A FRAMEWORK FOR DISTRIBUTED SERVICE INTEGRITY
ATTESTATION IN CLOUD COMPUTING

#1 P. PRATHYUSHA, M.Tech student,
#2 T. UPENDER, Associate Professor, HOD,
Department Of CSE
MOTHER THERESSA COLLEGE OF ENGINEERING & TECHNOLOGY, TS, 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. Brief Study on the above frame works are explained below. 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.

Keywords: Distributed Service, Integrity attestation, Cloud computing, Multitenant.

I. INTRODUCTION

Cloud computing is a technology helps us to keep up data and its application by using internet and central remote servers. 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 by 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 the cloud services 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. 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.
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.

II. RELATED WORK

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 DiffieHellman 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 data flow processing in cloud. This will will identify the untruthful data flow processing and will pinpoint malicious 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 AdapTest is another one existing technique, it provides a novel adaptive data driven runtime service integrity attestation framework. This method will significantly reduce the overhead of attestation and will shorten 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.

III. 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 it does not need any special hardware or secure kernel support. When we are considering the large scale cloud system multiple service providers may simultaneously 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 successfully. 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 architecture of the proposed system. In this the user give request to cloud
the service 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

IV. AN EFFECTIVE FRAMEWORK OF INTEGRATED SERVICE INTEGRITY ATTESTATION

Significant systems of multitenant cloud, numerous malicious attackers might commence colluding attacks on convinced targeted service functions to nullify assumption. To deal with the challenge, IntTest obtains a holistic method by thoroughly investigating consistency as well as inconsistency associations between several service providers in the complete cloud system. IntTest inspects per-function consistency graphs as well as the global inconsistency graph. The analysis of perfunction consistency graph can bound extent of damage that is caused by colluding attackers, while global inconsistency graph examination can effectively expose those attackers that attempt to compromise numerous service functions. IntTest can still find malevolent attackers even when they turn out to be popular for a number of service functions. IntTest offers a practical service integrity attestation system that does not believe trustworthy entities present on third party services provisioning sites necessitate application alterations [4]. To notice service integrity attack and find malevolent service providers, our algorithm depends on replay-based consistency check towards deriving consistency or inconsistency associations linking service providers. The perception following our approach is that when two service providers diverge with each other on processing result of similar input, not less than one of them has to be malevolent. We do not forward an input data item as well as its duplicates simultaneously as a substitute; we replay attestation data on several service providers subsequent to receiving of processing result of original data [5]. As a result, malevolent attackers cannot keep away from threat of being noticed when they generate fake results on innovative data. For scalability, we put forward randomized probabilistic attestation, which is an attestation method that by chance replays a subset of input data meant for attestation. By means of replaybased consistency check, we can check functionally corresponding service providers and get hold of their consistency as well as inconsistency relationships [6].

Fig 3: An overview of service integrity attacks.

V. 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 providers 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.

VI. CONCLUSIONS

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 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 methods.

REFERENCES


[2] Juan Du Daniel J. Dean, Yongmin Tan, Xiaohui Gu, Senior and Ting Yu Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds.


