A R DIGITECH
International Journal Of Engineering, Education And Technology (ARDIJEET)
www.ardigitech.in ISSN 2320-883X, VOLUME 1 ISSUE 1, 01/01/2013

Cloud Computing & Intrusion Tolerance with SOA: A Survey

Ms.Vipula M.Wajgade*1, Mr.Ravi Kiran Rajbhure*2
**1(Lecturer of SGT Institute of Technology,Gurgaon ,Haryana,India)*
**2(Lecturer of, Dept Of IT, Anuradha Engg.College,Chikhli,India)*
*vips.wajgade@gmail.com *1, ravi.rajbhure@hotmail.com *2*

Abstract:

Various emerging technologies have been developed to protect the systems against the intrusions made by un-authorized person or by an authorized person accessing unauthorized privilege. Cloud computing can be the best intrusion tolerant system when combined with SOA (service oriented architecture).semantic web can also be used as intrusion tolerant system with certain limitations.

Service oriented architecture when combined with cloud technology results in secure and robust system against intrusion, which gives data protection and is also responsible for defence in depth.

I.INTRODUCTION

History shows that attacks can never be completely prevented. It can only be avoided up to some Intrusion Tolerance. This ensures that system will remain intact after the attack retains the vulnerability up to certain extent.

II. INTRUSION TOLERANCE SYSTEM

The main motivation of providing the Tolerant system is to maintain the properties of security as Confidentiality, Integrity and Authenticity. The question arises how we can maintain Confidentiality, Integrity or Authenticity after being attacked. The Intrusion Tolerant system can still assume that the system is vulnerable despite of compromising some components of the system.

Extent. Thus the system is needed which has the multiple layers of defence. The evolution of information technology has enabled us to use different new technologies such as Cloud Computing, SOA and Semantic Webs. Cloud computing provide us with “on-click “computing power or the storage, and the SOA enables us to use the building blocks of the software as services. Whereas the semantic webs uses the automated processing agents to perform the task which needs human comprehension. Many researchers have been implementing various security mechanisms for providing defence in depth. Classical work of security has been classified into two main types as 1.Intrusion Prevention: Preventing or avoiding malicious attacks.

2. Intrusion Detection: Identifying that error has occurred due to malicious attack.

A new innovative approach has been implemented in last some decade called as

The fault, error and failure of the system are correlated. Fault in the system occurs when it achieves a stage that is undesirable. When fault occurs it causes the error and when error propagates it causes the failure of the system. We can describe the this fault, error and failure Model for the system as follows,

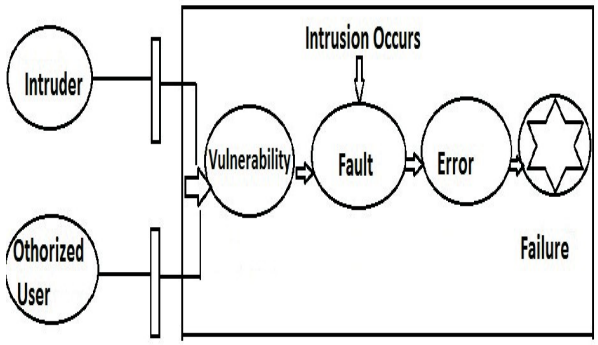

Figure 1:The Fault Model

Thus it is important to prevent the intrusion occurring in the system; it is to ensure that attacks do not take place against certain components. A system is said to be reliable if it delivers the deliverables in spite of the changes or the fault taking place, thus fault tolerance and reliability are closely related. For reliable system fault tolerance is essential.

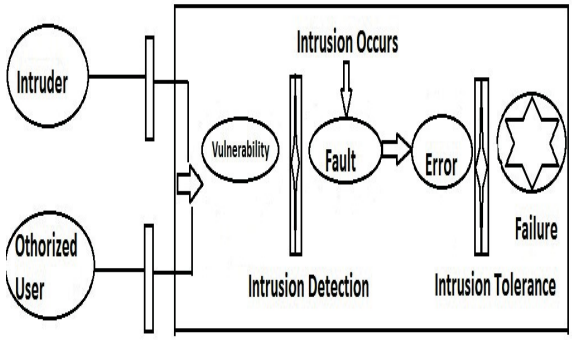

Figure 2: Intrusion Tolerance System

Thus an efficient system achieves reliability, availability, safety and security. The malicious attacks thus should be prevented if not it should be detected and in worst case if it occurs it should retain the system as intact against the attack or fault maintaining the reliability of the system despite of the changes compromised in certain components. With the growing need of security the system should retain some properties or things should remain the same are: Validation, Accountability and Trust.

III.MODERN TECHNOLOGIES

Service Oriented Architecture

Evolution in SOA technology has leaded us to consider the building blocks of software as services. Consumers can invoke the required service by sending the messages to service implementation; the messages are routed by service bus to implementation. This architecture also provides the service management like logging, auditing and billing. The quality of service in SOA can be achieved by providing reliability of services, management of services, security and availability. The main features of SOA are it is different from any other distributed systems that enable the consumers use different platform as services.

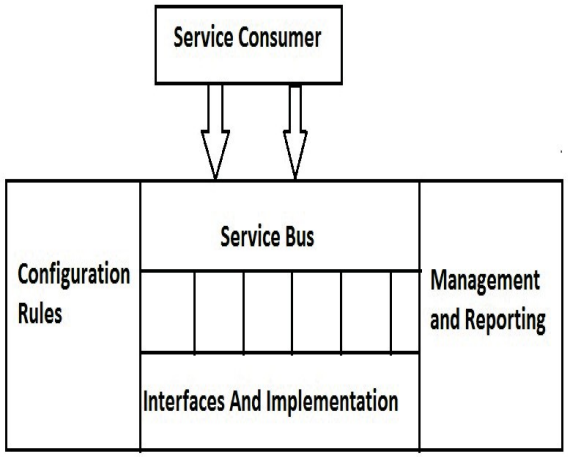

Figure 3: Service Oriented Architecture

SOA also brings the reusability of existing investments and provide suitable service to build a new platform with existing applications with the intention of keeping clients or consumers isolated from the changes being carried out in service implementation. It also enables to upgrade the individually, it is not required to rewrite an application.SOA on other hand provides flexibility in generating new applications.

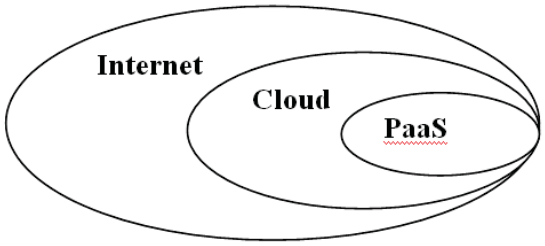

Figure 4 : Platform as a service

B Cloud Computing

Cloud computing is the internet based computing that relies on sharing the resources online. Different services are delivered to organizations on internet. The services are delivered in form of various clouds. The clouds are public cloud, private cloud and hybrid cloud. The segments of cloud computing are connectivity, application and storage. The services cloud offers has been classified as follows: Platform as a service (PaaS), Infrastructure as a service (IaaS), and Software as a service (SaaS).

C Semantic Web

Human interpretation of data or services in clouds can be handled with the automated agents of semantic web technology, the SOA and cloud computing collectively enables the semantic linking.

VI. SECURITY CONSTRAINTS

The cloud computing delivers the services on internet that is “on click” and dynamically loaded. But when it is delivered to user or consumer end to end security is not considered. The places where end user interaction is not considered may need some attention. The violation of privacy can be there with SOA accessing a cloud, thus with combined approach of these technologies it is easier

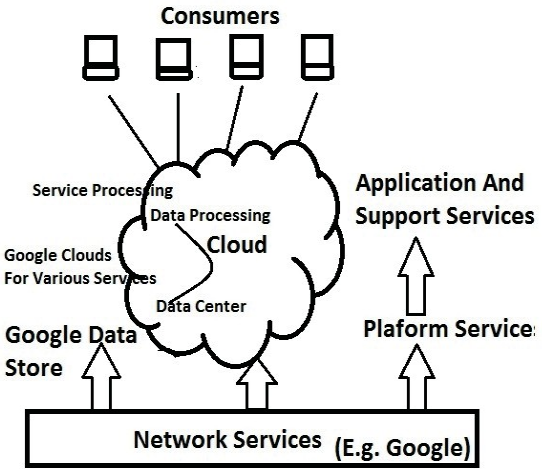

Figure 5: Cloud with SOA

to tolerate the intrusion that can likely to occur in the system. The combined approach can result in providing service-oriented security as everything is available as a service on demand. The mark-up language can be used to provide Information and Data security, authentication can also be provided with metadata. It is also possible to trust the system in terms of assurance.

V.CONCLUSION

The on demand availability of resources or services and the software building blocks of SOA, these features of SOA and cloud computing helps to design a system which is intrusion tolerant. The use of semantic webs as automated agents overcomes the human deficiency. This paper concludes how existing technologies when combined results in secured system and it can be easily implemented further with future trends.

REFERENCES:

[1]http://en.wikipedia.org/wiki/Global_Information_Grid

[2] Rushby, J. Design and Verification of Secure Systems. Proc. 8th ACM Symposium on Operating System Principles: 12–21, 1981

[3] http://altornetworks.com/products/vnf/

[4]https://hwww.trustedcomputinggroup.org/groups/

[5] Kissner, L., and Song, D. Privacy-preserving Set Operations. Advances in Cryptology, 2005.

[6] Wall Street Journal, Electriciy Grid in U.S. Penetrated by Spies (April2009): http://online.wsj.com/article/SB123914805204099085.html

[7] Trustworthy Cyber Infrastructure for the Power Grid (TCIP) home page:http://www.iti.illinois.edu/content/tcip-trustworthy-cyber-nfrastructurepower-grid

[8] Critical Utility Infrastructural resilience (CRUTIAL) project home page: http://crutial.cesiricerca.it/

[9] Ngamsuriyaroj, S.Rattidham, P Rassameeroj,Wongbuchasin, P.Aramkul, N.Rungmano, " Performance Evaluation of Load Balanced Web Proxies",IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), 2011

[10] Amandeep Verma1, Sakshi Kaushal: "Cloud Computing Security Issues and Challenges: A Survey", First International Conference on Advances in Computing and Communications (ACC 2011)

[11] Wasim ari, Vinicius V. Cogo, Alysson Bessani Marcelo Pasin, Hans P.Reiser : " Fault Intrusion Tolerance for cloud computing",2012

[12]]http://www.enisa.europa.eu/act/rm/_les/deliverables/cloud .../fullReport,2012

[13] "Intrusion Tolerance via Threshold Cryptography",http://crypto.stanford.edu/ dabo/ITTC/

[14] http://netbeans.org/about/, 2012-06-09