Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 14 Issue 2 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

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

By Koushik Akkinapalli & R. Rajeswara Rao
SITAM, India

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.

Keywords: *cloud computing, scalability, security, virtualization.*

GJCST-B Classification : *E.3, D.4.2*

Strictly as per the compliance and regulations of:

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

Koushik Akkinapalli [α] & R. Rajeswara Rao[σ]

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.**

Keywords: cloud computing, scalability, security, virtualization.

I. Introduction

Cloud 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 cloud deployment model specifies the location for physical servers that have been deployed. The deployment models are private cloud, community cloud, Public cloud and hybrid cloud [1]. In private cloud, only one organization makes use of services in the cloud. In community cloud, organizations with similar requirements shared cloud infrastructure. In public cloud, computing resources are accessible to all the users utilizing cloud services owned by the organization. In hybrid cloud, different deployment models are combined with various cloud infrastructures. [3].

The different services provided by the cloud are shown in fig below.

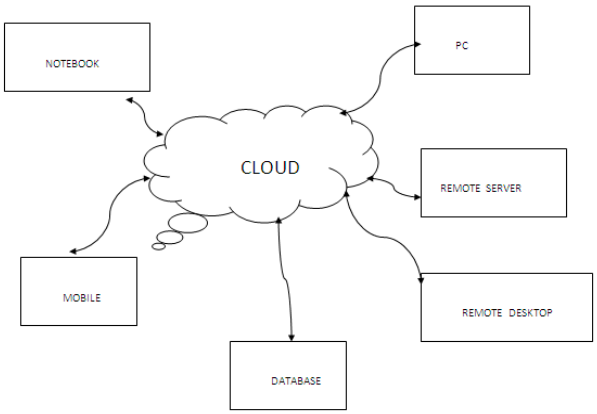

Figure 1 : Cloud Services

II. Encryption

It is the process of providing security to the user's data in such way that only authorized users can only access it. The several possible encryption techniques used for securing user's data in the cloud are given as follows[4,5].

- Attribute Based Encryption(ABE)
- Homomorphic Encryption.
- Cloud Computing Confidentiality Framework

a) *Attribute Based Encryption*

It is a cryptographic technique where encryption and decryption of data in the cloud is based on user's attributes and several access policies have been defined based on their attributes. The access policies can be classified into two types[6,7,8]

Author α: Asst Professor, Dept of CSE, SITAM, Vizianagaram, A.P., India. e-mail: akkinapallik@gmail.com
Author σ: Associate Professor, Dept of CSE, JNTUK, Vizianagaram, A.P., India. e-mail: raob4u@yahoo.com

- Key –policy ABE
- Ciphertext-policy ABE

The features of an ABE are listed below

- providing confidentiality for user's data.
- providing fine-grained access control for the user's data.
- Scalability
- providing user accountability
- preventing against collusion attacks[6].

i. *Process of ABE*

The process of ABE involves the following steps. The steps are summarized below

- The set of attributes are defined for different users hosting their data in the cloud.
- The key authority generates public key and master secret key for given set of attributes in order to encrypt the user's data
- The user is eligible to decrypt the encrypted data if number of attributes in user's data private key matches with set of attributes in encrypted data by specifying threshold value[6,9,10,11].

ii. *Key Policy ABE*

In this scheme access policy is built into user's private key and encrypted data is described with attributes of different users.

iii. *Advantage*

It provides more flexibility for controlling different users.

iv. *Disadvantage*

In this scheme, key authority can't decide the particular user who can decrypt the data [6,8].

v. *Ciphertext Policy ABE*

It overcomes the problem in Key policy ABE by building access policy directly into the encrypted data so that key authority can decide the particular user that can decrypt the data[6,8].

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 essential characteristics of Homomorphic encryption are given below[14,16,17].

- It is scalable cryptographic technique operating on any type of data hosted in the cloud.
- This scheme applies only to cloud providers.
- No authentication mechanism is needed.

i. *Homomorphism*

Let (A,+) and (B,*) be the two groups and there exists a relation f:A->B then f is group homomorphism in A and B if $\forall x,y \epsilon$ A such that f(x+y)=f(x)*f(y)[15].

ii. *Applications*

- Analyzing Biometric information
- Medical Analysis
- Marketing Analysis
- Survey Analysis

iii. *Process of Homomorphic Encryption*

The different steps in performing Homomorphic encryption is summarized below where + and * denotes two algebraic operations.

- Let $r \epsilon M$ 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 $(p,q) < r \epsilon M$.
- Encryption of p and q can be performed which is shown below.

$p' = p + (t1 * r)$ where $t1 \epsilon M$ is random large integer

$q' = q + (t2 * r)$ where $t2 \epsilon M$ 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. *Example Explanation of Homomorphic Encryption*

Given r=7,p=2,q=3,t1=4 and t2=5

$p' = p+(t1*r) = 2+(4*7) = 30$

$q' = q+(t2*r) = 3+(5*7) = 38$

$(p'+q') \bmod r = (30+38) \bmod 7 = 68 \bmod 7 = 5 (p+q)$

$(p'*q') \bmod r = (30*38) \bmod 7 = 1140 \bmod 7 = 6 (p*q)$[16].

v. *Advantages*

- provides confidentiality, integrity and data protection.
- reduces the burden to cloud providers each time in decrypting the data in cloud.

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,
- Data and system classification specifies what data needs to be secured and how valuable data and information systems are.
- Select security control selection of system along with data protection.
- Define the limitations in system taking into account trust, policy, system task and data protection dimensions
- Specify cloud security solutions (system, behavioral and hybrid) shown in fig below and make decision on cloud architecture [18].

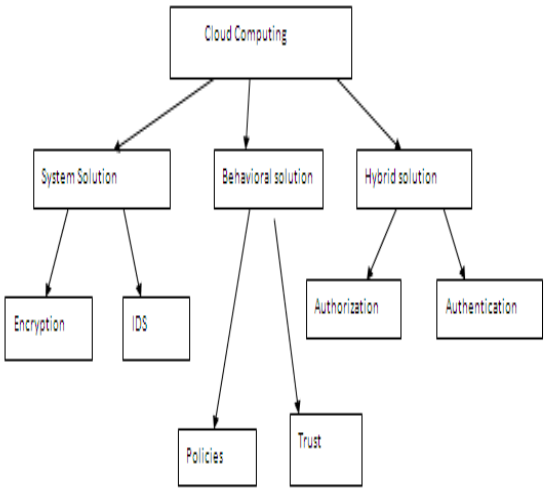

Figure 2 : Cloud Computing Confidentiality Framework

i. *Advantages*

- It provides authentication, confidentiality, integrity and data protection.
- It explains effective security controls for protecting data in private cloud environment

III. 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].

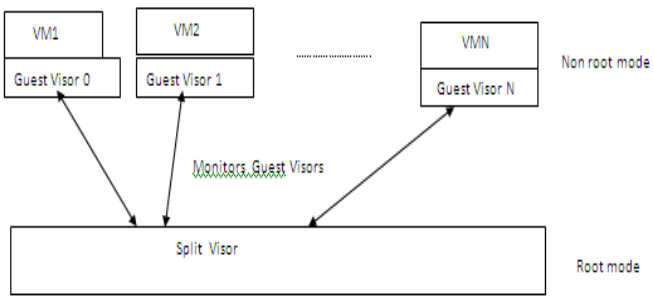

Figure 3 : Split Visor

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.

a) Advantage

- It is more secured architecture which is responsible for isolation between different users VM's.

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]

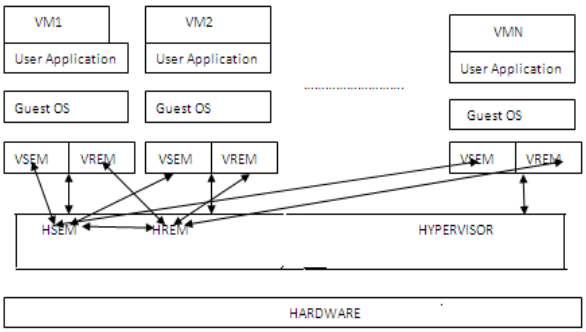

Figure 4 : VSEM And VREM

a) VM Security Monitor (VSEM)

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].

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.
- The proposed architecture provides efficient way for reducing the workload from hypervisor based virtualization.
- It also decentralizes the security related tasks between hypervisor and VM's [19].

V. 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.

References Références Referencias

1. Cloud computing security requirements and solutions: systematic literature review by Patrick Honer, University of Twente.
2. Revisiting cloud security issues and challenges by vaishali singh and s.k.pandey on July2013.
3. Cloud computing security issues and challenges by kuyoro s.o.ibikunle f,awodele o.
4. http://searchsecurity.techtarget.com/definition/encry -ption.
5. computer.howstuffworks.com/encryption.htm.
6. http://ijns.femto.com.tw/contents/ijns-v15-n4/ijns 2013-v15-n4-p231-240.pdf.
7. http://www.cs.uiuc.edu/class/fa07/cs498mmp/prese ntations/john.pdf.
8. http://www.slideshare.net/prosunjit/attribute-based - encryption.
9. http://cs.brown.edu/~mchase/papers/multiabe.pdf
10. http://eprint.iacr.org/2013/265.pdf.
11. Improving security and efficiency for multi-authority access control system in cloud storage by Qi Li JianfengMa Rui Li Ximeng Liu Jinbo Xiong, November 18, 2013.
12. Secure role based data access control in cloud computing by v.satya preiya, r.pavitra and dr.joshi on june 2011.
13. Towards securing apis in cloud computing by kumar gunjan, r.k.tiwari and g.sahoo.
14. http://www.ijarcsse.com/docs/papers/Volume_3/3_ March2013/V3I3-0229.pdf.
15. http://www.slideshare.net/chrisma0/introduction-to- homomorphic-encryption.
16. https://hcrypt.com/downloads/TD-001312.pdf.
17. http://people.csail.mit.edu/vinodv/6892 Fall20 /6892-lec01.pdf.
18. Enhancing security for secure cloud computing environment by divya chaudary on august 2013
19. Secure virtualization for cloud environment using hypervisor based technology by farzad sabahi, member IEEE on February 2012.
20. Improving Virtualization security by splitting Hypervisor into smaller components by wuqiong pan, yulong zhang,meng yu and jiwu jing.