ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Ensuring Security of Cloud System by Strategical Consistent Approach

Dr. CH GVN Prasad
Professor & HoD,
Department of CSE,
Sri Indu College of Engineering and Technology,
Hyderabad, T.S, India.

Nathi Kranthi Kumar
M.Tech Student,
Department of CSE,
Sri Indu College of Engineering and Technology,
Hyderabad, T.S, India.

Abstract:

Software-as-a-service system was based on concepts of software as a service as well as service-oriented structure that permits providers of application service to distribute their applications using cloud services. We study attestation method of service integrity which is a scalable approach offered for software-as-a-service cloud systems. Proposed integrated analysis method identify provider of malicious service offering misleading service function and the method offers realistic service proposal of integrity attestation that does not consider reliable entities on third-party service provisioning sites. It considers holistic system by means of examining consistency and inconsistency relationships between several providers in cloud system. By integrated approach, proposed system locates malevolent attackers and suppresses destructive attackers and limits scope of damage that is caused by colluding attacks. The integrity attestation technique does not require any unique hardware support and enforces minute performance impact to application, which makes it realistic for significant cloud systems.

Keywords: ***Software-as-a-service, Integrity attestation, Holistic system, Third-party service, Service-oriented structure, Cloud system.***

INTRODUCTION:

Cloud computing are shared by the providers of application service from various domains of security, that make them helpless towards malicious attacks. While the issues for protecting privacy were studied by earlier research studies, the problem of service integrity attestation was not been handled properly [1]. Reliability of service is most established trouble that has to be dealt with and may not consider the data that is processed by cloud system. While earlier works offered different solutions for integrity attestation of software, but these methods moreover need particular hardware or else secure kernel support that makes them tricky to be positioned on important cloud services. In our work we focus on the attacks of service integrity that make user to obtain the results of misleading the results of data processing. In our work we make a focus of processing services of data stream that are considered as killer applications for cloud systems.

We provide an attestation method of service integrity which is a scalable approach offered for software-as-a-service cloud systems. Intention of proposed integrated analysis method is to identify provider of malicious service offering misleading service function. The proposed attestation method of service integrity offers new integrated analysis method of attestation graph that offers tough attacker pinpointing power than earlier methods [2][3]. The method offers realistic service proposal of integrity attestation that does not consider reliable entities on third-party service provisioning sites. The integrity attestation technique does not necessitate any unique hardware support and enforces minute performance impact to application, which makes it realistic for important cloud systems. It locates spiteful attackers and moreover suppresses destructive attackers and limits scope of damage that is caused by colluding attacks.

2. METHODOLOGY:

An application service is composed from the elements of individual service that are provided by several providers of application service. These service components occur since service providers might generate elements of replicated service for load balancing purposes; accepted services might catch the attention of various service providers for earnings. We study an attestation method of service integrity which is a scalable approach offered for multiple cloud systems. We spotlight on services of data processing services which are more and more popular with applications in numerous domains. The proposed an attestation method of service integrity was based on earlier RunTest as well as AdapTest but can make available malicious attacker pinpointing control than earlier methods. RunTest as well as AdapTest and established major voting methods need to consider that benign service providers consider the most in each of the service function. Software-as-a-service system due to sharing nature, are susceptible to malevolent attacks however the software-as-a-service cloud differs from other systems by means of having unique features.

Third-party providers of application service do not reveal internal functioning details of software services for securing of intellectual property. Providers of cloud infrastructure as well as third-party service are autonomous entities. For managing of privacy, portal nodes contain comprehensive information regarding service functions that are provided by service providers within software-as-a-service cloud. We focus on the attacks of service integrity that make user to obtain the results of misleading the results of data processing. The attestation method of service integrity offers recent integrated analysis method of attestation graph that offers tough attacker pinpointing power than previous methods [4]. In multitenant cloud systems, several attackers might launch colluding attacks on service functions to invalidate assumption. Integrity attestation method will improve result quality by means of replacing bad results that are produced by malevolent attackers with good results that are produced by providers of benign service. The proposed approach considers holistic system by means of examining consistency and inconsistency relationships between several providers in cloud system. The approach considers per-function consistency graphs as well as global inconsistency graphs. Per-function analysis of consistency graph limits scope of damage that is caused by colluding attackers, while global analysis of inconsistency graph expose those attackers that compromise numerous service functions and hence proposed system locate malicious attackers while they become the majority for a number of service functions.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Software-as-a-service system because of their sharing nature, are susceptible to malevolent attacks. Neither cloud users nor individual providers of application service have knowledge regarding software-as-a-service cloud. We focus on the services of data processing services which are more and more popular with applications in numerous domains. We spotlight on attacks of service integrity that make user to obtain the results of misleading the results of data processing. We study an attestation means of service integrity which is a scalable approach offered for multiple cloud systems. The proposed an attestation method of service integrity was based on earlier methods but can make available malicious attacker pinpointing control than previous methods. By considering of integrated approach, proposed system locates malicious attackers and moreover suppresses destructive attackers and limits scope of damage that is caused by colluding attacks. The attestation method offers novel integrated analysis method of attestation graph that offers tough attacker pinpointing power than earlier methods [5]. The method offers realistic service proposal of integrity attestation that does not consider reliable entities on third- party service provisioning sites and considers holistic system by means of examining consistency and inconsistency relationships between several providers in cloud system. The proposed integrity attestation method offers result auto correction that replace results of corrupted data processing that is produced by malevolent attackers by superior results that are produced by providers of benign service. The integrity attestation technique does not necessitate any unique hardware support and enforces minute performance impact to application, which makes it realistic for important cloud systems. When provided a software-as-a-service system, intention of proposed integrated analysis method is to identify provider of malicious service offering misleading service function [6]. The proposed system considers the entire service components as a black box that does not necessitate any particular hardware support on cloud platform.

4. CONCLUSION:

Software-as-a-service system permits providers of application service for delivering their applications by means of massive cloud infrastructures. In Software-as-a-service cloud, service function is offered by various providers of application service. We spotlight on the attacks of service integrity that make user to obtain the results of misleading the results of data processing. We offer an attestation technique of service integrity which is a scalable approach offered for software-as-a-service cloud systems. The proposed method offers novel integrated analysis method of attestation graph that offers tough attacker pinpointing power than earlier methods. The proposed method was based on earlier methods but can make available malicious attacker pinpointing control than earlier methods. When specified a software-as-a-service system, intention of proposed integrated analysis method is to identify provider of malicious service offering misleading service function. It considers holistic system by means of examining consistency and inconsistency relationships between several providers in cloud system. The technique does not require any exceptional hardware support and enforces minute performance impact to application, which makes it realistic for important cloud systems. The proposed technique offers result auto correction that replace results of corrupted data processing that is produced by malevolent attackers by superior results that are produced by providers of benign service.

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] T. Garfinkel et al., “Terra: A Virtual Machine-Based Platform for Trusted Computing,” Proc. 19th ACM Symp. Operating Systems Principles (SOSP), Oct. 2003.

[5] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla, “Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems,” Proc. 20th ACM Symp. Operating Systems Principles (SOSP), Oct. 2005.

[6] E. Shi, A. Perrig, and L.V. Doorn, “Bind: A Fine-Grained Attestation Service for Secure Distributed Systems,” Proc. IEEE Symp. Security and Privacy, 2005.