ISSN:0975-9646

A Survey on Security Frameworks for Software-as-a-Service

Sithara Sahadevan , Jiby J Puthiyedam

Department Of Computer Science, College Of Engineering Poonjar,
Cochin University Of Science And Technology
Poonjar, Kottayam District, Kerala, India

***Abstract*—Software-as-a-service (SaaS) cloud systems allow application service providers to deliver their applications via massive cloud computing infrastructures. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. SaaS clouds are vulnerable to malicious attacks because of their sharing nature. Many security frameworks have been developed to address cloud security issues like IntTest, Privacy Proxy, Trusted virtual data center,Placement and Extraction method for Exploring Information Leakage, Stateful Dataflow Processing, Building Privacy-Conscious Composite Web Services, Anomaly Extraction and Mitigation using Efficient-Web Miner Algorithm.Breif Study on the above frame works are explained below.**

***Keywords*—: Distributed Service, Integrity attestation, Cloud computing, Multitenanat.**

I. INTRODUCTION

Cloud computing is a technology helps us to keep up data and its application by using internet and central remote servers [18]. Cloud computing has greater flexibility and availability at lower cost. The four deployment models operated by cloud computing are the: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud. Private cloud -- The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. Community cloud -- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on premise or off premise. Public cloud -- The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling thecloudservices and the comparison of private and public cloud.Hybrid cloud -- The cloud infrastructure is a composition of two or more clouds (private, community, or public).

There are different types of cloud service providers like Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).Here we are discussing about SaaS Cloud system. Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made this is available to customers over a network.SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) and many other new developmental approaches. SaaS service are suffered from many malicious attacks hence they need security. Below are the various frameworks proposed to provide security.

II. REVIEW OF EXISTING FRAMEWORKS

A. IntTest

Juan Du, Daniel J. Dean, made study on a powerful integrated service integrity attestation framework [11][12][13][14][10] called IntTest [1] for multitenant cloud systems which can pinpoint malicious attackers [3][17] even if they become majority for some service functions. This scheme does not need any application modifications or it does not assume trusted entities on third-party service provisioning sites. In large-scale cloud systems, multiple malicious attackers may launch colluding attacks on certain kinds targeted service functions and hence invalidate the service. In order to address this challenge, IntTest takes a holistic approach by systematically examining both consistency and inconsistency relationships among different service providers within the whole cloud system.

IntTest examines both per-function consistency graphs and also the global inconsistency graphs. Per-function graph analysis can limit the scope of damage caused by colluding attackers. The global inconsistency graph analysis can effectively expose those attackers that may try to compromise many service functions. IntTest can help to suppress aggressive attackers and limit the scope of the damage caused by colluding attacks. This is based on replay-based consistency check and the integrity attestation graph model.

Now consider the consistency check scheme for attesting three service providers' let them be p1, p2, and p3 that offer the same service function f. Here the portal [9][10] sends the original input data d1 to p1and gets back the result f (d1). Next, the portal sends d'1, a duplicate of d1 to p3 and gets back the result f (d'1). The portal then compares both outputs to see whether p1 and p3 are consistent. The main idea behind this approach is that if two service providers disagree with each other on the processing result of the same input, then at least one of them should be malicious. We do not send an input data item and its duplicates concurrently. Instead, we replay the attestation data on different service providers. After receiving the processing result of the original data In order

to reduce the delay caused by replay we can overlap the attestation and normal processing of consecutive tuples in the data stream and hence can hide the attestation delay from the user.

Advantages*: Low overhead, cost effective, guaranteed integrity, doesnot need special hard ware or kernel support.*
Drawbacks*: Input deterministic, Presence of Security Loop holes*

B. **Privacy Proxy**

Zhendong Ma, Jurgen Mangler, Wagner proposes a privacy enhanced design in the paper [2] that mainly aims to minimize personal data disclosure in nested web service by proposing a scalable and light-weight design that uses a privacy proxy to achieve data privacy. This paper also proposes the utilization of service level agreements (SLA's) for user benefits. Two design principles: (1) minimal disclosure- tight control over how many times personal data is accessed, (2) direct disclosure- allow for a means to determine by whom personal data is accessed. Privacy Proxy Service (PPS) is established as a trusted third party in the interaction between a customer and composite services. Its main function of PPS is to temporarily store a customer's personal data items, as well as to control and trace the access to such data. This design offers the following properties:

- Each PDI (personal data item) is stored separately.
- Each PDI is stored only for a limited amount of time.
- Each PDI is identified by a unique key, further referred to as ticket.
- Each PDI is only accessible once.
- Tickets are not linkable.

There are three interaction phases: Negotiation, Storage and Retrieval. During storage phase customer stores each PDI in the PPS and for each PDI, a ticket is returned. During the retrieval phase the Business services are communicating solely with the PPS only (no interaction with intermediate service).However this design does not prevent services from colluding.

Advantages: *Scalable, light weight, uses SLA's, transparent, no need to modify existing service and underlying infrastructure, less impact on overall performance.*
Drawback: *Doesn't prevent service from colluding hence cannot keep the overhead at minimal.SLA negotiations are not dynamic.*

*C.***Placement and Extraction method for Exploring Information Leakage**

This paper [3] aims at the practicality of mounting cross-VM attacks in existing third-party compute clouds. There are two main steps while considering attacks we consider require two main steps: placement and extraction. Placement refers to the adversary making arrangement for place their malicious VM on the same physical machine similar to target customer. Extraction refers to extract confidential information via a cross-VM attack. This mainly occurs due to the sharing of sharing of physical resources. Here there are two kinds of attackers being considered – first is those who cast a wide net and are interested in being able to attack some known hosted service and second is those focused on attacking a particular victim service. Amazon's Elastic Compute Cloud (EC2) service is taken as example here. Network Probing is used for understanding VM placement in the EC2 system and achieving co-resident we use hard-disk-based covert channel between EC2 instances or determining co-residence In the case of network based co-resident check we say two instances are likely co-resident if they have
(1) Matching Domo IP address,
(2) Small packet round-trip times, or
(3) Numerically close internal IP addresses
Brute force placement is the technique that is being used earlier .Later this was replaced by the new one that assumes an attacker can launch instances relatively soon after the launch of a target victim. The attacker then engages in instance flooding that is running as many instances in parallel as possible, in the appropriate availability zone and appropriate type. Since The EC2 placement algorithms seems inefficient to stop a dedicated attacker there is another method to "patch" all placement vulnerabilities: offload choice to users that is users re-quest placement of their VMs on machines that can only be populated by VMs from their account. Another kind of attack is cryptographic cross-VM attacks. But these kinds of attacks are very difficult to $realize. Co-residence detection can also detected by analysising load variation due to a publicly-accessible service running on the target.

Advantages: *Help to determine where in the cloud infrastructure an instance is located, whether two instance co resident on the same physical machine, whether an adversary launch instance can be co-resident with other user's instance, whether an adversary can extract cross VM-information leakage, make use of cache based load balancing for keystroke timing attack. Binding techniques are used to minimize the information leakage.*
Drawbacks: *Methods used for inhibiting side channel attack has two drawback-high overhead, nonstandard hardware, application specific and are not sufficient for mitigating risk, keystroke attacking can be applied only when attackers and victim shares the same core.*

D. **Stateful Dataflow Processing Services**

This paper [4] propose Robust Service Integrity Attestation (ROSIA) framework. This can efficiently verify the integrity of stateful dataflow processing services and pinpoint malicious service within a large-scale cloud system. ROSIA support stateful dataflow Services and hence achieves robustness. ROSIA performs integrity attestation by examining both consistency and inconsistency relationships. This frame work attains higher attack detection accuracy and also limits the scope of the damage caused by colluding attackers. This proposes two methods to attest stateful functions. One method is called indirect state recovery, which relies on replaying a sequence of historic input data to indirectly bring back the state. Another method is difference check, which derives consistency relationship between two stateful service components by comparing result difference produced by

two consecutive input data. The basic idea behind this is Replay-based Consistency Check.

Advantage: *This supports both stateless and stateful service functions, effective and imposes low overhead .This, based on the assumption that the total number of malicious service components is less than that of benign ones in the entire cloud system, higher detection rate and lower false positive rate in certain attack scenarios.*

Drawbacks*: Malicious service providers can escape from being detected by trying to form a majority clique in the per-function consistency Graph.*

E. Trusted Virtual Data Center

This paper [5] talks about a new technology called The trusted virtual data center (TVDc) which can address the need for strong isolation and integrity guarantees in virtualized environment. We can have controlled access to networked storage based on security labels and prototypes for the enforcement of isolation constraints and integrity checking.

Virtualization is a technology used in data enters for both commodity and high-end servers. This has the ability to aggregate multiple workloads to run on the same set of physical resources, thus resulting in increased server utilization and reduced space and power consumption. Virtualization utilizes a software layer, called virtual machine monitor (VMM) for creating virtual machines (VMs). TVDc provides isolation through employing an isolation policy and different types of workload isolation mechanisms. This policy will abstracts the physical infrastructure and allows for automated policy-driven configuration management of data center resources. The boundaries of a TVD can be defined by labeling all VMs and associated resources within the TVD with a unique TVD identifier known as a security label. Isolation policy has two parts: (1) the label Definition (2) anti-collocation definitions. The access control management is based on the security labels. The different kinds of isolation supported on the workload and administration planes are Data sharing, VMM system authorization, Collocation constraints and Management constraints. For integrity management we can use TVDc to establish trust in a remote computer by verifying the integrity of the software loaded that computer, whether it is a physical or virtual system. For Integrity attestation we require a database of reference measurements that can be compared with run-time measurements from VMs. Therefore isolation management, workload management, and access control are important aspects of cloud computing since there are increased possibilities of misconfiguration.This can cause an additional vulnerability.

Advantages: *Provides strong Isolation, Guarantees integrity, ability to aggregate multiple workloads, increased server utilization and reduced space and power consumption, flexibility in server deployment, workload mobility, global service availability at large scale at low cost, ensure that viruses and other malicious code cannot spread from one customer workload to another, prevent data from leaking from one customer workload to another, provides policy-driven security management.*

Drawbacks: *Placing different customers' workloads on the same physical machines may lead to security vulnerabilities, such as denial of service attacks, and possible loss of sensitive data, misconfiguration which caused increased vulnerability.*

F. Building Privacy-Conscious Composite Web Services

This paper [6] proposes a framework that can addresses consumer privacy concerns in the context of highly customizable composite web services. This approach involves service producers that exchange their terms-of-use with consumers in the form of models. This framework has automated techniques for checking these models at the consumer site for compliance of consumer privacy policies. In the case of a policy violation, this framework can supports automatic generation of obligations. These obligations are automatically enforced through a dynamic program analysis approach on the web service composition code. This framework consists of five major components: a) service composition code, b) service models, c) privacy policies, d) policy compliance checker and obligation generation, and e) obligation enforcer. Two important problems that need to be addressed in this are1) Policy compliance checking 2) Obligation enforcement. Another important technique which can be built by composing a number of smaller services is Service composition. This is introduced with the goal of providing consumer data privacy in service composition. The natural formalism in service composition includes construing every Component service as a function that maps a set of inputs to a set of outputs. The Privacy policy used here will describe the privacy requirements of a user by defining constraints on how her data could flow between different entities. We use the concept labels to specify the privacy policies. Labels are classified as data labels and principal labels. Labels have two types of attributes 1) Data label attributes and 2) Principal label attributes. A privacy policy can be formalized as a set of policy rules. To enforce obligations, the composite service needs to track whether the flow of consumer's data inputs respect these obligations. Hence through our framework, consumers can have facilities to specify their privacy concerns through use of privacy policies, while service providers express their terms of use through models.

Advantage: *It provides consumer privacy concerns in the context of highly customizable composite web services, supports automatic generation of obligations.*

Drawbacks*: Does not address malicious service providers that intentionally lie about their usage of consumer data, this frame work doesn't give any feedback to the service*.

G. Anomaly Extraction and Mitigation using Efficient-Web Miner Algorithm

This paper [7] deals with Anomaly deviation that affects network security. Anomaly extraction aims to automatically find the inconsistencies in large set of data observed during an anomalous time interval. Those extracted anomalies can be used for root cause analysis, network forensics, attack mitigation and anomaly modeling. Efficient-Web Miner Algorithm will be used to generate

the set of association rules applied on metadata. Thus these algorithms effectively find the flow associated with the anomalous events.

Advantage: *Root cause analysis, network forensics, attack mitigation and anomaly modeling..*

Drawbacks*: Cannot reduced the problem of candidate set generation by providing an improved candidate set pruning.*

H. **Result Analysis**

Considering the parameters like integrity, server utilization, extendibility ,overhead and vulnerabilities we could find that Trust virtual data center and Placement and Extraction method has high server utilization ,low overhead but they have denial of service, malicious service provides can still escape.Stateful data processing method seems to have low overhead and scalability but malicious providers can still escape while Privacy proxy can provide security to user data it cannot avoid colluding attacks. Privacy conscious composite web services has automated techniques for checking models at the consumer site for compliance of consumer privacy policies but still they cannot address malicious service providers that intentionally lie about their usage of consumer data, also have low server utilization. It has low overhead and is scalable. Anomaly extraction using minor algorithm has high server utilization but it has high overhead.IntTest has low overhead,scalable,high server utilization,doesnot require any special hard ware or secure kernel support and it can provide security from malicious service providers more effectively than any other frame works.

III.CONCLUSION

In this paper a wide survey of the different frameworks for providing security to SaaS has been carried out and pointed out their advantages and drawbacks. We need to further improve those frameworks or develop some efficient novel methods.

ACKNOWLEDGEMENT

First and foremost I offer my sincerest gratitude my guide, Jiby JP who has supported me though out my thesis with his patience and knowledge.

REFERENCE

[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"

[2]. Zhendong Ma_, J¨urgen Manglery, Christian Wagner_, Thomas Bleier__Austrian Institute of Technology, "Enhance Data Privacy In Service Compositions Through A Privacy Proxy"

[3]. Thomas Ristenpart_ Eran Tromer† Hovav Shacham_ Stefan Savage_Dept. of Computer Science and Engineering †Computer Science and Artificial Intelligence Laboratory University of California, San Diego, USA Massachusetts Institute of Technology, Cambridge, USA" Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute CloudsDept. of Computer Science and Engineering".

[4]. Juan Du, Xiaohui Gu, Ting Yu Department of Computer Science, North Carolina State University" On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems"

[5] S.Berger,Caceres,K. Goldman,D. Pendarakis,".Security for the cloud infrastructure:Trustedvirtual data center implementation".

[6] Wei Xu ¤ V.N. Venkatakrishnan y R. Sekar I.V. Ramakrishnan ,Department of Computer Science tony Brook UniversityStony Brook, NY 11790-4400 Email: venkat@cs.uic.edu5" A Framework for Building Privacy-Conscious Composite Web Services"

[4]. Juan Du, Xiaohui Gu, Ting Yu Department of Computer Science, North Carolina State University" On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems"

[6]. Wei Xu ¤ V.N. Venkatakrishnan y R. Sekar I.V. Ramakrishnan ,Department of Computer Science tony Brook UniversityStony Brook, NY 11790-4400 Email: venkat@cs.uic.edu5" A Framework for Building Privacy-Conscious Composite Web Services"

[7]. Gargi Joshi,Department of computer Engineering Dr. D. Y. Patil College of Engineering Of Pune, Ambi, Pune – 410506," Anomaly Extraction and Mitigation using Efficient-Web Miner Algorithm"

[9]. QoS-Assured Service Composition in Managed Service Overlay Networks," Proc. 23rd Int'l Conf. DistributedComputing Systems (ICDCS '03), pp. 194-202, 2003.

[10] .Towards Standardized Web Services Privacy Technologies," IEEE Int'l Conf. Web Services, pp. 174-183, June 2004.

[11]. Managing and Securing Web Services with VPNs," Proc. IEEE Int'l Conf. Web Services, pp. June 2004.

[13] Service-Oriented Virtual Private Networks for Grid Applications," Proc. IEEE Int'l Conf. Web Services, pp. 944-951, July 2007.

[12] .F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services," Proc. 12thInt'l Conf. Information Security (ISC), pp. 491-506, 2009.

[13] Managing Security in the Trusted Virtual Datacenter," ACM SIGOPS Operating Systems Rev, vol. 42, no. 1,pp. 40-47, 2008.

[14] Security Issues and Security Algorithms in Cloud Computing K.S.Suresh , Prof K.V.Prasad