ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Online - 2455-3891
Print - 0974-2441

Special Issue (April)

Full Proceeding Paper

AN AUTHENTICATED, SECURE VIRTUALIZATION MANAGEMENT SYSTEM IN CLOUD COMPUTING

DINESH KUMAR K, UMAMAHESWARI E

Department of CSE, Research Scholar, SCSE, VIT University, Chennai, Tamil Nadu, India. Email:asha.s@vit.ac.in

Received: 23 January 2017, Revised and Accepted: 03 March 2017

ABSTRACT

Cloud computing is one of the trending technologies that provide boundless virtualized resources to the internet users as an important services through the internet while providing the privacy and security. Using these cloud services, internet users get many parallel computing resources at low cost. It predicted that till 2016, revenues from the online business management spent $4 billion for data storage. Cloud is an open-source platform structure, so it is having more chances to malicious attacks. Privacy, confidentiality, and security of stored data are primary security challenges in cloud computing. In cloud computing, "virtualization" is one of the techniques dividing memory into different blocks. In most of the existing systems, there is only single authority in the system to provide the encrypted keys. To fill the few security issues, this paper proposed a novel authenticated trust security model for secure virtualization system to encrypt the files. The proposed security model achieves the following functions: (1) allotting the VM security monitor model for each virtual machine and (2) providing secret keys to encrypt and decrypt information by symmetric encryption. The contribution is a proposed architecture that provides a workable security that a cloud service provider can offer to its consumers. Detailed analysis and architecture design presented to elaborate security model.

Keywords: Cloud computing, Authentication, Encryption, Confidentiality, Virtualization.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19544

INTRODUCTION

Distributed systems as an area of research have seen a high growing progress for the past few years, driven by the use of new use cases to technical improvements. Cloud computing [1] is one such a famous model that has progressed from the adopting of utility computing, service oriented architectures, and virtualization. In other words, cloud is a storage remote location. Cloud can provide the services over private or public networks, i.e., local area network, metropolitan area network, wide area network, and virtual private network. Cloud computing refers to manipulating, accessing, and configuring the software and hardware resources remotely. Cloud computing is featured by those users who can easily utilize the platforms [2], for example, operating systems and middleware services, infrastructure, for example, networks, servers, and storages, and software's. In cloud computing service environments, two users play vital role: Cloud service providers and cloud users or consumers. One side, cloud provider maintains the huge computing services in their large server centers [2] to cloud users on the rent-usage basis. On the other side, there are cloud consumers use services from cloud owner to deploy their applications. First, a consumer will check the services, those services are suitable for their applications, and then, consumer sends a request for services to a cloud owner. When the cloud owner receives the user requests, will assign the required resources to the user as a cast of guest virtual machines (VMs) [3]. Then, the consumer will use the allotted resources to deploy their applications and pay for the services that are utilized by them.

In general, cloud consumers can run different applications and dissimilar operating systems in their VMs. The applications and operating systems may contain security vulnerabilities [4]. In cloud computing, there are several consumers on the similar physical machine operating system sharing resources in infrastructures. The susceptibilities in applications and other operating systems can be damaged by an attacker to create many types of vulnerabilities. In many existing systems, there is only single authority in the infrastructure system to provide the encrypted keys. In most of the existing system used, a single authority in issuing all the encrypted keys and the key escrow problem another issue. One physical machine has a divided into many VMs, for these machines, only one security model providing the encrypted keys that means there were several authorities and one central authority. In some cases, keys from different authorities were bound together by this identity to resist the collusion attack.

Aiming at efficiently solving the problem of collusion of encrypted keys with allotting the different security model for each VM. Unlike many existing systems, this VM security monitoring (VSM) model presents different security model to provide encryption keys. Next, each VM having different security model, this model generates the keys to encrypt the data. Furthermore, it enhances existing system in security. Specifically, it presents the advanced symmetric encryption to support robust security by encrypting the file with dissimilar privilege keys.

LITERATURE REVIEW

In this section, current works presented the two following aspects: (a) Related work and (b) motivation.

Related work

In cloud service provider environment, VMs from various organizations have to be organized on the single physical server to maximize the efficiencies of virtualization. Today, most of the organizations are looking toward to expand their services in cloud computing infrastructure, but most cannot afford the risk of compromising the privacy of their information and applications. Virtualized domain launches its own set of threats and vulnerabilities that include harmful operations between VMs and physical machines. Such as, from the cloud computing model view, serving models are depend on each other service model. The software applications are installed over the platform environment and the platform depends on the infrastructure model. This dependency of serving models on each other creates problems regarding security and privacy [24].

There can be strikes from attackers on the user VMs [6]. That is, attacker can manipulate the susceptibilities in the user VM for attacking reasons. Such attacks can effect on both user and the cloud structure. For example, threats such as VM enable another VM to allow the susceptibilities and

attacks in the VM supervisor and allow accessing the information from the main operating system. The malicious attacker can execute the DoS attacks by going down the server. There are so many chances are there to attack the system.

Based on advanced cloud protection system is proposed in [7] that main aim at rendering efficiency regarding privacy to the cloud environment resources. The advanced cloud protection system provides several privacy models to the cloud service provider resources besides network system against attacks on consumer and cloud service provider data. Advanced cloud protection system also provides audit ability for the activities of VMs. The advanced cloud protection system module is classified into many modules situated at the main operating system. This advanced cloud protection system model does not intimate when encrypted keys are colloid, that is, a big drawback of this module. Another proposed module for security tool, called cyber Guarder [8] offers VM network privacy and security through the virtual network devices deployment module. This VM security tool provides the virtual private network between VMs. This information is transferred through virtual private network bridge. However, in this module, authors are not concentrated on more security for information when passing through virtual network bridge. Wu *et al*. [9] proposed a virtual network model that provides safeguard against spoofing and sniffing attacks. In that model, they used hypervisor for virtual network configuration. However, the main drawback is virtual network model is considering security issues, which they are mentioned above. He *et al*. proposed cloud network security solution [10] by following a tree-rule firewall. They concentrated on firewall security. In this module, specified security policy is allotting for firewall system that stops the intruder attacks. However, this firewall security model is not concentrated on VM security and privacy. Xing *et al*. [11] proposed a system, SnortFlow for attacker prevention in cloud computing environment. This SnortFlow module is also implemented in Xen-based cloud. This module is mainly concentrated on controlling suspect traffic. Sometimes, authorized data also suspected by SnortFlow module. Wei *et al*. [12] proposed Mirage; this module is used for VM image management system for cloud environment. This Mirage provides security to the VM images. However, drawback is this module has filters for suspect's data; sometimes, these filters remove the data, which is infected by malware. In this case, users lose the required data. In VM escape [13], the authors proposed encrypted virtual disk images in cloud environment that provides the security and encryption to secure the VM images on the disk. This model is mainly used for encryption for VM images. These encrypted images are stored in disk, when malware attacks happen, attacker accessing the all VM images because all images are stored in disk space. Emura *et al*. [14] proposed the security policy in this scheme number of attributes in users private key and access policy of cipher text must be same. If both things are not match, then consumer will lose their informationbecause sometimes the user will not get the proper keys from encryption technique. Another constant size cipher text policy was proposed in [15], encryption and decryption techniques are not efficient; in that case, security was reduced to encrypt and decrypt the file. Next, security scheme was proposed [16] based on decisional Bilinear Diffie-Hellman problem. This scheme worked for, policy must be same of attributes in a private key, and had a high secure decryption technique.

Motivation

Motivated by these defects in most of the existing security models proposed a new security monitor model for monitoring each VM. The approach investigates the security and privacy of VM in the cloud computing environment from a global perspective. It also takes into account the privacy of heterogeneity in the VM environment as well as different symmetric encryption techniques. Furthermore, device algorithm to assist the VM for encryption and decryption techniques. Finally, the main approach is independent, lightweight and easy to deploy because its implementation is very simple.

PROPOSED SCHEDULING APPROACH

This section starts with the representation of the model of the proposed security model approach followed by a detailed description of the security model. Then focused on, the algorithm of encryption technique.

Proposed security model

The model of the proposed security model is shown in Fig. 1. It consists of different VMs allotted in single physical machine. The security module is responsible for providing security module for allotted VM. First, the security module determines whether VM is allotted or not. Once VM is allotted, it will send the information to main security module to allot the security model for new VM.

The overall workflow of this model can be roughly elaborated as: The VM pool contains different VM allotted by host operating system. The prediction security model collected the data from monitoring model, which is continuously monitoring regarding allotted VMs. Based on data, which is sent by monitoring model, prediction security model predict the information [22] and send the information to allocation model. According predicted data, allocation model will allot the security model for each and every VM.

Model description

VSM model, called as prediction security model developed for predicting the allocation of VM. Dinda [15] proposed one model to describe about CPU load. Motivated by this, used mathematical formula to predict resource usage in a period of time. In proposed model, used Iterated Function System (IFS) [5]. By using IFS collage theorem, can perform transformation checking to a given set and paste the results in model. Barnsley and Harrington [16] proposed another model to assist IFS, called fractal interpolation theory. By using, this method can perform deterministic iteration to any point and can get the attractor.

Algorithm 1

1. Procedure BUILDIFSFORDAY (D)
2. i = 0
3. StartTime = T_{now} - (N_a-1)*I
4. While startTime!= T_{now} do
5. CreateNewLogDataSet(i)
6. i = i + 1
7. StartTime = startTime+I
8. End while
9. j = 0
10. While j!= N_a do
11. Create normalized data set(j)
12. j = j + 1
13. End while
14. Build IFS(D)
15. For i from 0 to N_s step 1 do
16. Build IFS for day(S^i)
17. End for
18. End procedure.

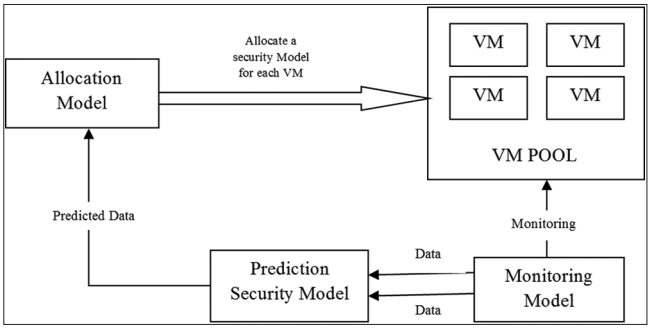

Fig. 1: Model of the proposed security model

Table 1: Parameters description

Symbol	Description
N_s	The number of similar days
N_a	The number of interpolation points
S^i	The i^{th} similar day
I	The interval between interpolation points in minutes
T_{now}	The current time

In the above algorithm D, will calculate the days for VM. Build IFS procedure generates IFSs for current day. Then, these IFS are aggregated into single IFS [5] with weight through create normalize data set procedure. Start time will note the allotted VM time and create the details in create new log data set. After calculation load of the VM pool, it will send the details to allocation model. Finally, allocation model will allot the security model for each VM.

Encryption technique

This section defines some secure primitives used in proposed security allocation model. For providing the security and privacy in the cloud environment, following symmetric encryption technique. This, technique uses a privacy key m to encryption and decryption of cloud data. This symmetric encryption method follows three functions:

a. KeyG (1) → m is the key generation algorithm that creates m using security parameter 1;
b. En (m,E) → C is the symmetric encryption technique that collects the privacy key m and message E and then outputs the cipher text C;
c. De (m,C) → E is the symmetric decryption algorithm that collects the secret m and ciphertext C and then outputs the original message E.

Proposed a new technique which could protect the security for predictable information. The main idea of proposed technique is that encryption key generation algorithm. Using hash functions to generate the tag functions and assigning the tags for each encryption key. By using this method, function cannot confuse about encryption keys. The key is define from the file F by using hash function $m_F = H(F)$. The encryption key m_F for file F in our system will be generated with prediction security model.

EXPERIMENTAL EVALUATION

In this experiment, set up has 5 VMs on a cloud simulation tool. The tasks are implemented when all the VMs are connected to the host operating system. VMs pool in every 90 seconds will check about allotted new VM. When a new machine is allotted, that details will be predicted by prediction security model. Then, allocation model will allot the security model for each VM to provide the encryption technique.

The prediction model measures the load balance of VM pool by using IFS model. The individual VMs standard deviation is considered for load balance calculation and sends the details to prediction security model.

RESULT ANALYSIS

All the values are concerned with the cloud simulation environment. This results will be help full to predict the load balance information regarding host operating system. In that case allocation model predict the information, which is sent by prediction security model, then allot the separate security model for each VM. Each different security model, producing the different encrypted keys for secure data. In that encryption model each encrypted key attached with tags by using hash function. For example, the security model 1, produces encrypted keys like Ak_1, Ak_2, Ak_3, Ak_4, same like that the security model 2, produces encrypted keys like Bk_1, Bk_2, Bk_3, Bk_4. By using this method, user cannot get wrong encrypted keys. This model is very simple to implement in all host operating systems.

CONCLUSION

In this proposed system, the prediction security model is very help full for to predict the information of VM pool. By using method, provider can predict the information easily regarding allotted VMs and provider will allot the separate security model for each VM. In encryption technique also used hashing technique to tag the encrypted keys, to avoid collusion among encrypted keys. This method will be very use full in heterogeneous cloud environment.

REFERENCES

1. Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, *et al*. Eucalyptus Open-Source Cloud Computing Infrastructure-An Overview. In: Proceeding IEEE/ACM International Symposium Cluster Computing Grid; 2009. p. 124-31.
2. Bari MF. Datacenter network virtualization: A survey. IEEE Commun Surv Tutor 2013;15(2):909-28.
3. Wei B, Lin C, Kong XZ. Dependability Modeling and Analysis for the Virtual Data Center of Cloud Computing, In Proceeding IEEE 13th International Conference High Performance Computing and Communications (HPCC), Banff, AB, Canada; 2011. p. 784-9.
4. "VM Escape." Available from: http://www.zdnet.com/blog/security/us-cert-warns-of-guest-to-host-vm-escape-vulnerability/12471.
5. Duan H, Chen C. Energy-aware scheduling of virtual machines in heterogeneous cloud computing systems. Future Gener Comput Syst 2016;???:???.
6. Juncheng P, Huimin D, Yinghui S, Dong L. Potential attacks against k-anonymity on LBS and solutions for defending the attacks. In: Advanced in Computer Science and its Applications. Berlin, Heidelberg: Springer; 2014. p. 877-83.
7. Lombardi F, Pietro RD. Secure virtualization for cloud computing. J Netw Comput Appl 2011;34(4):1113-22.
8. Li J, Li B, Wo T, Hu C, Huai J, Liu L, *et al*. Cyber-guarder: A virtualization security assurance architecture for green cloud computing. Future Gener Comput Syst 2012;28(2):379-90.
9. Wu H, Ding Y, Winer C, Yao L. Network Security for Virtual Machine in Cloud Computing. In: 5th International Conference on Computer Sciences and Convergence Information Technology; 2010. p. 18-21.
10. He X, Chomsiri T, Nanda P, Tan Z. Improving cloud network security using the tree-rule firewall. Future Gener Comput Syst 2014;30:116-26.
11. Xing T, Huang D, Xu L, Chung C, Khatkar P. Snortflow: A Openflow-Based Intrusion Prevention System in Cloud Environment. In: IEEE Research and Educational Experiment Workshop; 2013. p. 89-92.
12. Wei J, Zhang X, Ammons G, Bala V, Ning P. Managing Security of Virtual Machine Images in a Cloud Environment. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security; 2009. p. 91-6.
13. Kazim M, Masood R, Shibli MA. Securing the Virtual Machine Images in Cloud Computing. In: Proceedings of the ACM 6th International Conference on Security of Info and Networks; 2013. p. 425-8.
14. Emura K, Miyaji A, Nomura A. A Ciphertextpolicy Attribute-based Encryption Scheme with Constant Ciphertext Length, Information Security Practice and Experience-Fifth International Conference. In: Bao F, Li H,Wang G, editors. Lecture Notes in Computer Science F5451. Berlin, Heidelberg: Springer; 2009. p. 13-23.
15. Dinda PA. The statistical properties of host load. Sci Program 1999;7(3):211-29.
16. Barnsley MF, Harrington AN. The calculus of fractal interpolation functions. J Approx Theory 1989;57(1):14-34.
17. Umamaheswari E. Cloud testing Vs. Conventional software testing over a web service. Int J Sci Res 2015;4(9):???.
18. Umamaheswari E, Bhalaji N, Ghosh DK. Evaluating metrics at class and method level for java programs using knowledge based systems. ARPN J Eng Appl Sci 2015;10(5):2047-52.
19. Bobba R, Khurana H, Prabhakaran M. Attribute-sets: A practically motivated enhancement to attribute-based encryption. In: Computer Security ESORICS. Berlin, Heidelberg: Springer; 2009. p. 587-604.
20. Kim DS, Machida F, Trivedi KS. Availability Modeling and Analysis of a Virtualized System. In: Proceedings 15th IEEE Rim International Symposium Dependent on Computers. Shanghai, China; 2009. p. 365-71.
21. Gomes L, Costa A. Cloud Based Development Framework Using IOPT Petri Nets for Embedded Systems Teaching. In: Proceeding 2014 IEEE 23rd International Symposium Industrial Electron (ISIE). Istanbul, Turkey. p. 2202-6.
22. Umamaheswari E, Ghosh DK. Developing a reliability prediction

system using multivariate analysis theory on software quality metrics. Int J Emerg Technol Comput Sci Electron 2013;3(1):11-4.
23. Ajay DM, Umamaheswari E. Why, how cloud computing - How not, and cloud security issues. Glob J Pure Appl Math 2016;12(1):1-8.
24. Ajay DM, Umamaheswari E. An Initiation for Testing the Security of a Cloud Service Provider, Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC-16); 2016.
25. Ghosh DK, Bhalaji N, Umamaheswari E. Software engineering measures using radial basis function neural network. Int J Appl Eng Res 2014;9(23)