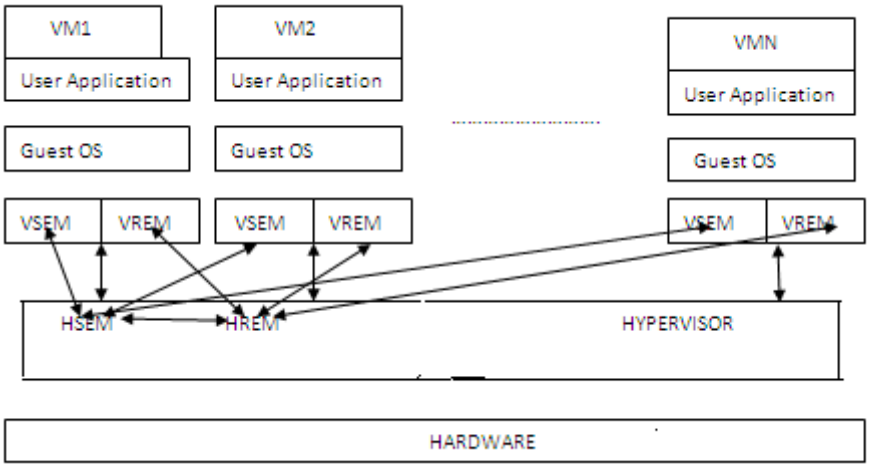


Figure 4: A



2

Figure 5: Figure 2 :



4

Figure 6: Figure 4 :

[Cloud computing security issues and challenges by kuyoro s.o.ibikunle f,awodele o] *Cloud computing security issues and challenges by kuyoro s.o.ibikunle f,awodele o*,

[computing security requirements and solutions: systematic literature review by Patrick Honer] *computing security requirements and solutions: systematic literature review by Patrick Honer*, University of Twente.

[Enhancing security for secure cloud computing environment by divya chaudary on (2013)] *Enhancing security for secure cloud computing environment by divya chaudary on*, august 2013.

[Qi Li JianfengMa Rui Li Ximeng Liu Jinbo Xiong (ed.) (2013)] *Improving security and efficiency for multi-authority access control system in cloud storage by*, `http://eprint.iacr.org/2013/265.pdf.11` Qi Li JianfengMa Rui Li Ximeng Liu Jinbo Xiong (ed.) November 18, 2013.

[Improving Virtualization security by splitting Hypervisor into smaller components by wuqiong pan, yulong zhang] *Improving Virtualization security by splitting Hypervisor into smaller components by wuqiong pan, yulong zhang*, (meng yu and jiwu jing)

[Revisiting cloud security issues and challenges by vaishali singh and s.k.pandey on ()] *Revisiting cloud security issues and challenges by vaishali singh and s.k.pandey on*, July2013.

[Secure role based data access control in cloud computing by v.satya preiya, r.pavitra and dr (2011)] *Secure role based data access control in cloud computing by v.satya preiya, r.pavitra and dr*, june 2011.

[Secure virtualization for cloud environment using hypervisor based technology by farzad sabahi, member IEEE on (2012)] *Secure virtualization for cloud environment using hypervisor based technology by farzad sabahi, member IEEE on*, February 2012.

[Towards securing apis in cloud computing by kumar gunjan, r.k.tiwari and g.sahoo] *Towards securing apis in cloud computing by kumar gunjan, r.k.tiwari and g.sahoo*,