Journal of Engineering and Applied Sciences 14 (Special Issue 6): 9509-9518, 2019
ISSN: 1816-949X

Security Issues, Attacks and Vulnerabilities for Virtualization in Cloud Computing and their Solutions

[1]Ahmed Ibrahim Turki, [2]Alyaa Hasan Zwiad and [3]Rafah M. Almuttairi
[1]Department of Physics, University of Samarra, Samarra, Iraq
[2]Department of Computer Science, University of Technology, Baghdad, Iraq
[3]Department of Studies and Planning, University of Babylon, Babylon, Iraq

Abstract: Cloud computing is a new technology designed to meet business requirements, reduce expenditure and solve IT management problems. Cloud computing relies on many applications such as virtualization but at the same time inherits its security problems. Virtualization architecture provides a powerful and integrated platform for system building. The use of virtualization depends on the layer of encapsulation software (Virtual machine monitor/hypervisor) that provides the operating system inputs and outputs and at the same time surrounds the operating system. The virtual machines does not depend on the state of the actual hardware as several virtual machines are installed on one set of devices. Virtualization inherits security issues inherent in the disconnection between logical and physical situations, causing security issues related to security and attacks on virtual machines. This survey presents and discusses security issues, attacks and vulnerabilities related to virtualization. Finally, range of solutions and appropriate security measures have been offered and applied to have secure virtualization.

Key words: Cloud computing, virtualization, virtual machine, security issues, attacks, VMM, vulnerabilities, countermeasures

INTRODUCTION

Cloud computing has recently emerged as a model that provides rapid elasticity on-demand self-service, measured service, resource pooling (Manna, 2018; Ganghishetti *et al*., 2011). According to NIST cloud computing is divided into four deployment models are public, private, community and hybrid clouds. In addition, the definition divides service models into three models, software as a service, infrastructure as a service and platform as service. The NIST definition of cloud computing provides a clear view of common characteristics like service orientation, geographic and allocation, virtualization and homogeneity, etc (Mell and Grance, 2009). Cloud computing offers a lot of services to both organizations and users, in terms of reducing operating expenses and capital expenditures. However, there are limitations on the use of cloud computing that stand in the way of its total adoption, security is the main concern of organizations and users (Subramanian and Jeyaraj, 2018). Virtual machines for users can be created, transferred, retrieved, copied and shared through virtualization, allowing users to run many applications (Jasti *et al*., 2010). Despite the virtualization features, the additional layer provides new opportunities for attackers, so, they must be secured (Owens, 2010). Any defect in the security of the physical device affects the security of the virtual machine, so, security is the biggest obsession because it adds more complexity of the link and more entry points. VM have many security issues in addition to being exposed to many attacks that lead to data protection violation, theft-of-service, bad manipulation of data and denial-of-service (Khan, 2016). In this study, we will present a number of previous work on security issues in cloud computing as well as identifying gaps in them. The study by Takabi *et al*., 2010) discusses many security issues such as data storage, privacy, trust, secure service tool, identity management, access control, authorization and authentication, variance, hypervisors, virtualization, resource sharing, applications and finally, outsourcing. But it does not provide any solutions to these issues in addition to the absence of open problems. The study by Pearce *et al*. (2013) presents a comprehensive and extensive study of security virtualization problems, providing an explanation of virtualization as well as a detailed framework. Then present the most important emerging issues of weak implementation and virtualization characteristics. The security problems in this study (Fernandes *et al*., 2014) have been very extensive when compared to other studies. Researchers provide very important recommendations for various open future challenges. The study by Khorshed *et al*. (2012)

Corresponding Author: Ahmed Ibrahim Turki, Department of Physics, University of Samarra, Samarra, Iraq

Table 1: Study security issues in virtualization and their solutions

Topics	Security issues	Solutions
Malware	Spreading of malware onto VMs, metamorphic engines, avoidance of malware	Intrusion prevention system Xing *et al*. (2013)
Issues in VM	Entropy generation strength, malware injection	CloudSec Ibrahim *et al*. (2011)
	Memory deduplication issues	Hypercoffer Xia *et al*. (2013)
	VM reset problem, re-usage, consistency, entropy depletion	Exterior a dual VM architecture Fu and Lin (2013)
Mobility	Replay attack, man in the middle attack	Security framework for virtual machine migration Tavakoli *et al*. (2012)
	Generation of untruth configurations, VM mobility, VM cloning	Protocol for virtual trusted platform module based virtual machine migration Wan *et al*. (2012)
Network virtualization	Virtualized communication medium, virtual devices software exposure, packet sniffing and spoofing, dynamic network property security. Effectiveness of network devices in virtual networks. Inapplicability of standard security mechanisms, limited network access, twofold traffic	Virtual network security He *et al*. (2014)
Virtual machine monitor	VMM zero day vulnerabilities	No hype Szefer *et al*. (2011)
	Load balancing in VMM, VM diversity	Split visor Pan *et al*. (2012)
	VM escape	Hyper lock Wang *et al*. (2012)
	Interposition, inspection, VMM separation, lack of monitor GUI, transparency of VMM, un-trusted VMM components, single point od failure, Hypervisor failure,	Hyper check Wang *et al*. (2013) De hype Wu *et al*. (2013)
VMs image management	Virtual machine sprawl, infected VMs, virtual machine transience	VM image privacy and integrity Kazim *et al*. (2013)
	Overlooked image repository, malicious code injection and VMs, theft cryptographic due to large size images	A VM image management system Wei *et al*. (2009)

and Srinivasamurthy *et al*. (2013) attack surfaces were used to classify attacks on clouds. The surface of the attack includes clouds, services and users with six interfaces. According to the report (Symantec, 2015) there was an increase in the rate of attacks on symantec devices at the rate of 1 of 3 and by 91%. The most important of these attacks was phishing that targeted cloud customers in 2013.

In this study, a comprehensive review of the literature on virtualization security was conducted. Many security issues related to virtual devices will be addressed to cover gaps in previous research as well, as summarize the appropriate solutions in Table 1. Identify attacks on vitalization through a broader analysis that includes all information and countermeasures that are reliable and in compliance with applicable regulations, laws and standards. In addition, identify vulnerabilities of virtualization systems, security measures and cloud service models that are affected by them. Some surveys focus on cloud security problems in general, here, we provide a comprehensive survey of all security problems related to virtualization. For this reason, the research question will be: what are the security issues and the most important attacks and vulnerabilities on virtualization which should be examined and studied in depth in order to handle with them?

MATERIALS AND METHODS

Virtualization: Through virtualization, users can create, migrate, retrieve and share virtual machines, as well as running a range of applications (Jasti *et al*., 2010). At the same time gives the attacker a new chance of attack because of the virtual layer. Any security defect in the physical device affects the security of the virtual machine (Ertaul *et al*., 2010). All types of attacks on natural infrastructures can affect virtual environments. That's why security is a big challenge for virtualization because it adds more interconnection complexity to connectivity and more entry points.

Shared resources: Virtual machines can share I\O, CPU, memory and others on the same server. Virtual machines on the same server can share the input and output unit, CPU, memory and more. Sharing resources can reduce the security of virtual machines. A malicious virtual machine can infer some information about virtual machines that share shared resources and memory without having to put the virtual machine monitor at risk (Hashizume *et al*., 2013).

Public virtual machine image repository: Virtual machines can be created by configuration files which are a pre-filled program template called virtual machine image (Hashizume *et al*., 2013). The user may use his stock image in advance in the provider's repository or create his own image. Amazon, for example, provides a public repository of images that official users can download or download a virtual machine image. At the same time, images containing malicious code stored in the repository can be stored by malicious users who misuse these codes for the cloud system or for users (Subashini and Kavitha, 2011; Morsy *et al*., 2010; Jansen, 2011). In a valid account, an attacker could add viruses such as a trojans to the image. When this image is reused by another user, the VM will be infected with hidden viruses, resulting in inadvertent data leaks (Subashini and Kavitha, 2011).

Life cycle of VM: It is necessary to understand and know the life cycle of the virtual machines and the changes that occur in their situations as they move through the environment. The discovery of harmful programs is very difficult because the virtual machines can be ON or suspended and OFF. Moreover, virtual machines can be vulnerable even when they are not connected to the internet (Morsy *et al*., 2010).

Virtual machine rollback: If an error occurs, VM can be rolled back to their previous state. However, rolled back VM to the previous state but this procedure makes them re-enable the passwords or accounts disabled or display the security vulnerabilities that have been addressed. The virtual machine can be rolled back by a so-called "snapshot" but can lead to weaknesses or other configuration errors (Rittinghouse and Ransome, 2009).

Security issues of virtualization: Virtual cloud computing is heavily used in the industrial field, making it highly reliable for cloud computing, especially, for business purposes. Virtual machines, therefore, require a lot of confidence from the cloud provider. Virtualization is a prerequisite for any service in cloud environments. The concept of virtualization and multi-tenancy modeling offers a lot of profit but it brings in many attacks and threats. Virtual and logical isolation is the most important thing researchers do today. Creating virtual images and services through the virtual simulation program brings several viruses that cause damage to the virtual code. This study discusses security topics related to virtualization: malware, issues in virtual machine, mobility, network virtualization, virtual machines monitor and VMs image management. Table 1 offers all topics, issues and its solutions through efficient and reliable virtualization in the cloud.

Malware: Dependence on infrastructure encourages the help of malware. Virtualizationand sand boxing technique is an open door to many malware programs, although, it offers many advantages. There is a difficulty in the success of malware on the VM but if successful, it is very harmful, especially, the reliable of virtual machines. Hypervisor works on several platforms such as VMware, Microsoft Hyper-V, Virtual-PC and some Linux systems making it vulnerable to malicious attacks. Security experts at the University of North Carolina puts an appropriate solution to protect the hypervisor from malware (Sood and Enbody, 2012).

Issues in VM: The cloud infrastructure contains VM which is necessary for each client but it brings more security threats. Malicious software injection through eavesdropping allows malicious code to be entered into a VM or SaaS or PaaS. These codes execute malicious instructions that direct the user to a malicious site. Some attackers use arbitrary commands, private key, plain text to get a copy of the data on the virtual machines. Another security problem in shared environments is the elimination of deduplication which reduces physical memory. Moreover, there is a problem resetting virtual machines where they work on VirtualBox and VMware, it can result in random repetition or reuse of virtual machines (Yilek, 2010).

Mobility: The process of moving and copying virtual machines is called cloning. This process is a problem because copying virtual machines trusts the same initial state and software. So, the owner's private information and secret key can be leaked to another virtual machine (Pearce *et al*., 2013).

Network virtualization: Radio networks and Ethernet networks are difficult to manage due to deformities and discontinuities. Security problems can be caused by traffic in the network. Because of heavy traffic in virtual networks, traditional network solutions may not work. Firewalls and VLANs are less secure in virtual infrastructure. For example, the Amazon EC2 network suffers from an abnormal packet delay, inadequate network connectivity, instability UDP and TCP. These problems are abnormal and bring an administrative access issue in addition to network tailoring, allowing attackers to cause serious damage to the virtual infrastructure, putting user's data at risk. In addition, there are other security issues that the virtual network suffers like network based VM attack, spoofing, packet sniffing (Pearce *et al*., 2013).

Virtual machine monitor: VM is a software that organizes the connection of virtual machines to hardware, isolates and manages all virtual machines that are running and manages all virtual resources. Entry points and interconnect complexity in VMM can increase attack vectors. The guest user needs trust on VMMs and underlying virtual machines. The transparency of VMM may cause rootkits attacks based on VMM which affects trust. The path of non-linear or erroneous execution in virtual machines is a problem of VMM that can stop the implementation of the linear program. For example, restoring some snapshots or virtual machines can cause loss of log files, database information, application setup and monitoring data. A problem can arise in data storage during the snapshot operation. Inspection, separation and isolation are all areas of concern. Finally, VM escape where hypervisor and VMM are under the attacker's control (Perez-Botero *et al*., 2013; Bahram *et al*., 2010).

VMs image management: The provider can create, copy and modify images for virtual machines because of the dynamic nature and flexibility of the cloud. The volatile environment of the cloud can bring several problems. The database contains images of default devices that can be saved and commented on easily. Users can create new images for virtual machines or use old images because of the dynamic of the cloud. This causes problems where a malicious user or attacker can upload a malicious image that can cause serious damage because it contains malicious software which puts user data at risk (Vaquero *et al*., 2011).

RESULTS AND DISCUSSION

Virtualization based attacks: In cloud computing, loopholes in virtualization are exploited to violate them adversely affecting cloud services. Virtual machines cause many security risks to the system you are working on. We will explain below the types of attacks.

VM scheduler attack (A1): A few weaknesses in the scheduler are sufficient to theft of service or drop in resources (Rong *et al*., 2013). The time slot balance is maintained in order to execute virtual machines by scheduling virtual machines after a specified time. Improved versions of scheduler (Zhou *et al*., 2011) can improve the security aspect of monitoring programs while retaining efficiency.

VM rollback and migration attacks (A2): The contents of virtual machines become vulnerable to different attacks when they are migrated to a new physical host. During migration, the saved status log for the undo application is accessed. The resume/suspend activities make the migration of virtual machines more secure (Szefer and Lee, 2012).

VM creation attacks (A3): During the creation of VM. It is possible to place malicious code that is repeated within the image of virtual machines. Security breaches can be detected and avoided through scanners and filters provided by the VIMS (Virtual Image Management System) (Fernandez *et al*., 2013).

Cross-VM side channel attacks (A4): Information related to cryptographic keys, resource usage, etc. can be extracted from the target virtual machine that is on the same physical device by the side channel attack. Time information can be exploited from shared memory or cache by these attacks. Compulsory implementation algorithms and encryption and authentication mechanisms are countermeasures through which these attacks can be mitigated (Tandon and Agrawal, 2014).

Effects of attacks: Attacks on the cloud cause services and data to deteriorate on the cloud platform. The consequences of these attacks can be divided as follows:

Theft-of-service: The service theft attack causes the scheduler to have vulnerabilities. Where the attacker targets the scheduling policy, so, that, he can get free services or steal resources (Rong *et al*., 2013).

Denial-of-service: To disable customer service delivery, the attacker targets platform of cloud. For example, a malicious source inside the cloud platform would respond to a service request from customers on the pretext of resource availability (Karnwal *et al*., 2012; Almuttairi *et al*., 2018).

Malicious manipulation-of-data: The connection between the cloud and user interface includes SOAP&HTTP protocols with some scripting languages, making communication vulnerable to threats. Therefore, an attacker could exploit these vulnerabilities to manipulate data maliciously (OWASP., 2015).

Violation-of-data protection: The availability of data to non-owner users makes them vulnerable to infringement. Data protection is violated by several threats and techniques such as third-party clouds and data deduplication (Tandon and Agrawal, 2014).

Analysis of virtualization based attacks and their countermeasures: Services are provided using the service delivery model in the cloud computing platform. The cloud platform in each of its layers is subjected to many attacks, causing degradation of the quality of service and violation of data protection for malicious purposes. This study provides a contribution to the detection of all attacks based on virtualization and their countermeasures (Table 2).

Countermeasures for A1: VM scheduler attack

HyperSafe: The flow control of hypervisor is provided by HyperSafe. It provides protection by two techniques: conversion of control data to index indexes using restricted indexing, protection of memory pages using unbreakable lock to ensure that protected writing is not manipulated. To verify the effectiveness of these measures, there were four attacks on hypervisor such as manipulating the return schedule, modifying the page table, executing the injected code and modifying the

Table 2: Comparison of virtualization-based attacks in the cloud

Attacks/Mechanisms	Vulnerable components	Effects	Layers	Counter measures
A1				
Scheduling timed using hypervisor	VM scheduler	Theft of service	SaaS	Hyper safe (Wang and Jiang, 2010)
Relocation and access to VM image by insecure hypervisor	Hypervisor, VM image	Malicious manipulation of data, violation of data protection	IaaS	Offensive decoy technology (Stolfo *et al*., 2012)
VM hopping and VM escape to impact hypervisor execution and get information of other virtual machines	Hypervisor and VM	Denial of service, violation of data protection	SaaS, PaaS and IaaS	Noise injection and enables overlapping (Liu *et al*., 2014)
Detect virtual machines hosted through energy consumption logs	Storage and VM	Violation of data protection	IaaS	Offensive decoy technology Stolfo *et al*. (2012)
A2				
Connections for memory access and VM migration	Network and hypervisor	Denial of service and violation of data protection	IaaS SaaS and PaaS	VNSS (Xiaopeng *et al*., 2010)
A3				
VM creation/VM replication	VM image	Violation of data protection	SaaS and IaaS	Authentication mechanism (Fernandez *et al*., 2013)
A4				
Side-channel attack to gain access to a cache of virtual machines	Shared caches	Violation of data protection	IaaS	VM police (Su, 2013)
Virtual machine side-channel attack	Time shared caches	Violation of data protection	IaaS	

hypervisor code. The results showed that HyperSafe reduced the performance of the expenses and prevented all these attacks (Wang and Jiang, 2010).

Offensive decoy technology: This technique monitors data access to the cloud and detects abnormal patterns. When unauthorized data are suspected, challenge questions are used to verify them, as well as a misleading attack by using large amounts of decoy information against the attacker. This way the data is protected by the user's truth of abuse. The results of a local file show that this technology provides high levels of user data security in the cloud environment (Stolfo *et al*., 2012).

Noise injection and enables overlapping: In this technique attacks are mitigated, especially, potential side channels. The scheduler can insert the noise periodically, as well as control the interoperability time with the different virtual machines. This process is performed through a proposed prototype that allows for noise injection and inter-control. Initial assessments show success by reducing side channel attacks, as well as reducing overhead, balancing security and performance (Liu *et al*., 2014).

Countermeasures for A2: VM rollback and migration attacks

VNSS: A security framework has been proposed to allocate security policies for VM and also protects the virtual machine from direct migration. An initial system was implemented based on the Xen hypervisors used userspace tools such as (conntrack-tools, xm commands program and iptables) and stateful firewall technology. The empirical results showed that security policies are successful for application as well as migration to FTP applications is done securely (Xiaopeng *et al*., 2010).

Countermeasures for A3: VM creation attacks

Authentication mechanism: In this mechanism, a warehouse is created for the purpose of securing images of virtual machines in the cloud. This repository is used an authenticator to authenticate official users, check for image access tracking and screen to scan images. Developers can use this repository to address attacks (Fernandez *et al*., 2013).

Countermeasures for A4: Cross-VM side channel attacks

VM police: Virtual machines police are used to prevent side channel attacks. Where the host to launch the virtual machines police containing the components of the programs as an anti-attack. Control of scheduling of virtual machines police is done through security, load and performance requirements (Su, 2013).

Vulnerabilities of virtualization: Flaws that allow a successful attack on the system can be called vulnerabilities. According to the open group's risk classification, vulnerabilities arises where there is a difference between the object's resistance and the agent's threat (AlZadjali *et al*., 2015). Cloud computing relies on a lot of technologies such as virtualization, web browsers and web services in developing cloud environments. Therefore, the presence of any gap in any of these techniques reflected the impact on

Table 3: Vulnerabilities in virtualization

Vulnerabilities in	Descriptions	Layers	Counter measures
Virtual networks	Virtual bridges are shared by VM Wu *et al.* (2010)	I	Virtual network security Wu *et al.* (2010) FRS techniques Wylie *et al.* (2001) Digital signatures Somani *et al.* (2010)
Hypervisors	Complicated hypervisor code Wang and Jiang (2010) Exploit the flexible configuration of the hypervisors in order to meet the needs of the organization Wang and Jiang (2010)	I	TVDc Berger *et al.* (2009) TCCP Santos *et al.* (2009) Hyper safe Wang and Jiang (2010)\
Virtual machine images	Difficulty patching images of virtual machines because they are inactive artifacts Uncontrolled placement of virtual machine images in public storehouses Morsy *et al.* (2010)	I	Mirage Wei *et al.* (2009)
VMS	Possible covert-channels in the collocation of virtual machines Ranjith *et al.* (2012); Zhang *et al.* (2012)	I	FRS techniques Wylie *et al.* (2001) Digital signatures Somani *et al.* (2010) Encryption Harnik *et al.* (2010) Homomorphic encryption Tebaa *et al.* (2012)
	Absolute allocation/deallocation of resources with virtual machines Ranjith *et al.* (2012) Unlimited migration: virtual machines can be emigrated from server to another because of hardware maintenance, fault tolerance or load balance Dawoud *et al.* (2010)	I	
	Uncontrolled snapshots: flexibility can be provided by copying virtual machines which leaks data, Garfinkel and Rosenblum (2005)	I	TCCP Santos *et al.* (2009) VNSS Xiaopeng *et al.* (2010) PALM Zhang *et al.* (2008)

the cloud significantly. Table 3 provides a detailed analysis of vulnerabilities in virtualization. Including a brief description of vulnerabilities, the cloud service model that is affected as well as countermeasures.

Countermeasures for virtual networks

Virtual network security: Communication between virtual machines is ensured by a virtual network framework based on the Xen. This framework provides two default configuration modes for virtual networks: “routed” and “bridged”. There are three layers of the virtual network model: shared networks, routing layers, firewalls and pores that prevent virtual machines from spoofing and sniffing (Wu *et al*., 2010).

Fragmentation-redundancy-scattering technique: In this technique, sensitive data is fragmented into non-important fragments, so, one fragment cannot be used because the data will look vague and incomprehensible. These fragment are deployed in different locations and in a non-duplicate manner in the distributed system which provides intrusion tolerance (Wylie *et al*., 2001).

Digital signatures: The data can be secured while being transmitted over the internet by using the RSA algorithm in digital signature technology. RSA is one of the most widely used algorithms to protect data within cloud environments (Somani *et al*., 2010).

Countermeasures for hypervisors

Trusted virtual datacenter: Ensures integrity and isolation in cloud environments. It assembles VMS to have common goals in trusted virtual domains. Trusted virtual domains provides isolation between VLANs, hypervisor-based isolation and workloads. Trusted virtual domains provides system integration by using a load time documentation mechanism (Berger *et al*., 2009).

Trusted cloud computing platform: Help cloud service providers to provide implementation environments known as a closed box. Checks whether the environment is secure before users launch their virtual machines. The Trusted cloud computing platform adds two key elements: a trusted coordinator and a trusted VMM. The trusted nodes group is run by the trusted coordinator which in turn operates trusted virtual machines for the purpose of monitoring and maintaining them in a third party (Santos *et al*., 2009).

Countermeasures for virtual machine images

Mirage: This approach offers security features such as: tracking source maintenance, image filters, repository maintenance services, access control framework. Remove sensitive data from images or cannot scan images to get rid of malicious software one of the limitations of this approach. In addition, these filters can raise privacy concerns and breach the privacy of client data as content can be accessed (Wei *et al*., 2009).

Countermeasures for virtual machine

Encryption: Sensitive data has long been secured by powerful encryption algorithms such as AES. Storing or sending data in an encrypted manner that guarantees its security and integrity. The data can be protected while transferring using SSL technology (Harnik *et al*., 2010).

Homomorphic encryption: There are three basic processes for data in cloud: storage, processing and transport. For secure data transfer and storage encryption techniques can be used. Your service provider must decrypt this data to process it, thereby violating its privacy. But there is a coding method called homomorphic encryption that can be applied to secure the cloud. This type of encryption allows arbitrary computation of encrypted data without having to decrypt it (Tebaa *et al*., 2012).

Palm: To maintain privacy and integrity during and after migration, a safe framework for live migration has been proposed. The first model is based on the GNU Linux and Xen, the tests on this system showed good results but there is a slight down time in addition to the migration time due to encryption and decryption operations (Zhang *et al*., 2008).

CONCLUSION

In this survey, a lot of details about the virtualization system have been presented for cloud computing which means that it inherits its security problems. Although, virtualization is an old model, it has a vital role with current software architecture and hardware. The techniques related to virtualization were studied, especially, the security issues related to the integration of modern programs and devices. Virtualization for many users allows virtual server sharing for this to be a major focus of cloud computing users. The presence of different virtualization techniques is another challenge because each type needs different security mechanisms. Some attacks target virtual networks or virtual machine monitors, especially when communicating with VMs remotely.

This study also focuses on attacks and vulnerabilities that are important to understand, helping organizations to adopt cloud computing. Understanding and identifying security issues and vulnerabilities contributes to making the system more powerful and can mitigate attacks resulting from system vulnerabilities. Current security solutions and countermeasures that contribute to the prevention or mitigation of these attacks have also been listed. Here, novel security solutions are needed in addition, classical solutions that have been developed and may not work well because of the complexity of cloud environments.

Finally, virtualization can be considered a double-edged sword, so, it must be dealt with carefully, especially, on the security side.Virtualization optimizes software accountability and security isolation and provides security features for availability, confidentiality and integrity, if security solutions are implemented well.

REFERENCES

AlZadjali, A.M., A.H. Al-Badi and S. Ali, 2015. An analysis of the security threats and vulnerabilities of cloud computing in Oman. Proceedings of the 2015 International Conference on Intelligent Networking and Collaborative Systems, September 2-4, 2015, IEEE, Taipei, Taiwan, pp: 423-428.

Almuttairi, R.M., M.K. Al-Anni and D.A. Aljburi, 2018. Implementing secure cluster using Hadoop and Snort for ID (intrusion detection). J. Eng. Appl. Sci., 3: 9789-9799.

Bahram, S., X. Jiang, Z. Wang, M. Grace and J. Li *et al*., 2010. DKSM: Subverting virtual machine introspection for fun and profit. Proceedings of the 2010 29th IEEE Symposium on Reliable Distributed Systems, October 31-November 3, 2010, IEEE, New Delhi, India, ISBN:978-0-7695-4250-8, pp: 82-91.

Berger, S., R. Caceres, K. Goldman, D. Pendarakis and R. Perez *et al*., 2009. Security for the cloud infrastructure: Trusted virtual data center implementation. IBM. J. Res. Dev., 53: 1-12.

Dawoud, W., I. Takouna and C. Meinel, 2010. Infrastructure as a service security: Challenges and solutions. Proceedings of the 7th International Conference on Informatics and Systems, March 28-30, 2010, Cairo, Egypt, pp: 1-8.

Ertaul, L., S. Singhal and G. Saldamli, 2010. Security challenges in cloud computing. Proceedings of the International Conference on Security and Management SAM'10, July 12-15, 2010, CSREA Press, Las Vegas, USA., pp: 36-42.

Fernandes, D.A., L.F. Soares, J.V. Gomes, M.M. Freire and P.R. Inacio, 2014. Security issues in cloud environments: A survey. Int. J. Inf. Secur., 13: 113-170.

Fernandez, E.B., R. Monge and K. Hashizume, 2013. Two patterns for cloud computing: Secure virtual machine image repository and cloud policy management point. Proceedings of the 20th International Conference on Pattern Languages of Programs, October 23-26, 2013, ACM, Monticello, Illinois, ISBN:978-1-941652-00-8, pp: 1-15.

Fu, Y. and Z. Lin, 2013. EXTERIOR: Using a dual-VM based external shell for guest-os introspection, configuration and recovery. ACM. Sigplan Not., 48: 97-110.

Ganghishetti, P., R. Wankar, R.M. Almuttairi and C.R. Rao, 2011. Rough set based quality of service design for service provisioning in clouds. Proceedings of the International Conference on Rough Sets and Knowledge Technology, October 9-12, 2011, Springer, Berlin, Heidelberg, Germany, ISBN:978-3-642-24424-7, pp: 268-273.

Garfinkel, T. and M. Rosenblum, 2005. When virtual is harder than real: Security challenges in virtual machine based computing environments. Proceedings of the 10th International Workshop on Hot Topics in Operating Systems, June 12-15, 2005, Santa Fe, New Mexico, USA., pp: 20-26.

Harnik, D., B. Pinkas and A. Shulman-Peleg, 2010. Side channels in cloud services: Deduplication in cloud storage. IEEE Secur. Privacy, 8: 40-47.

Hashizume, K., N. Yoshioka and E.B. Fernandez, 2013. Three Misuse Patterns for Cloud Computing. In: Security Engineering for Cloud Computing: Approaches and Tools, Rosado, D.G., D. Mellado, E. Fernandez-Medina and M. Piattini (Eds.). IGI Global, Pennsylvania, USA., pp: 36-53.

He, X., T. Chomsiri, P. Nanda and Z. Tan, 2014. Improving cloud network security using the Tree-Rule firewall. Future Gener. Comput. Syst., 30: 116-126.

Ibrahim, A.S., J. Hamlyn-Harris, J. Grundy and M. Almorsy, 2011. Cloudsec: A security monitoring appliance for virtual machines in the IaaS cloud model. Proceedings of the 2011 5th International Conference on Network and System Security, September 6-8, 2011, IEEE, Milan, Italy, ISBN:978-1-4577-0458-1, pp: 113-120.

Jansen, W.A., 2011. Cloud hooks: Security and privacy issues in cloud computing. Proceedings of the 2011 44th Hawaii International Conference on System Sciences, January 4-7, 2011, IEEE, Kauai, Hawaii, USA., ISBN:978-1-4244-9618-1, pp: 1-10.

Jasti, A., P. Shah, R. Nagaraj and R. Pendse, 2010. Security in multi-tenancy cloud. Proceedings of the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, October 5-8, 2010, IEEE, San Jose, California, USA., ISBN:978-1-4244-7403-5, pp: 35-41.

Karnwal, T., T. Sivakumar and G. Aghila, 2012. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. Proceedings of the 2012 IEEE Student's International Conference on Electrical, Electronics and Computer Science, March 1-2, 2012, IEEE, Bhopal, India, ISBN:978-1-4673-1516-6, pp: 1-5.

Kazim, M., R. Masood and M.A. Shibli, 2013. Securing the virtual machine images in cloud computing. Proceedings of the 6th International Conference on Security of Information and Networks, November 26-28, 2013, ACM Aksaray, Turkey, ISBN:978-1-4503-2498-4, pp: 425-428.

Khan, M.A., 2016. A survey of security issues for cloud computing. J. Network Comput. Appl., 71: 11-29.

Khorshed, M.T., A.B.M. Ali and S.A. Wasimi, 2012. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Comput. Syst., 28: 833-851.

Liu, F., L. Ren and H. Bai, 2014. Mitigating cross-VM side channel attack on multiple tenants cloud platform. J. Comput. Acad., 9: 1005-1013.

Manna, M.E., 2018. A Cloud-based encryption for document storage using salesforce.com. J. Eng. Appl. Sci., 13: 2382-2387.

Mell, P. and T. Grance, 2009. The NIST definition of cloud computing. National Inst. Standards Technol., 53: 20-50.

Morsy, M.A., J. Grundy and I. Muller, 2010. An analysis of the cloud computing security problem. Proceedings of the International Workshop on APSEC Cloud, November 30, 2010, Sydney, Australia, pp: 1-6.

OWASP., 2015. Vulner ability scanning tools-OWASP. OWASP, Maryland, USA.

Owens, D., 2010. Securing elasticity in the cloud. Commun. ACM., 53: 46-51.

Pan, W., Y. Zhang, M. Yu and J. Jing, 2012. Improving virtualization security by splitting hypervisor into smaller components. Proceedings of the IFIP Annual International Conference on Data and Applications Security and Privacy, July 11-13, 2012, Springer, Berlin, Germany, ISBN:978-3-642-31539-8, pp: 298-313.

Pearce, M., S. Zeadally and R. Hunt, 2013. Virtualization: Issues, security threats and solutions. ACM Comput. Sur., Vol. 45. 10.1145/2431211.2431216

Perez-Botero, D., J. Szefer and R.B. Lee, 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. Proceedings of the 2013 International Workshop on Security in Cloud Computing, May 8, 2013, ACM, Hangzhou, China, ISBN:978-1-4503-2067-2, pp: 3-10.

Ranjith, P., C. Priya and K. Shalini, 2012. On covert channels between virtual machines. J. Comput. Virol., 8: 85-97.

Rittinghouse, J.W. and J.F. Ransome, 2009. Cloud Security Challenges. In: Cloud Computing: Implementation, Management and Security, Rittinghouse J.W. and J.F. Ransome (Eds.). CRC Press, Boca Raton, Florida, USA., ISBN:9781439806807, pp: 158-161.

Rong, H., M. Xian, H. Wang and J. Shi, 2013. Time-stealer: A stealthy threat for virtualization scheduler and its countermeasures. Proceedings of the International Conference on Information and Communications Security, November 20-22, 2013, Springer, Cham, ISBN:978-3-319-02725-8, pp: 100-112.

Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Proceedings of the 2009 International Conference on Hot Topics in Cloud Computing, June 15, 2009, USENIX, Berkeley, California, USA., pp: 1-5.

Somani, U., K. Lakhani and M. Mundra, 2010. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. Proceedings of the 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC 2010), October 28-30, 2010, IEEE, Solan, India, ISBN:978-1-4244-7675-6, pp: 211-216.

Sood, A.K. and R.J. Enbody, 2012. Targeted cyberattacks: A superset of advanced persistent threats. IEEE. Secur. Privacy, 11: 54-61.

Srinivasamurthy, S., D.Q. Liu, A.V. Vasilakos and N. Xiong, 2013. Security and privacy in cloud computing: A survey. Parallel Cloud Comput., 2: 126-153.

Stolfo, S.J., M.B. Salem and A.D. Keromytis, 2012. Fog computing: Mitigating insider data theft attacks in the cloud. Proceedings of the IEEE Symposium on Security and Privacy Workshops (SPW), May 24-25, 2012, IEEE, San Francisco, California, ISBN:978-1-4673-2157-0, pp: 125-128.

Su, T.A., 2013. A mechanism to prevent side channel attacks in cloud computing environments. Proceedings of the 2013 International World Congress on Computer Science, Computer Engineering and Applied Computing, October 23-25, 2013, San Francisco, California, USA., pp: 1-7.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.

Subramanian, N. and A. Jeyaraj, 2018. Recent security challenges in cloud computing. Comput. Electr. Eng., 71: 28-42.

Symantec, 2015. Internet security threat report. Symantec, Mountain View, California, USA. https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

Szefer, J. and R.B. Lee, 2012. Architectural support for hypervisor-secure virtualization. ACM. SIGARCH. Comput. Archit. News, 40: 437-450.

Szefer, J., E. Keller, R.B. Lee and J. Rexford, 2011. Eliminating the hypervisor attack surface for a more secure cloud. Proceedings of the 18th ACM International Conference on Computer and Communications Security, October 17-21, 2011, ACM Chicago, Illinois, USA., ISBN:978-1-4503-0948-6, pp: 401-412.

Takabi, H., J.B. Joshi and G.J. Ahn, 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Privacy, 8: 24-31.

Tandon, S. and V. Agrawal, 2014. Cache-based side-channel attack on aes in cloud computing environment. Intl. J. Eng. Res. Technol., 3: 1080-1084.

Tavakoli, Z., S. Meier and A. Vensmer, 2012. A framework for security context migration in a firewall secured virtual machine environment. Proceedings of the International Meeting on European Network of Universities and Companies in Information and Communication Engineering, August 29-31, 2012, Springer, Berlin, Germany, ISBN:978-3-642-32807-7, pp: 41-51.

Tebaa, M., S. El Hajji and A. El Ghazi, 2012. Homomorphic encryption method applied to Cloud Computing. Proceedings of the 2012 National Conference on Days of Network Security and Systems, April 20-21, 2012, IEEE, Marrakech, Morocco, ISBN:978-1-4673-1050-5, pp: 86-89.

Vaquero, L.M., L. Rodero-Merino and D. Moran, 2011. Locking the sky: A survey on IaaS cloud security. Computing, 91: 93-118.

Wan, X., X. Zhang, L. Chen and J. Zhu, 2012. An improved vTPM migration protocol based trusted channel. Proceedings of the 2012 International Conference on Systems and Informatics (ICSAI2012), May 19-20, 2012, IEEE, Yantai, China, ISBN:978-1-4673-0198-5, pp: 870-875.

Wang, C., Q. Wang, K. Ren, N. Cao and W. Lou, 2012. Toward secure and dependable storage services in cloud computing. IEEE Trans. Serv. Comput., 5: 220-232.

Wang, J., A. Stavron and A. Ghosh, 2013. Autonomic Recovery: HyperCheck: A Hardware-Assisted Integrity Monitor. Master Thesis, Defense Technical Information, Fort Belvoir, Virginia, USA.

Wang, Z. and X. Jiang, 2010. Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. Proceedings of the 2010 IEEE International Symposium on Security and Privacy, May 16-19, 2010, IEEE. Berkeley, California, USA., ISBN:978-1-4244-6894-2, pp: 380-395.

Wei, J.P., X.L. Zhang, G. Ammons, V. Bala and P. Ning, 2009. Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACM Workshop on Cloud Computing Security, November 13, 2009, Chicago, Illinois, USA, pp: 91-96.

Wu, C., Z. Wang and X. Jiang, 2013. Taming hosted hypervisors with (mostly) deprivileged execution. Proceedings of the 20th Annual International Symposium on Network and Distributed System Security NDSS, February 24-27, 2013, The Internet Society, San Diego, California, USA., pp: 1-15.

Wu, H., Y. Ding, C. Winer and L. Yao, 2010. Network security for virtual machine in cloud computing. Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology, November 30-December 2, 2010, IEEE, Seoul, South Korea, ISBN:978-1-4244-8567-3, pp: 18-21.

Wylie, J., M. Bakkaloglu, V. Pandurangan, M. Bigrigg and S. Oguz, *et al*., 2001. Selecting the right data distribution scheme for a survivable storage system. Master Thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania.

Xia, Y., Y. Liu and H. Chen, 2013. Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks. Proceedings of the 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA), February 23-27, 2013, IEEE, Shenzhen, China, ISBN:978-1-4673-5585-8, pp: 246-257.

Xiaopeng, G., W. Sumei and C. Xianqin, 2010. VNSS: A network security sandbox for virtual computing environment. Proceedings of the 2010 IEEE Youth Conference on Information, Computing and Telecommunications, November 28-30, 2010, IEEE, Beijing, China, ISBN:978-1-4244-8883-4, pp: 395-398.

Xing, T., D. Huang, L. Xu, C.J. Chung and P. Khatkar, 2013. Snortflow: A openflow-based intrusion prevention system in cloud environment. Proceedings of the 2013 2nd International Workshop on GENI Research and Educational Experiment, March 20-22, 2013, IEEE, Salt Lake City, Utah, USA., pp: 89-92.

Yilek, S., 2010. Resettable public-key encryption: How to encrypt on a virtual machine. Proceedings of the International Conference on Cryptographers Track at the RSA, March 1-5, 2010, Springer, Berlin, Germany, ISBN:978-3-642-11924-8, pp: 41-56.

Zhang, F., Y. Huang, H. Wang, H. Chen and B. Zang, 2008. PALM: Security preserving VM live migration for systems with VMM-enforced protection. Proceedings of the 2008 3rd Asia-Pacific Conference on Trusted Infrastructure Technologies, October 14-17, 2008, IEEE, Hubei, China, ISBN:978-0-7695-3363-6, pp: 9-18.

Zhang, Y., A. Juels, M.K. Reiter and T. Ristenpart, 2012. Cross-VM side channels and their use to extract private keys. Proceedings of the 2012 ACM Conference on Computer and Communications Security, October 16-18, 2012, ACM, New York, USA., ISBN:978-1-4503-1651-4, pp: 305-316.

Zhou, F.F., M. Goel, P. Desnoyers and R. Sundaram, 2011. Scheduler vulnerabilities and coordinated attacks in cloud computing. Proceedings of the 10th IEEE International Symposium on Network Computing and Applications, August 25-27, 2011, Cambridge, MA., pp: 123-130.