TWO-LEVEL SECURITY FRAMEWORK FOR VIRTUAL MACHINE MIGRATION IN CLOUD COMPUTING

By

YASHVEER YADAV * C. RAMA KRISHNA **

* Ph.D. Scholar, Applied Science Department of Computer Applications, I. K. Gujral Punjab Technical University, Punjab, India,
** Professor and Head, Department of Computer Science and Engineering, NITTTR, Chandigarh, India.

Date Received: 30/12/2017 Date Revised: 08/03/2018 Date Accepted: 21/03/2018

ABSTRACT

Cloud computing is a new generation utility computing. It provides the control to use computing as a utility which can be used anywhere at any time. It's highly elastic and can be grown or shrink according to user demand. The elasticity of computing power in cloud is based on the migration of virtual machine from overutilized servers to underutilized servers and vice-versa.Virtual machine migration (VMM) is used to reduce the power consumption of cloud environment that leads to green computing. In virtual Machine Migration, virtual machines are migrated from one physical server to another physical server that may lead to security threats like Replay, 'Time-of-Check' to 'Time-of-Use' (TOCTTOU), Resumption Ordering etc. Several experiments have been conducted by using KVM/QEMU(Kernel-based Virtual Machine/Quick Emulator) hypervisor. It is found that tampering of data by Man-In-The-Middle (MITM) is possible in information gathering phase and TOCTTOU can be injected. This may lead to serious security threat and can create hotspot at the destination host, which can degrade the performance of overall cloud experience. Hotspot is the situation where physical host is not able to fulfil the requested resources requirement. In this paper, a Two-level Security Framework has been proposed for protecting the VMM process from tampering of data and TOCTTOU problem. Further, the results of proposed technique have been compared with predefined RSA (Rivest–Shamir–Adleman) encryption and decryption technique in terms of time that can be used to protect the tampering of data in information gathering phase. The results indicate that this proposed technique reduces the time from 12.2 to 10.3 seconds (network size of 28 physical host) for protecting the data in information gathering phase of virtual machine migration process.

Keywords: Virtual Machine, Virtual Machine Placement, Two-Level Security Framework, Virtual Machine Migration.

INTRODUCTION

In recent times, cloud computing has become more and more popular. It is a type of computing which is now accessible by small companies as well as by big enterprises. Cloud computing gives the utility to add computing resources as required and release them when these resources are no more required. The requirements of clients are changing very frequently according to their needs. The cloud platform dynamically adjusts resource requirement according to client requirements (Yadav and Krishna, 2016). Cloud users need to pay for what they use as per the Pay-per-Use model. Cloud computing is attractive to recent business and IT industries because it enables utilizing huge computing resources from the cloud servers as a service, instead of owning it. In cloud computing, services are availed through Internet, based on the Pay-per-Use basis (Bhardwaj et al., 2015). Virtualization is a key concept of cloud computing. Virtualization is the power to develop virtual version of something rather than real one. Virtualization has enabled the abstraction of computing resources such that a single physical machine is able to function as a set of multiple logical Vms (Buyya et al., 2015). In cloud computing, virtualization provides the facility to use several parallel virtual machines. These virtual machines are deployed like real physical host and can perform all the tasks that a

real physical machine can perform. A cloud user can increase the computing power of these virtual machines according to computing need. These virtual machines are highly reconfigurable and their computing power can be increased or decreased according to the requirement. The high reconfiguration of virtual machines is managed by a process called as virtual machine migration. In virtual machine migration, virtual machines are migrated from one physical server to another physical server based on load balancing algorithms. Virtual machines are migrated to the physical host according to their resource requirements. The migration of virtual machines from one physical server to another physical server presents serious security risk such as Replay, 'Time-of-Check' to 'Time of- Use', Resumption Rodering, MITM attack, etc.

It has been observed that cloud computing is not growing as expected, because of some serious security issues. The report issued by Forbes (State of Cloud Adoption and Security, 2017) claim that, only 23% of cloud users trust security in cloud computing. It is stated that companies are dropping the use of cloud computing. They claim that the distrust on cloud environment forces the user not to use the cloud to store their confidential data. This leads to a significant drop out rate of 29% in a year (State of Cloud Adoption and Security, 2017). The cloud computing environment is totally different from the traditional computing environment. Cloud computing environment poses new security risks, therefore, to plug in these issues a new or modified security framework is required.

In cloud computing, small and medium organizations register themselves to the cloud broker to forward their access computing power to clients. It is not economically feasible for them (small and medium organizations) to manage in house cloud services. Cloud broker is a third party organization which provides the cloud services to the end users. Cloud Service Broker (CSB) is a third party business or individual who acts as an intermediary between the cloud owner and the users. Cloud broker helps the subscriber to identify best suitable cloud provider for their business. It saves users' service search time and provides information about how to use cloud (Kumar and Kumar, 2016). Multiple companies register themselves to the cloud broker and cloud broker adds their resources to the shared pool of resources. These registered companies do not have direct contact or contract with the end user. Computing resources provided by cloud broker can be distributed in nature. A client company availing the cloud services from a broker may have servers from two or more different cloud hosting sites. In this scenario, each site should maintain the same level of security. If any of the site compromises its security, it will lead to a high risk situation for the entire cloud infrastructure. Besides, VMM from one physical site to another physical site may lead to serious security risk to the client data, due to the untrusted environment of cloud computing.

The remaining paper is organized as follows: Section 1 discusses the related work. The problem formulation has been discussed in section 2. In section 3, the proposed model has been described. Section 4 presents results and discussion. Finally conclusion is presented in the last Section.

1. Related Work

Security issues in cloud environment are the prime concern of cloud users. Security is continuously affecting the growth of cloud computing. Security threats can be divided into two categories: internal security threats and external security threats. Internal security threats are performed by the authorized entities. These entities are authorized users and service host companies. External security threats are threats which are performed from the outside of cloud platform without using authorized access permissions. Some of the reports suggested that internal threats are much higher than external threats (TagElsir et al., 2015). Some of the serious internal threats are data breach, data loss, account hijacking, virtual machine to virtual machine attack, denial of services and insecure Application Programming Interfaces (APIs). To protect the cloud environment from these threats, several security frameworks have been developed. Muthunagai et al. (2012) proposed a novel protection system for detecting guest-to-guest attack in the virtual cloud environment called as Efficient Cloud Protection System (ECPS). ECPS

model provides effective access to cloud resources to the users, by providing access to the commonly used cloud resources. It saves time spent in accessing resources which are used frequently. ECPS model integrates the functions of cloud security like warning records, interceptor etc. It reduces the computation cost that further leads to enhance the security of overall cloud protection system. ECPS model also protects every guest virtual machine connected to the host and provides guard from the attack.

McDermott et al. (2012) proposed a Xenon research prototype, that provided a secure virtualization infrastructure based on complex commodity hardware for the military cloud environment. It applied a separate kernel approach to virtual machine monitor that was reasonably larger than a strict separation kernel. It provided a separate virtual machine manager for each running virtual machine. Initially, it partitioned all the computation power into virtual machines. Then it minimized the size of virtual machine manager and also minimised the complexity. After this, it isolated the virtual machines to use well-understood communication path between the virtual machines and the network. Separate virtual machine managers provided secure separation between running virtual machines. It also took care of complex commodity operating systems and shared complex commodity hardware architecture. Xenon was developed as a research prototype, it was not targeted for a common criteria evaluation. In Xenon, authors did not define security policies and protection profile. Xenon is suitable for validation of EAL 5 level assurance. Li et al. (2013) proposed a virtualization architecture to secure virtual machine execution environment in an untrusted management operating system. This architecture included secure runtime execution environment, secure secondary storage and secure network interface. Authors validated the system by implementing their secure runtime environment on the Xen virtualization platform. In this architecture, there were dedicated modules for protecting the cloud environment from expected security threats. These modules were highly coupled to provide integrity between the modules. The proposed virtualization architecture decreases the overall performance of the physical machine up to 1.06 percent due to high number of modules. This percentage also goes high at the time of domain build, domain saves, and domain restore operations. This model was also unable to handle Distributed Denial of Service (DDoS) attack at large level.

Wu et al. (2013) proposed SecMon framework for managing the security between running virtual machines on a physical host. SecMon is a virtual machine introspection framework for monitoring physical host server based on hardware virtualization. Authors used the windows operating system platform to develop a monitoring module at hardware virtual machine domain and install monitoring module in it. Windows monitoring module was responsible for the lifetime security of the running virtual machine starting from bootstrap to shutdown. SecMon used monitoring module for virtual machines named as Priv_WinDom with Windows operating system installed in hardware virtual machine domain, and secured the Priv_WinDom from bootstrap to shut down, in order to avoid the threat of user level tools in Domain-0. It expanded the application range of virtual machine introspection technology because of their monitoring virtual machine based on Windows operating system. Oktay et al. (2013) proposed a system, which was based on hybrid approach called as circular chain virtual machine protection system. This system protected the cloud environment from the untrusted employees and untrusted cloud users in a circular chain manner. This system was an improved form of existing adjoint virtual machine model. Adjoint VM model used three types of methods which were host-based IDS, trusted computing and virtual machine monitor based Intrusion Detection System (IDS) to secure the system from the internal and external threats in cloud environment. Authors used Adjoint VM model to build a more secure model for cloud users, by adding extra security mechanism between running virtual machines. This model constructed a circular chain structure to enhance the global security of the system. The responsibility of security and confidentiality is not only on the cloud providers and cloud

administrators, but also on a running virtual machine which protects another virtual machine in a circular manner. Users can also monitor and manage their security and confidentiality on their own. The system uses symmetric and asymmetric keys for providing encryption and decryption.

Bin Sulaiman et al. (2014) implemented IPsec transmission channel for live migration of virtual machines to achieve a secure transmission of data between a source host and a destination host. IPsec added additional overheads to the migration process. To reduce these overheads, the authors tuned the Maximum Transmission Unit (MTU) and Maximum Segment Size (MSS) values to improve the virtual machine migration performance. Authors described that performance of live migration using IPsec secured implementation was increased by using higher values of MTU. The higher value of MTU with larger MSS also showed improvement in the overall migration time. This was because the higher size of datagram packet transmits more data but also leads to the fragmentation of packets. Fragmentation used the extra time and CPU computing power, which resulted in increased total migration time. Majhi and Dhal (2016a) proposed a new security context migration framework for static as well as dynamic environment of cloud computing. The proposed framework consisted of five basic phases. In this framework, it first generated a list of security context files on each virtual machine based on both host and network security data. In the second phase, it identified the difference in security context, generated shared list which consisted of product set of security data of source host and destination host. In third phase, it identified the applications which were dependent on the security context. In fourth phase, extractor module generated different sets of security data based upon current context data and shared list. In fifth phase, extracted security data was deployed into the destination virtual machine and physical host.

Majhi and Dhal (2016b) proposed security enforcement framework for virtual machine migration in data centers. Their framework had three parts: 1) Migration management 2) Authentication, and 3) Migration analysis and monitoring. The migration management module has two parts: 1) data encryption 2) data decryption and host to host protection. Authors suggested that data encryption and decryption could be done using Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) technique. In data authentication, the data center needed to be authenticated itself, before participation in migration with other data centers. Authors suggested to use Diffie-Hellman key exchange algorithm and Internet Key Exchange (IKE) for authentication. In the migration analysis and monitoring module, the data center would act as monitoring stub. It would be equipped with Intrusion and Detection System (IDS) to check the outside vulnerability.

2. Problem Formulation

In Virtual Machine Migration (VMM) process, it is examined that virtual machine migration takes place using Transmission Control Protocol (TCP) connection. The security of data which would be migrated is provided by Secure Sockets Layer (SSL) connection. In VMM process, after the victim virtual machine is selected, the next step is to select the destination host. Destination host selection is a complex task because the migration of victim virtual machine can create hotspot at destination host and further need of migration may be required in near future. Selection of destination host is based on available resources at destination host. The information about the available resources needs to be transferred to source host. The methods of data gathering is broadly divided into two categories: 1) Periodic resources information updation and 2) On request resource information updation.

In periodic resource updation (Oh et al., 2013), host in the network broadcasts their available resource information after the specific interval of time. Each host broadcasts their available resources and also receives the same information from other hosts. Then, each physical host updates their table of available resources in the network. This technique speeds up the VMM process because the hotspot node has information about the available resources in the network in advance. One drawback in this

technique is, it generates lots of unnecessary network load even when VMM is not required.

In on request resource information updation (Oh et al., 2013), information about the available resources is shared only when a overloaded host generates the request for information about the available resources in the network. This resource information is sent only once by other physical host only on request. It reduces the network traffic but this technique increases the total migration time and virtual machine remains in running state where hotspot is detected. This technique is better than periodic updation because it reduces network traffic, and ultimately less traffic on network leads to fast transfer of data from source host to destination host.

Once the physical host gets the information, it applies different techniques to select the best destination host. (Luo et al., 2008; Liu et al., 2014; Gerofi et al., 2010; Ferreto et al., 2011; Gao et al., 2013; Kanagavelu et al., 2014) have defined different techniques to select destination host on the basis of available Central Processing Unit (CPU), Random Access Memory (RAM) secondary memory and network resources. The information about the resource availability at other hosts in the network is gathered during the information gathering phase. In literature, it has been found that there is no such mechanism to verify the data which was gathered in the information gathering phase. Diffie-Hellman and IKE techniques are used to authenticate the authenticity of the physical host but they do not authenticate the data sent by already authenticated physical host. RSA, AES, and DES are used in VMM process to encrypt and decrypt the data which is being transferred. It's not feasible to apply encryption and decryption techniques at the data gathering phase because it leads to computational overheads on the hotspot suffered physical host and consumes more time. MITM attack and Time-of-check to Time of-use (TOCTTOU) attack could be launched if the protection for migration is not properly implemented (Zhang et al., 2008; McPhee, 1974; Bishop and Dilger, 1996).

2.1 Problem Demonstration

In order to perform MITM attack, an experimental environment has been developed. All the running physical servers and their processes are deliberately set to develop a scenario where an attack can be performed. In this experimental setup, dedicated Dell Power Edge R520 server and Dell OptiPlex 980 and HP Compaq elite 8300 were used as hosting devices. Server is equipped with 64 GB of RAM and 1 TB of storage. All the other hosting devices are equipped with 4 to 64 GB of RAM and 320 GB to 1 TB of Hard Disk. The further details of the experimental hardware setup is given in Table 1. Cisco 2960x Ethernet switch has been used to establish connection between nodes. Nodes run Network File System (NFS) service to share image of virtual machine to other nodes, so that the migrated virtual machine can be resumed at the destination host. All physical machines run on Ubuntu 14.04 as operating system and use KVM (Kernel Virtual Machine) with QEMU as a hypervisor. KVM is an industrial grade virtualization platform implemented on the Linux kernel. It operates as Linux kernel module that provides a user space process access to the hardware virtualization features of various processors. Coupling KVM with QEMU allows QEMU to offer viable para-virtualization. 28 physical hosts have been deployed in which half of the machines run on Windows operating system and other half on Ubuntu operating system. VMs have virtual memory varying from 512 MB to 4 GB depending upon OS type. Salient details of running VM instance are shown in Table 2.

Physical Machine	Number of Machines	CPU Type	Number of Cores	CPU Clock	RAM
Dell Opti Plex 980	12	I5 –650	4	3.2 – 3.46 GHz	4
HP Compaq Elite 8300	11	I7 –3770	4	3.4 – 3.9 GHz	8
Dell Power Edge R520	5	Xeon – E5-2420	24	2.2 GHz	64

Table 1. Experimental Environment Setup

VM ID	OS	vCPU	vRAM (in MB)	Secondary Storage (in GB)
VM1	Windows 7	1	2048	15
VM2	Windows 8	2	4096	15
VM3	Windows 10	2	4096	15
VM4	Ubuntu 16.04	1	1024	8
VM5	Ubuntu 14.04	1	512	8

Table 2. Salient Features of Running VMs

Wireshark (Wireshark, 2017) has been used to capture the running network traffic. Scapy (Scapy, 2017) tool is used for recrafting the packets. These crafted packets are further forwarded to the destination host. It has been found that, it is possible to tamper packets and TOCTTOU attack can be launched. One physical host can be targeted to create hotspot situation by other authenticated physical hosts.

As KVM/QEMU do not provide any mechanism for data gathering, a custom module has been developed which can be triggered along with VMM trigger and can send request for available resources to the other nodes in the network. The client-server architecture is used where hotspot physical host is considered as client (sends request to other hosts in network) and rest of the nodes in the network are considered as servers. Network traffic is monitored by using Wireshark network analysis tool. Once the packet is successfully captured, the packet is crafted using Scapy tool and is forwarded to the destination host. To create hotspot situation, different workloads like VM creation, Ideal VM, Data copy, SPECjvm2006 and Memtester have been used. In this work, different combinations of these workloads have been used to develop a hotspot on physical hosts. The results of different experiments are shown in Table 3 and Figure 1.

Day	Hotspot Occurred	No. of Tampered Packets	VM Migrated to the Target Destination Host
1	15	7	4
2	25	10	6
3	54	23	13
4	36	14	9
5	28	13	9
6	22	16	7
7	12	5	1

Table 3. Data Collected Over Time Period of a Week

On the basis of these results, it can be concluded that KVM/QEMU needs light weight security framework that can validate the data gathered before the SSL connection in untrusted environment. This framework should be easily integrated with existing KVM/QEMU architecture module to avoid overheads.

3. Proposed Two-level Security Framework

In order to develop a solution for the MITM attack and TOCTTOU, differentiation between them is required. In MITM attack, information needs to be verified and host can be untrusted. In TOCTTOU, only verification of data is required and host remains trusted.

To guard the system against TOCTTOU, a novel methodology has been proposed which uses token

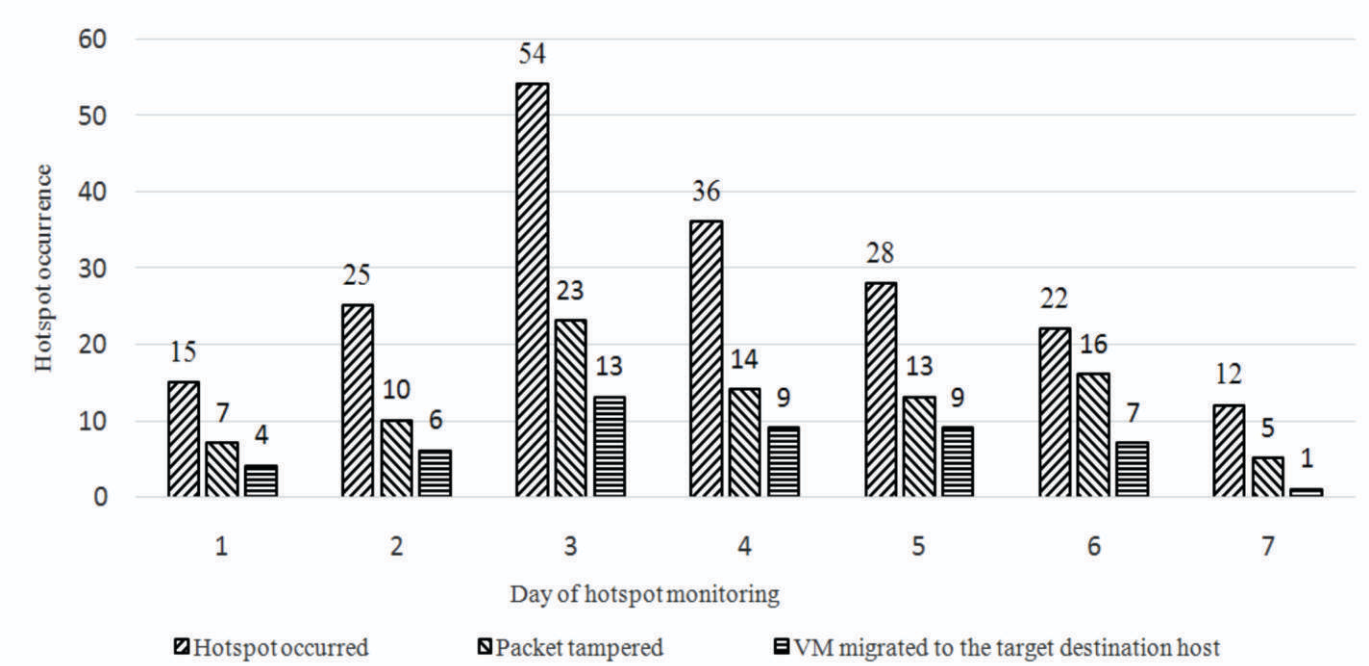

Figure 1. Results Over the Time Period of a Week

system. If any node wants to gather the information about the available resources in the network, it first inquires about the token. If the token is not in use, then it can broadcast the request for available resources information. In this experiment setup, it is found that, the time taken by hosts to reply is between 2 ms to 3 ms. Also, this time (2 ms to 3 ms) has been considered as the Time Window (TW). The proposed technique takes 10.3 seconds of average time for selecting the best possible destination host with the network of 28 physical hosts. Once the nodes send their information about the available resources, they wait for 10.3 seconds and do not respond to any other requests to avoid TOCTTOU attack. In 10.3 seconds of time, the proposed technique gathers the reliable information about available resources in the network, selects the best and reliable destination host for the victim virtual machine and establishes the SSL connection between source host and destination host.

To protect tampering of data in information gather phase, this work proposes two-level security framework. In KVM/QEMU approaches, once the destination host is selected, virtual machine is migrated using SSL connection. SSL connection is established between source host to destination host based on the data gathered in data gathering phase. In this approach, the running virtual machine is sorted in descending order on the basis of resource consumption (i.e. CPU, RAM, Secondary memory and Network Bandwidth). First the top most virtual machine is selected to migrate to the destination host as a victim virtual machine. In the next phase, the destination host which has the maximum resource availability is selected by using Max algorithm (Ayoub et al., 2017). The response time of the selected destination host is checked. If the response time of the selected destination host is in the TW, it is considered that there is no tampering of data and the virtual machine is sent to the destination host. If the response time is out of the TW, SSL connection is established between source host and selected destination host and verification module is run. Verification module again asks the destination host to send information of available resources. If this new information matches the previously sent information, VMM process is continued and the virtual machine is migrated to the destination host. If this new information does not match the previous information due to packet tampering, the node is still considered as the possible destination host, so that the migration process does not get delayed. If this node still can fulfill the requirement of the resources of victim virtual machine, then the VMM process is initiated. Otherwise, the SSL connection is teared down and the next entry of the available destination host is selected. The same thing is continued until the suitable destination host for VMM is selected. SSL connection is established between source host and destination host only when the response of the host is out of the TW and is asked to send the available resource information over the SSL connection. This information cannot be tampered because all the communication is done over a secure SSL connection. Therefore the proposed technique is able to handle possible tampering of data. The complete work flow of the proposed two-level security framework is given in Figure 2. The computing cost for verification module remains constant as it verifies one physical host at a time. In this technique, first level security is provided by SSL connection and second level security is provided by verification module.

4. Results and Discussion

In traditional approaches, MITM attack is handled by using encryption and decryption using RSA, AES, and DES algorithms. By using these techniques, one can handle MITM attack. These algorithms need additional computing power and it also generates lot of network traffic that can delay the overall virtual machine migration process. Cloud computing architecture is different from the traditional architecture where parameters like network delay and computing cost also needs to be taken care for maintaining the Service Level Agreement. Network delay and computing cost are used to grade the performance of overall cloud environment that directly affects the quality of service in cloud computing. The network delay and computing cost made the encryption and decryption algorithms, a non-feasible solution for the cloud environment. Therefore, a two-level security architecture has been developed to guard the system

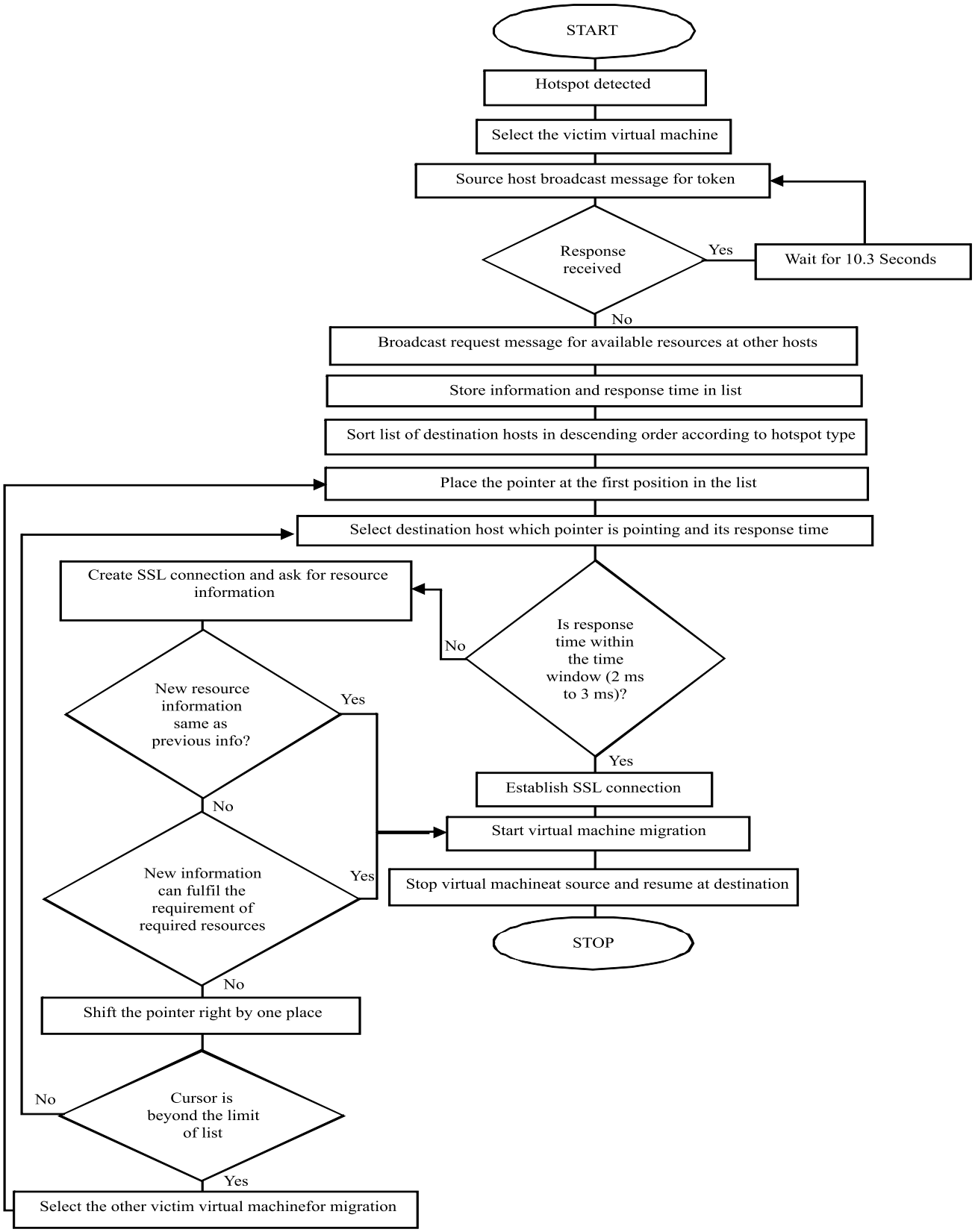

Figure 2. Proposed Two Level Security Framework

against MITM attack without using encryption and decryption algorithms. TW has been used to validate the receiving messages in a controlled environment. SSL connection is established only when the reply from the destination is out of the TW and seems fishy. This avoids the unnecessary verification and validation of all the data. To validate the proposed two-level security framework, the results of proposed two-level security framework have been compared with RSA algorithm. RSA algorithm does not guard the system from TOCTTOU, but the proposed technique does this by using the waiting time of 10.3 seconds. Therefore TOCTTOU is not used in the present experimental procedure.

To implement the proposed two-level security framework, the same testbed has been used, which used for the problem demonstration. Singh and Supriya (2013) was deployed the RSA, DSA, and AES techniques. They have compared them in many parameters including time. In this technique, the authors taken same packet size of 153 bytes. DSA and AES cant be used for authentication, they were not considered RSA can be used for encryption and description and also can be used for authentication with digital signature, thus RSA has been considered. The comparison between RSA and proposed technique has been shown in Table 4. The results show that RSA technique takes more time as compared to proposed Two Level Security Framework to serve the same objective.

Conclusion

Cloud computing has become an essential component of IT industries. It has changed the way of traditional computing. Virtualization provides the basic power to cloud computing. Virtualization provides the capability of elasticity of computing power to cloud computing. Like other technologies, security in cloud environment is a serious concern.

In this paper, security issues related to VMM process are discussed. The issues in information gathering phase has been highlighted. The experiments were conducted using KVM/QEMU hypervisor. KVM/QEMU do not provide any security framework to gather the data from the network hosts. Hence, empirical data has been used to demonstrate a scenario, where hotspot can be created intentionally in KVM/QEMU hypervisor environment by other host in the untrusted network to degrade the performance of all running virtual machines on victim physical host. Results demonstrated that, in data gathering phase data can be tampered, or TOCTTOU attack can occur. To guard the data at data gathering phase and guard the system from TOCTTOU, a two-level security architecture has been proposed. The proposed two level security model first differentiates MITM attack and TOCTTOU. The proposed model uses 10.3 second (with the network size of 28 hosts) of waiting time to avoid all the TOCTTOU attacks. From the experiments, it is found that, a normal transmission between source physical host and destination physical host takes time between 2ms to 3ms. The proposed model uses this time (2 ms to 3 ms) as a TW to differentiate normal packet and tampered packet. MITM attack is handled by two-level security architecture, it uses the predefined SSL at the first level to establish secure connection between a host and destination. At second level, verification module verifies the data which was gathered before SSL connection. Results shown significant improvement in terms of time as compared to RSA. The proposed framework can be bundled and used as module to protect the gathered data in QEMU/KVM virtual environment.

	Encryption Time (s)	Decryption Time (s)	Total Time (s)
RSA	7.3	4.9	12.2
Proposed Technique	Not Applicable	Not Applicable	10.3

Table 4. Comparison between RSA and Proposed Technique in Terms of Time

References

[1]. Ayoub, O., Musumeci, F., Tornatore, M., & Pattavina, A. (2017). Efficient routing and bandwidth assignment for inter-data-center live virtual-machine migrations. *IEEE/OSA Journal of Optical Communications and Networking,* 9(3), B12-B21.

[2]. Bhardwaj, A., Singh, V. K., Vanraj & Narayan, Y. (2015, December). Analyzing BigData with Hadoop cluster in HDInsight azure Cloud. In *IEEE India Conference (INDICON), 2015 Annual IEEE* (pp. 1-5). IEEE.

[3]. Bishop, M., & Dilger, M. (1996). Checking for race

conditions in file accesses. *Journal on Computing Systems,* 2(2), 131-152.

[4]. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Journal Future Generation Computer Systems,* 25(6), 599-616.

[5]. Ferreto, T. C., Netto, M. A. S., Calheiros, R. N., & De Rose, C. A. (2011). Server consolidation with migration control for virtualized data centers. *Journal on Future Generation Computer Systems,* 27(8), 1027-1034.

[6]. Gao, Y., Guan, H., Qi, Z., Hou, Y., & Liu, L. (2013). A multi-objective ant colony system algorithm for virtual machine placement in cloud computing. *Journal of Computer and System Sciences,* 79(8), 1230-1242.

[7]. Gerofi, B., Fujita, H., & Ishikawa, Y. (2010). An efficient process live migration mechanism for load balanced distributed virtual environments. In *Cluster Computing (CLUSTER), 2010 IEEE International Conference on* (pp. 197-206). IEEE.

[8]. Kanagavelu, R., Lee, B. S., Le, N. T. D., Mingjie, L. N., & Aung, K. M. M. (2014). Virtual machine placement with two-path traffic routing for reduced congestion in data center networks. *Journal on Computer Communications,* 53(1), 1-12.

[9]. Kumar, P., & Kumar, R. (2016). Optimal resource allocation approach in cloud computing environment. In *Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on* (Vol. 10, pp. 112-117). IEEE.

[10]. Li, C., Raghunathan, A., & Jha, N. K. (2012). A trusted virtual machine in an untrusted management environment. *IEEE Transactions on Services Computing,* 5(4), 472-483.

[11]. Liu, J., Su, L., Jin, Y., Li, Y., Jin, D., & Zeng, L. (2014). Optimal VM migration planning for data centers. In *Global Communications Conference (GLOBECOM), 2014 IEEE* (pp. 2332-2337). IEEE.

[12]. Luo, Y., Zhang, B., Wang, X., Wang, Z., Sun, Y., & Chen, H. (2008). Live and incremental whole-system migration of virtual machines using block-bitmap. In *Cluster Computing, 2008 IEEE International Conference on* (pp. 99-106). IEEE.

[13]. Majhi, S. K., & Dhal, S. K. (2016a). A security context migration framework for Virtual Machine migration. In *Computing and Network Communications (CoCoNet), 2015 International Conference on* (pp. 452-456). IEEE.

[14]. Majhi, S. K., & Dhal, S. K. (2016b). An authentication framework for securing virtual machine migration. In *Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on* (pp. 1283-1286). IEEE.

[15]. McDermott, P. J., Montrose, E. B., Li, M., Kirby, J., & Kang, H. M. (2012, October). The Xenon separation VMM: Secure virtualization infrastructure for military clouds. In *Military Communications Conference, 2012-Milcom 2012* (pp. 1-6). IEEE.

[16]. McPhee, W. S. (1974). Operating system integrity in OS/VS2. *IBM Systems Journal,* 13(3), 230-252.

[17]. Muthunagai, S. U., Karthic, C. D., & Sujatha, S. (2012, April). Efficient access of cloud resources through virtualization techniques. In *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on,* (pp. 174-178). IEEE.

[18]. Oh, S., Kang, M. Y., & Kang, S. (2013). Effective hotspot removal system using neural network predictor. In *Asian Conference on Intelligent Information and Database Systems* (pp. 478-488). Springer, Berlin, Heidelberg.

[19]. Oktay, U., Aydin, M. A., & Sahingoz, O. K. (2013). Circular chain VM protection in AdjointVM. In *Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on* (pp. 93-97). IEEE.

[20]. Osman, T. T. A., babiker, A. A., & Mustafa, N. (2015). Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view. *IOSR Journal of Computing Engineering,* 17(2), 93-96.

[21]. Scapy. (2017). Retrieved from http://www.secdev.org/projects/scapy/

[22]. Singh, G., & Supriya. (2013). A study of encryption

algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications,* 67(19), 33-38.

[23]. State of Cloud Adoption and Security 2017. (2017). Retrieved from https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security

[24]. Sulaiman, N. A. B., & Masuda, H. (2014). Evaluation of a secure live migration of virtual machines using Ipsec implementation. In *ILAI 3rd IEEE International Conference on Advanced Applied Informatics* (pp. 687–693).

[25]. Wireshark. (2017). Retrieved from https://www.wireshark.org/

[26]. Wu, X., Gao, Y., Tian, X., Song, Y., Guo, B., Feng, B., & Sun, Y. (2013, February). SecMon: a secure introspection framework for hardware virtualization. In *Parallel, Distributed and Network-Based Processing (PDP), 2013 21st Euromicro International Conference on* (pp. 282-286). IEEE.

[27]. Yadav, Y., & Krishna, C. R. (2016). A Novel Approach for Virtual Machine Migration in Cloud Computing. *International Journal of Computer Technology and Applications,* 9(18), 8973-8980.

[28]. Zhang, F., Huang, Y., Wang, H., Chen, H., & Zang, B. (2008). PALM: security preserving VM live migration for systems with VMM-enforced protection. In *Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific* (pp. 9-18). IEEE.

ABOUT THE AUTHORS

Yashveer Yadav is a Ph.D. Student, Applied Science Department of Computer Applications, I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India. He has completed his Master of Computer Applications from I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India in 2008. He has one and a half years of industry experience as Application Programmer. He has four years of teaching experience as Assistant Professor. His research interests include Cloud Computing, Machine Learning and Cyber Security. Currently, he is working in the area of Virtual Machine Migration.

Dr. Rama Krishna is working with Department of Computer Science & Engineering, National Institute of Technical Teachers' Training & Research, Chandigarh since 1996 and currently holding the position of Professor& Head. He received B.Tech. from JNTU, Hyderabad, India, M.Tech. from Cochin University of Science & Technology, Cochin, India and Ph.D from IIT, Kharagpur, India. He is a Senior Member of IEEE, USA. To his credit, he has more than 80 research publications in referred International / National Journals and Conferences. He acted as an Associate Editor for International Journal of Technology, Knowledge and Society. He is a member in Advisory / Technical committees of many National and International Journals and Conferences and also chaired many technical sessions. He is reviewer of Elsevier Journal of Vehicular Communications, Elsevier Journal of Computers & Security, Elsevier Journal of Information and Software Technology. He has 20 years of experience in organizing more than 100 training programmes in the upcoming areas of CSE and IT for the faculty of engineering colleges, polytechnics and industry professionals. He is instrumental in launching various initiatives at NITTTR Chandigarh towards paperless office. His areas of research interest include Computer Networks, Wireless Networks, Cryptography & Cyber Security, and Cloud Computing.