International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Integrity Attestation for Software-as-a Service Clouds

Chashu Mol R[1], Alfia A P[2]

Mount Zion College of Engineering Mount Zion College of Engineering

Abstract: ***Software-as-a service (SaaS) makes use of a cloud computing infrastructure to deliver their applications to many users regardless of their location. Because of this sharing nature SaaS clouds are vulnerable and provide more opportunities for attackers to exploit the system vulnerability and perform strategic attacks. In this paper, we present IntTest, an effective service integrity attestation framework for SaaS clouds. IntTest provides an integrated graph attestation analysis method that can pinpoint malicious service providers than existing methods. Also IntTest will automatically correct the corrupted result that are produced by the malicious service providers and replace it with good results produced by benign service providers. Our experimental results show that our scheme is effective and can achieve higher accuracy in pinpointing the attackers than the existing approaches.***

Keywords: Service Integrity Attestation, Cloud Computing

1. Introduction

Cloud computing relies on sharing of resources over a network. Cloud computing mainly focuses on maximizing the effectiveness of the shared resources. Software as a service describes any cloud service where consumers are able to access software applications over the internet. Clouds are providing many types of services like applications, infrastructures etc. Software-as-a-service (SaaS) clouds (e.g., Amazon Web Service (AWS) and Google AppEngine) build upon the concepts of software as a service and service-oriented architecture (SOA) which enable application service providers (ASPs) to deliver their applications via the massive cloud computing infrastructure[1].Cloud computing infrastructures are shared by using ASPs from different security domains, because of that its vulnerable.

Now a days the cloud computing technology is popular because it is an attracting technology in computer science field. This paper concentrate on the integrity attacks on software as a service clouds and because of that the user will receive bad results after processing the data. Fig.1 shows the integrity attacks in software as a service clouds. Majority of software as a service cloud solutions are based on a multi-tenant architecture. In the previous research papers confidentiality and privacy protection problems are studied extensively but the service integrity attestation problem was not properly addressed. In software as a service cloud one of the most important problems that need to be addressed is this service integrity, no matter whether the data processing in cloud is public or private data. In the previous papers they are provided some software integrity attestation techniques but most of them requires special trusted hardware or secure kernel supports and because of these reasons that cannot be deployed in large scale cloud computing. This paper presents IntTest, a new framework for multi tenant cloud systems. This technique provides the novel integrated attestation graph analysis technique that will provide a stronger attacker pinpointing power than the existing schemes. It will automatically enhance the result quality by replacing the bad results that are produced by the attackers by good results that are produced by the benign service providers. This can achieve higher attacker pinpointing accuracy than existing techniques Run Test and Adap Test.

Figure 1: Software-as-a Service

Specifically, RunTest and AdapTest as well as traditional majority voting schemes need to assume that benign service providers take majority in every service function.

In large-scale multitenant cloud systems, large number of malicious attackers may launch colluding attacks on the targeted service functions to make them malicious. To address this challenge, IntTest takes a holistic approach by systematically examining both consistency and inconsistency relationships among different service providers within the entire cloud system. IntTest checks both per-function consistency and the global inconsistency graphs. An advantage of using this IntTest is it cannot only pinpointing the malicious attackers more efficiently but also it can suppress aggressive attackers and also limit the scope of damage that are caused by the attacks. The experimental result shows that IntTest can achieve more accuracy in pinpointing malicious attackers than any other existing schemes. Also this IntTest is more scalable and it will reduce overhead produced by the attestation more than the other voting schemes.

This paper implements

- Efficient and distributed service integrity attestation framework for large scale cloud computing infrastructures.
- An integrated service integrity attestation scheme that can achieve higher pinpointing accuracy than existing techniques.
- A result auto correction technique is used that will automatically correct the corrupted results produced by malicious attackers and replace it with good results.

- The analytical study and experimental evaluation used to quantify the accuracy and overhead of the service integrity attestation method.

The rest of this paper is organized as follows. Section 2 presents the related work. Section 3 provides the proposed system in detail. Section 4 presents the main modules. Finally, the paper concludes in section 5.

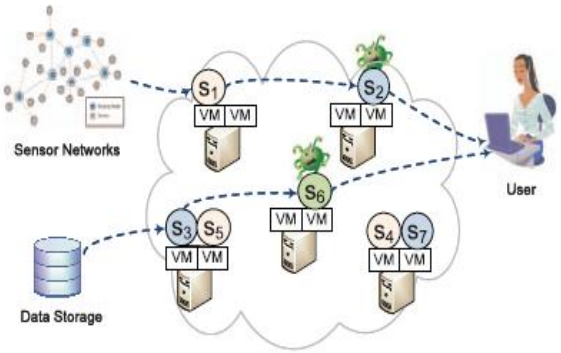

Figure 1: Service integrity attacks in clouds

2. Related Study

In recent years many integrity attestation schemes have been developed for software as a service clouds. For example the BIND technique, AdapTest technique, RunTest technique etc. but all of these are having some problems some of them needs secure kernel support and special trusted hardware components. In BIND (Binding Information and Data) technique is a verification method of integrity services that are provided by the software as a service cloud system. It was a fine grained attestation framework and can provide the verification through a secure kernel or by a third party. This technique uses the following steps: 1) attestation annotation mechanism 2) sandbox mechanism 3) verification of authenticator through hash. BIND method uses the Diffee-Hellman key exchange for the purpose of integrity attestation. Another existing technique is TEAS (Timed Executable Agent System) this is used for protecting the integrity of cloud computing platforms. An agent generation and verification algorithm is used in this TEAS method.

Another one existing technique is the runtest, it is a scalable runtime integrity attestation framework. It provides a light weight application level attestation method to assure the integrity of daa flow processing in cloud. This will will identify the untruthful data flow processing and will pinpoint mallicious data processing service provider and atlast it will detect the attackers behaviour. This RunTest will provide the benign service providers and will determine the malicious behaviour of the attackers. But the disadvantage is its low performance. The AdapTet is another one existing technique, it provides a novel adaptive data driven runtime service integrity attestation frmaework. This method will significantly reduce the overhead of attestation and will shoten the delay. It treats all components as black boxes and it does not need any special hardware or software requirements. In this AdapTest it will reduce the attestation overhead and the detection of malicious attackers or service providers will be high when compared to other techniques. All the above methods that are used in the existing papers are having some disadvantages. And to overcome that disadvantages this IntTest is using. And by using this IntTest it will provides more integrity and it will provide more accuracy in pinpointing the malicious attackers and service providers. Also it will provide a result auto correction method and will correct the bad results and replace it with good results and also in this it doesnot require any special hardwares and secure kernel support.

3. Proposed System

Software as a service and service oriented architecture are the basic concepts of SaaSclouds and this will allow the application service provider to deliver their application via cloud computing infrastructure. In our proposed method we are introducing a new concept called IntTest. The main goal of IntTest is, it can pinpoint all the malicious service providers. IntTest will treat all the service providers as black boxes and this does not need any special hardware or secure kernel support. When we are considering the large scale cloud system multiple service providers may simultaniously compromised by a single malicious attacker. In this we assume that the malicious nodes are not having any knowledge about the other nodes except those which they are directly interacting.

In this proposed system we are making some assumptions. First of all we are assuming that the total number malicious service components are less than that of the total number of benign service providers in the entire cloud. This assumptions is very important because without this assumption, it would be difficult for any attack detecting scheme to work succesfully. The second assumption is the data processing services are important deterministic. That is, the same input that are giving by a benign service component will always produce the same output. And finally we assume that the inconsistency caused by hardware or software faults can be excluded from malicious attacks. Fig. 2 shows the over all aarchitecture of the proposed system. In this the user give request to cloud the serive will be deployed in the cloud the cloud will forward the user request to the SaaS and the response will be send to the cloud by the SaaS. And then the IntTest process will be done. After that the result auto correction will be done. After that the result will be send to the user by the cloud. The architecture shows this IntTest module in detail.

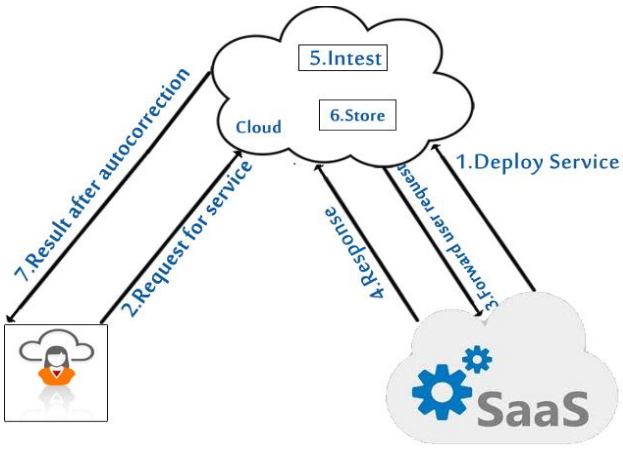

Figure 2: Over all architecture of the proposed method

4. Modules

In this section we present the main modules in the proposed system. Mainly it consists of four modules that are described below.

4.1 Baseline Attestation Scheme

IntTest is used to detect the service integrity attack and to pinpoint malicious service providers. For that first we are deriving the consistency and inconsistency relationship between service providers. Consider the fig 3 it shows the consistency check method. In that p1,p2 and p3 are the service providers. All of them offers the same function f. The portal sends the original data d1 to the service providers p1 and gets the processing result f(d1). Then the portal sends the duplicate of d1 to p3 and gets the result f(d1'). And if both of them are same means it is consistent and if not means they are inconsistent.that is if two service providers disagree with each other, when processing the same input then any one of them will be malicious. Thus the malicious attackers cannot escape from detecting when they are providing bad results with good results.

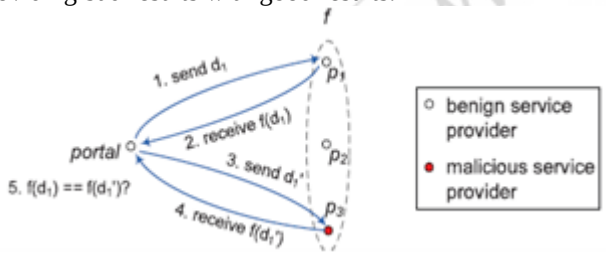

Figure 3: Consistency check

4.2 Integrated Attestation Scheme

Here we present an integrated attestation graph analysis algorithm.

Step 1: Consistency analysis: In the first step it will examine the per-function consistency graph and will pinpoint suspicious service providers. The consistency links in the consistency graph will provide a set of service providers. It will keep consistent with each other on a specific service function. The benign service providers will always keep consistent with each other and will form a clique in terms of consistency links. The colluding attackers can try to escape from being detected. Then next we must examine the per-function in consistency graph too.

Step 2: Inconsistency analysis: This inconsistency graph will contain only the inconsistency links, this may exist in different possible combinations of the benign node and the malicious node set. First we assume that the total number of malicious service providers in the cloud system is not more than the benign service providers, then we can pinpoint a set of malicious service providers. If two service providers are connected by an inconsistency link, we can say that any one of them is malicious.

4.3 Result Auto Correction for Attacks:

IntTest can not only pinpoint malicious service providers but also it will autocorrect the corrupted data processing results with good results to improve the result quality of the cloud data processing service. Without our attestation scheme, once if an original data input is changed by any malicious attacker, then the processing result of that input will be corrupted and which will result in degraded result quality. IntTest provides the attestation data and the malicious node pinpointing results to detect and correct compromised data processing results[1]. IntTest will examine both the inconsistency and consistency graphs to make a final decision to pinpoint the malicious service provider. This technique can achieve higher detection rate than any other existing technique and will have low false alarm rate than others. Also IntTest can achieve higher detection accuracy than any other techniques when malicious service providers attack more nodes. This method will identify the attackers even though they attack a very low percentage of services.

5. Conclusion

In this paper we introduced a novel integrated service integrity attestation graph analysis scheme for multitenant software-as-a-service cloud system. IntTest uses a reply based consistency check to verify the service providers. IntTest will analyses both the consistency and inconsistency graphs to find the malicious attackers efficiently than any other existing techniques. And also it will provide a result auto correction to improve the result quality.

6. Acknowledgment

The author gratefully acknowledge the valuable comments and suggestions of the reviewers, which have improved the presentation and also thankful to the reference paper authors. And they are especially grateful to Prof. Smitha Miss for her kind help during the review process of this paper.

References

[1] Juan Du, Daniel J. Dean, Yongmin Tan, Xiaohui Gu, and Ting Yu "Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014

[2] Du.J, Wei.W, Gu.X, and Yu.T, "Runtest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures," Proc.ACM Symp. Information, Computer and Comm. Security (ASIACCS),2010.

[3] Du.J, Shah.N, and Gu.X, "Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems," Proc. Int'l Workshop Quality of Service (IWQoS), 2011. Virtual Computing Lab, http://vcl.ncsu.edu/, 2013.

[4] Shi.E, Perrig.A, and Doorn.L.V, "Bind: A fine-grained attestation service for secure distributed systems," in Proceedings of the IEEE Symposium on Security and Privacy, 2005.

Author Profile

Chashu mol R received degree in Computer Science & Engineering from VINS Christian college of Engineering, Nagercoil, Tamil nadu in 2012. She is now doing M.Tech in Computer Science & Engineering

Alfia A P received degree in Computer Science & Engineering from the Odaiyappa college of Engineering and Technology, Theni, Tamil nadu in 2013. She is now doing M.Tech in Computer Science & Engineering