International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 3 Issue 1 ǁ Jan. 2015 ǁ PP.28-34

Generic Security Framework for Multiple Heterogeneous Virtual Infrastructures

Darshan R, Chetan Raga
Department of Information Science and Engineering, RV College of Engineering, Bangalore-560059

Abstract **-** Virtualization continues to take center stage at IT industry, yet many organizations are finding it difficult to secure virtualized environments. Security is a critical component in the growing IT system surrounding virtualization. Many organizations find the security challenges associated with virtualization to be a major hurdle, companies of all kinds across all industries are looking towards addressing business and security needs in the virtual infrastructure. There are many research work done before about how to check the compliance status of the cloud platform, not of the virtual machines running on the platform. This paper proposes the security framework for multiple heterogeneous virtual machines which assess the compliance security of the virtual machines. In this paper we make use of REST APIs, using which we create remote session on the virtual machines and fetch the machine values which will be parsed to get the required values for assessment.

Keywords – Security, Compliance, Virtual machines, REST APIs;

I. Introduction

In today's world of fast growing technology which expects good reliability, performance, scalability, cost, agility, security and few other important characteristics, cloud and virtualization has taken its stake compared to other traditional systems by far. This has resulted in drastic increase in the number of cloud vendors. The fact that the vendors are increasing on day to day basis has helped the customers to compare among the vendors based on the above mentioned characteristics and select the more appropriate vendors which suits their system. But to compare among the vendors it is very difficult because the cloud computing is not completely standardized which means there are no certain standardized method to build the system. This applies to security compliance too, where we do not have standard set of security policies based on which the system has to be developed. One of the major security obstacles to widespread adoption of cloud computing is the lack of near-real-time audit ability [1]. And also the terms such as "risk," "threat," and "vulnerability" are often used as if they were interchangeable [2].

Cloud vendors should follow some standardized form of development process which abides by rules and policies given by the security rules vendors of industry standards such as HIPAA [3], PCI etc. The most important concern with cloud computing and virtualization is the various security issues. Although all major cloud vendors provide security measures for their respective clients, it is highly impossible for a client to compare and verify the security measures provided by different vendors under common security policies. Taking this issue into consideration, Cloud security alliance (CSA) [4] has developed policies and guidelines to facilitate a common and secure interface through which a cloud provider is able to provide security information to their clients. Cloud audit is one such framework developed by CSA as a part of the Governance, Risk Management and Compliance (GRC) stack. Cloud Audit mainly focuses on providing a common interface for the auditing process for cloud vendors. Cloud control matrix (CMM) [6] is developed to guide cloud vendors and its clients to assess the complete risk factors related to a particular cloud vendor. The other industry accepted standards are ISACA COBIT [7], HIPAA [8], PCI DSS [9], ISO [10], and NIST [11].

The policies and framework provided from Cloud Audit and CCM are used to check the security compliance of the system in which the related information flow from a cloud vendor, and there are also methods to check how to automatically generate this compliance-related information [12]. But one thing which is still under research is a generic framework which will allow clients to check for the security compliance of their multiple systems such as windows systems, Linux systems as well as virtual systems. In order to develop a generic framework for the security-compliance assessment process of multiple heterogeneous systems, we have used various techniques that will allow us to obtain the required information.

This paper also includes the following sections: Section II introduces the background for issues in cloud computing and security compliance. Section III gives an overview of the system architecture. Section IV gives detailed flow of the proposed architecture. Section V, we briefly discusses two test cases that we have implemented as proof-of-concept. In section VI, we present algorithm in section VII we discuss related works

in this field. Section VIII discusses analytical perspectives on the developed solution. And finally in Section XI, we conclude our paper along with some suggestions for future work.

II. Security issues and Compliance check

There are number of security issues such as data security, trust, network traffic, multiple cloud tenants, need for better access control, identity management etc, in this section we try to understand what exactly is security compliance is all about. In the words of Bruce Schneier [13]:

"Computer security is a 40-year-old discipline; every year there's new research, new technologies, new products, even new laws. And every year things get worse".

This definition of the computer security gives and brief idea of how rapidly the change is happening in the technological field. Hence there is significant necessity for developing the system which is highly secured and compliant to the industry standards.

The Webster Dictionary defines compliance as: *"conformity in fulfilling official requirements"*.

This paper focuses on security compliance for multiple heterogeneous machines. IT security requirements can be classified into two types [14]:-

i) Functional requirements, which require some functional security feature such as mandatory access control, and
ii) Assurance requirements, which specify the evidence needed to establish that the functional requirements are met.

According to Klaus Julisch, IBM research the definition of the security compliance problem is as follows:

"Given an existing IT systems S and an externally imposed set R of security requirements, the security compliance problem is to make system S comply with the security requirement R and to provide the assurance that an independent auditor will accept as evidence of the compliance of system S with requirement R".

We can summarize this as every IT system irrespective of the kind of machine it is such as windows, Linux, virtual machines, every machine should be compliant to the industry standard set of rules and policies given by the vendors such as HIPAA [8], DISA, PCI [9], ISO [10], NIST [11] [23] etc, which guarantees by far how secure the system is and what are the remediation's that are to be done if not compliant.

III. Difficulties in developing a generic framework

There are so many research works that are going on regarding the security compliance and building the framework to support the security check based on the industry standards. But there are complexities in developing a generic framework since we have to follow the guidelines given by different vendors.

- There are no standard set of generic rules to be followed.
- Very little guidance for implementation in the standards.
- Fetching data/information from different systems requires different methods.
- Correctness of security compliance.

The challenges and difficulties mentioned above are basic and generic problems that we have to address while developing the generic framework. There are more complex challenges and difficulties that arise when considering cloud and virtual machines. We propose a generic framework which will assess the compliance of traditional machines as well as virtual machines. The block diagram is as shown in the fig.1.

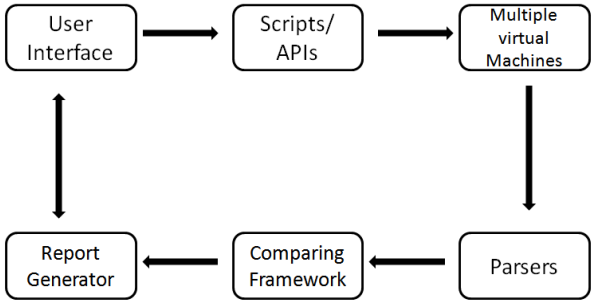

Fig. 1 Block Diagram of the Generic Framework for Assessment

IV. System Architecture

Fig.1 represents the system architecture that we have developed to build a generic framework for assessing compliance of multiple heterogeneous machines. The main components of the proposed architecture are as follows:

1) User: - User refers to both admin and the client who starts the process of assessment of the multiple machines.

2) User Interface: - UI can be built using JAVA, in which we give textboxes to enter the credentials and a button to click for assessment check.
3) Virtual Machines: - Machines may be any virtual machines, windows machine, Linux machines that we are trying to connect and create a remote session on that machine. It may have 'n' number of machines.
4) APIs/Scripts: - Session creation is done by using some APIs given by the vendors as well as by making use of scripts written using Power shells, Power CLI, Perl scripts [19] etc,
5) DOM/SAX Parsers: - Fetching the required information from huge data that we get after using suitable APIs has to be parsed according to the rules and policies of industry standards. DOM and SAX parsers are the best available parsers [20] [21].
6) Database: - Database is used to store the values that are fetched from the system and also to store the log.
7) Comparing framework: - After the process of parsing and fetching the required information, we have to compare the values with the standard values given by the policy/rules vendors such as HIPAA, DISA etc,
8) Report Generation: - The last part of the assessment process is generating the compliance report which says whether the system or machine is compliant on particular rules or not. In this project we display the report in the form of HTML page which gives the pictorial representation of the result.

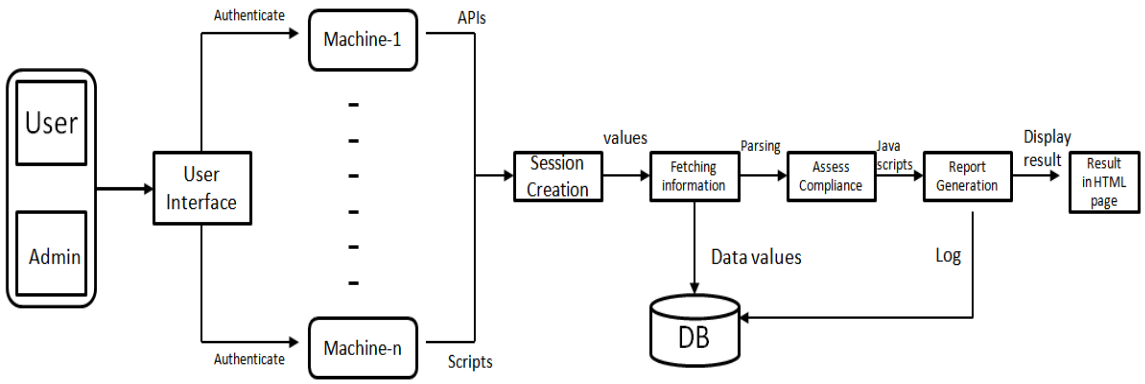

Fig. 2. System Architecture for Generic framework for Compliance assessment of multiple machines

As represented in the figure, we can use different approaches to create a remote session with the machines such as using APIs like REST APIs which uses HTTP protocol for communication [18], java APIs, and we can do the same using scripts such as Power shell scripts, Power CLI scripts, shell scripts etc, The workflow of the REST is explained in this section in which we make an 1) HTTP request normally GET, PUT, POST, and DELETE. The target of the given request will be either a well known URL or the URL obtained from the xml response to an earlier request. 2) HTTP response includes a body, usually the response body will be the xml representation of an object, which includes elements and attributes that represents particular object properties also the links that implement operations on the object or provide references to containing objects. The response also includes HTTP response code, indicating whether the request succeeded or failed, and might be accompanied by a URL [16].

HTTP Request Methods	Operation Performed
POST	Sends http request to the server and creates an object
GET	Retrieves the representation of an existing object.
PUT	Modifies an existing object.
DELETE	Deletes an existing object.

V. Phases of Algorithm for assessing compliance

Step 1: - User credential authentication

The user credentials for the multiple machines are given by the clients, the process initiates in this manner and followed by authentication of the credentials. If the username, password, IP address are given correctly by the user only then the process starts.

Step 2: - Creating the remote session on the machines

The second step is creating the remote session with machines whose credentials are given by the customers. To create the remote session we use APIs, scripts etc, from which we try to fetch as many information such as network security, storage security, data security, system security etc

Step 3: - Select the rules and policies given by industry standards

Selecting the different rules and policies given by the industry standards on which the assessment has to run will be done in this step. High priority rules are selected which we later implement. To implement the rules we write scripts through which the job is done easier compared to other methods.

Step 4: - Fetch the information from remote machine

After creating the remote session we fetch the system values regarding the network, storage, system security. This information that we fetch will be used to compare with the standard values and assess the compliance.

Step 5: - Parsing and validating the information

The information that we fetch will be huge and we have to parse only the required system values and to do this we use DOM/SAX parser where we write java code to parse the required information.

Step 6: - Assessment framework

After parsing the required values we compare those values with the standard values and check whether the system is compliant to those standard rules given.

Step 7:- Progress details

During the whole process the progress of the assessment is shown to the user which indicates the percentage of process completion, machine on which the assessment is going on at that particular moment, the rules being assessed and so on.

Step 8:- Assessment report

The final step of the assessment process is generating a result report, we have developed a HTML report where we make use of java scripts and display the result through HTML page.

VI. Flow Chart for Assessment

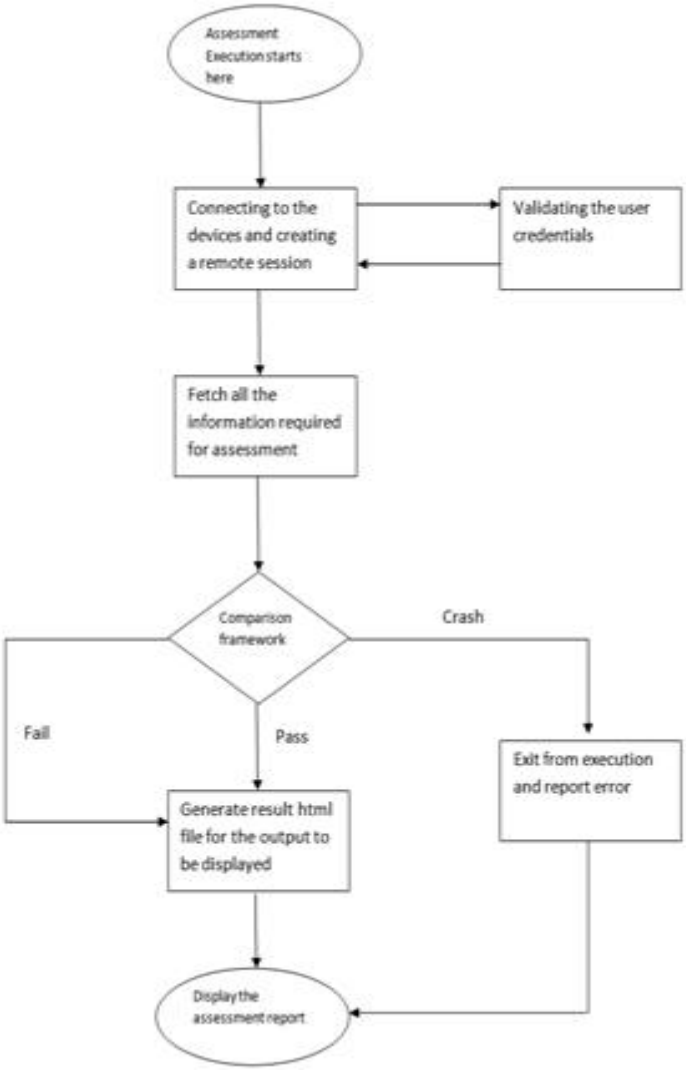

Fig. 3 Flow chart

The fig. 3 represents the flow chart for the development of generic assessment framework, where we have the flow of the whole process starting from connecting and creating a remote session and fetching all the required information, comparing with the standard values and generating the compliance result.

VII. Results and Comparison

For the sake of demonstration we have implemented our framework on three heterogeneous virtual systems which are related to different industry standards rules given by HIPAA, PCI, and so on. The graph represents the number of rules that are compliant with the standard values given by the vendors. As we can see in the fig.4 for use case-1 there are 3 cases in which the first virtual system shows that there are 28 rules out of 40 rules selected which are compliant and rest 12 are not compliant. Similarly, the second virtual system has 25 rules and out of which only 13 are compliant and third system has 12 rules in which 10 are compliant. For use case-2 as in the fig.5, we have 5 machines in which the number of rules implemented for each machines are 15, 40, 10, 25, 30 respectively and rules which are compliant to the industry standards are 12, 24, 7, 16, 24.

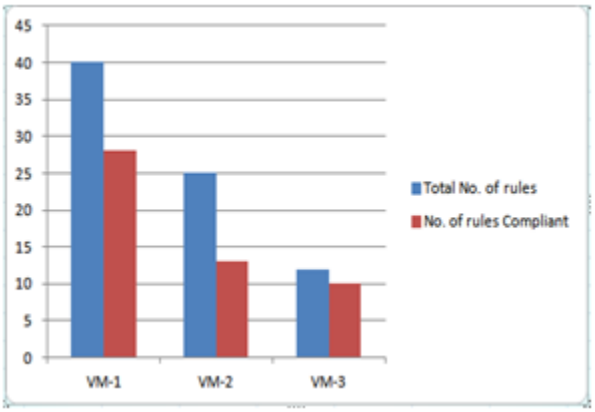

Fig.4 Graphical representation of use case-1

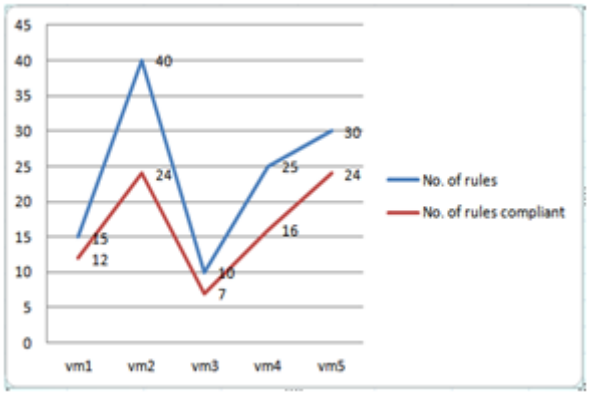

Fig.5 Graphical representation of use case-2

VIII. Discussion

Data security in the world of virtual system and cloud computing has a vast research going on all over the world [22]. There are few frameworks which assess the security compliance of the cloud systems but there were no generic frameworks as such. The generic framework has benefited the client in many ways where tremendous amount of work load is reduced by allowing the customers to check for the compliance of their multiple heterogeneous systems at one shot. Let it be a virtual cloud, virtual machines any virtual infrastructures. The clients can be aware of the security related issues in their organization and can have a failure free organization. The framework allows the customers to check the whole system compliance at once it becomes cost effective too whereas before in order to check for the security compliance of their organization the clients had to use different tools for different systems. In these many ways the generic framework for compliance assessment has benefited the users.

The framework that we have explained in this paper gives the user the report which indicates the number of rules for which the system is compliant. What to do for those rules for which the system is not compliant? Hence this becomes scope for future enhancement where we have to develop a framework which enforces the client to change the system values such that the system becomes compliant to all the rules given by the industry standards. And also the remediation can be taken up as a future scope where the admin has the power to change the values when he comes to know that the system is not compliant on particular rules.

IX. Conclusion

In this paper we have presented architecture to build a generic tool/framework for assessing the compliance check on multiple heterogeneous systems. We started with mentioning the security issues and introduction on compliance check. Later in the paper we discussed the difficulties in developing a generic framework for assessing the compliance of the system. The architecture for the generic framework gives the core components involved in building the framework such as REST APIs, Power CLI scripts, parsers, comparing frameworks, Java scripts, HTML and so on. Later we have presented the algorithm and the flow chart for the framework development where we can see the step by step procedure of the whole process. Next we compare the results obtained from the use cases that we have taken to demonstrate the compliance check on multiple systems.

References

[1] J. Park, E. Spetka, H. Rasheed, P. Ratazzi, and K. Han, "*Near-real-time cloud auditing for rapid response*," in Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on IEEE, March 2012, pp. 1252 –1257.

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

[3] "*HIPAA and QMS Based Architectural Requirements to Cope with the OCR Audit Program*", Gardazi, S.U, Shahid, A.A, Salimbene, C. Mobile, Ubiquitous, and Intelligent Computing (MUSIC) 2012 Third FTRA International Conference on Digital Object Identifier: 10.1109/MUSIC.2012.50, Publication Year: 2012, Page(s): 246-253.

[4] "*Cloud Security Alliance*," https://cloudsecurityalliance.org/ [accessed 13.03.2013].

[5] "*Cloud Audit*," https://cloudsecurityalliance.org/research/cloudaudit/ [accessed 13.03.2013].

[6] "*Cloud Control Matrix (CCM): Cloud Security Alliance*," https://cloudsecurityalliance.org/research/ ccm/ [accessed 13.03.2013].

[7] "*COBIT-IT Governance Framework - Information Assurance Control — ISACA*," http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx [accessed 19.09.2012].

[8] "*Understanding Health Information Privacy*," http://www.hhs.gov/ocr/privacy/hipaa/understanding/ index.html [accessed 19.10.2012].

[9] "*Official Source of PCI DSS Data Security Standards*," https://www.pcisecuritystandards.org/security standards/index.php [accessed 18.10.2012].

[10] "*ISO 27001, ISO27001 Information Security Standard*," http://www.itgovernance.co.uk/iso27001.aspx [accessed 19.09.2012].

[11] "*NIST.gov - Computer Security Division - Computer Security resource Center*," http://csrc.nist.gov/ publications/PubsDrafts.html [accessed 20.09.2012].

[12] "*Towards Building an Automated Security Compliance Tool for the Cloud*", Ullah, K.W, Ahmed, A.S, Ylitalo, J. Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on Digital Object Identifier: 10.1109/TrustCom.2013.195 Publication Year: 2013, Page(s): 1587-1593.

[13] "*Testimony and Statement for the Record of Bruce Schneier*", on http://www.iwar.org.uk, 2001.

[14] Security Compliance: The Next Frontier in Security Research, Klaus Julisch IBM Research Säumerstrasse 4 8803 Rüschlikon, Switzerland kju@zurich.ibm.com.

[15] "*Scripting JAX-WS [JavaScript]*" Vinoski, S. Internet Computing, IEEE Volume: 10, Issue: 3Digital Object Identifier: 10.1109/MIC.2006.65 Publication Year: 2006, Page(s): 91-94.

[16] "*Construction Methodology for a Remote Ultrasound Diagnostic System*", Koizumi, N, 2009 Robotics, IEEE Transactions on (Volume:25, Issue: 3).

[17] "*Mashup service release based on SOAP and REST*", Huijie Su ; Bo Cheng ; Tong Wu ; Xiaofeng Li Computer Science and Network Technology (ICCSNT), 2011 International Conference on Volume:2 Digital Object Identifier:10.1109/ICCSNT.2011.6182150, Publication Year: 2011, Page(s): 1091-1095.

[18] "*Modeling the performance of HTTP over several transport protocols", Heidemann, J, Obraczka, K. ; Touch, J.Networking, IEEE/ACM Transactions on Volume:5*, Digital Object Identifier: 10.1109/90.649564, Publication Year: 1997 , Page(s):616-630.

[19] "*Perl: not just for Web programming*",Dominus, M.-J. Software, IEEE Volume:15, Digital Object Identifier: 10.1109/52.646885, Publication Year: 1998, Page(s): 69-74.

[20] "*Parallel Speculative Dom-based XML Parser*", Ma Jianliang ; Shaobin Zhang ; Tongsen Hu ; Minghui Wu ; Tianzhou Chen, High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on Digital Object Identifier: 10.1109/HPCC.2012.15, Publication Year: 2012, Page(s): 33-40.

[21] "*The Application and Analysis of Netconf Subtree Filtering Based on SAX and DOM*", Yazhou Xiang ; Bin Zhang ; Guohui Li ; Yan Li ; Xuesong Gao, 2010 International Conference on Volume: 3,Digital Object Identifier: 10.1109/ICMTMA.2010.562, Publication Year:2010, Page(s):758-761.

[22] "*Data Security in the World of Cloud Computing*", Kaufman, L.M. Security & Privacy, IEEE, Issue: 4, Publication Year: 2009, Page(s): 61-64.

[23] "*Guidelines on security and privacy in public cloud computing*," W. Jansen and T. Grance, Special Report 800-144, National Institutes of Standards and Technology (NIST), Gaithersburg, MD, January 2011.