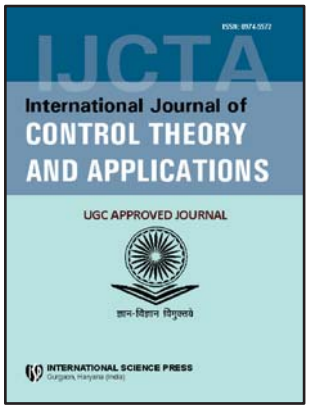

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 31 • 2017

SuVa Security Framework for Cloud Migration

Ir. Vadivu Vijayaragavan[a] and K. SivaSankar[b]

[a]*Research Scholar, Department of Computer Science and Engineering, Noorul Islam University Kumaracoil, Thuckalay, Kanyakumari District, Tamilnadu State, India- 629 180*

E-mail: vadivuv@gmail.com

[b] *Assistant Professor, Department of Information Technology, Noorul Islam University Kumaracoil, Thuckalay, Kanyakumari District, Tamilnadu State, India.*

Abstract: Cloud computing is one of the emerging fields in the computer world these days. Now companies are shifting their focus onto cloud computing. Cloud migration is the process of transitioning all or part of a company's data, applications and services from onsite computers behind the firewall to the cloud or moving them from one cloud environment to another. If vulnerability is present in the premise's data then soon after the migration to the cloud, the vulnerability also in turn is been transferred to the cloud environment. This paper mitigates this issue and presents a solution for. This paper focuses to present the methodology as a security framework.

Keyword: *Cloud Computing, Cloud Security Framework, Cloud Vulnerability Assessment, Cloud Penetration Testing, Cloud Migration Framework, Migration, Security Framework.*

1. INTRODUCTION

The CSA (Cloud Security Alliance ed..) Guide defines Cloud Computing (CC) as, "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.* networks, server, storage, applications, and services) [1]. Categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. Vulnerability refers to the security flaws in a system / cloud that allows an attack to be successful. A vulnerability scanner can scan an entire cloud system for known vulnerabilities typically work in conjunction with a database full of known vulnerabilities and cross check the database with any exploits the scanner may find. Vulnerability Assessment is the process of pinpointing, computing and ranking the vulnerabilities in the system [11]. Therefore, it is necessary for cloud administrators to provide a service to scan and test the resources of their clients for the benefit of both, despite the load on the cloud to perform the service. At present, the cloud provider scans the resources after migration of the client's data in cloud. This evolves in a bigger risk that when the client's data/application/operation system is already affected/infected with malware then the entire cloud infra is affected.

If vulnerability is present in the premise's data then soon after the migration to the cloud, the vulnerability also in turn is been transferred to the cloud environment. This causes high risk to the whole cloud environment by transferring the vulnerability into the cloud and giving a chance to the attacker to inject malware. This issue is mitigated in this paper and presents a solution for this. It has been further investigated taking that time and money factors, this paper focuses only on what's methodology is all about and shows how this can be extrapolated in implementing this framework in real time environment. SuVa Security Framework can be inserted in Cloud Computing layer to list out the vulnerabilities proactively. This paper will not focus on implementation and validation part of this framework.

2. LITERATURE REVIEW

B. Grobauer et al., 2011 [2] helps to understand the vulnerabilities in detail by defining and examines the factors contributing to risk according to the Open Group's risk taxonomy. It describes NIST five essential cloud characteristics of vulnerabilities. Architectural components and vulnerability's cloud service models is presented and discussed about cloud software infrastructure and environment, computational resources, storage and communication.

A. Durrani et al., 2014 [3] highlights the vulnerabilities that exist in applications available on the cloud and aims to make an analysis of different types of security holes found in these applications by using open source vulnerability assessment tools. It identifies the security requirements pertinent to these applications and makes an assessment whether they met these requirements by testing two of these applications using the vulnerability tools. It also provides remedial measures for the security holes found in these applications and enables the user to select a secure provider for themselves while at the same time enabling the cloud provider to improve their services and find a competitive edge in the market.

R. C. Chiang et al 2015 [4] presented a novel I/O workload based performance attack which uses a carefully designed workload to incur significant delay on a targeted application running in a separate VM but on the same physical system. Such a performance attack poses an especially serious threat to data-intensive applications, which require a large number of I/O requests. Performance degradation directly increases the cost of per workload completed in cloud-computing systems. Experiment results demonstrated the effectiveness of our attack on different types of victim workloads in real-world systems with various numbers of VMs.

3. SUVA SECURITY FRAMEWORK FOR CLOUD MIGRATION

The objective of SuVa Security Framework (SuVa SF) uses combination of automated tools and techniques. This process undertakes analysis of on-premise's (source) infrastructure or/ or web application in order to determine the existence of and the extent of any vulnerability. All vulnerabilities are then categorized against criteria of Criticality, Exploitability, Impact and Probability; this will illustrate the true risk levels and provide "in-context" advice, how these vulnerabilities can be mitigated by means of possible solution, which shall be agreeable by both organization and cloud service providers. Vulnerability assessment service will provide with a detailed report on vulnerabilities and a range of recommendations to help to overcome issues listed. Further, vulnerability assessment will be carried out which is followed by penetration testing to validate vulnerabilities found during scan. The findings of the vulnerability assessment & penetration testing are mapped against solution / action that need to be taken.

Reports are tailored made by report engine, to meet the needs of the organization and cloud service provider. It shall provide delivering high quality professional reports that outlines clearly the vulnerabilities identified during the assessment, their potential impact and more importantly report recommends processes for

remediation. These reports are designed to be relevant and readable at all levels of organization, in particular to the technical teams who are responsible for executing potential solutions indicated. Since the SuVa SF uses various techniques to scan variety of vulnerable categories, report will be compiled and delivered as consolidated specified by stakeholders.

3.1. Introduction SuVa Security Framework

"SuVa Security Framework for Cloud Migration" is methodology presented in this chapter. During On-premise to Cloud migration, the application and / system data transferred to Cloud Infrastructure. The problem is that vulnerability and / or threats, which exist already in the premise, are migrated to Cloud. Only after the completion of migration, cloud provider initiates for the vulnerability scan and addresses the issue. The SuVa security framework presented below provides the methodology wherein these vulnerability scans are done proactively before loading into cloud environment.

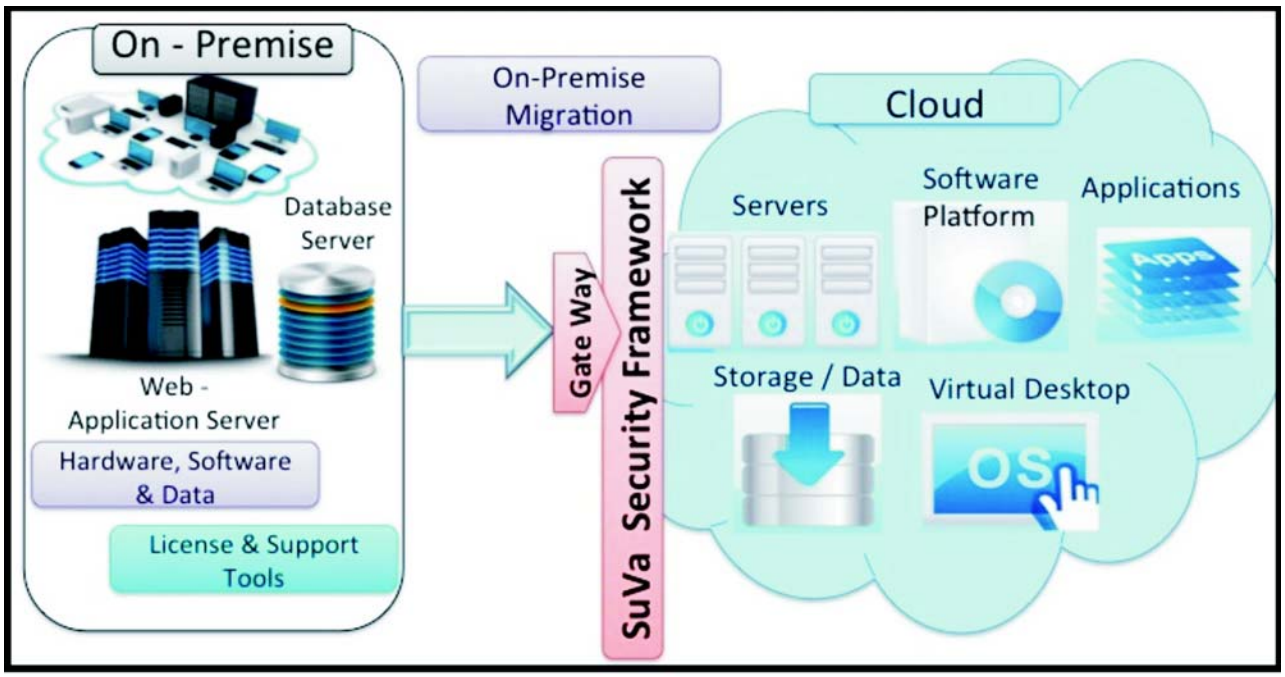

Figure 1: On-premise to Cloud Migration with Security Framework

This security framework is embedded in CC architect (Fig 2). So in the course data migration process it goes through the SuVa Security Framework as a Gateway to enter the cloud server. During this process of migration, data is simultaneously scanned for vulnerability assessment and corresponding reports are delivered. Thus SuVa Security Framework is a methodology, which proactively does the vulnerability assessment in cloud deployments. Each component of security framework is explained in detail. SuVa security framework is presented in Cloud Computing architecture as 'to-be' scenario.

Fig 1 shows the On-Premises to Cloud migration and the Security Framework at the entry "Gateway" point of cloud environment at a high level. This figure provides an idea where the framework stays in cloud.

SuVa Security Framework (SuVa SF) thus can be represented as a layer in the Cloud Computing Architecture Layer. It is another form of representation within the Cloud Computing framework Fig 2.

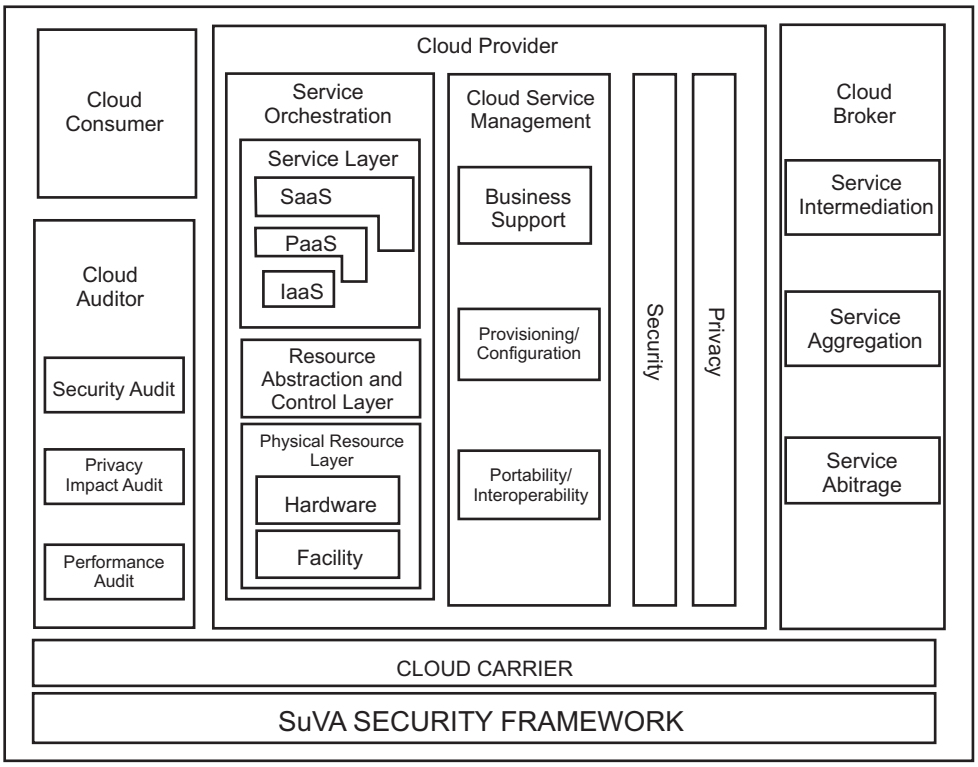

Figure 2: Cloud Computing Architect with SuVa Security framework

3.2. SuVa Security Framework

Following paragraphs illustrates the SuVa SF in detail. SuVa SF has Security Module Platform in which the framework deployed. SuVa SF has six actors namely (*i*) Business Logic (*ii*) Workflow Engine (*iii*) Scheduler (*iv*) Scan Engine (*v*) Reporting Engine and (*vi*) Validation. All six actors play a vital part in the SuVa SF.

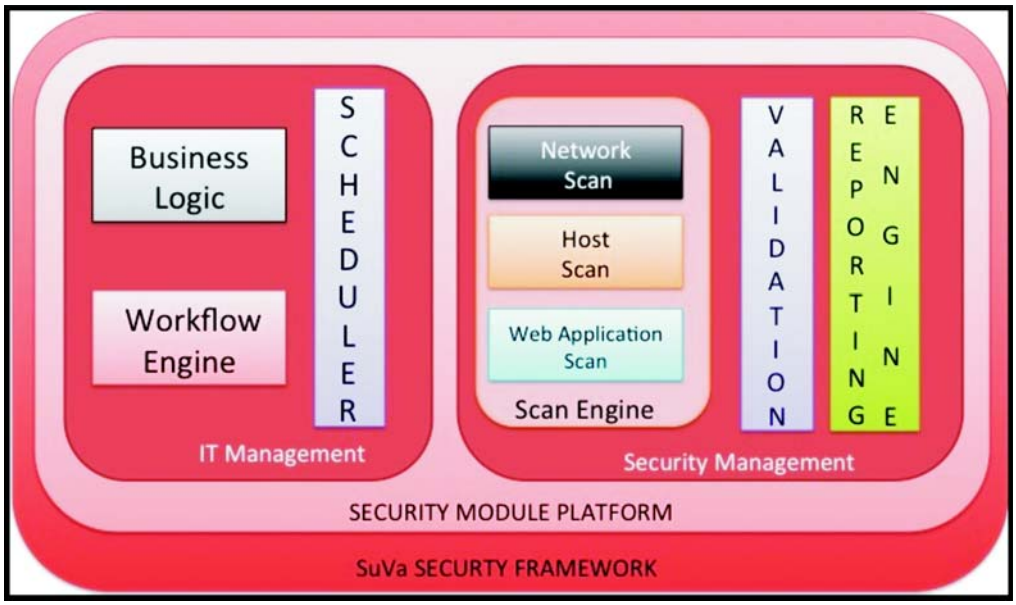

Figure 3: SuVa Security Framework

Business logic, workflow engine and scheduler are core components of IT management. Scan engine, reporting engine and validation are part of security management / vulnerability management.

Business Logic : First step is to identify the business rules applicable to various scenarios taking into consideration of source system's data that might trigger logic necessary for three broader categories of vulnerabilities; network scan, host based scan and web application based scanning. This business logic should be designed and developed based on case-to-case basis. Business logic basically determines what level of details that scanning should perform. For example, business logic would define to scan for agentless auditing, reporting and patch management integration in case of network based scanning.

The impact of business logic varies from application to application.

Business logic tests should be designed to ensure that (*i*) the control is in place to implement the business rule, (*ii*) the control is implemented correctly and cannot be bypassed or tampered with, and (*iii*) the control is used properly in all the necessary places. Business rules should be clearly defined and checked against during the different development phases of the framework: design, implementation and testing. Clear documentation and threat modeling/abuse cases and code reviews should be used.

Workflow Engine : Basically the workflow engine calls various type of vulnerability scans periodically as defined by scheduler. Depending on the business logic already defined the workflow acts. For example, as defined in the business logic the workflow triggers the all three categories of scan sequentially. After completing of the scan, the next action validation takes place. Fig 4 exhibits a simple flow chart of an example workflow.

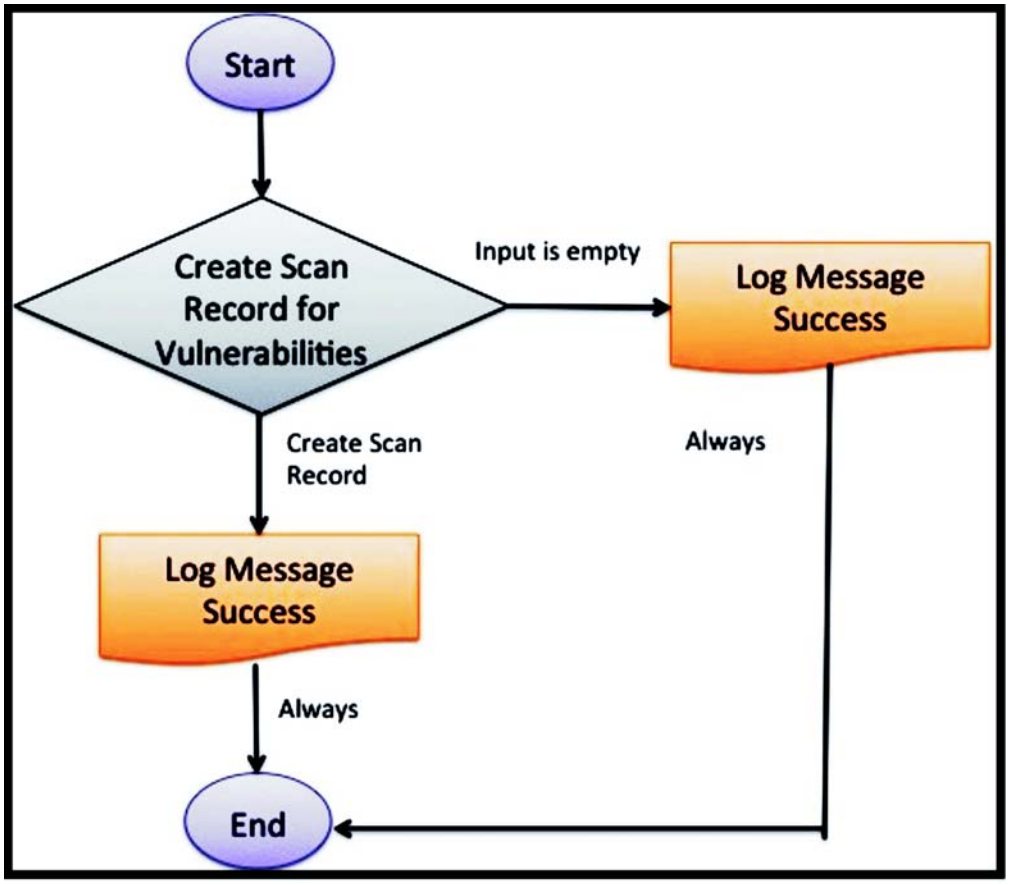

Figure 4: Workflow Diagram

Scheduler : Scheduler is a component of SuVa SF that provides the ability to schedule the launch of programs or scripts at pre-defined times or after specified time intervals. Task scheduler / Scheduler to automatically start and stop certain tasks at defined times and intervals. The task scheduler to start and stop certain automated tasks out of hours while not working, and to save work periodically or at a specific time. Each task needs to have a start time configured. Optionally, configure the task to repeat at a defined interval. For example, schedule a task to run a backup results script every night. Scheduler should be already programed to trigger the certain workflow. Workflow is been already predefined to execute certain task which process is clearly linked to business logic.

Scan Engine – Reporting – Validation : Scan engine component consists of network scan, host scan and web application scan. The SuVa SF executes three level of scanning mentioned above. These are the core components of SuVa SF, where the actual vulnerability scans takes place. During this process, the data are scanned for all vulnerabilities found in network based, host based and web application based. In common practices 'as-is' note that only certain type of tool does certain category of scans whereas in SuVa SF, all category of vulnerability assessment scans executed together with penetration testing which takes place as per the work flow instruction. When the scans completed, reports are stored in the report engine. The main task of the report engine is that it will compile the reports delivered by the various categories of scans and delivers a consolidated report. The consolidated report contains both vulnerability and penetration test reports. In 'as-is' scenario the reports are delivered only tools wise individual reports with separated reports for vulnerability assessment and penetration testing report.

The vulnerability assessment and penetration testing reports address all the issues found the system / server / storage. Reports not only contain the issues to address but also deliver the possible solution to eradicate the issue.

3.3. Execution Flow of SuVa Security Framework

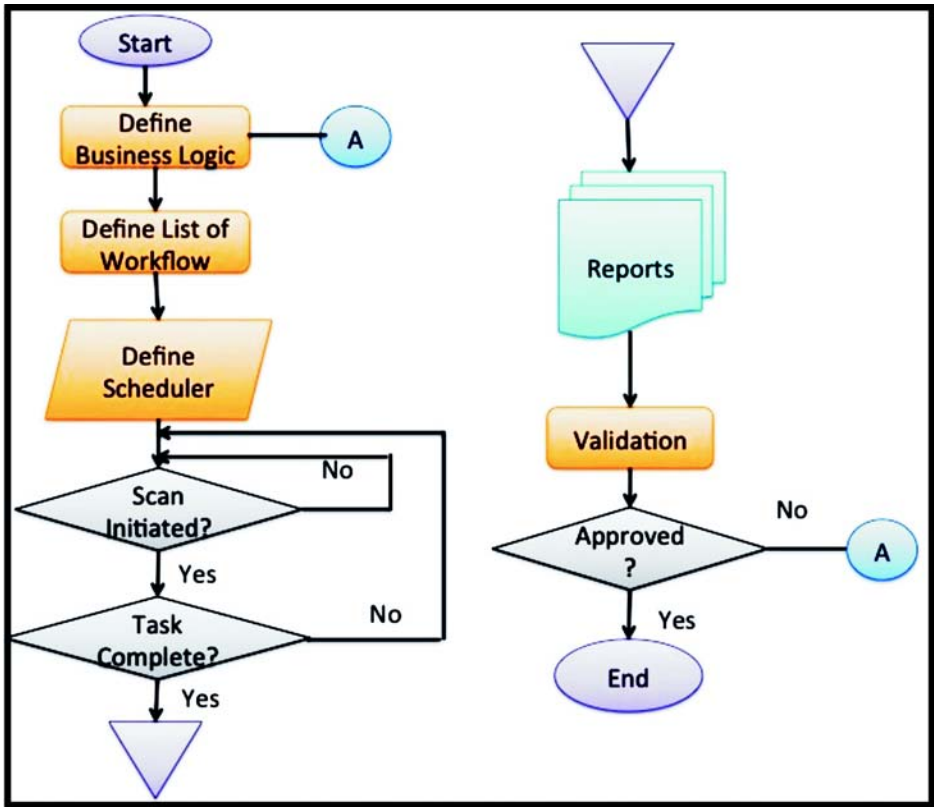

Figure 5: SuVa Security Framework – Flow Chart

Execution of the flow of SuVa SF is as follows; first for any transfer of data to the cloud business logic(s) is to be defined prior. Business logic can vary upon for each every business process as the case may be. Once this is done, workflow is defined for which processes, what are the vulnerability assessments and penetration tests need to be carried-out. Once the workflow is finalized the time bound is defined on workflow basis. Thus the scheduling is defined for all the processes that are present in the system.

Scheduler thus initiates the scan process for vulnerability assessment and penetration testing. When the task is completed then the reports are generated. When scan is not initiated then it is again sent back scan again. When the task is not completed then again the scan is initiated. Reports thus generated are complied and designed to produce a consolidated view of all categories of vulnerabilities and outcome of penetration testing. Then the validation process takes place. Once the validation process ends successfully, the process ends. When the validation is not successful then the process will be started again.

4. CONCLUSION

In this paper, SuVa Security Framework is proposed architecture that acts as a gateway into the cloud during on-premise to cloud migration. Framework proactively initiates the scan process for vulnerability assessment and penetration testing of on-premise data before migrating the data into the cloud. By implementing SuVa framework, the results delivered are highly reliable. Results thus delivered validates with list of vulnerabilities found in the on-premise's data. At present there is no such framework exists that proactively initiates to find vulnerabilities in on-premise's data. SuVa Security Framework is an excellent architect framework in real life business scenario, which is a new methodology to be implemented during on-premise to cloud migration. Implementing this methodology brings huge value additions to organization as well as cloud providers, in tackling cloud security (cyber security) issues. It also brings safer and cleaner cloud environment. As discussed in one of the above chapters, the business loss due to the absence of SuVa SF leads to migrate 'Garbage-In' into the cloud, which costs billions of dollars.

Considering the complexity of SuVa SF to implement in the real cloud environment, in near future, planning to qualify this framework in a virtual environment. This will be taken as the continuation of further explorative study.

REFERENCES

[1] Cloud *Security Alliance ed*.. Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0. CSA, 2011. Web 2 April 2012. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf…

[2] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50-57, March-April 2011.

[3] A. Durrani, "Analysis and prevention of vulnerabilities in cloud applications," *2014 Conference on Information Assurance and Cyber Security (CIACS)*, Rawalpindi, 2014, pp. 43-46.

[4] R. C. Chiang, S. Rajasekaran, N. Zhang and H. H. Huang, "Swiper: Exploiting Virtual Machine Vulnerability in Third-Party Clouds with Competition for I/O Resources," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 6, pp. 1732-1742, June 1 2015.

[5] Keiko Hashizume, David G Rosado , Eduardo Fernández-Medina and Eduardo B Fernandez : An analysis of security issues for cloud computing, *Journal of Internet Services and Applications*2013.

[6] J. M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono and N. Marnau, "Security and Privacy-Enhancing Multicloud Architectures," in *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 212-224, July-Aug. 2013.

[7] Sun-young Im, S. H. Shin, Ki Yeol Ryu and Byeong-hee Roh, "Performance evaluation of network scanning tools with operation of firewall," *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, Vienna, 2016, pp. 876-881.

[8] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: *Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg*, Beijing, China, pp 69–79.

[9] Rapid 7 (2012). Metasploit Framework User Guide. Retrieved 31 March 2012 from Rapid 7:https://community.rapid7.com/docs/DOC-1751

[10] Mr. Shrikant D. Bhopale, "Cloud Migration Benefits and Its Challenges Issue", *IOSR Journal of Computer Engineering (IOSR-JCE) ISSN : 2278-0661, ISBN : 2278-8727, PP : 40-45.*

[11] Sachin Umrao, Mandeep Kaur & Govind Kumar Gupta, "Vulnerability Assessment and Penetration Testing"**,** International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012.