International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 36 • 2017

A Comparative Analysis of Approaches to Prevent Data Leakage Over Public Cloud

Arun Kumar Yadav[a] Rajendra Kumar Bharti[b] and Ram Shringar Rao[c]

[a]*Ph.D. Scholar, Department of CSE, Uttarakhand Technical University Dehradun, Uttarakhand*
E-mail: arun26977.utu@gmail.com
[b]*Department of CSE, BTKIT Dwarahat, Uttarakhand*
E-mail: rajendramail1980@gmail.com
[c]*Department of CSE , IGNTU Amarkantak, Madhya Pradesh*
E-mail: rsrao08@yahoo.in

Abstract: Since last few years, cloud computing is in demand due to its resource sharing capability. Cloud computing offers XaaS services to the end users on rental basis. Due to this, storage infrastructure at cloud may be shared among multi-tenant and exhibited the data on shared storage to be accessed by unauthorized users. This ensample challenges the data security, unauthorized access control or haphazard host access at multitenant storage environment. These challenges limit the number of databases to be shifted over the public cloud. This paper presents a comparative analysis of approaches to prevent data leakage over public cloud and open a way to transfer the private databases over public cloud with improved performance.

Keywords: *XaaS; multi-tenant storage; public cloud; data security; data leakage.*

1. INTRODUCTION

Cloud computing offers economical and great performance benefits to businesses and organization through the use of information technology but due to risk factors associated with multi-tenancy public cloud, most of the companies are not accepting the cloud computing. In multi-tenancy public cloud environment, computing services and applications of companies are running on virtual machines (VM) with other company's virtual machines (VM) hosted on shared infrastructure [1]. One of the major security risks with multi-tenancy environment is that data may be exposed to a third party due to many factors. This is referred to as data leakage. As per the Gartner's survey, virtualized servers are less secured than physical servers [2] and companies would not adopt cloud computing for the reason of security and data privacy issues. Therefore, cloud service providers (CSP) need to resolve the security and related issues with high quality services.

Data leakage can be defined as unauthorized transfer of data to the third party. Data leakage may be happened in multi-tenancy or in private cloud environment but its probability is high in public cloud. Number of techniques have been proposed by the researchers to prevent the sensitive data from data leakage over public cloud.

National *e*-governance division is also initiating to start various *e*-projects where users will not be required to submit hard copies of documents anywhere. In reference to successful implementation of *e*-governance projects, safe and secure private space on public cloud needs to be reticent.

The rest of the sections in paper have been organized as follows: Section 2 discusses the related works proposed by authors. Comparative analysis of Approaches/Models has been discussed in Section 3. Section 4 concludes the work and suggests the future directions for further research.

2. RELATED WORKS

Author proposes a protocol [3] which allows a third party auditor to work on behalf of data owner to maintain the data security and access control during outsourcing of complex data. Proposed scheme offers the data auditing without demanding the local copy of data. Also, at the same time TPA does not learn the knowledge about the data stored on cloud. The audit protocol constructs a scalable framework to ambush the fraud and reduces the data leakage over cloud. The proposed scheme is light-weight, preserves the privacy and also determines the corrupt data. On the other hand, this scheme increases the additional computational cost and does not ensure the data security from malicious users.

Security model inflicts the access control to storage devices in SANs and address the issues where single N_port of storage device in SAN network can be shared among many logical servers [4]. The approach based on OSD security model is based on mapping the objects to LUs at storage devices. Model classifies the SCSI commands as **read**, **write** or **control** and three bits of code given to the users to access the LUs. The given three bits of code to the users contain the privileges that users have on mapped LUs. The model uses a channel id to perform read, write or control. Thus it is considered to maintain the integrity and reliability of transport channel. Apart from all the features mentioned above, this model does not include the client authentication and secured VM provisioning.

VMware ESX server [5] offers high security and isolated access of virtual machines. Only particular storage units can be seen and accessed by the virtual machines as the ESX server administrator permits. Operating system on virtual machines cannot be configured to discover the other units which are not permitted by the ESX administrator. Multiple ESX servers now perform concurrent access storage in isolated manner. This protection mechanism enables the progressive service as VMotion. Although, the VMotion is supported by server but it is vulnerable in virtual machine provisioning in multitenant environment.

Four approaches have been proposed for LUNs security from intruders [6]. First approach is, where host software interlopes the I/O requests from a LAN to file server for getting the permission to access the storage which is under the control of file server. But, this approach has a limit with the SCSI release in the SCSI-3 specifications that has not been implemented by vendors. Other complications with the approach is about its implementation at hardware level because software vendors uses non-standard file system like Data Direct, Mercury Computer Systems, CrosStor.

In second approach, authors have proposed LUNs security using drivers which mask off the LUNs so that particular host will not be able to scan. This approach offers the operators to set the list of WWNs and LUNs for the authorized hosts. The solution has limits in large installations because it needs to ensure the proper partitions of LUNs across all hosts consoles. Other limitation is with rogue servers which may not coordinate its security services with other servers.

In third approach, authors have discussed Switch Zoning, which offers port level masking for all the nodes that are known to the switch using hosts. All the hosts will be able to see all the LUNs that are addressed through that port. Limitation with proposed approach is less flexibility but offers extensive security between initiator and targets attached on the switch. Whereas, fourth approach is mapping within a storage controller, storage subsystem such as Freedom Storage 7700E offers the masking within the storage controller. This approach gives the access to different LUNs on same storage port, is independent of any SAN infrastructure and limits the initiator to see only masked LUNs. Mapping within a storage controller approach does not support mixed environment of different vendor's storage devices.

The technical report presented by VMware[7] have introduced ESX Server 2.5, which support raw device mapping and uses a special file in VMFS volume to act as a proxy for raw devices. The said file maintains the metadata to manage and redirects the access to the raw LUNs. ESX Server 2.5 supports the VMotion to migrate the VMs and distributed file system features like file locking and permissions over VMs. Having all these advanced features, server does not support the devices attached to shared adapter and there is no redo log facility in physical compatibility mode.

VMware presented a report [8], that introduces VMware ESX Server 3.0.1 which offers Virtual machine file system (VMFS), virtual raw device mapping (RDM) and physical raw device mapping. VMFS and RDM proffers file locking, permissions, tenacious naming and VMotion. RDM feature in ESX server supports clustering between VMs or between physical and virtual machines at lower level disk control but the report does not touch the security domain in multi-tenant environment.

Two-level HIBE scheme has been presented to support the availability and consistency of the shared data among multi-users in cloud computing environment [9]. HIBE assures the data confidentiality in un-trusted cloud and interdict the data leakage and enables one-to-many encryption standard. Presented scheme has low overhead over computation, user revocation, storage and communication. On the other side, privacy issues have been raised by the author in scheme.

SLIM security model [10] presents an isolation scheme for tenant in existing application level security. Security model has considered two types of malicious users. In case 1 malicious user may belong to same tenant and may try to access the resources of other user and in case 2 malicious users try to access the resources of other tenant users. Every system user in this model will have a unique id and resources are assigned on user id. Resources belonging to one user id will not be accessed through other user id. SLIM take action to ensure the right tenant privileges and upsurge of privileges. Security model blocks all the data access requests that do not emanate from the gatekeepers. But, Application level security presented here may not be sufficient to secure the users' data in multi-tenant cloud.

Approach presented in [11] continuously validates the user interactions with a system and takes the automated preemptive actions to protect the system. A pre-defined road map of entire system is created for the valid users and added to finite state machine (FSM) database. The protection system monitors the user's interaction with the system. A log file of user interaction is generated and investigates with the FSM database to identify the attacker. The approach uses a special code known as spore which collects the information of user's activities in system. If any malicious user is identified then a duplicate environment is created with false data. The major issue with approach is its complexity for multi-tenancy cloud environment because system monitoring cause addition loads.

Furthermore, the preceding schemes proposed by several authors resolve some of the security issues with storage infrastructure but major issues are intact in multi-tenant public cloud environment and it has been confirmed from the previous approaches that application level security solutions are not plentiful for storage infrastructure security. The ensuing sections present the comparative analysis of approaches on various parameters and also identify the issues that can figure out in further research.

3. COMPARATIVE ANALYSIS

In this section, we have identified the following parameters for comparative analysis of preceding approaches. The keys for the selected parameters are shown in Table 1.

The parameters have been assigned ranges between 1 and 5. The highest value to any parameter states that the approach is performing exceptionally well in that parameter and lowest value states that the approach is lagging.

Table 1
Keys and Parameters

Keys	*Parameters*
CC	Computational cost
DSMP	Data Security in Multi-tenant Public Cloud
CA	Client Authentication
VMP	VM provisioning in Multi-tenant Public Cloud
HC	Hardware Compatibility

Table 2
Comparision of Approaches/Models

S. No.	*Proposed Approaches/Models*	*CC*	*DSMP*	*CA*	*VMP*	*HC*
1.	TPA	1	1	1	1	4
2.	OSD	2	3	2	1	2
3.	ESX Server (ES)	3	2	3	1	2
4.	Host Software (HS)	2	3	2	1	3
5.	Driver	3	2	1	1	2
6.	Switch Zoning (SZ)	2	4	4	2	1
7.	Masking within Storage controller (MSC)	3	2	4	1	1
8.	ESX Server 2.5 (ES-2.5)	3	4	4	3	2
9.	ESX Server 3.0.1 (ES-3.0.1)	3	4	4	3	2
10.	HIBE	3	3	2	2	3
11.	SLIM	2	2	3	1	3
12.	FSM	1	2	1	1	3

Table 2 shows the comparisons of preceding approaches/ models based on listed parameters. Evaluated parameters define the quality of proposed approaches/models. The comparative analysis has been shown in Fig. 1.(*a*) and Fig. 1.(*b*).

Fig. 1.a shows the comparative analysis of TPA, OSD, ESX Server (ES), Host Software (HS), Driver and switch zoning (SZ) approach on the basis of defined parameters as computational cost (CC), data security over multi-tenant public cloud (DSMP), client authentication (CA), VM provisioning in public cloud (VMP) and hardware compatibility. Fig. 1.a undoubtedly shows that base ESX server and driver approach has low overhead on computational cost, Object-based storage device (OSD) and Host software is performing well over data security in multi-tenant public cloud but is not up to the highest level which is required. Only base ESX server giving accepted on client authentication and TPA and Host software are quite excellent over hardware compatibility but no approach is offering virtual machine provisioning in public cloud.

Analysis of switch zoning (SZ), masking within storage controller (MSC), ESX server 2.5 (ES-2.5), ESX Server 3.0.1 (ES-3.0.1), HIBE, SLIM and FSM approaches have been presented in Figure 1.b. Masking within storage controller, ESX server 2.5, ESX Server 3.0.1 and HIBE shows low overhead on computational cost, whereas switch zoning, ESX server 2.5 and ESX Server 3.0.1 offers excellent security in multi-tenant public cloud environment which can be taken as a reference to prevent the data leakage in multi-tenant public cloud environment. Switch zoning, masking within storage controller, ESX server 2.5 and ESX Server 3.0.1 are ensuring the high level of client authentication to block the malicious users. ESX server 2.5 and ESX Server 3.0.1 support the fair VM provisioning features. HIBE, SLIM and FSM approaches are portable with any storage environment.

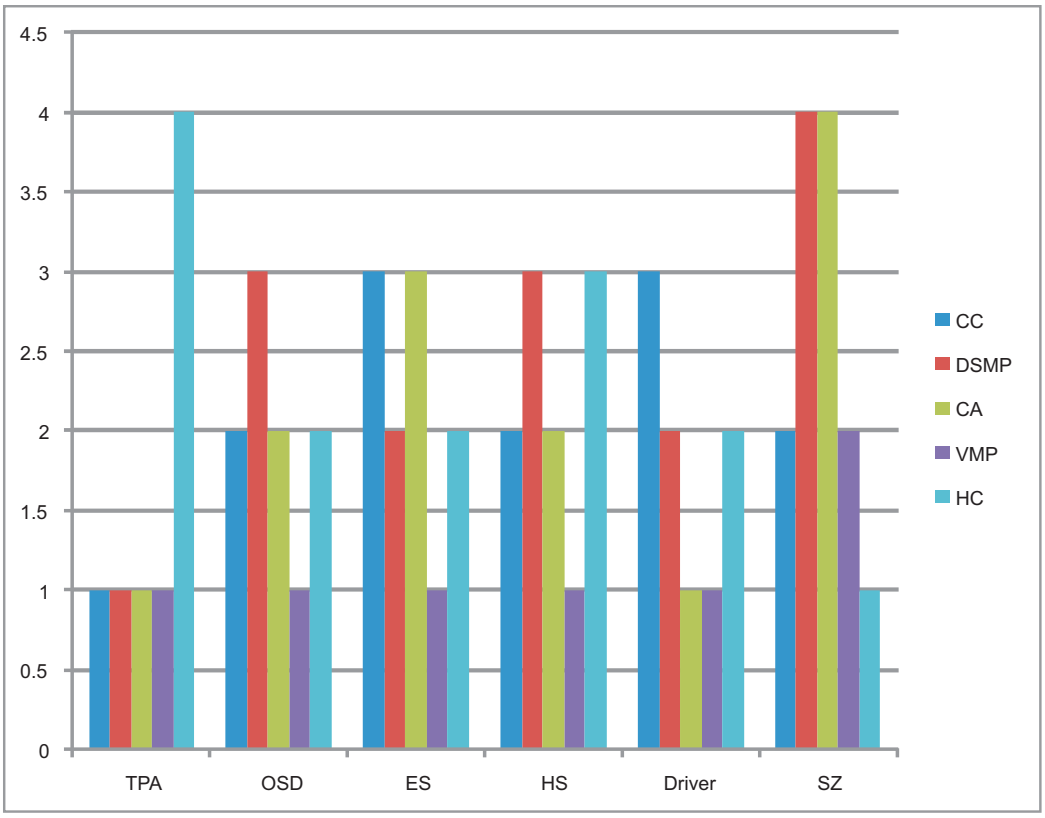

Figure 1: (*a*) Comparison of S. No. 1-6 Approaches/Model

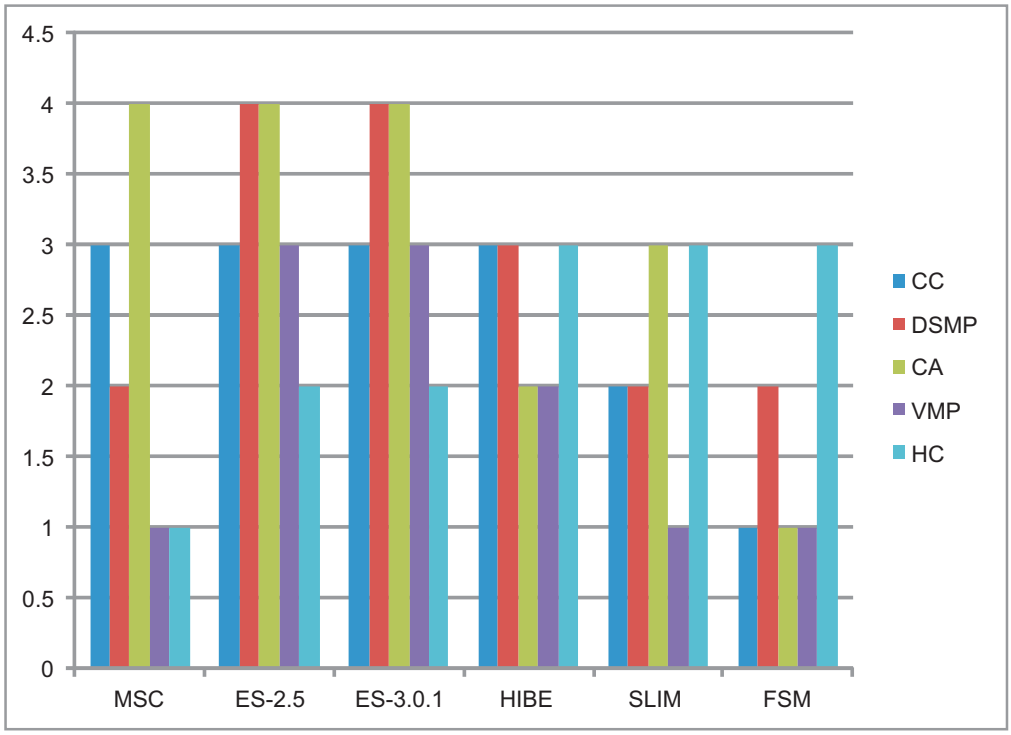

Figure 1: (*b*) Comparison of S. No. 7-12 Approaches/Mode

The analysis presented in this section clearly shows that switch zoning, ESX server 2.5 and ESX server 3.0.1 supports excellent security in multi-tenant environment over public cloud and also offers satisfactory results in virtual machines provisioning over the same environment.

4. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we have presented comparative analysis of approaches/models to prevent data leakage in multi-tenant environment over public cloud. The results presented in previous section shows that switch zoning, ESX server 2.5 and ESX server 3.0.1 are offering exemplary security and VM provisioning services in multi-tenant public cloud. Cloud computing offers pool of storage and other IT resources shared by users. This leads the security and privacy problems over public cloud. Number of companies/organizations are maintaining their own private servers with limited resources and compromising with performance and availability services. Companies/ organizations are needed to shift their private data over public cloud to have the improved performance and data availability 24x7 but due to unavailability of sufficient security solutions, private data has not been moved to public cloud. The only application level security solutions are available and used by most of the cloud service providers (CSP) for securing the data over public cloud which is not adequate and unassailable. Application level security offers only single level security which can be easily bypassed by attacker and results into data leakage. Hardware level security solutions can only secure the private data over multi-tenant public cloud and will ensure the companies to move their data over secured public cloud and definitely will improve the performance and data availability.

Switch zoning, ESX server 2.5 and ESX server 3.0.1 approaches can be used to propose hardware level security solutions for public cloud. In our future work, we will use these approaches to propose secure architecture and algorithm to resolve the security issues over multi-tenant public cloud.

REFERENCES

[1] Bobbie Johnson. (2012). Business still wary of the legal and security issues concerning cloud computing. Available: http://gigaom.com/cloud/security-still-the-no-1-obstacle-to-cloud-adoption

[2] Stamford, Conn., (March 15, 2010). Available: http://www.gartner.com/it/page.jsp?id=1322414

[3] Dr. S.Sakthivel, B. Dhiyanesh: A privacy-preserving storage security for spatial data in dynamics cloud environment. In: 4th IEEE Conference ICCCNT 2013, pp. 225-231.IEEE Press,(2013)

[4] Michael Factor et. al.: Capability based Secure Access Control to Networked Storage Devices. In: 24th IEEE Conference on Mass Storage Systems and Technologies (MSST 2007). pp. 114 – 128. IEEE Press, San Diego, CA.(2007)

[5] VMware. (2006).VMware ESX Server: Providing LUN Security. Available: http://www.vmware.com/pdf/esx_lun_security.pdf

[6] Hu Yoshida. LUN Security Considerations for Storage Area Networks. Hitachi Data Systems. December 2013. Available: ftp://utcc.utoronto.ca/docs/9985V/Hitachi/Whitepapers/WP91%20San%20Lun%20Secur.pdf

[7] VMware. (2015).VMware ESX Server: Using Raw Device Mapping. Available: https://www.vmware.com/pdf/esx25_rawdevicemapping.pdf

[8] VMware. (2015). VMware ESX Server 3.0.1: Performance Characteristics of VMFS and RDM. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmfs_rdm_perf.pdf

[9] Xin Dong et. al.: SECO: Secure and scalable data collaboration services in cloud computing. Journal on Computers & Security. Elsevier, 50, 91-105 (2015)

[10] Michael Factor et. al.: Secure Logical Isolation for Multi-tenancy in Cloud Storage. In: 2013 IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST). pp 1 – 5. IEEE Press, Long Beach, CA(2013)

[11] Jason Flood et. al.: A Proposed Framework for the active detection of security vulnerabilities in multi-tenancy Cloud Systems. In: 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT). pp. 231-235. IEEE Press, Bucharest (2012)