International Institution for Technological Research and Development
Volume 1, Issue 1, 2015

Survey Paper on Pinpointing Integrity of Service provider in cloud computing System

Shaishav R. SHah[*], Madhushree B. [**]
P.G. student, Assistant professor

Abstract- Cloud systems enable application service providers to deliver their applications via massive cloud computing infrastructures. However, due to their sharing nature, SaaS clouds are vulnerable to malicious attacks. This review paper provides a better understanding of the cloud computing integrity and identifies important research security issues in cloud system.

Index Terms- Integrity in cloud, cloud system, security issues in cloud, Pinpoint Malicious Activity

I. Introduction

Due to the unprecedented success of internet in last few years, computing resources is now more ubiquitously available. Cloud systems have recently emerged as popular re-source leasing infrastructures. Application service providers (ASPs) can lease a set of resources from the cloud system to offer software as a service without paying the expensive cost of owning and maintaining their own computing infrastructures. the Internet has evolved into an important service delivery infrastructure instead of merely providing host connectivity.

In this paper we discuss different types of attack model and it's proposed solution. There are many types of security issues are there but in this paper we will study about vulnerability of services and service providers. Services can be compromised by compromised service provider or compromised node. There are many techniques and method are there for solving our purpose to protect cloud by this type of malicious activity. But there are some pros and cons of these methods. Here we will study about problems and their solution given by many frameworks.

II. Reviewed Paper

In this section, I first give a brief background overview about the cloud computing infrastructure and data-intensive computing applications that can be delivered as services via the cloud infrastructure. then describe the integrity attack scenarios that are addressed by some papers.

1)A Framework for Building Privacy-Conscious Composite Web Services

Wei Xu, V.N.Venkatakrishnan, R. Sekar, I.V.Ramakrishnan , create a frame work using 5 components Service composition code, service models, privacy policies, policy compliance checker and obligation generation, and obligation enforcer for addressing the challenges raised in terms of consumer information policy. They have proposed framework for preserving privacy in web-services.in their suggestion consumer can have facilities to specify their privacy concerns through use of privacy policies while service providers express their terms of use (of private data) through models.

2) *On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems*

Juan Du, Xiaohui GU, Ting Yu, present RObust Service Integrity Attestation (ROSIA) framework that can be efficiently verify the integrity of stateful dataflow processing services and pinpoint malicious service providers within a large-scale cloud system. This framework consist 3 parts first *Replay-based Consistency check* between service provider with same service function. Then second one is consistency graph and inconsistency graph model to aggregate attestation results, third one is pinpointing algorithm that takes the graph as input and output malicious service providers. In this paper, they have presented the design and implementation of ROSIA, a robust service integrity attestation system for processing stateful dataflow applications in cloud systems. Algorithm finalizes the list of malicious service providers based on the results of both consistency graphs and inconsistency graphs.

3)*Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures*

Zhou Li, Sumayah Alrwais,Yinglian Xie, Fang YuXiaoFeng Wang , explain their study on malicious Web infrastructures in this paper. Using nearly 4 million malicious URL paths crawled from different attack channels; they perform a large- scale study on the topological relations among hosts in the malicious Web infrastructure. Their study reveals the existence of a set of topologically dedicated malicious hosts that play orchestrating roles in malicious activities.

They develop a topology-based technique that detects these hosts without even knowing exactly what they do. This approach utilizes the PageRank algorithm to capture those with high status on the dark side of the Web but very much unknown on the bright side, and brings to the light thousands of dedicated hosts missed by the state-of-the-art malware scanner. That many of those hosts are Actually TDSes(Traffic Distribution Systems), which play a key role in traffic exchange in malicious activities.

4) *Regenerating Cloud Attack Scenarios using LVM2 based System Snapshots for Forensic Analysis*

G. Geethakumari, Abha Belorkar , define following methods Defining attacks as clusters, Assigning weights to dimensions, The current code module distance, Determining the threshold value, The snapshot duration., Regenerating the event. The potential of this work to be applied to more practical and popular cloud application environment relies heavily on the tools employed for accurate and exhaustive identification of all the parameters (variables) that characterize malicious activities in the cloud. Also, the corresponding weights of these parameters may be assessed more accurately if advanced Machine Learning techniques are used. Similar appropriate techniques may also be used for a more precise detection of the threshold value.

5) *Intrusion detection system: A comprehensive review*
Purpose of *Hung-Jen Liao* to outline modern Intrusion detection system. Intrusion detection methodologies are classified as three major categories. Signature-based Detection, Anomaly-based Detection, Stateful Protocol Analysis.

6) *RunTest: Assuring Integrity of Dataflow Processing innCloud Computing Infrastructures*

Juan Du, Wei Wei, Xiaohui Gu, and Ting Yu , present RunTest , a scalable runtime integrity attestation framework to assure the integrity of dataflow processing in cloud infrastructures. RunTest provides light-weight application-level attestation methods to dynamically verify the integrity of data processing results and pinpoint malicious service providers when inconsistent results are detected. RunTest Contains two algorithm first Consistency clique discovery algorithm, which is use to find consistency between service providers and second algoridhm is Cloud Dataflow Integrity attack detection algorithm. They have presented the design and implementation of RunTest, a new service integrity attestation system for verifying the integrity of dataflow processing in multi-tenant cloud infrastructures.

7) *Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems*

Juan Du, Xiaohui Gu present AdapTest, a novel adaptive data-driven runtime service integrity attestation framework for multi-tenant cloud systems. AdapTest can significantly reduce attestation overhead and shorten detection delay by adaptively selecting attested nodes based on dynamically derived trust scores. AdapTest Contains three algorithm Weighted Attestation Graph, Per-Hop Adaptive Attestation, Multi-Hop Adaptive Attestation.

8) ***Scalable Distributed Service Integrity Attestation for Software as-a-Service Clouds***

Juan Du, Daniel J. Dean, Yongmin Tan, Xiaohui Gu, Ting Yu Csystem create a new framework for SaaS . IntTest provides a novel integrated attestation graph analysis scheme that can provide stronger attacker pinpointing power than previous schemes. IntTest can automatically enhance result quality by replacing bad results produced by malicious attackers with good results produced by benign service providers. IntTest employs randomized replay-based consistency check to verify the integrity of distributed service components without imposing high overhead to the cloud infrastructure. IntTest is lightweight, which imposes low-performance impact to the data processing services running inside the cloud computing infrastructure.

III. FINDINGS

There are many types of Methods and Algorithm with their Features and problem. Some method is very efficient as per Performance and efficiency of output. But there are many limitations and assumption make that algorithm weak and inefficient.

IV. CONCLUSION

High availability of cloud and complexity of cloud system make some loop holes in system because of the third party software and intruder which n=make cloud untruth full and un reliable while there are any techniques to prevent the cloud services but there is some limitations and some ups and down which makes services pernicious and compromised.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments.

REFERENCES

*[1] Wei Xu, V.N.Venkatakrishnan, R. Sekar, I.V.Ramakrishnan*On this and that *A Framework for Building Privacy-Conscious Composite Web Services*

[2] Juan Du, Xiaohui GU, Ting Yu On this and that. *On Verifying Stateful Dataflow Processing Services in Large- Scale Cloud Systems*

[3] Zhou Li, Sumayah Alrwais,Yinglian Xie, Fang YuXiaoFeng Wang On this and that. *Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures*

[4] G. Geethakumari, Abha Belorkar On this and that. *Regenerating Cloud Attack Scenarios using LVM2 based System Snapshots for Forensic Analysis*

[5] Hung-Jen Liao , Chun-Hung Richard Lin , Ying-Chih Lin , Kuang-Yuan Tung On this and that. *Intrusion detection system: A comprehensive review*

[6] Juan Du, Wei Wei, Xiaohui Gu, and Ting Yu On this and that. *RunTest: Assuring Integrity of Dataflow Processing innCloud Computing Infrastructures*

[7] Juan Du, Xiaohui Gu On this and that. *Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems*

AUTHORS

First Author – Shaishav R Shah,, LJIET and shah.shaishav@outlook.com.

Second Author – Mrs. Madhushree B., LJIET and bmadhushree.lj@gmail.com