International Journal For Technological Research In Engineering
Volume 3, Issue 7, March-2016 *ISSN (Online): 2347 - 4718*

STABLED MULTI CLOUDS FOR DATA CONSISTENCY WITH QUALITY

Batta Sudheer Kamal[1], Anantha Rao.G[2]
[1]Student of M.Tech (CSE) and Department of Computer Since Engineering,
[2]Department of Computer Science, Dr.Samuel George Institute of Engineering & Technology, Markapur.

Abstract: Software as a Service (SaaS) is a software distribution model in which a vendor or service provider develops the applications and this is made available to customers over a network. SaaS clouds are vulnerable to malicious attacks because of their sharing nature. IntTest, a scalable service integrity attestation framework has been anticipated and it uses a novel integrated attestation graph analysis scheme to pinpoint attackers. 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, Software as a Service

I. INTRODUCTION

Cloud computing has emerged as a cost-effective resource leasing paradigm, which obviates the need for users maintain complex physical computing infrastructures by themselves. Software-as-a-service (SaaS) clouds 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, illustrated by fig 1.

Fig 1: Software-as-a Service

In particular, our work focuses on data stream processing services that are considered to be one class of killer applications for clouds with many real-world applications in security surveillance, scientific computing, and business intelligence. However, cloud computing infrastructures are often shared by ASPs from different security domains, which make them vulnerable to malicious attacks. For example, attackers can pretend to be legitimate service providers to provide fake service components, and the service components provided by benign service providers may include security holes that can be exploited by attackers. Our work focuses on service integrity attacks that cause the user to receive untruthful data processing results, illustrated by Fig. 1. Although confidentiality and privacy protection problems have been extensively studied by previous research, theservice integrity attestation problem has not been properly addressed. Moreover, service integrity is the most prevalent problem, which needs to be addressed no matter whether public or private data are processed by the cloud system. Although previous work has provided various software integrity attestation solutions, those techniques often require special trusted hardware or secure kernel support, which makes them difficult to be deployed on large-scale cloud computing infrastructures. Traditional Byzantine fault tolerance (BFT) techniquescan detect arbitrary misbehaviors using full-time majority voting (FTMV) over all replicas, which however incur high overhead to the cloud system.

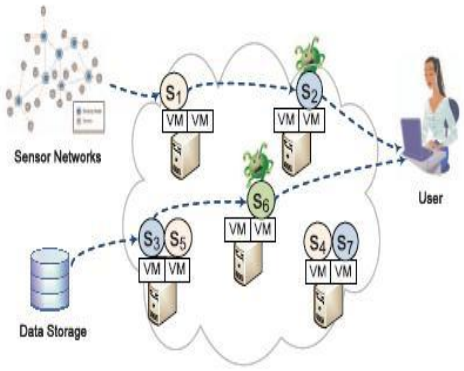

Fig 2: Service integrity attacks in cloud

In this paper, we present IntTest, a new integrated service integrity attestation framework for multitenant cloud systems. IntTest provides a practical service integrity attestation scheme that does not assume trusted entities on third-party service provisioning sites or require application modifications. IntTest builds upon our previous work RunTest and AdapTest but can provide stronger malicious attacker pinpointing power than RunTest and AdapTest. Specifically, both RunText and AdapTest as well as traditional majority voting schemes need to assume that benign service providers take majority in every service function. However, in large-scale multitenant cloud systems, multiple malicious attackers may launch colluding attacks on certain targeted service functions to invalidate the assumption. To address the challenge, IntTest takes a holistic

approach by systematically examining both consistency and inconsistency relationships among different service providers within the entire cloud system. IntTest examines both per-function consistency graphs and the global inconsistency graph. The per-function consistency graph analysis can limit the scope of damage caused by colluding attackers, while the global inconsistency graph analysis can effectively expose those attackers that try to compromise many service functions. Hence, IntTest can still pinpoint malicious attackers even if they become majority for some service functions. By taking an integrated approach, IntTest can not only pinpoint attackers more efficiently but also can suppress aggressive attackers and limit the scope of the damage caused by colluding attacks. Moreover, IntTest provides result autocorrection that can automatically replace corrupted data processing results produced by malicious attackers with good results produced by benign service providers. Specifically, this paper makes the following contributions:

- We provide a scalable and efficient distributed service integrity attestation framework for largescale cloud computing infrastructures.
- We present a novel integrated service integrity attestation scheme that can achieve higher pinpointing accuracy than previous techniques.
- We describe a result auto correction technique that can automatically correct the corrupted results produced by malicious attackers.
- We conduct both analytical study and experimental evaluation to quantify the accuracy and overhead of the integrated service integrity attestation scheme.

We have implemented a prototype of the IntTest system and tested it on NCSU's virtual computing lab (VCL) , a production cloud computing infrastructure that operates in a similar way as the Amazon elastic compute cloud (EC2). The benchmark applications we use to evaluate IntTest are distributed data stream processing services provided by the IBM System S stream processing platform an industry strength data stream processing system. Experimental results show that IntTest can achieve more accurate pinpointing than existing schemes (e.g., RunTest, AdapTest, and full-time majority voting) under strategically colluding attacks. IntTest is scalable and can reduce the attestation overhead by more than one order of magnitude compared to the traditional full-time majority voting scheme.

Existing System

Which enable application service providers (ASPs) to deliver their applications via the massive cloud computing infrastructure. In particular, our work focuses on data stream processing services that are considered to be one class of killer applications for clouds with many real-world applications in security surveillance, scientific computing, and business intelligence. However, cloud computing infrastructures are often shared by ASPs from different security domains, which make them vulnerable to malicious attacks. For example, attackers can pretend to be legitimate service providers to provide fake service components, and the service components provided by benign service providers may include security holes that can be exploited by attacker.

Proposed System

Software as a service and service oriented architecture are the basic concepts of SaaS clouds 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 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.

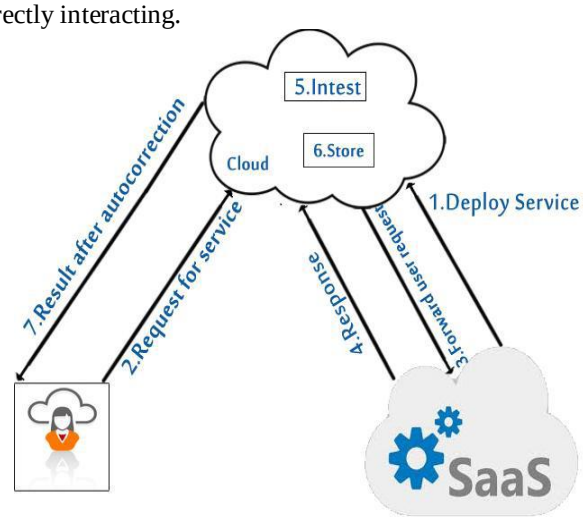

Fig 3: architecture of the proposed System

In this paper, we present IntTest, a new integrated service integrity attestation framework for multitenant cloud systems. IntTest provides a practical service integrity attestation scheme that does not assume trusted entities on third-party service provisioning sites or require application modifications. IntTest builds upon our previous work RunTest and AdapTest but can provide stronger malicious attacker pinpointing power than RunTest and AdapTest. Specifically, both RunText and AdapTest as well as traditional majority voting schemes need to assume that benign service providers take majority in every service function. However, in large-scale multitenant cloud systems, multiple malicious attackers may launch colluding attacks on certain targeted service functions to invalidate the assumption. To address the challenge, IntTest takes a holistic approach by systematically examining both consistency and inconsistency relationships among different service providers within the entire cloud system. IntTest examines both per-function consistency graphs and the global.

Modules

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

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.

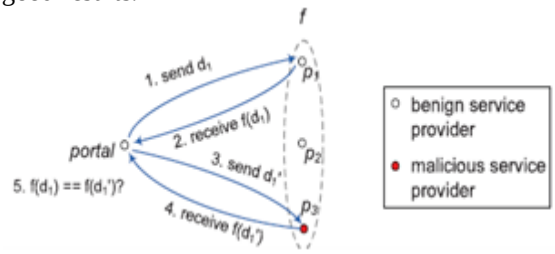

Fig 4: Reply based Consistency check

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.

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.

II. 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.

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

[3] Google App Engine, http://code.google.com/appengine/, 2013.Software as a Service, http://en.wikipedia.org/wiki/Software as a Service, 2013.

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

[5] J. Du, N. Shah, and X. Gu, "Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems," Proc. Int'l Workshop Quality of Service (IWQoS), 2011

[6] 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

[7] 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.

[8] 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.

[9] 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

Batta Sudheer Kamal pursuing her M.tech in computer science from Dr.Samuel George Institute of Engineering and Technology, Markapur, Prakasam District, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI.

Anantha Rao .G is a Associate Professor of Dr.Samuel George Institute of Engineering & Technology ,MARKAPUR.He received M.Tech in Software Engineering from JNTU Kakinada University..Hegained 6years Experience on Teaching. He is a good Researcher in Image Processing, Algorithms', Computer Networks. He attended Various National and International Workshops and Conferences.

