iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security in Cloud over Virtual Environment

S. Kalaiarasi Karunya[1], A.Umamageswari[2]
[1]M.E., [2]Assistant Professor, Department of Computer Science and Engineering
DMI College of Engineering, Chennai, India

Abstract— The Security issues in cloud concerns and mainly associated with security issues faced by cloud service providers and the service issues faced by the cloud customers. The administrator will track the information of both authorized and unauthorized person. If they are unauthorized means the used will be blocked automatically. The process will done through the deterrent application. A deterrent is a system designed to prevent unauthorized access from a private network. Create a deterrent rule that permits the ping command first and identify the unwanted request. If the IP address of request is correct the connection is granted to SQL Database server. If the IP address request is not within the range specified, then connection is failed.The connection established only when the client passes through deterrent in sql database. Deterrent Technique is proposed for security System. It is generated for the application of deterrent viewer. Physical address, IP address are used to block the authorized person.
Index Terms— Deterrent Technique, cloud environment, cloud manager.

I. INTRODUCTION

A good firewall security has been enforced for obstruction and filtering the unwanted requests coming back from the purchasers before the request approach the virtual machine. During the request process, if the user requests the high level of knowledge from the cloud, then supported the payment created by the cloud user, they will use and access the data's from the cloud server. The MAC (media access control) address, science address associated system data are going to be blogged If an unauthorized or unsought person attempting to access. Ontology for the cloud in an attempt to establish the knowledge domain of the area of cloud computing and its relevant components. We used compensability as our methodology in constructing our cloud ontology which allowed us to capture the inter-relations between the different cloud components. We presented our proposed ontology as a stack of cloud layers, and discussed each layer's strengths, limitations as well as dependence on preceding computing concepts. Few recent online articles attempt to establish a similar structure for cloud computing and its components [1]. Virtual machine (VM) introspection is a powerful technique for determining the specific aspects of guest VM execution from outside the VM. Unfortunately, existing introspection solutions share a common questionable assumption. This assumption is embodied in the expectation that original kernel data structures are respected by the untrusted guest and thus can be directly used to bridge the well-known semantic gap[4]. Cloud services such as Amazon's Elastic Compute Cloud and IBM's Smart Cloud are quickly changing the way organizations are dealing with IT infrastructures and are providing online services. Today, if an organization needs computing power, it can simply buy it online by instantiating a virtual server image on the cloud. Servers can be quickly launched and shut down via application programming interfaces (API), offering the user a greater flexibility compared to traditional server rooms. Virtual machine introspection (VMI) is a mechanism that allows indirect inspection and manipulation of the state of virtual machines. The indirection of this approach offers attractive isolation properties that has resulted in a variety of VMI-based applications dealing with security, performance, and debugging in virtual machine environments. Because it requires privileged access to the virtual machine monitor, VMI functionality is unfortunately not available to cloud users on public cloud platforms[6]. This are the technique used in the deterrent process.

The following are the contributions made in the proposed work:

A. MAC address is a unique address assigned to almost all networking hardware's. Creating Deterrent rules based on MAC address this also very effective while accessing system from cloud server. The address filters to prevent devices from sending outgoing TCP/UDP traffic to the WAN.
B. It is used to check whether the person is authenticated or unauthenticated user in a database while access the information in cloud server.
C. Authenticated user information is stored in database this helps to make a user to access the cloud server. And, system information (IP address, Mac address) are also checked in a database to allow the user to utilize the system.
D. Performance will be evaluated by administrator. All the information about authorized and unauthorized person detail will be stored in server database. And also performance speed will be checked.

E. Deterrent that allows to block programs from being accessed by other people on the internet or network. It helps to keep computer secure. Testing a blocking rule. And this rule used to test the website and block the website by network administrator.

F. A Deterrent product is required to support virtual devices.

G. In network not necessary to configure security policy for each interface in a network.

H. Create resource based packet filtering within same virtual device to remove zones in a network

In Section 2, literature survey on security in cloud computing. In Section 3, a system model encompassing a mobile cloud computing system is presented. In Section 4, the proposed algorithm for attribute-based encryption and re-encryption suitable for mobile users of the cloud is presented. In Section 5, the results of the implementation of proposed scheme on actual mobile devices and an operational cloud system are presented and discussed. Section 6, provides concluding remarks and the future enhancement.

II. LITERATURE SURVEY

Many solutions may be used to exchange encrypted data with a cloud provider in a secure manner, such that the cloud provider is not directly entrusted with key material, auditing is carried for ensuring availability of data. Ontology for the cloud in an attempt to establish the knowledge domain of the area of cloud computing and its relevant components. We used compensability as our methodology in constructing our cloud ontology which allowed us to capture the inter-relations between the different cloud components. We presented our proposed ontology as a stack of cloud layers, and discussed each layer's strengths, limitations as well as dependence on preceding computing concepts. Few recent online articles attempt to establish a similar structure for cloud computing and its components. Although they attain some valuable understanding of several cloud services and components, they tend to be more general classifications. We believe our proposed cloud ontology is more comprehensive, and encompass more detailed analysis of the cloud computing knowledge domain. While they refer to the core cloud computing services, their inter-relations have been ambiguous and the feasibility of enabling their inter-operability has been debatable. Furthermore, each cloud computing service has a distinct interface and employ a different access protocol. A unified interface to provide integrated access to cloud computing services is non existent, although portals and gateways can provide this unified web-based user interface[1] Virtual machine (VM) introspection is a powerful technique for determining the specific aspects of guest VM execution from outside the VM. Unfortunately, existing introspection solutions share a common questionable assumption. This assumption is embodied in the expectation that original kernel data structures are respected by the untrusted guest and thus can be directly used to bridge the well-known semantic gap. In this paper, we assume the perspective of the attacker, and exploit this questionable assumption to subvert VM introspection. In particular, we present an attack called DKSM (Direct Kernel Structure Manipulation), and show that it can effectively foil existing VM introspection solutions into providing false information. By assuming this perspective, we hope to better understand the challenges and opportunities for the development of future reliable VM introspection solutions that are not vulnerable to the proposed attack. Virtualization provides a way of getting around such constraints. Virtualizing a system or component— such as a processor, memory, or an I/O device—at a given abstraction level maps its interface and visible resources onto the interface and resources of an underlying, possibly different, real system. Consequently, the real system appears as a different virtual system or even as multiple virtual systems[2]. Cloud services such as Amazon's Elastic Compute Cloud and IBM's Smart Cloud are quickly changing the way organizations are dealing with IT infrastructures and are providing online services. Today, if an organization needs computing power, it can simply buy it online by instantiating a virtual server image on the cloud. Servers can be quickly launched and shut down via application programming interfaces (API), offering the user a greater flexibility compared to traditional server rooms. I will describe the design and implementation of an automated system that we used to instantiate and analyze the security of public AMIs (Amazon Machine Images) on the Amazon EC2 platform, and provide detailed descriptions of the security tests that we performed on each image. Our findings demonstrate that both the users and the providers of public AMIs may be vulnerable to security risks such as unauthorized access, malware infections, and loss of sensitive information. The Amazon Web Services Security Team has acknowledged our findings, and has already taken steps to properly address all the security risks we present in this talk[3]. Virtual machine introspection (VMI) is a mechanism that allows indirect inspection and manipulation of the state of virtual machines. The indirection of this approach offers attractive isolation properties that has resulted in a variety of VMI-based applications dealing with security, performance, and debugging in virtual machine environments. Because it requires privileged access to the virtual machine monitor, VMI functionality is unfortunately not available to cloud users on public cloud platforms. In this paper, we present our work on the Cloud VMI architecture to address this concern. Cloud VMI virtualizes the VMI interface and makes it available as-a-service in a cloud environment. Because it allows introspection of users' VMs running on arbitrary physical machines in a cloud environment, our VMI-as-a-service

abstraction allows a new class of cloud-centric VMI applications to be developed. We present the design and implementation of CloudVMI in the Xen hypervisor environment. We evaluate our implementation using a number of VMI applications, including a simple application that illustrates the cross-physical machine capabilities of Cloud VMI[4].Cloud computing provides access to data, but the challenge is to ensure that only authorized entities can gain access to it. When we use cloud environments, we rely on third parties to make decisions about our data and platforms in ways never seen before in computing. It's critical to have appropriate mechanisms to prevent cloud providers from using customers' data in a way that hasn't been agreed upon. It seems unlikely that any technical means could completely prevent cloud providers from abusing customer data in all cases, so we need a combination of technical and nontechnical means to achieve this. Clients need to have significant trust in their provider's technical competence and economic stability. The main issue for cloud computing is to build a new layer to support a contract negotiation phase between service providers and consumers and to monitor contract enforcement. Unfortunately, security, privacy, and trust are inherently non-quantitative and difficult to bargain, but there should still be ways to assure customers that services are provided according to what a service provider claims in the contract[5].

Virtual machine introspection (VMI) describes the method of monitoring and analyzing the state of a virtual machine from the hypervisor level. Using knowledge of the virtual hardware architecture, it is possible to derive information about a guest operating system's state from the virtual machine state. We argue that by deriving this information it is possible to build VMI applications which are more robust against circumvention techniques than applications that do not rely on hardware knowledge. we present various ways to leverage Intel's x86 architecture as well as the virtualization extensions from both Intel (VT-x) and AMD (SVM) to derive such information. Additionally, we describe how this derived information may be used in VMI-based security applications and against which threats they are most applicable. The most crucial part of any VMI application is the extraction of appropriate system state information from the binary data that comprises the virtual machine state. This process is called view generation. Any information that is not extracted from this binary data will not be available for further processing. Therefore the view generation must retain all information relevant for a given application. It is also important to perform this view generation in the most robust manner possible, that is, it is ideally immune to any malicious influence [6].

Cloud computing is a type of Internet-based computing, and it is one of the foundations of the next generation of computing. Computing services, such as data, storage, software, computing, and application, are delivered to local devices through Internet. In cloud computing, the service is fully served by the provider and the client needs nothing but a personal device and Internet access. The cloud computing can either be hosted on-site by the company or off-site such as Microsoft's Sky Drive, Google Drive, Samsung's S-Cloud service, Apple's I Cloud, Amazon's Cloud Drive. Recent applications, e.g., multimedia streaming, virtual reality, and robotics, have used cloud computing provide the services. Also, platforms like Google Apps YouTube, Vimeo, Flickr, Slideshare and Skype adopt the cloud computing technology. As cloud computing becomes more and more popular, how to secure cloud computing and protect data security deserves studying. Some issues in cloud computing security are surveyed and Studied. At this time, the data security and the personal privacy should be assured. The cloud provider should guarantee these data and personal information in host database against all accesses of the unauthorized insiders or the malicious outsiders. Accordingly, some secure cloud computing schemes based on secret sharing approach were proposed. For example, the PASS (data Privacy by Authentication and Secret Sharing) in prevents client's data privacy from the unauthorized access. The PASS adopts public key cryptosystem to encrypt its share, and this increases the transmission cost [7]. Scalability is critical to the success of many enterprises currently involved in doing business on the web and in providing information that may vary drastically from one time to another. Maintaining sufficient resources just to meet peak requirements can be costly. Cloud computing provides a powerful computing model that allows users to access resources on-demand. In this paper, we will describe a novel architecture for the dynamic scaling of web applications based on thresholds in a virtualized Cloud Computing environment. We will illustrate our scaling approach with a front-end load-balancer for routing and balancing user requests to web applications deployed on web servers installed in virtual machine instances[8]. A dynamic scaling algorithm for automated provisioning of virtual machine resources based on threshold number of active sessions will be introduced. Our work has demonstrated the compelling benefits of the Cloud which is capable of handling sudden load surges, delivering IT resources on-demands to users, and maintaining higher resource utilization, thus reducing infrastructure and management costs[9].
Denial-Of-Service attacks consume the resources of a remote host or network, thereby denying or degrading service to legitimate users. Such attacks are among the hardest security problems to address because they are simple to implement, difficult to prevent, and very difficult to trace[10]. In the last several years, Internet denial-of-service attacks have increased in frequency, severity, and sophistication. Howard reports that between the years of 1989 and 1995, the number of such attacks reported to the Computer Emergency Response Team (CERT) increased by 50% per year. More recently, a 1999 CSI/FBI survey reports that 32% of respondents detected denial-of-service attacks directed against their sites. Even more worrying,

recent reports indicate that attackers have developed tools to coordinate distributed attacks from many separate sites. Unfortunately, mechanisms for dealing with denial-of-service have not advanced at the same pace. Most work in this area has focused on tolerating attacks by mitigating their effects on the victim. This approach can provide an effective stopgap measure, but does not eliminate the problem, nor does it discourage attackers [11]. A trust model to reason about and improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust model provides an approach for the owners to determine the trustworthiness of individual roles in the RBAC system. The data owners can use the trust models to decide whether to store their encrypted data in the cloud for a particular role. The proposed trust model takes into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. In addition, we present a design of a trust-based cloud storage system which shows how the trust model can be integrated into a system that uses cryptographic RBAC schemes. We have also described the relevance of the proposed trust model by considering practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners of cloud storage service.[13] To enforce the access control policies in the cloud, cryptographic RBAC schemes have been developed, which combine cryptographic techniques and access control to protect the privacy of the data in an outsourced environment. Using these cryptographic schemes, the owner of data can encrypt the data in such a way that only the users with appropriate roles as specified by a role-based access control policy can decrypt and view the data. The issue of trust is critical in cloud storage systems; the stored data in the cloud is secure under the assumptions that roles are properly administered by trusted authorities, roles manage the user membership in a trusted manner and qualified users also behave in a trusted manner [14].

Intrusion Detection is an indispensable second line of defense since traditional prevention mechanisms are not strong enough to protect MANET[15]. In this paper, we present an Intrusion Detection engine that is part of a local Intrusion Detection System (IDS) composed of a Data Collector, an Intrusion Detection engine and an Intrusion Response engine. We focus on the design of the Intrusion Detection engine that is based on a type of neural networks known as emergent Self-Organizing Maps (eSOMs). By combining machine learning, information visualization and watermarking techniques, we are able to evaluate how secure a MANET is against attacks[16]. The global map is used in order to perform secure and efficient routing by avoiding paths that include nodes which are victims of attacks. Watermarking techniques are then applied in order to prevent the possible modification of the produced maps.

The success of this method is based on the exploitation of the main advantages of neural networks and watermarking techniques in the design of the Intrusion Detection engine, which is part of a local IDS agent.

Malicious nodes in MANET may target to exploit features of the physical, MAC or network layers. The majority of the so far proposed security approaches in such networks has focused in the network layer, while little attention has been paid on the MAC layer security. The role of the MAC layer in wireless ad hoc networks is substantial, as it is responsible for maintaining the communication between nodes and the scheduling of the access in a shared radio channel. The MAC layer is directly affected by almost every intrusion, since it is placed in the first layers of the protocol stack.

III. SYSTEM MODEL

System model consist of the architecture diagram of the entire work. This explains clearly what the proposed work is.

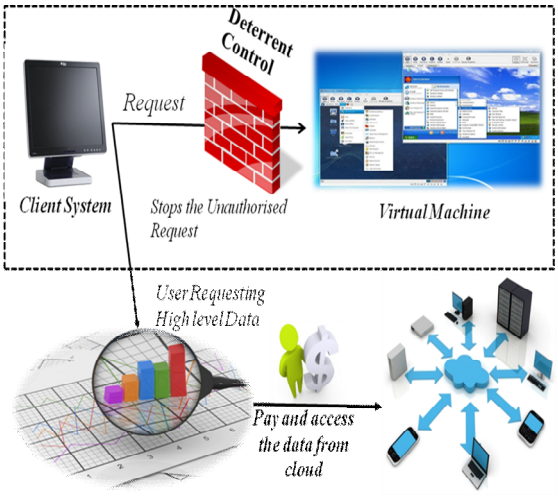


Figure 1. Architecture Diagram

A. Cloud environment

The public cloud is used here for storing the details of the users. Public cloud allows system and services to be easily accessible to the general public. Public cloud may be less secure because of its openness. Deterrent done in the cloud provides additional security to the data.

B. Result

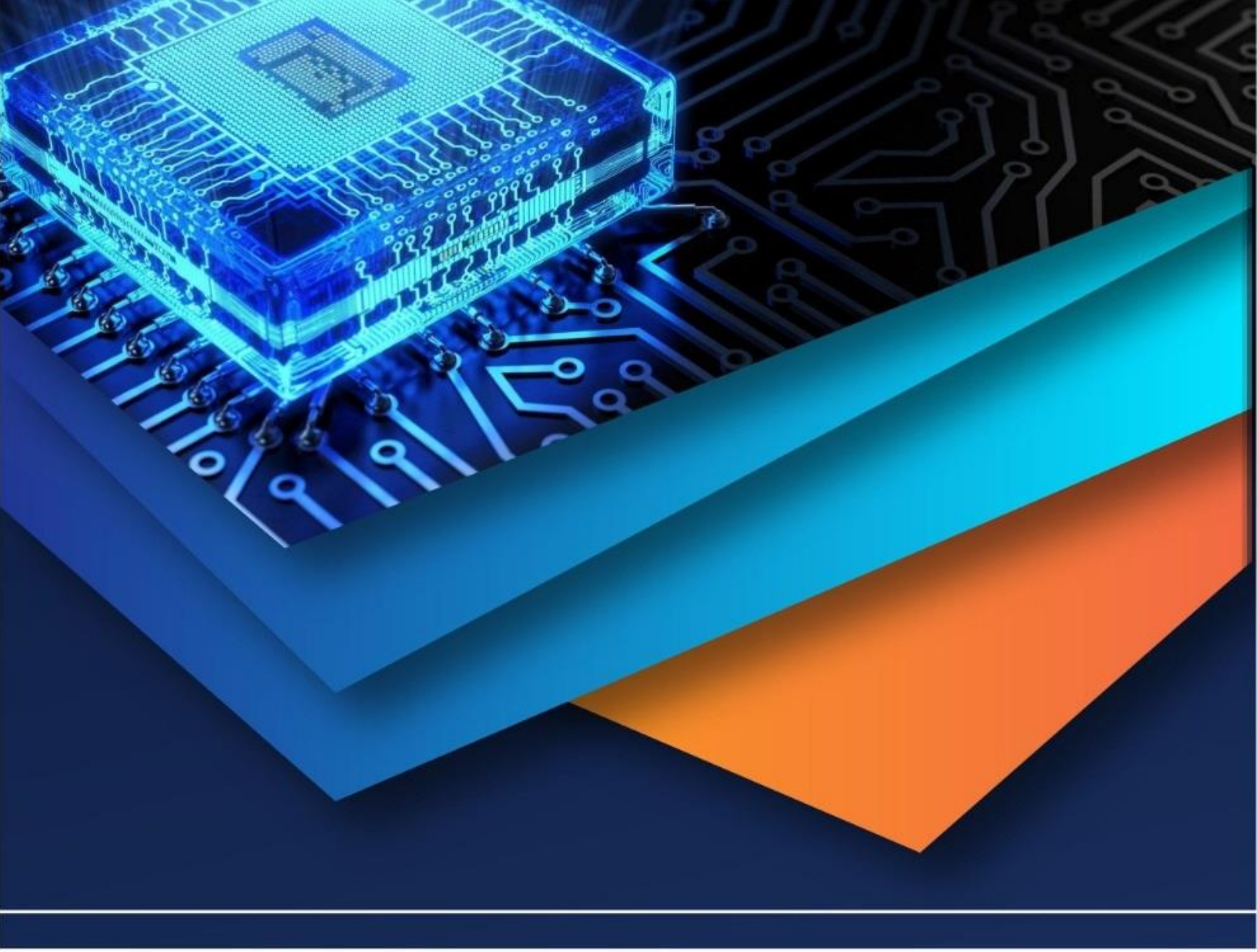
Deterrent is used for providing security in a private cloud system it is handled by system administrator. You can track the user who entered to the cloud server to access the authorized data.

IV.CONCLUSION

A main goal of project is a Cloud service discovery system. It is specially designed for users who want to find a Cloud service over the internet. A Cloud ontology is also introduced for enhancing performance of the CSDS. The contributions of this work include: 1) building of the Cloud service discovery system and 2) constructing the Cloud ontology. It is the first attempt in building an agent-based discovery system that consults an ontology when retrieving information about Cloud services. When the Cloud computing is more commonly and widely used in the near future, it can be helpful for Cloud users who want to find a Cloud service under their specific preference. By consulting a Cloud ontology to reason about the relations among Cloud services, the CSDS is more successful in locating Cloud services and more likely to discover Cloud services that meet consumers requirements. Since this is an on-going work, the Cloud service discovery system is currently being enhanced future works include: 1) making more depth of the Cloud ontology so that it can make more difference between two services in terms of service utility and 2) completing functionalities of query processing, filtering and rating. which have been partially implemented.

REFERENCES

[1] L. Youseff, M. Butrico, and D. Da Silva, “Towards a unified ontology of cloud computing,” in Proc. 2008 Grid Computing Environments Workshop
[2] J. E. Smith and R. Nair, “The architecture of virtual machines,” IEEE Internet Comput., May 2005.
[3] J. Somorovsky “All your clouds belong to us—security analysis of cloud management interfaces,” in 2011 ACM Comput. Commun. Security Conf..
[4] T. Garfinkel and M. Rosenblum, “A virtual machine introspection based architecture for intrusion detection,” in Proc. 2003 Netw. Distrib. Syst. Security Symp.
[5] H. Takabi, J. B. D. Joshi, and G. J. Ahn, “Security and privacy challenges in cloud computing environments,” IEEE Security Privacy, vol. 8, no. 6, Nov.–Dec. 2010.
[6] J. Pfoh, C. Schneider, and C. Eckert, “Exploiting the x86 architecture to derive virtual machine state information,” in Proc. 2010 Int. Conf. Emerging Security Inf., Syst. Technol.
[7]. S. T. Jones, et al., “VMM-based hidden process detection and identification using lycosid,” in Proc. 2008 ACM Virtual Execution Environments.
[8] C. Yu, et al., “Protecting the security and privacy of the virtual machine through privilege separation,” in Proc. 2013 Int. Conf. Comput. Sci. Electron. Eng.
[9] T. C. Chieu, et al., “Dynamic scaling of web applications in a virtualized cloud computing environment,” in Proc. 2009 IEEE Int. Conf. e-Business Eng.
[10]. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network support for IP traceback,” ACM/IEEE Trans. Netw., vol. 9, no. 3, pp. 226–237, June 2001.
[11]. R. Stone, “CenterTrack: an IP overlay network for tracking DoS floods,” in Proc. 2000 Usenix Security Symp.
[12].B. Balacheff, et al., Trusted Computing Platforms — TCPA Technology in Context. Hewlett-Packard Books, 2003.
[13].H. Debar, D. Curry, and B. Feinstein, The Intrusion Detection Message Exchange Format, RFC 4765, Mar. 2007.
[14]. J. Ryan and M. J. Lin, “Intrusion detection with neural networks,” inProc. 1998 Advances Neural Inf. Process. Syst.
[15]. S. Bahram, et al., “DKSM: subverting virtual machine introspection for
fun and profit,” in Proc. 2010 IEEE Symp. Reliable Distrib. Syst
[16]. Y. Zhang, et al., “Cross-VM side channels and their use to extract private
keys,” in 2012 ACM Comput. Commun. Security Conf.
[17]. J. Idziorek, M. F. Tannian, and D. Jacobson, “The insecurity of cloud utility models,” IEEE Cloud Comput., pp. 14–18, May–June 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY