ISSN (Online): 2455-7838
SJIF Impact Factor : 6.093

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed
International Online Journal

Volume: 3, Issue:12, December 2018

Published By
EPRA Journals

SJIF Impact Factor: 6.093 Volume: 3 | Issue: 12 | December | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

METRIC BASED SELF ASSESSING INTERNAL ARCHITECTURE FOR SECURITY CLOUD (MESASIA)

Deepak Gupta

Asst.Professor ,GLBAJAJ Institute of Technology & Management

ABSTRACT

Designing the best of the security models to cope up with the contemporary security requirement has been a fashionable trend in the Information Technology World. Many security models for cloud computing have been delivered, but the thirst of having a multi-purpose security model providing ultimate answer to theincomprehensible security has notyet been quenched. In this paper, we have tried to propose a new security model for the clouds which will cater the necessary objective of the security concern as seen in the Information Technology now-a-days and will act as a multipurpose security cloud. It is metric based security model which will not only help to quantify the security implemented but also define new ideas of delivering security with no extra cost by analyzing the predefined standards and renewing them if necessary.

KEYWORDS*: Security Model, Security Metrics, Security Frameworks, Metric based Model, Cloud Security, Security Cloud*

I. INTRODUCTION

Clouds, the technology with the essence of human behavior-sharing, have been the recent whistleblower in the IT world. Most of the IT giants have already implemented the cloud paradigm in their organizations to get economic, strategic and competitive edge over others. Still being in the nascent stage, cloud has emerged as an inevitable need to the organizations across the globe. Organizations are moving to clouds but with extreme care and precautions as there are far more security issues than the advantages it provides. The organizations have to rely on the cloud service provider for most of the security concerns be it any service model of the cloud-IaaS, SaaS, VaaS or PaaS.

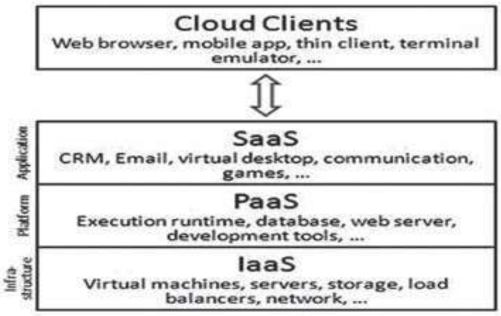

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Fig 1.Cloud Computing Service Models [2]

Cloud computing is not only about sharing resources, infrastructure or platform but also the vulnerabilities –as all the tenants of a cloud will suffer from the same vulnerabilities that the cloud is having. Though there are a lot of models proposed for the security implementation of the cloud but none of them guarantee the extreme safeguard to the data and against the vulnerabilities evolving dynamically. To understand the level of security and assess it properly, it needs to be measured first. If one cannot measure, then one can never evaluate the thing-be it physical or abstract. Generating specific security metrics and assessing them according to some standards can make a way out. In this paper we have merged the concept of security metrics with security intelligence and proposed an architecture which when implemented on clouds will not only provide security at the first, but also evaluate the implemented security internally thereby helping to manipulation of the security requirements and the controls accordingly for a tight security.

The paper format continues as follows: Section II deals with the related work dealing with the models used as/for security architectures; Section III discusses the preliminaries of the model being proposed; Section IV details the metric based self assessing internal architecture for security clouds(MESASIA) thereby emphasizing on the essential need of security metrics;Section V concludes the paper with description on future work to be done and references.

II. RELATED WORK

Cloud computing securityhas been widely researched and many security models in accordance to the state of the cloud, resource provisioning, multi-tenancy, and service models have been proposed accordingly. Tsai et al [1] have proposed a centralized control mechanism considering the virtualization in clouds. With the consideration that no two VMs of the competitors shall run on the same physical machine to minimize the inter-VM attacks, they have proposed the Chinese Wall Security Policy and upon it, developed the Chinese Wall Control Mechanism System.

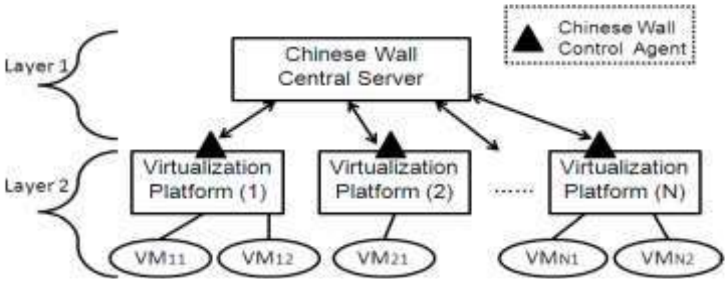

Layer 1
Layer 2
Chinese Wall Central Server
Chinese Wall Control Agent
Virtualization Platform (1)
Virtualization Platform (2)
......
Virtualization Platform (N)
VM11
VM12
VM21
VMN1
VMN2

Fig.2 System Architecture of Chinese wall Central Management System (CWCMS)[1]

Alzain et al [3] used the concept of multiple clouds for security and proposed MCDB, the Multi-Clouds Database Model based on Multiple Cloud Service providers comparing itwith the single cloud service provider as in Amazon cloud services.

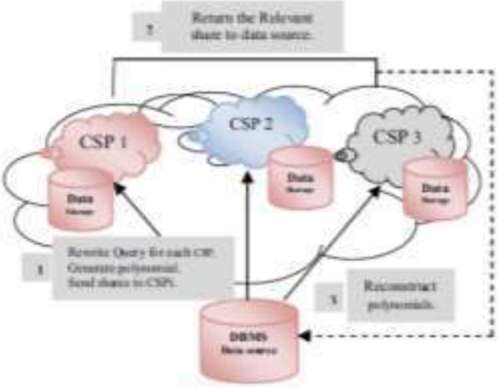

2
Return the Relevant share to data source.
CSP 1
CSP 2
CSP 3
Data Storage
Data Storage
Data Storage
1
Rewrite Query for each CSP. Generate polynomial. Send shares to CSPs.
3
Reconstruct polynomials.
DBMS Data source

Fig 3.MCDB Architecture for securing cloud[3]

Sun et al [4] introduced TMFC, a subjective trust management model based on the fuzzy set theory. They proposed a formal model first then considering the new definitions of trust according to the nature of the cloud systems proposed the TMFC Algorithm. Their model, TMFC could enhance the robustness, fault tolerance and hence secure the cloud properly.

Srivastava et al[5] analyzed the cloud security landscape on war foot basis and proposed a an architecture based on proactive methodology which implements a security cloud in order to actively monitor the CSP, the cloud service provider for any policy violations which is then reported back and analyzing them necessary decisions are taken by the clients.

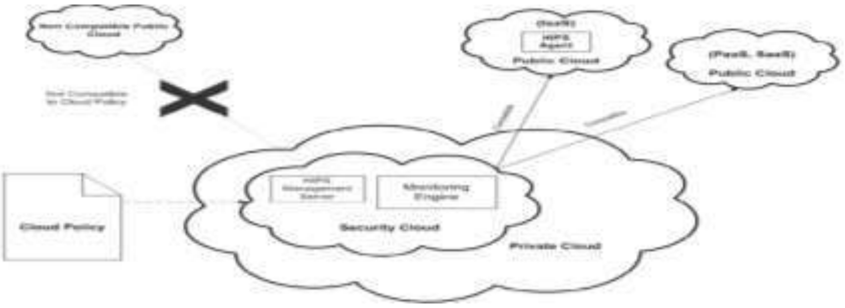


Fig.4 Proactive Methodology based Security Architecture [5]

Mirkovic [7] has proposed a measurable model for cloud on the basis of some security controls (like ITIL'sCMDB and ISO27001) defining some metrics principles. Besides the security model, he has also provided several tools like test harness systemfor the evaluation of security in different cloud models.

Tianfield [8] analyzed the key challenges and issues of security in cloud computing and considering the impacts of the cloud features proposed security architecture for clouds as shown in the figure below.

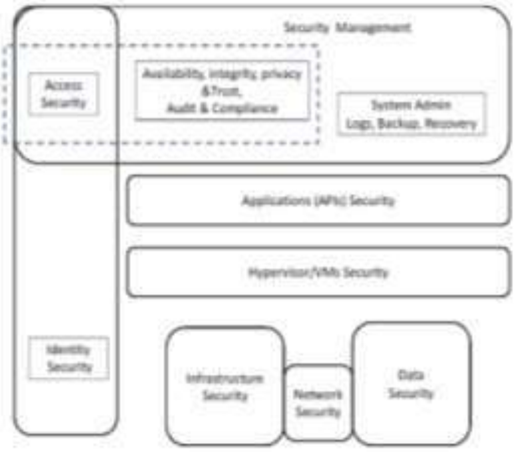


Fig.5 Cloud Security Architecture based on cloud characteristics [8]

Mohamed et al [9] investigated the basic cloud computing problem of data security, and have proposed layered security architecture for cloud data from different tenants and also implemented the standard encryption mechanisms for further safeguarding the data. Their proposed security architecture comprises of three layers– viz. 1. Authentication;2.Encryption; 3.Recovery as depicted in the figure below:

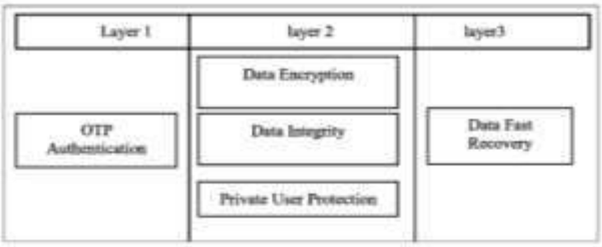


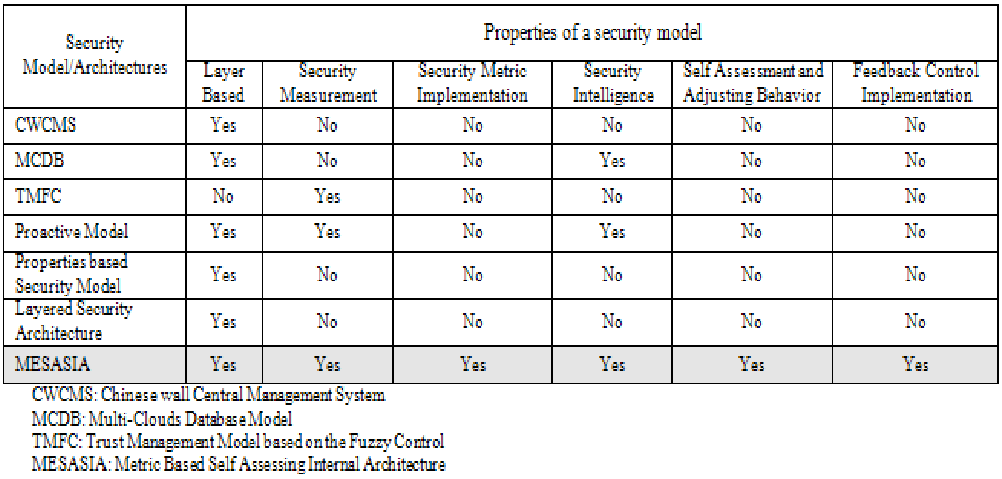
Fig.6 Layered Security Architecture for Data Security [9]

From the above discussions on various security architecture,one thing is confirmed that cloud security issues are endless be it data security, insiders attacks or its own basic features like multi tenancy or resource provisioning. Due to this, and despite of the advantages cloud implementations provide ,security issues have worked like the negative feedback to the cloud users.

A. What did the security architectures discussed above lack in spite of the functionalsecurity they provide?

Not considering the specific model or architecture, we would like to discuss some of the issues we discovered in the above security models.

Table 1: Comparision of the Different Security Architectures



Security Model/Architectures	Properties of a security model					
	Layer Based	Security Measurement	Security Metric Implementation	Security Intelligence	Self Assessment and Adjusting Behavior	Feedback Control Implementation
CWCMS	Yes	No	No	No	No	No
MCDB	Yes	No	No	Yes	No	No
TMFC	No	Yes	No	No	No	No
Proactive Model	Yes	Yes	No	Yes	No	No
Properties based Security Model	Yes	No	No	No	No	No
Layered Security Architecture	Yes	No	No	No	No	No
MESASIA	Yes	Yes	Yes	Yes	Yes	Yes

CWCMS: Chinese wall Central Management System
MCDB: Multi-Clouds Database Model
TMFC: Trust Management Model based on the Fuzzy Control
MESASIA: Metric Based Self Assessing Internal Architecture

On the basis of the table 1and the comparisons made according to the properties exhibited by the models we have deduced the following conclusion:

1. There is no standard policy of implementing the levels of security and also no certain extent or the limit has been well defined.
2. Except one,Mirkovic [7],none of the models advocate the security measurement and use of security metrics.
3. Specifically, no intelligent mechanism has been incorporated in the models except that in the proactive security model [5], where the private cloud based security cloud has been implemented.
4. None of the security models have self assessing and adjusting systems which is very essential in today's environment where vulnerabilities and threats can occur anytime and dynamic resiliency is the contemporary necessity.
5. Is only data the most essential one? What about service hijacking? Most of the security models help in the security of the data that too with only some sort of encryption mechanism.
6. No feedback control has been provided in any of the above discussed models, even in the proactive security model [5], where it seems to be very much essential.
7. Using multiple clouds for providing security as in MCDB security architecture[3] ,is like extending the number of vulnerabilities and making the security management difficult to be maintained as one has to secure every cloud independently.

Consolidating the facts and figures from the issues discussed, we have tried to model a security architecture which will be metric based and intelligent enough to assess itself and implement the security according to the situation and necessity by using the security intelligence.

III. THE PRELIMINARIES

In this section we will discuss about the preliminaries- the Security Cloud, Security Metrics and the Security Intelligence which are the key features of the model being proposed and without which it will be difficult to understand the underlying principle of the model.

A. Security Cloud

Security cloud have been defined in various ways –both as a separate, independent cloud used to monitor and provide security to the private clouds and as the technological infrastructure provided primarily meant for security aspects provisioned on a private cloud. On the first reading both might look same but they are different conceptually. One definition is just like having a bodyguard moving with the person and the other one is giving cover from the distance or the security guard of a mansion. The concept of security cloud has been used in the Proactive Methodology based Security Architecture [5] illustrated in the Fig 4.

The security cloud can act as the authenticator which will monitor legal use of the cloud environment as defined in the SLA. Apart from this security cloud will function like the security manager which will manage the security of the given cloud on the basis of the predefined security standards and the protocols.

B. Security Metrics

Security metrics are the tools that help in understanding and assessing the performance of the implemented security mechanics, coverage and /or the extent of security provided, and decision making of various security processes, mechanisms and procedures [6].The security metrics help in quantifying the security aspect and provide a comparable basis for decision making.

C. Security Intelligence

Security intelligence is the basic algorithm which will work on evaluating and adjusting the security implemented as per the requirement. The security algorithm implemented as the intelligence will get the initial parameters from the security management system, security protocols and the type of vulnerability occurred .Its key responsibility will be to analyze the scenario of the system by validating the parameters and generate the security requirement report to be used by the relevant systems and achieve the immunity against the vulnerabilities.

Security intelligence comprises of the following features-log management, anomaly detection, configuration and vulnerability management and security algorithms etc.

D. Security Management

Security management means managing the security infrastructure and helping the cloud or system attain immunity against the vulnerabilities and attacks. Securitymanagement comprises of various modules like access control, dealing with the security issues like confidentiality, integrity,availability, privacyetc along with log management, backups and recovery as well.

IV. METHODOLOGY

A. Metric Based Self Assessing Internal Architecture For Security Cloud(MESASIA)

This section will witness the self assessing, metric based architecture which will help in the assessment and evaluation of the security implemented and also adjusting it dynamically according to the necessity of the environment. The architecture is designed sophisticatedly with intent that it caters the necessary objectives of the organizations and basically the clouds security requirements.

MESASIA is basically a segmented architecture which is well defined into three major segments viz.1.Collection and Classification 2.Metric Formulation and 3.Metric Evaluation and Security Management. Each segment comprises of a variety of the tasks to be done and each is as essential as the other .The system designed first collects the necessary data from the environment (necessary arrangements are to be done, still in nascent stage) and provide it to the security intelligence module (a big data analytic module with a large number of functions like log analysis,vulnerability testing etc). After proper analysis and algorithmic implementation the security requirements will be generated and necessary controls activated respectively. The security requirements formulated bythe security intelligence module are then taken to the process-policy framework which will analyze the requirements and deduce necessary policies to be used by the system which are forwarded finally for evaluation and the security management system. Then the major task is implemented on the metric framework which will first evaluate the security provided and if it finds there is something lacking and is not at par then the feedback is sent back to the security intelligence module which performs reevaluation and reprocessing of the security vulnerability. And the process continues till final security implementation is done after confirming that it is the most appropriate one.

The modules described will have internal configurations of algorithms and data structure to take the necessary actions as needed. MESASIA will be doing two functions at a time, though complex but when implemented it will provide security as well as weigh it too.

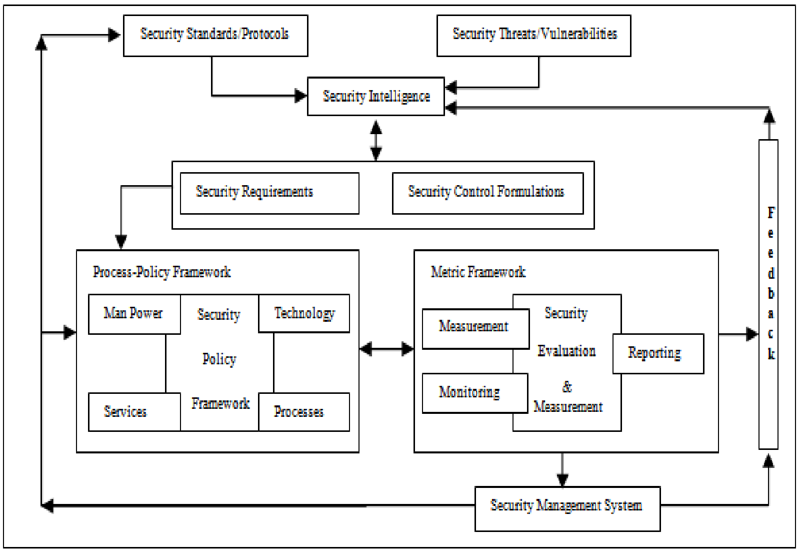


Fig. 7 Metric based Self Assessing Internal Architecture for Security cloud (MESASIA)

B. Functional Segmentation of MESASIA

The functional segmentation of the security model – MESASIA includes the followings:

1. ***Collection and Classification***

This segment comprises of the pre-stored security standards and protocols in the database server that will be used by the security intelligence to test depth of the vulnerabilities detected by the private cloud. The security intelligence module consists of the analytic algorithm that will analyze and further supervise the Security Requirement Module and the Control formulation module to generate the necessary control actions.

The tasks performed in this segment are:

a) Collection of the logs, vulnerabilities details, protocols reports, first incidental reports etc.

b) Analysis of the collected reports and logs using some secret algorithm in the security intelligence module.

c) Classification of the vulnerability according to the analytic algorithm as threat levels-High, Medium or Low.

d) Reanalysis if the security management fails and/ or frameworks provide insufficient information for the security implementation.

2. ***Metric Formulation***

This segment will deal with the deduction of the policies as stored in the database based on the type of vulnerability assessed from human being to the technology, Services to the processes.Actual implementation of the policy framework will be dynamic which will be changing according to the rules .It can be regarded as a rule based classification that will help in implementing the policies according to the type of vulnerability as defined by the security intelligence module after classification. If the policy does not exist then the security management system provides it necessary instructions to formulate new policy and store for further use. The policies formulated are then sent to get evaluated so that the cloud provider and its tenants know the index of the security implemented by the security cloud.

3. ***Metric Evaluation And Security Management***

This segment will be the most comprehensive and the important one as this will bear the metric analyzer engine for analyzing the policy of security to be implemented and quantify it for further use. Here the assessment of the security, its reanalysis, monitoring of the security to be implemented is done and in case if there exists slightest of the sensitivity then it is sent as the feedback to the security intelligence module which will reassess the issue again and the process of policy assessment and development will continue until the metric framework approves.

The Metric Framework has to necessarily perform the following tasks:

1. Monitoring and Evaluating the policies identified for implementing the security.
2. Assessing the security measures to be taken and finalizing the implementation.
3. In case of improper security policies or measures, give feedback as the report with all necessary details to the security intelligence module which will reconsider the issue, reassess the scenario and reinitiate the security procedures.
4. After the proper policy verification and evaluation, the security management system is guided to take the necessary actions on the cloud or system.The rightly devised policy now is converted into the security protocol or standard and stored into the database server for further use in case the same thing exists again.
5. The security management system will take care of all the implementations of the security procedures, policy implementations and log management.

V. CONCLUSION

We have tried to formulate the security model which is self assessing in nature .It performs the tasks of self assessment of the security implemented along with high level of security implementation. In one go it seems easy to implement the model proposed but there various hurdles for the exact implementation, some of which have been discussed previously in Gupta et al [6].Dynamic security concerns, reassessment, security algorithms (formulations and implementations) are the basis for this model along with a bit of big data analytics (We have used here as security intelligence).So this model is a blend of cloud computing technologies and big data ,the two technological giants of today's world along with the metric based computations for evaluation of the security.

VI. FUTURE SCOPE

We have proposed the theoretical concepts of the model here, which will be practically implemented once the necessary algorithms are devised. Apart from this we will look forward in metering the security metrics and provide a more refined model with proper practical implementations so that it can be compared and implemented in the industry with high adaptability.

VII. REFERENCES

1. *Tien-Hao Tsai, Yen-Chung Chen, Hsiu-Chuan Huang, Pei-Ming Huang and Kuo-Sen Chou "A Practical Chinese Wall Security Model in Cloud Computing" ,Institute of Computer Science and EngineeringNationalChiao Tung University Hsinchu, R.O.C.*
2. *www.wikipedia.com*
3. *Mohammed A. AlZain, Ben Soh and Eric Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing" in 2011 Ninth IEEE*

International Conference on Dependable, Autonomic and Secure Computing

4. *Xiaodong Sun, Guiran Chang, Fengyun Li," A Trust Management Model to enhance security of Cloud Computing Environments" in 2011 Second International Conference on Networking and Distributed Computing*
5. *PrashantSrivastava, Satyam Singh, Ashwin Alfred Pinto, ShvetankVerma, Vijay K. Chaurasiya, Rahul Gupta," An architecture based on proactive model for security in cloud computing" in IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 20111*
6. *Deepak Gupta, Ehtiram Raza Khan," Security Metrics: Expectations & the Reality" published in www.ijarcsse.com,Volume 5, Issue 3, March 2015 ISSN: 2277 128X*
7. *OrlanMirkovic, Ericsson Nikola Tesla, Zagreb, Croatia," Security Evaluation in Cloud" in MIPRO 2013, May 20-24, 2013, Opatija, Croatia*
8. *HuagloryTianfield, School of Engineering and Built Environment ,Glasgow Caledonian University, United Kingdom" Security Issues In Cloud Computing" in 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea*
9. *EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby "Enhanced Data Security Model for Cloud computing" presented in The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track.*