International Journal of Scientific Research in Computer Science and Engineering **Review Paper**
Vol.6, Issue.1, pp.37-43, Feb (2018) **E-ISSN:** 2320-7639

Security Challenges of Virtualization in Cloud Environment

Anitha H M[1*], P.Jayarekha[2]

[1*]Dept of Information Science & Engineering., BMSCE, Autonomous College under VTU, Bangalore, India
[2] Dept of Information Science & Engineering., BMSCE, Autonomous College under VTU, Bangalore, India

[*]Corresponding Author: *anithahm.ise@bmsce.ac.in*

Available online at: www.isroset.org

Received 25/Dec/2017, Revised 12/Jan/2018, Accepted 28/Jan/2018, Online 28/Feb/2018

Abstract–Cloud computing is the latest technology used by different category of users. Cloud computing services such as Software as service, Platform as service and Infrastructure as service are offered to the users using virtualization technology. Virtualization enables sharing resources of one system such as CPU, Memory and Storage to many users as per the requirement. Mainly Infrastructure as service is offered to the users through the virtual machines. Although there are advantages of using the virtual machines, security is one of the aspect which is taken care to a lesser extent. Virtual machines are exposed to different attacks such as malwares, malicious users. There are threats like denial of service, cross virtual machine attacks, insecure virtual machine migration, attacks on virtual machine image and hypervisor etc., hence virtual machine security has to be looked with high priority. Mitigation of the risks at virtualization level are surveyed.In this paper, several security vulnerabilities are identified and present various algorithms and implemented approaches to provide security to virtualization layer.

Keywords—Virtual Machine, Hypervisor, Virtualization, Cloud provider,Denial of Service, Cross Virtual Machine attacks.

I. INTRODUCTION

Cloud computing is an emerging technology which takes the advantage of using services from anywhere and any device. Cloud users can share the data, access the services as per their requirements. It is an opportunity to all the users to utilize the benefits of cloud computing in all the fields.

Advantages of cloud computing [1] such as low infrastructure investment for industries, scalability for services, economic improvement and global reachability for different applications have attracted the users to larger extent. Users can pay for whatever the services they are offered. Virtualization is the one vital element of cloud computing which plays a key role in infrastructure as service. Cloud service providers make use of virtualization technologies by the pay as use model through the internet. Virtualization is becoming popular as many users can share the resources and different operating systems can be run on the same physical machine [2].It is one of the best techniques to reduce the cost of investment in IT industry. Virtual machine (VM) runs on the top of the virtualized system.

Although there are several advantages of Virtualization, there exists the security flaws which are to be taken care. The VM is allocated to the cloud user based on their request. By placing the different VMs belonging to different users on the same Physical machine, efficient utilization of resources is achieved but at the risk of security threat from collocated VMs and hypervisor. It is necessary to analyze different quality of services provided when users are utilizing the services from the provider. It is required to concentrate on two features, viz CPU utilization rate and VM stability during the attacks. In this paper, the security vulnerabilities due to co-resident VMS, attacks on virtual machine images and hypervisor are presented and explored the solutions for the various attacks in virtualization layer. The paper is organized as follows section 1 gives the introduction ,section 2 explains the background of virtualization, section 3 explains security vulnerabilities at virtualization level, section 4 gives solutions to the vulnerabilities and section 5 provides conclusion.

II. BACKGROUND

Traditional System

In traditional system, application [3] runs on the operating system and hardware dedicated for only one user as shown in the figure 1. Some of the drawbacks of the traditional system are resources cannot be scaled up, when required resources are less. Sharing of resources facility is not provided in traditional system. Resources are allocated to the user based on the request. If the resources are not used completely, resources cannot be allotted to the other user.

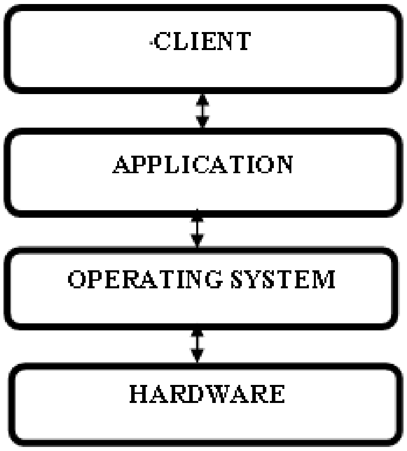

Figure 1. Traditional System

Virtualized Systems
In the virtualized systems, underlying pooled resources are shared among many users. Based on the demand and specifications of hardware and operating systems of the user, virtual machines are provided. Virtualized system is shown in the figure 2 which consists of Virtualization layer, operating system and applications. Virtualization [4] can be defined as a technology of sharing the resources of computer such as memory, CPU and storage to many users as per the need of the user dynamically.

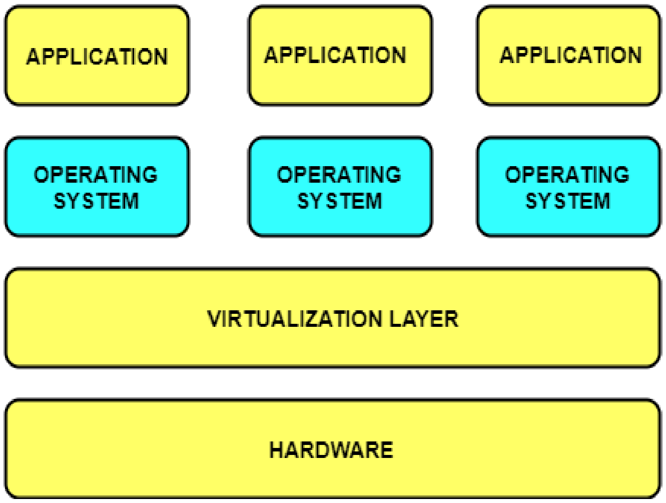

Figure 2 Virtualized System

Types of Virtualization [27]
Type 1 virtualization: virtual machine monitor or hypervisor runs directly on the top of hardware. Virtual machines run on the top of hypervisor. This is also known as bare metal or native virtualization.
Type 2 virtualization: Hypervisors or VMMs run on the top of operating system. The view of host OS is abstracted from the guest operating system.

Virtual machines provide the features [2] like isolation of users from each other, where the users can access the virtual machines allotted to them and recording the states in which data of the virtual disks are stored as a file. Usually VMs take a snapshot of the storage. This provides data integrity whenever there is an alteration in the data. State restoration creates kiosk in the server by inconsistent data.

Components Involved in Virtualization
The components of virtualization are hardware, operating system, virtual machine monitor or hypervisor, virtual machines and cloud users shown in the figure 3 are explained as follows.

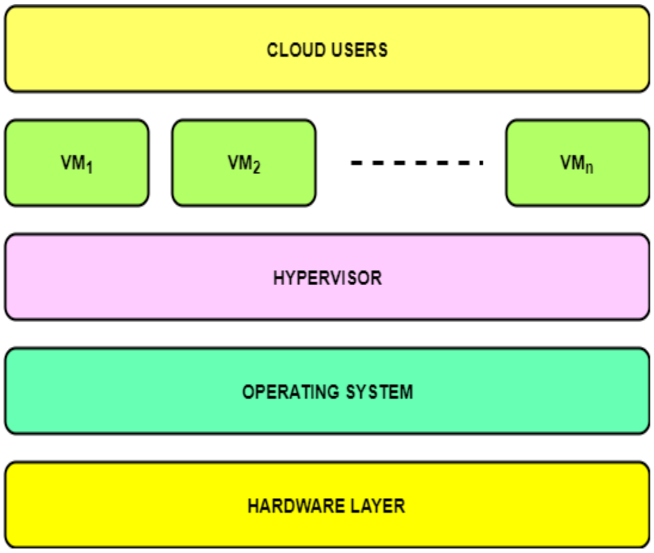

Figure 3 Components of Virtualization.

- Virtual Machine (VM): In cloud computing environment, virtual machine is the abstraction of the physical computer hardware which is dedicated for the use of users as needed.
- Hypervisor: Hypervisor is the software program to control all the operations of the virtual machines like launching of virtual machine, migration and shutting down when all the required tasks are finished.
- Cloud Provider: Cloud provider is the third party involved in providing the services like infrastructure, platform or software to the users as per their requirement and demand.
- Cloud User: Cloud user is one who needs the services from cloud environment and access the services by paying money through the internet.
- Operating System: The operating system present in the host is known as host OS and the OS present in the virtual machines is called as the guest OS. It is required that guest and host OS to be similar. Guest OS not necessarily be same as host OS.

- Hardware Layer: The hardware is shared among different virtual machines.

Advantages of Virtualization [5]

- Availability: Availability of VMs is increased so that failure of any one of the VMs does not affect the availability of VMs to the user.
- Cost Reduction: There is drastic reduction in cost of investment on bigger servers. Small servers are equipped to increase the storage and processing capacity among them.
- Performance Enhancement: Failure of one Virtual Machine does not degrade the performance of other VMs.
- Load Balancing: Load balancing can be achieved by migrating a running VM from source to destination as per the availability of resources in the destination machine.
- Scalability: Whenever there is a need of more resources, resources can be obtained by shifting the required resources from available pool of resources.

III. Security Vulnerabilties at Virtualization Level

Attacks on Virtual Machine

Virtual machine is the component which is required by the users to run their applications. In the course of launching the VMs and placing them, different risks are observed. The risks that are commonly observed are Denial of Service, Cross VM Attacks, and Insecure VM Migration.

These vulnerabilities are explained below.

- Denial of Service: Virtualization is a concept where cpu, memory and storage are shared by VMs. Denial of service is an attack where in the attacker tries to take all the resources [6,17,27] from the host and prevents the legitimate user from getting services as well as resources. During this condition, when a new request comes for resource, host denies the allocation as the resources are held by attacker VM. This reduces the response time of the host leading to performance degradation.
- Cross VM Attacks: Many VMs belonging to different users can placed in the same host. This is an advantage when one VM wants to communicate or share the data to other VM. But this advantage becomes a threat when a malicious VM [6, 7, 9] attacks another VM placed in the same host.

  Cross VM attacks may happen in the following ways:

  Normally isolation of VMs are there in the cloud provider area. If there is no proper isolation between the VMs, malicious applications of any VM can get access to the root.

  Covert channels succeed to gather information in the presence of VM isolation and access control mechanisms. Usually covert channels [11] are used to communicate among the VMs to send and receive the information. This attack gathers the sensitive information held by the VM. Cloud service provider has the access to the physical resources.

  Cloud service provider [10] could also launch the attacks on VMs by placing the malicious VM and cause side channel attack. This kind of Attacks may lead CPU cache leakage and results in loss of sensitive data.

Insecure VM Migration:

Virtual machine migration takes place when there is a need for load balancing, insufficient resources available in the current host or any other issues. VMs can be moved to other physical machine in the network based on the requirement like user who wants to cancel and shortage of resources. VMs migration [8] can happen to an untrusted host or an attacker. So attacker can initiate several migrations due to which Denial of Service can result. During migration, VMs are susceptible to attacks like man in middle and DDOS. When VM images are migrated from one host to another, a copy of VM image might be there in the host. There are 8 security aspects with respect to live VM migration from one server to other server [25]. The security aspects are access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy. When a VM is migrated from one host to another host, the following important elements of security are to be followed

- Both source host and destination hosts should be trusted.
- Access control mechanisms are to be incorporated to avoid unauthorized access.
- Migration softwares involved must take care of data integrity and confidentiality.

Attacks on VM Image

VM image is generated when a VM is running. Usually cloud service provider creates a set of VM images. When user requests for VM, the VM image is delivered. Sometimes few users wish to distribute their image with permissions to retrieve and access. so the users place the VM image in the cloud. If a user wants to check the VM's state at a particular time, user can go back to the previous state and get the details from VM[17].VM image might pose the security problem such as disclosing user credentials and sensitive data in the VM.

Attacks on Hypervisor

Hypervisor is the main part in the virtualization layer and can be compared with brain of the human body. Hypervisor is responsible for creating, monitoring and migration of VMs when required. Attacks happen on the hypervisor through the Physical machine itself or guest VM. Hypervisor can be single point of contact for the virtualized systems[13]. Inspite, there is security provided for the VM or isolation provided among the VMs, if hypervisor fails or any kind of attack on it, will lead to the access to the VMs. An attacker can install malicious VM[10] in the guest OS, so that it gleans the memory and complete hardware details of the system.

IV. MITIGATING VULNERABILITIES AT VIRTUALIZATION LEVEL

Security Solutions for Virtual Machine

Denial of Service: In the cloud environment there are authorized users and attackers. In order to differentiate between them two methods[12] are suggested. In the first method analyze the behavior of the user. If any suspicious behavior is noticed, the user is further monitored to decide whether authorized user or not. For example user might request for data file from the server for one or two times. This is termed as normal activity. if the user requests same data file more than average number of times, then it is not a normal behavior. Second method follows challenge response mechanism, where series of questions are sent to determine whether the user is authorized or malicious based on their answers. In this way, if user's authenticity is known and denial of service can be avoided.

Mitigating Cross VM Attacks: Threats on VM like cross VM attacks can be taken care through meticulous VM placement. Li min et al[15] have implemented a VM placement algorithm based on the VM vulnerabilities. There are two categories of attacks: firstly, find the vulnerability of hypervisor. If the hypervisor is compromised, all the VMs can be accessed which are under hypervisors control. In Second category, compromise other VMS on the same host and pose side channel attacks. The authors have reduced both categories of attacks. It is observed that cloud services survivability is increased to 74.28 and seen the improvement of 27.15 in average survivability. VMs can be authenticated for the users. When a user requests for VM to the cloud service provider, VM is launched to the user. If the VM is authenticated[14] the user continues to take services from the provider, otherwise user requests to stop the malicious VM. The service provider launches one more VM for the user and authentication process continues. To improve the inter communication security among the virtual machine[16], a new architecture is proposed in which the security policies are defined to prevent the spoofing attacks. In order to avoid cross VM attacks, data center level security aware placement and migration algorithm[18] and Physical machine level security aware placement and migration algorithm are proposed. The first algorithm is based on the datacenter score depends on the resources available like computing capacity, memory, hard disk space and bandwidth. If the user request comes with its requirements, data center score(DCS) is computed given as given below in the equation 1. Here the score means the physical machines which have the resources and preference factor given by the VM.

$$DCS= f.W \tag{1}$$

where f = (pf,dist(k,j),cc,cm,cd,cb) where pf represents preference factor. Preference factor values are 0 if it is preferred else infinity. dist(k,j) represents the distance between locations user j and datacenter k. cc, cm, cd, cb are other factors mentioned earlier computing capacity, memory, disk space and bandwidth. W represents set of weights provided by the user. Based on the users preferences VM is placed to physical machine(PM). In the second algorithm, based on the scores of PMs, VM is placed. If an adversary VM is present in any PM,VM is migrated to other PM based on the placement strategy. Based on the affinity and conflicts[19], VMs are placed in the cloud environment. Affinity is the VMs is the score obtained by arranging VMs based on their belongingness to same physical machine and same rack in the datacenter. VMs belonging to same Physical machine or rack are grouped and using greedy algorithm, place the VMs. In continuation with greedy algorithm, heuristic algorithm is used. Conflicts are opposite of affinity where VMs belong to different physical machine. Average runtime of VM to be successfully placed is less than 1 second.

Advanced cloud protection system(ACPS) is proposed to take care of integrity of guest VMs and physical machine monitors the VMs[21] and other cloud infrastructure connected. ACPS protects from the internal attacks of other VMs and external attacks of cloud. ACPS is located at the physical machine only and transparent to all virtual machines. It has an interceptor to monitor any unusual activities and reports to warning recorder if any abnormal activities are noticed. These activities are examined by the evaluator. All the time components are active and functioning to detect any threats. The proposed method is used to measure in CPU -intensive, mixed work load and I/O intensive Applications. It is observed that performance is degraded in the range of 4 to 6 percentage.

Solutions for VM Migration: The authors [25] have suggested that both source machine and destination machine has to be authenticated. While moving VM and data from one host to other, data integrity should be given higher priority. Methods suggested are CoM framework which includes intrusion detection system(IDS) and intrusion prevention system(IPS).The features like Data confidentiality and integrity are not observed in this method. Virtual Trusted Platform Module(TPM) based approach is used. This method verifies integrity of both source and destination machines.

The disadvantage of this method is not supporting live migration. Role based migration[26] protects against the unauthorized access and defends against attacks like man in middle and DDOS. The authors[26] have implemented secure live virtual machine migration framework. VM Migration takes place in the same LAN making use of open source hypervisor such as Xen. Role based access control method is used by setting different level of access. All the levels of users doesn't have the same level of access. This access control mechanism restricts access to all users. Super user privileges are granted only to few users, who is authorized [28] to do all kinds of functional operations. Average downtime is reduced to 24.1 seconds.

Solutions for Virtual Machine Image Security: Security threats with respect to virtual machine images have been resolved with some approaches. VM images must be maintained with security updates timely to avoid attacks from malicious users or any other kind of applications. Integrity of VM images is primary need to accomplish the overall security of the cloud. Image management system[23] has been proposed to achieve the security and integrity of VM images. The features which make up this system are Access control system, Filters, Provenance tracking system and maintenance services. Access control investigates the unauthorized access of the images and sets proper access rules for the images. In this system only trusted users can modify and publish the images. Users without proper access permissions can retrieve and run the image. Filters monitor and maintains secrecy of important data such as personal information. It avoids publishing of sensitive information. Provenance tracking system checks the image accounting information and keeps a regular check of history of operations performed on it. Maintenance services include timely scanning of virus, malware and applying security updates. There is a limitation of automated monitoring of images and sensitive information in this system.

Mirage image repository [22] has been implemented which contains the images in file system structural format. Here intermediate nodes represent the files and leaves store the file data. This system is fast as deployment is faster and various operations like searching, comparing and analysis of images can be performed. Mirage system is built with various components namely content addressed store (CAS), catalog Manager and client interface. CAS uniquely stores objects encrypted using SHA-1.Same identifiers are assigned for similar objects. Images cannot be changed until identifier is changed. Versioning is used to keep track of new object. Old objects are removed from the CAS when a new object is added. Images are converted in to two acceptable formats by image indexer namely first format acceptable by mirage system and second format by hypervisor. Metadata of the image is stored in catalog manager of the mirage. Metadata of the image are CAS identifier, Current status, creation time of image and includes parent identifiers if the image is derived from some other image.

Solutions for Hypervisor Attacks: Hypervisor or virtual machine manager is one of the major component of the virtualization. It is responsible for all the activities. Security measures like controlling unauthorized access, hypervisor introspection [20] are some of the ways to mitigate the risks at the hypervisor level. Intrusion Detection System can be incorporated at the hypervisor level [24]. IDS can monitor the attacks at the hypervisor.

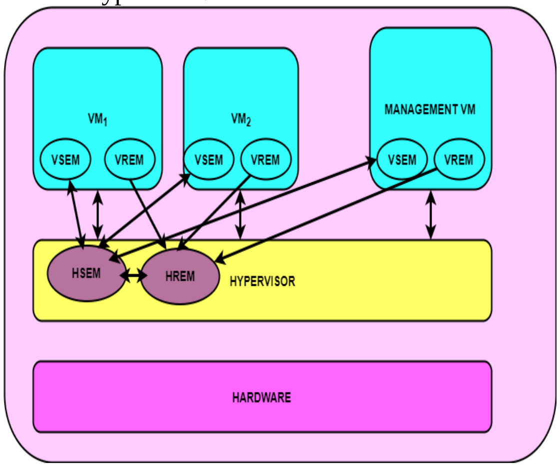

Figure 4. Secured Virtualization Architecture [24]

Secured virtualized architecture as shown in fig-4 is proposed to reduce the attacks. This architecture makes use of several elements which communicate among themselves effectively. The elements are virtual machine security monitor (VSEM), virtual machine reliability monitor (VREM), hypervisor security monitor (HSEM) and hypervisor reliability monitor (HREM).Figure 4 shows the architecture of the secured virtualization. VMs are monitored by HSEM in two stages. In the first stage, VSEM monitors the VMs as per the information provided by the HSEM. If any unusual behaviours are noticed, VSEM goes to the second stage. In the second stage resource utilization and packet flow is monitored and reported to HSEM. Based on the reliability information obtained, HSEM decides whether VM is attacker or not. This improves the performance as resource usage details of VM is gathered.

V. Conclusion

Cloud computing is inseparable from virtualization, which is the heart of the Cloud computing. Cloud computing can be secured only if the virtual machines are secured. VM security has to be reviewed with major importance. This paper presents the virtualization layer security vulnerabilities such as are Denial of Service, Cross VM Attacks, Insecure VM Migration, Attacks on VM image and Attacks on Hypervisor.

Various measures addressing this attacks are also explored. Denial of service attack can be mitigated by observing behavior of virtual machine. Several methods to avoid cross VM attacks are explored. VM image vulnerabilities are overcome by monitoring the access to VM and changes are continuously monitored. Secured Virtualization architecture is explored to mitigate hypervisor risks.Implemented approaches and methods to address these vulnerabilities are holistically discussed. In future, it is planned implement the security at virtualization level.

ACKNOWLEDGMENT

The authors thank BMSCE Management for providing constant support in the course of writing the paper. The authors would also like to acknowledge and thank TEQIP Phase-III, BMSCE.

REFERENCES

[1] Avram, Maricela-Georgiana. "Advantages and challenges of adopting cloud computing from an enterprise perspective." Procedia Technology 12 ,pp.529-534,2014.

[2] Shoaib, Yasir, and Olivia Das. "Pouring Cloud Virtualization Security Inside Out." arXiv preprint arXiv:pp.1411.3771,2014.

[3] Traditional systems and virtualized systems, https://www.vmware.com/pdf/virtualization.pdf. Accessed on January 25,2018.

[4] S Malhotra, Lakshay, Devyani Agarwal, and Arunima Jaiswal. "Virtualization in cloud computing." J. Inform. Tech. Softw. Eng4.2 ,2014.

[5] Daniel A. Menasce, "Virtualization: Concepts, applications, and performance modeling." In Int. CMG Conference, pp. 407-414. 2005.

[6] Jenni Susan Reuben, "A Survey on Virtual Machine Security", Seminar of Network Security, Helsinki University of Technology, 2007.

[7] Farzad Sabahi, "Virtualization-level security in cloud computing." Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, pp. 250-254, 2011.

[8] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B.. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1 (2013): 5,2013.

[9] Christopher Jarabek, "A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management ", from University of Calgary: http://people.ucalgary.ca/~cjjarabe/pa pers /jarabek_cloud_security.pdf, 2011.

[10] Kazim, Muhammad, Rahat Masood, Muhammad Awais Shibli, and Abdul Ghafoor Abbasi. "Security aspects of virtualization in cloud computing." In Computer Information Systems and Industrial Management, pp. 229-240. Springer, Berlin, Heidelberg, 2013.

[11] Covert channels, https://www.sans.org/security-resources/ idfaq/what-is-covert-channel/ -and-what-are-some-examples/2/17.Accessed on 3 November 2017.

[12] Leginamate users and Attackers,https://blog.radware.com/security/2013/06/distinguish-between-legitimate-users-and-/attackers-the-secret-/-sauce-of-ddos-protection/.Accessed on 3 November 2017.

[13] Virtual Machine Access, https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.Accessed on 25 january,2018.

[14] Li, Min, Yulong Zhang, Kun Bai, Wanyu Zang, Meng Yu, and Xubin He. "Improving Cloud Survivability through Dependency based Virtual Machine Placement." In SECRYPT, pp. 321-326. 2012.

[15] Wahid, Khan Ferdous, Nicolai Kuntze, and Carsten Rudolph. "Trusted Virtual Machine Management for Virtualization in Critical Environments." In ICS-CSR. 2013.

[16] Wu, Hanqian, Yi Ding, Chuck Winer, and Li Yao. "Network security for virtual machine in cloud computing." In Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pp. 18-21. IEEE, 2010.

[17] Schwarzkopf, Roland, Matthias Schmidt, Christian Strack, Simon Martin, and Bernd Freisleben. "Increasing virtual machine security in cloud environments." Journal of Cloud Computing: Advances, Systems and Applications 1, no. 1 (2012): 12,2012.

[18] Almodawar, Abdalrhman, Mahmoud Al-Ayyoub, and S. Mohammad. "Security-aware placement and migration algorithm in iaas interclouds." The fourth international conference on information and communication systems (ICICS 2013). 2013.

[19] Su, Kui, Lei Xu, Cong Chen, Wenzhi Chen, and Zonghui Wang. "Affinity and conflict-aware placement of virtual machines in heterogeneous data centers." In Autonomous Decentralized Systems (ISADS), 2015 IEEE Twelfth International Symposium on, pp. 289-294. IEEE, 2015.

[20] Wang, Gary, Zachary John Estrada, Cuong Manh Pham, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer. "Hypervisor Introspection: A Technique for Evading Passive Virtual Machine Monitoring." In WOOT. 2015.

[21] Lombardi, Flavio, and Roberto Di Pietro. "Secure virtualization for cloud computing." Journal of Network and Computer Applications 34.4 (2011): 1113-1122,2011.

[22] Ammons, Glenn, Vasanth Bala, Todd Mummert, Darrell Reimer, and Xiaolan Zhang. "Virtual machine images as structured data: the mirage image library." Proceedings of the USENIX HotCloud , 2011.

[23] Wei, Jinpeng, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. "Managing security of virtual machine images in a cloud environment." In Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 91-96. ACM, 2009.

[24] Sabahi, Farzad. "Secure virtualization for cloud environment using hypervisor-based technology." International Journal of Machine Learning and Computing 2.1 (2012): 39,2012.

[25] Aiash, Mahdi, Glenford Mapp, and Orhan Gemikonakli. "Secure live virtual machines migration: issues and solutions." Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on. IEEE, 2014.

[26] Anala, M. R., Jyoti Shetty, and G. Shobha. "A framework for secure live migration of virtual machines." Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. IEEE, 2013.

[27] Nagesh, O. Sri, Tapas Kumar, and Venkateswara Rao Vedula. "A Survey on Security Aspects of Server Virtualization in Cloud Computing." International Journal of Electrical and Computer Engineering (IJECE) 7.3 (2017): pp.1326-1336,2017.

[28] Anitya Kumar Gupta, Srishti Gupta, "*Security Issues in Big Data with Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.6, pp.27-32, 2017.

AUTHORS PROFILE

Anitha H M has pursued her B.E in Computer Science and Engineering, MTech from VTU and currently pursuing her Ph.D. under the guidance of Dr.P.Jayarekha. She has over 15 years of teaching experience. Her research interests are cloud security, virtualization technology and computer networks. She is currently working as Assistant Professor in Department of Information Science and Engineering at BMS College of Engineering, Bangalore.

Dr. P. Jayarekha has completed MTech in Computer Science from VTU securing second rank and Ph.D. in Computer Science. She has more than two decades of teaching experience. She has published many papers in national and international conferences and journals. Presently she is working as Associate Professor in the Department of Information Science and Engineering at BMS College of Engineering, Bangalore.