www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13422-13425

Review on Security Issues of SaaS Clouds

Ritesh Mahendra Ahire[1], Prof.Ganesh Kadam[2]
Department of Computer Engineering, Savitribai Phule PuneUniversity
SKN'Sinhgad Institute of Technology and Science, Lonavala, Pune, Maharashtra, India.
ritzforum@gmail.com

Abstract- Cloud frameworks frequently has long running applications, for example, monstrous information handling which gives more chance to aggressor to adventure frameworks vulnerabilty and perform vital attacks.Sensitive information of an association is set in the control of outsider utilizing cloud computing,which presents singificant level of danger on the protection and security of data.Need of extraordinary equipment or secure part bolster necessity for respectability verification is enlightened in this exploration work This broad overview paper intends to expand and break down the various uncertain issues viz. Autocorrection of debased information and mallicious assaults undermining the distributed computing environment reception and dissemination influencing different partners and end clients connected to it.Key Words: Integrity attestation, Cloud computing, Stakeholders

.

Introduction

Cloud computing is evolved to revolutionize computing as a service .It provides on demand computing resources dynamically hence company can fundamentaly change their information technology strategy.As with any new technology this new way of doing business brings with it new challenges specially when considering the security and privacy of the information stored and processed within cloud.Cloud security requires total situational awareness of threats to the network,infrastructure and information.

Abstraction is nothing but the biggest merit and demerit of the cloud utility ,since abstraction allows cloud to be pervasive and removes the knowledge of underlying fabric of processor ,storage and networking security of cloud to strengthen the cloud environment,But such abstraction keeps the information owner unnoticed about underlying knowledge of cloud fabric hence the phenomenon of securing application and information becomes very complex

for information owners.Many traditional security principle used today to secure data and network depends upon the information owners ability to manage the underlying fabric of server,router,firewalls and intrusion detection system to become aware about when attacks are ocuring and to counter to the threats by preventing access to the resources and isolating pieces of the fabric that are being attacked.In a cloud such traditional tactics do not work as the service provider cant allow information owners or client to manipulate the security setting of fabric.If these are allowe,it would be possible for the client to change the security setting favouring to their own benefits or malliciously changing the security of other clients.

This scenario is not acceptable since the information owner can not manage the security posture of their computing environment hence strong security model is needed to safeguard the information owners data without altering and interfering the security privillages.

Many of such threats are countered by SaaS cloud system because in SaaS clouds only portal nodes have global information about which service function are provided by which service provider .Both the service providers and SaaS clouds are an autonomous entities.Researchers of the Saas clouds provides holistic approach by examining both consistency and inconsistency relation between different service providers within entire cloud system.

The frequently observed security threat of malicious service providers that offers untruthfull service function is a big challenge nowadays in SaaS cloud system and is addressed by Xiaohui Gu, Juan Du and Nidhi Shah by proposing RunTest and AdaptTest mechanisms[2].Limitations of these mechanisms are overcomed using IntTest mechanism as Proposed by Xiaohui Gu and team[1] .

Literature Review

Success of any new compting technology is depends upon the fundamental factor "How much secure it is?"To give more comfort to the customers and make Trust us policy of cloud environment more faithful.The chief concern of the cloud always revolves around security.In SaaS model cloud service

provider exclusively manages the required computing infrastructure and software to support customer relationship management (CRM),Email,and Information management.SaaS releives the users from hardware maintanace and instalation of softwares.But as far as security threat is concern SaaS model also suffers from the various issues as shown in FIG below[1].

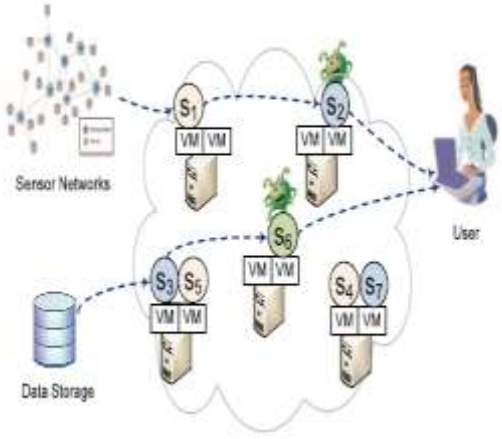


FIG.[1]Service integrity attack in Cloud based data processing.Si denotes various service componants and VM denotes virtual machines

A malicious attacker with fake credentials and identity can pretend to be a legitimate service provider and start providing untruthfull services by fooling the vulnerable sevice providers.Attackers can be stealthy in nature which leads to more complexities,hence such detection are required which are hidden from attacker.Besides, scalable detection schemes are required because misbehaviour of attacker may be unpredictable and occasional.More technically the system architecture prone to threats can be understood by following architecture(2)

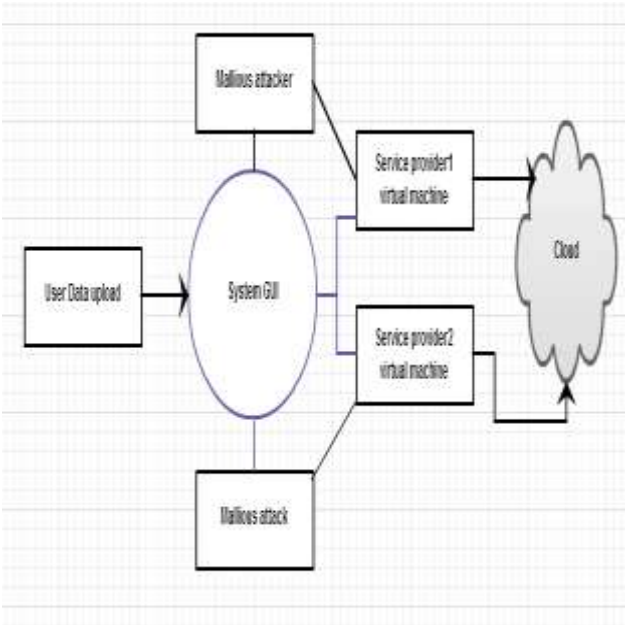


FIG.(2)System Architecture

In above large scale cloud computing system colluding attacks aslo need to be monitored.Traditional Byzentine system can detect arbitrary behaviour using full time majority voting machine over all replicas but at the cost of heavy overhead on cloud system.

Supporting mechanisms of previous research Namely AdaptTest which reduces the attestation overhead by 60% and reduces the mallicious pinpointing delay upto 40%.[2] Secondly RunTest mechanism which pinpoints the mallicious service provider identifies the untruthfull data processing result and descovers the colluding attack pattern [3].

Dealing with fake legitimacy of attacker is addresed by using integrated and hollistic approch of consistancy and integrity graph.Mechanism Proposed by Xiaohui GU and team discards the assumptions mede in previous research works which is number of honest service providers should always be greater than mallicious service providers,Such notion makes the research more realistic and acceptable.Since every research goes through radical changes all the time,supplimentry hypothesis are must to make research work stagnant and aiming towards objectives.viz 1)Data processing services are input deterministic and 2)Result inconsistancies caused by softwares and hardwares should be treated as natural events.

Juan Du,Daniel J.Dean,Yongmin Tan ,Xiaohui Gu,Ting Yu Proposed ”Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds”[1]where they talks about novel scheme that can provide stronger attacker pinpointing power than previous schemes.Moreover ,automatically enhancement of result quality by replacing bad result produced by malicious attacker with good results produced bygenuineservice providers.

Authors Patric C.K. Hung ,Elena Ferrari and Barbara Carminati as a team gives brief ovewiew on the research issues of web services privacy technology.It focuses on business policies enclose requirements such as required security tokens,required encryption algorithms and privacy norms.Their paper:”Towards standardization Web Services Privacy Technology”IEEE international Conference on Web Services (ICWS’ 04)0-7695-2167-3/04 proposes a privacy policy skeleton that can be complimented and aligned with web security discretion in near future[4].

Lina Alchaal and Vincent Roca in their paper “Managing and Securing Web Services with VPNs”IEEE(ICWS’04)0-7695-2167-3/04 exaplains about integration of two or more new technologies in a new powerfull fusion model that1)enables an easy management of web services.2)provides web services security thanks to the use of dynamic and programmable VPNs,and 3)remains straightforward and fully incorporated.[5]

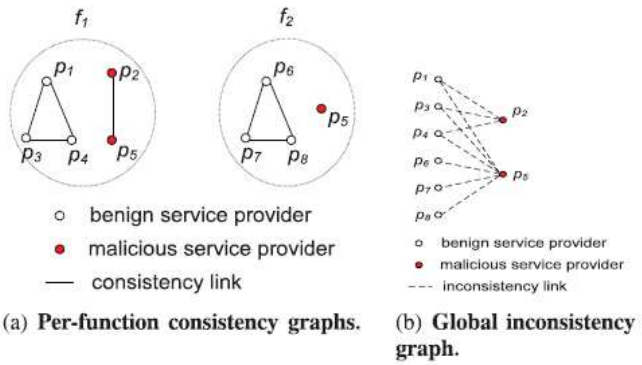
Reserchers Elanie Shi,Adrian Perrig,Leendert Van Doorn in their work”BIND:A Fine-Grained Attestation Service for Secure Distributed Systems”IEEE(S&P’05)1081-

6011/05.suggest instead of attesting entire memory content,BIND attest only piece of code we are apprehensive about,This greatly simplifies verification.BIND also reduces the gap between time of attestation and time of use by providing sound boxing mechanism.Besides, BIND provides general solution towards establishing a trusted environment for destributed system designers.[6]

"SWATT:SoftWare-based ATTestation for Embedded Devices"IEEE(S&P'04) 1081-6011/04 proposed by Arvind Seshadri ,Adrian Perrig,Leendert van Doorn and Pradeep Khosla talks about tactics which verifies the memory contents of embedded devices and establishes the absence off malicious changes to the memory content without physical accessing the memory of devices.SWATT also detects any change in memory content thereby detecting viruses ,trojen horses,unexpected configuration settings.[7]

Senior IEEE members Inseok Hwang,Sungwan Kim,Youdan Kim and Chze Eng Seah in their research "A Survey of Fault Detection,Isolation,and Reconfiguring Methods"IEEE 1063-6536/2009' Discuses various model based techniques to generate residuals that are robust to noise ,mysterious disturbance and model suspicions as well as various statistical techniques of testing the residuals for sudden changes.Later they discus about various techniques of implementing reconfigurable control strategy in response to faults.[8]

As compared to privacy and confidentiality concern that have been addresed by previous research,the result integrity concern is the most prevalent which need to be addresed no matter whether public or private data are processed by the cloud system.Moreover to detect the service integrity attack the duplicate copy of data is created known as attestation scheme is developed where grapical environment is used and cliques of graph are observed ,Observe the FIG.[3].Theory of consistancy treats the nodes which are out of clique of graph as malicious whereas theory of consistancy talks about If two nodes are connected by inconsistancy link ,both must agree with each other,otherwise one of them is mallicious node. It gives maximum vertex cover of mallicious nodes by giving lower bound.



(a) **Per-function consistency graphs.** (b) **Global inconsistency graph.**

FIG.[3]Attestation Graphs[1]

Proposed system finalize the mallicious service providers based on the result of both consistancy and inconsistancy graphs along with additional facility of Corrupted result autocorrections.

Conclusion

Cloud computing ,envisioned as the next generation architecture of IT Enterprise is a talk of the town these days.Although it has revolutionized the computing world, it is prone to manifold security threats varying form network level threats to application level threats.In order to keep the cloud secure ,these threats need to be controlled.For this paper various research paper are carefully studied to get a ground on security measures for cloud.To improve the security measures of SaaS clouds different algorithms and graphs are suggested here.Many of them solves the problem of security issue.Yet ideal security objective for SaaS clouds always remained the pending issue due to lack of smart attestation frameworks.In this paper various security concern for cloud computing environment from multiple perspective and the solutions to prevent them have been presented.

References

1**]** Juan Du, Member, IEEE, Daniel J. Dean, Student Member, IEEE, Yongmin Tan, Member, IEEE,Xiaohui Gu, Senior Member, IEEE, and Ting Yu, Member, IEEE: Scalable Distributed Service IntegrityAttestation for Software-as-a-Service Clouds IEEE transactions on parallel and distributed systems, vol. 25, no. 3, march 2014

2] Nidhi Shah Xiaohui Gu Juan Du: Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems 978-1-4577-0103-0/11/$26.00 _c 2011 IEEE.

3] Wei Wei, Juan Du ,Xiaohui Gu, and Ting Yu: RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures

4]Patric C.K.Hung, Elena Ferrari and Barbara Carminati: "Towards standardization Web Services Privacy Technology"IEEE international Conference on Web Services (ICWS' 04)0-7695-2167-3/04

5] Lina Alchaal and Vincent Roca in their paper "Managing and Securing Web Services with VPNs"IEEE(ICWS'04)0-7695-2167-3/04

6] Elanie Shi,Adrian Perrig,Leendert Van Doorn in their work"BIND:A Fine-Grained Attestation Service for Secure Distributed Systems"IEEE(S&P'05)1081-6011/05

7] Arvind Seshadri ,Adrian Perrig,Leendert van Doorn and Pradeep Khosla: "SWATT:SoftWare-based ATTestation for Embedded Devices"IEEE(S&P'04) 1081-6011/04

8] members Inseok Hwang,Sungwan Kim,Youdan Kim and Chze Eng Seah: research "A Survey of Fault Detection,Isolation,and Reconfiguring Methods"IEEE 1063-6536/2009'

9]Amazon Web Services, http://aws.amazon.com/, 2013.

10]Google App Engine, http://code.google.com/appengine/, 2013.

11]SaaS, http://en.wikipedia.org/wiki/Software asa Service, 2013.