International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 635-644
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Safe and Trustworthy VMS for Cloud Computing Applications

[1] Ch.Srividya , [2] A.Lakshmi , [3] A.Umadatta
[1]Department of Computer Science Engineering, Institute of Aeronautical Engineering,
Dundigal, Hyderabad, India. Chsrividya12@gmail.com
[2,3]Department of Information Technology, Institute of Aeronautical Engineering,
Dundigal, Hyderabad. alurilakshmi@gmail.com, umadattaa@gmail.com

Abstract - Access control, Availability, Confidentiality, Security of stored data and trust are among the primary security aspects in cloud computing. In most existing system there is only single authority in the system to provide the encrypted keys. To fill the few security issues, this paper proposes a novel authenticated trust security model for secure virtualization system to encrypt the files. The proposed security model achieves the following function: 1) allotting the VSM(VM Security Monitor) model for each virtual machine.Our main contribution is a security architecture that provides a flexible security that a cloud service provider can offer to its consumers. Detailed analysis and architecture design presented to elaborate security model.

Distributed and Cloud computing are the two emerging technologies that gives boundless "Virtual Resources" to web users as administrations or services over the entire web, while giving security and protection. In recent years, cloud service providers offer a gigantic storage systems and parallel processing resources with less cost. As indicated by IHS survey, overall the organizations are spending 190 billion dollars for the cloud services and its infrastructure. Cloud is an open platform structure, and it's continuous and defenceless attacks are a major issue in this area. Access control, Availability, Confidentiality, Security of put away information and trust are among the essential security angles in distributed computing. In most existing framework there is just single specialist in the framework to give the scrambled keys. To fill the few security issues, this paper proposes a novel confirmed trust security display for secure virtualization framework to encode the documents. The proposed security demonstrate accomplishes the accompanying capacity: 1) dispensing the VSM (VM Security Monitor) display for each virtual machine. Our primary commitment is a security engineering that gives an adaptable security that a cloud specialist organization can offer to its buyers. Detailed investigation and design architecture are exhibited to expand security demonstrate.

Keywords:Cloud Computing, Access control, Encryption, Confidentiality, Virtualization.

1. INTRODUCTION

Distributed Systems as an area of research has seen a high growing progress for past few years, driven by the use of new use cases to technical improvements. Cloud computing [1] is one such famous model that has progressed from the adopting of utility computing, service oriented architectures and virtualization. Cloud computing is a new trend computing model to provide

convenient, on-demand network access for shared pool of configurable computing resources such as servers, services, storage, applications and networks resources that could be provisioned and released with minimal provider management effort or services provider interactions. The term Cloud refers to a Network or Internet. In other words we can say that Cloud is storage remote location. Cloud can provide the services over private and public networks, i.e., LAN, MAN, WAN or VPN. Cloud computing refers to manipulating, accessing and configuring the software and hardware resources remotely. Cloud computing mainly offers the platform independency, as the software is no needed to be installed locally on the PC. Cloud Computing is featured by those users can easily utilize the platforms [2] e.g., operating systems and middleware services, infrastructure e.g., networks, servers and storages, and software's e.g., application programs offered by cloud service providers in an on-demand manner. In cloud computing service environments, two users plays vital role: cloud service providers and cloud users or consumers. On one side, cloud service providers [3] maintain massive computing resources in their largeserversanddatacentres and rent resources out to consumers on a per-usage basis. On the other side, there are consumers who have applications and lease resources from service providers to run their applications. First, a consumer sends a request for computing resources to a cloud service provider. When the cloud service provider receives the request, it looks for resources to satisfy the request and assigns the resources to the requesting user, typically as a form of virtual machines (VMs). Then the consumer utilizes the assigned resources to run their applications and pays for the resources that are used. When the consumer is done with the resources, they are returned to the provider.

In general, in cloud consumers can run different applications and different operating systems in their virtual machines. The operating systems and applications may contain security vulnerabilities [4]. In Cloud computing there are several consumers on the same physical machine operating system sharing resources in infrastructures. The vulnerabilities in applications and operating systemcanbe exploited by an attacker to create different types of vulnerabilities. These attacks can be on cloud infrastructure as well as against other virtual machines belonging to the other consumer. 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 virtual machines, 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.

1.1 Contribution

In this paper, aiming at efficiently solving the problem of collusion of encrypted keys with allotting the different security model for each virtual machine. Unlike many existing systems, this VSM model presents different security model to provide encryption keys. Next, each virtual machine having different security model, this model generate the keys to encrypt the data. Furthermore, we enhance our system in security. Specifically, we present the advanced symmetric encryption to support stronger security by encrypting the file with differential privilege keys.

1.2 Organization

The rest of this paper proceeds as follows. In section 2, we briefly elaborated about the existing security issues. In section 3, we propose the system model for our security model. In section 4, we present the implementation of our prototype and explained about simulation setup. In section 5, we present the evaluation results. Finally we draw conclusion in section 6.

2. LITERATURE REVIEW

In this section, current works presented the two following aspects: (A) Related Work; (B) Motivation.

2.1 Related Work

In cloud specialist organization condition, virtual machines from different associations must be composed on the single physical server with a specific end goal to augment the efficiencies of virtualization. To begin with, cloud specialist co-ops ought to be gain from Managed Service Provider (MSP) show and guarantee that their purchasers applications and data are secure in the event that they want to hold their customer base and aggressiveness. Today the majority of the associations are looking toward to grow their administrations in distributed computing framework, yet most can't bear the cost of the danger of trading off the security of their data and applications. IDC as of late directed a review of 455 IT administrators and their line-of-business (LOB) associates to impart their insights and comprehend their organizations' utilization of IT cloud administrations. Among all issues security positioned first as the best difficulties. Predominantly in virtualizations advances some security dangers and vulnerabilities notwithstanding imparted dangers to the regular IT foundations. Cloud qualities, asset pooling permits the utilization of same pool by numerous purchasers through virtualization advances. In spite of the fact that, the virtual advances present quick flexibility and ideal administration of assets and administrations, they likewise present certain dangers in the framework. Multi occupancy prompts the dangers of information perceivability to other buyer and hint of client activities. Virtualized condition presents its own arrangement of dangers and vulnerabilities that incorporate malevolent tasks between virtual machines and physical machines. For example, from the cloud benefit display see, the administration models are rely upon each other administration show. The SaaS applications are sent over the PaaS condition and the PaaS is relies upon the IaaS. This reliance of administration models on each different makes issues with respect to security and protection. For instance, if an interlopers prevails to take control of PaaS, the outcome will be affected IaaS that is using PaaS. At that point affected IaaS can pass the malevolent to SaaS. The employments of multi shoppers utilizing virtualized assets that may have a place with same physical assets present numerous security issues. The ideal portion of different occupants and apportioned assets is a perplexing task and needs substantially more elevated amount of protection and security. In the accompanying discourse we show the security issues and difficulties being looked by the distributed computing. There are number of works that view the cloud security challenges [5] shape cloud benefit display viewpoint.

A) Shared Infrastructure

Resource pooling characteristic not only results in sharing of storage and computational resource but also allowing the sharing of network infrastructure components. The sharing of network means allow attackers the window of cross tenant attack. But, by resource pooling characteristic attacker activities are increased. The access capability increases the malicious user attacks to another machine.

B) Hypervisor issues

The main module of virtualization is hypervisor. The virtual machine management is the responsibility of the virtual machine monitor. Generating and managing virtual machines, is other function performed by virtual machine monitor. If attacker hand over the virtual machine monitor system then attacker can control all virtual machines. The metadata also can goes under control attacker.

C) Data Privacy

The data in the foundation is substantially more powerless against dangers as far as honesty, accessibility and secrecy in contrast with processing model. On the off chance that number of clients is increment then improvement additionally fundamental for information security. In a common situation, the security quality of cloud levels with the protection quality of its weakest substance. One fruitful assault on a solitary virtual machine will bring about unapproved access to the data of all clients.

D) Data Recovery weakness

Due to flexibility and asset pooling attributes, the cloud permits dynamic and on-request asset giving to the buyer. The administrations designated to a specific purchaser might be

allotedto other client at some later purpose of time. So information recuperation vulnerabilities can lead significant issues to delicate client information.

E) Data Storage Issues

The distributed computing condition display does not give full control over information to clients. The shopper can appreciates restricted level of control just on virtual machines. The downside of control over information brings about enormous information security dangers than the regular figuring model. In distributed computing, virtualization and multi-occupancy drives the conceivable outcomes of assaults.

F) Virtual Machine Migration

The virtual machine movement method is one the well known strategy to procedure of moving a virtual machine to another physical machine without closing down the virtual machine. For the most part, this movement procedure is utilized to support of load adjusting. Amid the movement system, the substance of virtual machine are presented to the system that may drives security and uprightness concerns. The virtual machine relocation is basic procedure and should be done in a secured way.

G) Virtual Machine Image Sharing

A Virtual machine picture is utilized to instantiate virtual machines. A client can make possess virtual machine picture from shared picture vault. By and large virtual machine permits transferring and downloading pictures from store. Sharing virtual machine picture in stores is a typical undertaking. For this situation, vindictive client can hack the code of the picture to search for convenient assault point. Barely any aggressors will present the malware in virtual machine framework. On the off chance that the virtual machine picture isn't legitimately cleaned, it can lead a few issues to the clients.

H) Virtualization Issues

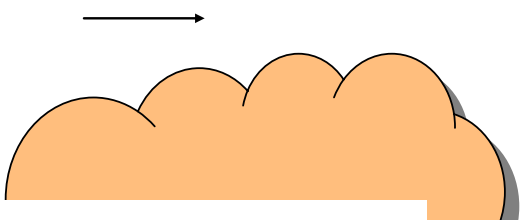
Virtualization procedure is one of the fundamental trademark in distributed computing. Virtualization permits the utilization of single physical asset by various clients. For each client, isolate virtual machine will be designated. A virtual machine screen is the module deals with the every virtual machine and enables different working frameworks to run all the while on the single physical framework. Here disadvantage is, if aggressor control the one virtual machine then they can control whole physical machine setup.

I) Virtualization Network

In distributed computing, virtualization arrange is a coherent system based on single physical system. The virtual systems are in charge of correspondence between virtual machines. The product based system parts, for example, switches and connects, bolster the systems administration of virtual machines over the host. Security instrument over the physical system can't screen the activity over virtualized organize. This turns into a genuine test as malignant exercises of the virtual machines. The virtualized organize is shared among various virtual machines that causes the likelihood of specific assaults, for example, Denial of Service (DoS), ridiculing and sniffing of virtual system.

There can be assaults from clients on the client virtual machines [6]. That is, aggressor can misuse the vulnerabilities in the client virtual machine for malevolent purposes. Such assaults can target both client and the cloud foundation. For instance, assaults, for example, virtual machine escape empower the virtual machine to permit the vulnerabilities and assaults in the virtual machine screen and permits getting to the special data from the host working framework. The vindictive aggressor can play out the refusal of administration assaults by slamming the server. The accompanying Fig. 1, malignant aggressor display demonstrates the how pernicious will ruin the whole cloud framework. There is such a large number of chances are there to assault the framework.

In view of Advanced clo[illegible]ork (ACPS) is proposed in [illegible]ing effectiveness with respect to security to the cloud condition assets. The ACPS gives a few security administrations to the cloud specialist organization assets including system against assaults on customer and cloud specialist co-op information. ACPS likewise gives review capacity to the activities of virtual machines. The ACPS module is



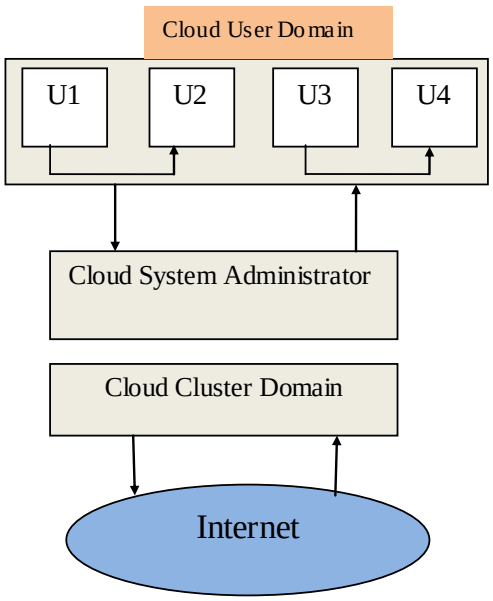


Fig. 1: Malware Attack in Cloud computing environment

Isolated into various modules situated at the host working framework. In these, one interceptor module will deal with suspicious activities are noted by the malware recorder module and put away in malware cautioning module. This ACPS demonstrate does not personal when scrambled keys are colloid. That is the huge downside of this module. Another proposed module for security device, called CyberGuarder in [8] gives virtual machine arrange protection and security through the virtual system gadgets organization module. This virtual machine security apparatus gives the virtual private system between virtual machines. The data is transmitted through virtual private system connect. In any case, in this module, creators are not focused on greater security for data when going through virtual system connect. Wu et al. [9] proposed a virtual system display that gives shield against caricaturing and sniffing assaults. In that model they utilized Xen hypervisor for virtual system design. In any case, the primary downside is virtual system demonstrate is thinking about security issues, which they are specified previously. He et al. displayed cloud arrange security arrangement [10] by following a tree-lead firewall. The creators are focused on firewall security. In this module determined security arrangement is allocating for firewall framework that is stop the gatecrasher assaults. In any case, this firewall security demonstrate isn't focused on virtual machine security and protection. Xing et al. [11] proposed a framework called SnortFlow for interruption anticipation in distributed computing condition. This SnortFlowmodule, additionally actualized in Xen-based cloud. This module is chiefly focused on controlling presume activity. Now and then, approved information likewise suspected by SnortFlow module. Wie et al. [12] proposed Mirage, this module is utilized for virtual machine picture administration framework for cloud condition. This Mirage gives security to the virtual machine pictures. Be that as it may, disadvantage is this module hasfilters for suspect's information, now and then these channels expel the information, which is tainted by malware. For this situation clients lose the required information. In [13], the creators proposed scrambled virtual plate pictures in cloud (EVDIC) condition that gives the security and encryption to secure the virtual machine pictures on the circle. This module is for the most part utilized for encryption for VM pictures. These encoded pictures are put away in plate, when malware assaults happens, aggressor getting to the all virtual machine pictures, since all pictures are put away in circle space.Emura et al. in [14], proposed the security strategy, in this plan number an of properties in clients private key and access approach of figure content must be same. In the event that the two things are not coordinate, at that point customer will lose their data. Since, some of the time client won't get the correct keys from encryption system. Another consistent size figure content approach was proposed in [15], encryption and decoding strategies are not proficient, all things considered security was lessened to scramble and unscramble the record. Next, security plot was proposed [16], in view of Decisional Bilinear Diffie-Hellman (DBDH) issue. This plan worked for, arrangement must be same of characteristics in a private key, and had a high secure unscrambling system.

2.2 Motivation

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

3. PROPOSED SEHEDULING 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 we focus on the algorithm of encryption technique.

3.1 Proposed Security Model

The model of the proposed security model is shown in Fig.2. It consists of different virtual machines allotted in single physical machine. The security module is responsible for providing security module for allotted virtual machine. First, the security module determines whether virtual machine is allotted or not. Once virtual machine is allotted, it will send the information to main security module to allot the security model for new virtual machine.

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

-

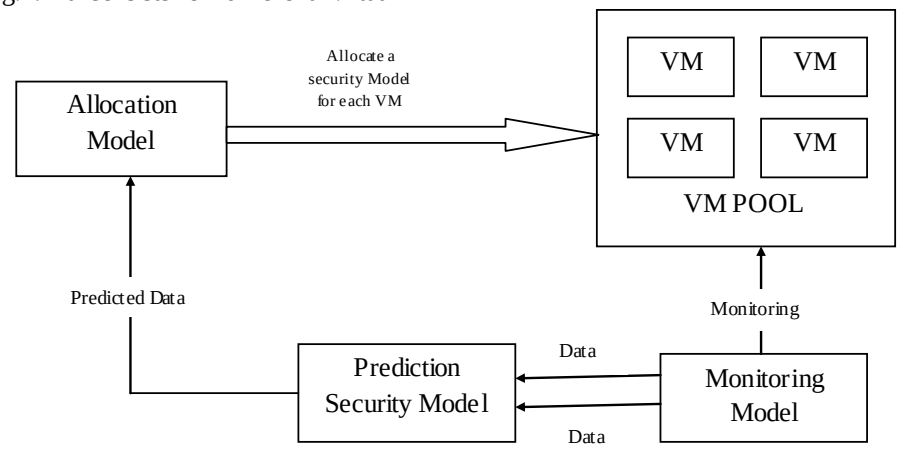


Fig. 2: Model of the Proposed Security Model

3.2Model Description

This section describes about Virtual Machine Security Monitoring (VSM) Model,called as prediction security model. We developed for predicting the allocation of virtual machine. Dinda [17] proposed one model to describe about CPU load. Motivated by this, we used mathematical formula to predict resource usage in a period of time. In our model, we used Iterated Function

System (IFS). By using IFS collage theorem, we can perform transformation checking to a given set and paste the results in model. Barnsley [18] proposed another model to assist IFS, called Fractal Interpolation Theory. By using, this method we can perform deterministic iteration to any point and we can get the attractor.

3.3Encryption Technique

This section defines some secure primitives used in our security allocation model. For providing the security and privacy in cloud environment, we are following symmetric encryption technique. This, technique uses a common secret key m to encrypt and decrypt

cloud data. This symmetric encryption scheme consists of three primitive 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 takes the secret key m and message E and then outputs the ciphertext C;
c. De(m,C)→ E is the symmetric decryption algorithm that takes the secret m and ciphertext C and then outputs the original message E.

We proposed a new technique which could protect the security for predictable information. The main idea of our technique is that encryption key generation algorithm. We are using hash functions to generate the tag functions. We are 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.

4. EXPERIMENTAL EVALUATION

4.1 Simulation Setup

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

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

5. RESULT ANALYSIS

In this section we are going to deal with the result analysis of the proposed algorithm. All the values are concerned with the cloud simulation environment. In Fig. 3, we can observe that the standard deviation of proposed algorithm showing the number of virtual machines. This results will be help full to predict the load balance information regarding host operating system.

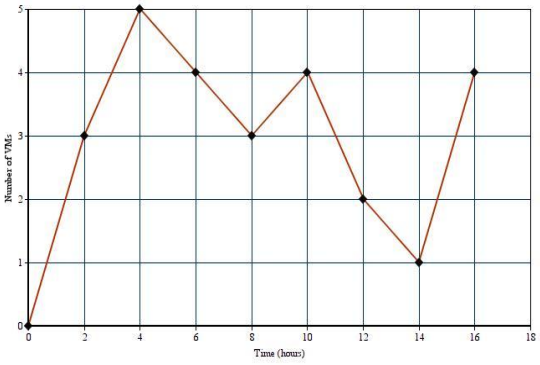


Fig. 3: Allotted Virtual machines in Host operating systems

The above figure, showing the results of prediction security model, at 0 point no virtual machines are allotted after two hours totally 3

virtual machines are allotted in 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 virtual machine. 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.

6. CONCLUSION

In this proposed system, the prediction security model is very help full for to predict the information of virtual machine pool. By using method, provider can predict the information easily regarding allotted virtual machines and provider will allot the separate security model for each virtual machine. In encryption technique also we 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] D. Nurmi*et al.*, "'Eucalyptus open-source cloud computing infrastructure—An overview," in *Proc. IEEE/ACM Int. Symp. Cluster Comput. Grid*, 2009, pp. 124–131.

[2] M.F. Bari, "Datacenter Network Virtualization: A Survey," *IEEE Comm. Surveys & Tutorials*, vol. 15, no. 2, 2013, pp. 909–928.

[3] B. Wei, C. Lin, and X. Z. Kong, "Dependability modeling and analysis for the virtual data center of cloud computing," in *Proc. IEEE 13th Int. Conf. High Perform.Comput.Commun. (HPCC)*, Banff, AB, Canada, 2011, pp. 784–789.

[4] "VM escape." Available: http://www.zdnet.com/blog/security/ us-cert-warns-of-guest-to-host-vm-escape-vulnerability/12471

[5] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30. doi: 10.1007/978-1-4614-9278-8_1.

[6] P. Juncheng, D. Huimin, S. Yinghui, L. Dong, Potential attacks against k-anonymity on LBS and solutions for defending the attacks, in: Advanced in Computer Science and its Applications, Springer, Berlin, Heidelberg, 2014, pp. 877–883.

[7] F. Lombardi, R.D. Pietro, Secure virtualization for cloud computing, J. Netw.Comput. Appl. 34 (4) (2011) 1113–1122.

[8] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, K.P. Lam, Cyber-guarder: a virtualization security assurance architecture for green cloud computing, Future Gener. Comput. Syst. 28 (2) (2012) 379–390.

[9] Kumar, K. Dinesh, and E. Umamaheswari. "An Authenticated, Secure Virtualization Management System in Cloud Computing." *Asian Journal of Pharmaceutical and Clinical Research* (2017).

[10] X. He, T. Chomsiri, P. Nanda, Z. Tan, Improving cloud network security using the tree-rule firewall, Future Gener. Comput. Syst. 30 (2014) 116–126.

[11] T. Xing, D. Huang, L. Xu, C. Chung, P. Khatkar, Snortflow: a openflow-based intrusion prevention system in cloud environment, in: IEEE Research and Educational Experiment Workshop, 2013, pp. 89–92.

[12] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managing security of virtual machine images in a cloud environment, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 2009, pp. 91–96

[13] M. Kazim, R. Masood, M.A. Shibli, Securing the virtual machine images in cloud computing, in: Proceedings of the ACM 6th International Conference on Security of Info and Networks, 2013, pp. 425–428.

[14] Emura K, Miyaji A, and Nomura A, "A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length," Information Security Practice and Experience—Fifth International Conference, F. Bao, H. Li and G. Wang, eds., Lecture Notes in Computer

Science F5451, Berlin: Springer-Heidelberg, pp. 13-23, 2009.
[15] Herranz J, Laguillaumie F, and Ràfols C, "Constant size ciphertexts in threshold attributebased encryption," Public Key Cryptography— Thirteenth International Conference on Practice and Theory in Public Key Cryptography, P.Q. Nguyen and D. Pointcheval, eds., Lecture Notes in Computer Science F6056, International Association for Cryptologic Research, pp. 19-34 2010.
[16] Attrapadung N, Libert B, and Pana□eu E.D, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," Public Key Cr yptography—Fourteenth International Conference on Practice and Theory in Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, eds., Lecture Notes in Computer Science F6571, International Association for Cryptologic Research, pp. 90-108 2011.
[17] P. A. Dinda, The statistical properties of host load, Scientific Programming 7 (3) (1999) 211–229.
[18] M. F. Barnsley, A. N. Harrington, The calculus of fractal interpolation functions, Journal of Approximation Theory 57 (1) (1989) 14–34.
[19] H. Wu, Y. Ding, C. Winer, L. Yao, Network security for virtual machine in cloud computing, in: 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, pp. 18–21.
[20] R. Bobba, H. Khurana, M. Prabhakaran, Attribute-sets: a practically motivated enhancement to attribute-based encryption, in: Computer Security ESORICS, Springer, Berlin, Heidelberg, 2009, pp. 587–604.
[21] D. S. Kim, F. Machida, and K. S. Trivedi, "Availability modeling and analysis of a virtualized system," in *Proc. 15th IEEE Pac. Rim Int. Symp. Depend. Comput.*, Shanghai, China, 2009, pp. 365–371.
[22] L. Gomes and A. Costa, "Cloud based development framework using IOPT Petri nets for embedded systems teaching," in *Proc. 2014 IEEE 23rd Int. Symp.Ind. Electron. (ISIE)*, Istanbul, Turkey, pp. 2202–2206.

Author is currently working in the School of CSE, VIT University, as a Associate Professor. She received her Ph.D. degree from Anna University. She published many research journals on cloud domain. Her research area is grid computing and also interests in cloud computing, fog computing.

Author is currently pursuing the Ph.D. degree in the School of CSE, VIT University. she received his B.Tech and M.Tech degrees under JNU. Her research area is cloud computing and also interests in grid computing, computer networks.