ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

An Effective Approach for Maintaining High Accurateness in Cloud Environment

Mr. Rajeshwar Rao Kodipaka[1], Mr. M. Amarendhar Reddy[2], B. Venkat Ramudu[3]

Asst. Professor, Department of CSE, MallaReddy Engineering College (Autonomous), Hyderabad, India[1, 3]

Asst. Professor, Department of IT, B.V. Raju Institute of Technology, Medak, India[2]

Abstract: Generally Software-as-a-service clouds were built on software as a service along with service-oriented architecture. This assists the providers of application service in conveying their applications by means of substantial cloud computing infrastructure. In the traditional efforts while confidentiality as well as privacy protection exertions was broadly studied, the problem of service integrity attestation has not been appropriately addressed. In our work we mainly spotlight on data processing services which have turned out to be popular with applications in numerous usage areas. We present IntTest, which is a scalable and efficient integrated service integrity attestation structure intended for software-as-a-service cloud multitenant cloud systems. The proposed approach offers a novel integrated attestation graph analysis method which can not only identify attackers more resourcefully by taking an integrated approach, but also can hold back aggressive attackers and limit the scope of damage that is caused by colluding attacks.

Keywords: Software-as-a-service, Integrated attestation graph analysis, Cloud computing, IntTest, Attackers.

1. INTRODUCTION

Infrastructures of cloud computing are usually shared by application service providers from various domains of security which make them exposed to malicious attacks. Service integrity is the most prevailing problem that has to be addressed regardless of processing of public or private data by cloud system [1]. In major multitenant systems of cloud, numerous malicious attackers might commence colluding attacks on definite targeted service functions to nullify the assumption. In our work we focus on services of data streaming applications for clouds with numerous real-world applications. In our work to address this challenge we present IntTest, which is an integrated service integrity attestation structure intended for multitenant cloud systems. IntTest put forward result auto-correction that can automatically restore corrupted data processing results that are produced by malevolent attackers with superior results that are produced by benign service providers. IntTest approach considers a holistic approach by thoroughly examining consistency as well as inconsistency relationships between several service providers within complete cloud system. IntTest offers a realistic service integrity attestation system that does not imagine trustworthy entities on third-party service.

2. MODELLING OF CLOUD MODEL OF SAAS

Software-as-a-service clouds mostly were put up on concepts of software as a service along with service-oriented architecture which facilitate application service providers in conveying their applications by means of substantial cloud computing infrastructure. In a comprehensive Software-as-a-service cloud, identical service function can be offered by various application service providers [2][3]. These components of functionally equivalent service exist due to service providers might generate replicated service components in support of load Balancing as well as fault tolerance purposes; and popular services might attract several service providers for profit. To maintain automatic service composition, we can install a set of portal nodes that serve as the gateway for user to access composed services in Software-as-a-service cloud. The portal node can combine various service components into composite services on the basis of user's needs. Altered from other distributed systems for instance peer-to-peer networks as well as volunteer computing setting, Software-as-a-service cloud systems acquire a set of distinctive features. Application service providers of third-party usually do not want to make known internal functioning details of their software services for protection of intellectual property. Both cloud infrastructure providers as well as third-party providers are independent entities. It is not practical to enforce any special hardware or else protected kernel support on individual service provisioning sites. For privacy fortification, only portal nodes encompass global information regarding which service functions are offered by which service providers in Software-as-a-service cloud. Our work draw attention in the direction of on data processing services which have turned out to be more and more popular with applications in numerous real-world usage areas.

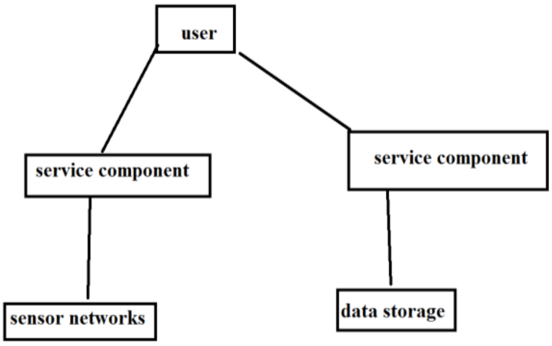

Fig1: An overview of service integrity attacks.

DOI 10.17148/IJARCCE.2015.41039

In our work present IntTest, which is a scalable and efficient integrated service integrity attestation structure intended for software-as-a-service cloud multitenant cloud systems. IntTest offers a novel integrated attestation graph analysis method that can make available stronger attacker pinpointing power than earlier schemes. Given a Software-as-a-service cloud system, objective of IntTest is to identify any malevolent service provider that offers a misleading service function [4]. IntTest considers all service components as black boxes, which does not necessitate any special hardware on cloud platform.

3. AN OVERVIEW OF PROPOSED IntTest SYSTEM

IntTest put up on earlier work and AdapTest but can grant well-built malicious attacker pinpointing control than RunTest and AdapTest. RunText and AdapTest as well as conventional majority voting methods need to imagine that providers of benign service receive majority in each service function. IntTest scrutinize per-function consistency graphs as well as global inconsistency graph. The analysis of per-function consistency graph can limit extent of damage that is caused by colluding attackers, while global inconsistency graph analysis can efficiently depict those attackers that attempt to compromise numerous service functions for this reason, IntTest can still identify malicious attackers although they turn out to be majority for several service function. IntTest offer result auto-correction that can automatically restore corrupted data processing results that are produced by malevolent attackers with superior results that are produced by benign service providers. It presents a realistic service integrity attestation system that does not imagine trustworthy entities on third-party service. By taking an integrated approach, IntTest can not only identify attackers more resourcefully but also can hold back aggressive attackers and limit the scope of damage that is caused by colluding attacks. In our work we focus on services of data streaming applications for clouds with numerous real-world applications. Our work spotlight on data processing services which have turned out to be more and more popular with applications in numerous real-world usage areas [5]. IntTest can not only identify malicious service providers but moreover automatically spot on corrupted data processing results to get better result quality of cloud data processing service. The offers a novel integrated attestation graph analysis method that can make available stronger attacker pinpointing power than earlier schemes. To distinguish service integrity attack as well as pinpoint malicious service contributor, our algorithm depends on replay-based consistency check to obtain consistency/inconsistency relationships among service providers. The intuition following our method is that when two service providers differ with each other on processing result of the 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 attestation data on several service providers after receiving processing resultoriginal data consequently, malicious attackers cannot avoid risk of being detected when they construct false results on original data [6]. By means of replay-based consistency check, we can check functionally equivalent service providers and get hold of their consistency as well as inconsistency relationships.

4. CONCLUSION

We draw attention towards services of data stream processing that are considered for clouds with abundant applications. Our work put forward an effective and scalable IntTest, which is efficient integrated service integrity attestation structure intended for software-as-a-service cloud multitenant cloud systems. Scalable IntTest approach takes for consideration a holistic approach by thoroughly examining consistency as well as inconsistency relationships between several service providers within complete cloud system. The proposed system offer result auto-correction that can automatically restore corrupted data processing results that are produced by malevolent attackers with superior results that are produced by benign service providers. The system put forward realistic service integrity attestation system that does not imagine trustworthy entities on third-party service. To make a distinction of service integrity attack as well as pinpoint malicious service contributor, our algorithm depends on replay-based consistency check to obtain consistency/ inconsistency relationships among providers of service.

REFERENCES

[1] L.Alchaal, V.Roca, and M.Habert,"Managing and Securing Web Services with VPNs," Proc.IEEE Int'l Conf.Web Services, pp. 236- 243, June 2004.
[2] H. Zhang, M.Savoie, S.Campbell, S.Figuerola, G.von Bochmann, and B.S.Arnaud,"Service-Oriented Virtual Private Networks for Grid Applications, "Proc. IEEE Int'l Conf. Web Services, pp. 944-951, July 2007.
[3] M. Burnside and A.D. Keromytis, "F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services," Proc. 12th Int'l Conf. Information Security (ISC), pp. 491-506, 2009.
[4] J.L. Griffin, T. Jaeger, R. Perez, and R. Sailer, "Trusted Virtual Domains: Toward Secure Distributed Services," Proc. First Workshop Hot Topics in System Dependability, June 2005.
[5] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.
[6] T. Ho et al., "Byzantine Modification Detection in Multicast Networks Using Randomized Network Coding," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2004.

BIOGRAPHIES

MR. RAJESHWAR RAO KODIPAKA (ISTE, CSI LIFE MEMBER), Working as Asst. Professor, in Department of CSE in MallaReddy Engineering College (Autonomous), Hyderabad. He has vast experience in teaching. His research includes data mining; Cloud computing, Software Engineering and Computer networks.

M. AMARENDHAR REDDY is presently associated with B. V. Raju Institute of Technology (UGC - Autonomous), Narsapur, Medak (Dist), Telangana State as Asst. Professor in Information technology Department with 10 years of rich experience in Teaching, Administration and Research in the area of Object Oriented Modeling, Software Engineering Data Warehousing & Mining and Programming Languages.

B VENKATA RAMUDU is working as Asst. Professor Malla Reddy Engineering College (Autonomous), Hyderabad. His research interests in Computer Networks, Cryptography and security.

DOI 10.17148/IJARCCE.2015.41039