IJRRECS/March 2015/Volume-3/Issue-3/3836-3840 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MAINTENANCE OF MULTITENANT CLOUD STRUCTURE BY RELIABILITY ATTESTATION SYSTEM

Juwairia Tahniath[1], Akheel Mohammed[2]

[1]M.Tech Student, Dept of CSE, VIF College of Engg & Tech, Moinabad, R.R Dist, T.S, India

[2]Associate Professor, Dept of CSE, VIF College of Engg & Tech, Moinabad, R.R Dist, T.S, India

ABSTRACT:

Infrastructures of cloud computing are shared by application service providers from dissimilar security domains, which make them susceptible to malevolent attacks. Our work spotlights on services of data processing which have turn out to be more and more accepted with applications in numerous real-world usage domains. In our work we put forward IntTest, which is an efficient framework of service integrity attestation for Software-as-a-service clouds and provides a new integrated attestation scheme of graph analysis that can make available stronger attacker pinpointing power than earlier schemes. In extensive multitenant cloud scheme, numerous malevolent attackers may possibly commence colluding attacks on convinced targeted service utility to cancel the supposition. To tackle challenge, IntTest takes a holistic method by methodically examining constancy as well as inconsistency associations among dissimilar service providers in complete cloud system. Specified software-as-a-service cloud system, the objective of IntTest is to identify any malevolent service provider that put forward an untruthful service utility. IntTest can automatically improve result excellence by means of replacing extreme results produced by malevolent attackers with superior results produced by providers of benign service. IntTest treats the entire service components as black boxes, which does not necessitate any particular hardware or protected kernel support on cloud proposal.

Keywords: IntTest, Software-as-a-service, Multitenant cloud, Service providers, Kernel support.

1. INTRODUCTION:

Software-as-a-service clouds build upon concepts of service-oriented architecture which facilitate application service providers to distribute their applications by means of enormous cloud infrastructure [1]. Even though earlier work has offered a variety of software integrity attestation solutions those methods often necessitate extraordinary trusted hardware which makes them tricky to be deployed on extensive cloud infrastructures. Infrastructures of cloud computing are shared by application service providers from dissimilar security domains, which make them susceptible to malevolent attacks. Intention of our work is focused on attacks of service integrity that cause user to obtain misleading data processing consequences as shown in fig1. Although privacy as well as confidentiality protection exertions have been expansively studied by earlier research problem of service integrity attestation has not been appropriately tackled [2]. Service integrity is the majority of prevalent trouble, which desires to be, addressed no issue whether public or else private data are practiced by cloud system. In our work we put forward

IntTest, which is an efficient framework of service integrity attestation for Software-as-a-service clouds and provides a new integrated attestation scheme of graph analysis that can make available stronger attacker pinpointing power than earlier schemes. IntTest treats the entire service components as black boxes, which does not necessitate any particular hardware or protected kernel support on cloud proposal. IntTest is scalable and decrease attestation transparency by more than one order of extent evaluated to conventional full-time mainstream voting system and can automatically improve result excellence by means of replacing extreme results produced by malevolent attackers with superior results produced by providers of benign service.

2. METHODOLOGY:

Specified software-as-a-service cloud system, the objective of IntTest is to identify any malevolent service provider that put forward an untruthful service utility. Our work spotlights on services of data processing which have turn out to be more and more accepted with applications in numerous real-world usage domains. In an extensive Software-as-a-service clouds cloud, the similar service function can be provided by dissimilar application service providers. IntTest construct upon our

preceding work RunTest as well as AdapTest but can make available stronger malevolent attacker pinpointing control than RunTest in addition to AdapTest. RunText along with AdapTest as well as conventional majority voting methods need to believe that benign service contributor take mainstream in each service utility [4]. In extensive multitenant cloud scheme, numerous malevolent attackers may possibly commence colluding attacks on convinced targeted service utility to cancel the supposition. To tackle challenge, IntTest takes a holistic method by methodically examining constancy as well as inconsistency associations among dissimilar service providers in complete cloud system. IntTest inspect per-function constancy graphs as well as global inconsistency graph and can attain additional accurate pinpointing than active schemes in intentionally colluding attacks. IntTest treats the entire service components as black boxes, which does not necessitate any particular hardware or protected kernel support on cloud proposal. IntTest is scalable and decrease attestation transparency by more than one order of extent evaluated to conventional full-time mainstream voting system.

3. AN EFFICIENT FRAMEWORK OF SERVICE INTEGRITY ATTESTATION:

To notice service integrity attack also pinpoint malevolent service providers, our algorithm depends on replay-based constancy check to obtain consistency or inconsistency associations among service providers [3]. The perception behind our approach is that when two service providers differ by each other on processing result of similar input, not less than one of them has to be malicious. For scalability, we put forward randomized probabilistic confirmation, an attestation method that at random replays a subset of input data in support of attestation. For combined data-flow processing services comprising of numerous service hops, every service hop is composed of functionally corresponding service contributor. We make use of consistency graph along with inconsistency graph to combined pairwise attestation consequences for additional analysis. The graphs reveal consistency or inconsistency associations across numerous service providers above a period of instance. Earlier than introducing attestation graphs, we describe constancy links as well as inconsistency links. We subsequently build

consistency graphs in support of each function to confine constancy associations between service providers provisioning similar function. Two service contributors that are reliable for one utility are not unavoidably reliable for an additional function and hence we detain constancy graphs in individual functions. The per-function consistency graph examination can limit extent of damage caused by means of colluding attackers, whereas comprehensive inconsistency graph analysis can efficiently expose attackers that aim to compromise numerous service functions. IntTest can identify malevolent attackers even if they turn out to be mainstreams for several service functions [5]. By means of taking an integrated advance, IntTest can not only identify attackers more resourcefully but moreover can contain aggressive attackers and limit scope of damage caused by means of colluding attacks. IntTest makes available effect autocorrection that put back corrupted data handing out results produced by malevolent attackers with superior results produced by benign service contributor [6].

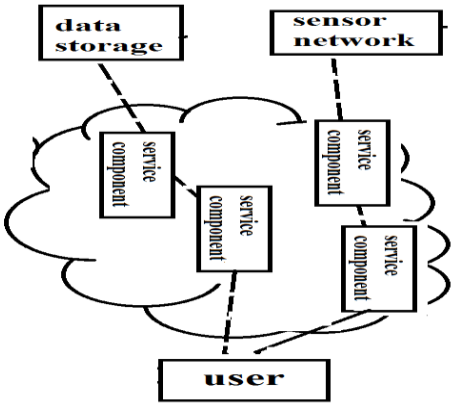

Fig1: An overview of Service integrity attack in cloud system

4. CONCLUSION:

Although privacy as well as confidentiality protection exertions have been expansively studied by earlier research problem of service integrity attestation has not been appropriately tackled. Even though earlier work has offered a variety of software integrity attestation solutions those methods often necessitate extraordinary trusted hardware which makes them tricky to be deployed on extensive cloud infrastructures. In our work we put forward IntTest, which is an efficient framework of service integrity attestation for Software-as-a-service clouds and provides a new integrated attestation scheme of graph analysis that can make available stronger attacker pinpointing power than earlier schemes. Specified software-as-a-service cloud system, the objective of IntTest is to identify any

malevolent service provider that put forward an untruthful service utility. IntTest can automatically improve result excellence by means of replacing extreme results produced by malevolent attackers with superior results produced by providers of benign service. IntTest construct upon our preceding work RunTest as well as AdapTest but can make available stronger malevolent attacker pinpointing control than RunTest in addition to AdapTest. IntTest treats the entire service components as black boxes, which does not necessitate any particular hardware or protected kernel support on cloud proposal. In extensive multitenant cloud scheme, numerous malevolent attackers may possibly commence colluding attacks on convinced targeted service utility to cancel the supposition. IntTest is scalable and decrease attestation transparency by more than one order of extent evaluated to conventional full-time mainstream voting system.

REFERENCES

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You Get Off My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS), 2009.

[2] W. Xu, V.N. Venkatakrishnan, R. Sekar, and I.V. Ramakrishnan, "A Framework for Building Privacy-Conscious Composite Web Services," Proc. IEEE Int'l Conf. Web Services, pp. 655-662, Sept. 2006.

[3] P.C.K. Hung, E. Ferrari, and B. Carminati, "Towards Standardized Web Services Privacy Technologies," IEEE Int'l Conf. Web Services, pp. 174-183, June 2004.

[4] 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.

[5] 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.

[6] 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.