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

Achieving Improved Result Quality and Higher Accuracy Using Scalable and Efficient Service Integrity Verification Framework for Saas Clouds

Saleem Sayad
M.Tech Student
Department of Computer Science Engineering,
Rise Krishna Sai Praksam Group of Institutions,
Ongole, Andhra Pradesh.

Pilli Dharmendra Kumar
Associate Professor,
Department of Computer Science Engineering,
Rise Krishna Sai Praksam Group of Institutions,
Ongole, Andhra Pradesh.

Abstract:

SaaS, or Software as a Service, describes any cloud service where consumers are able to access software applications over the internet. The applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organisations. Software-as-a service (SaaS) makes use of a cloud computing infrastructure to deliver their applications to many users regardless of their location. Because of this sharing nature SaaS clouds are vulnerable and provide more opportunities for attackers to exploit the system vulnerability and perform strategic attacks. 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:

Service Integrity Attestation, Cloud Computing, SaaS, Attestation.

Introduction:

Cloud computing is the lease of the resources through which the users can use the resources depending upon the requirement and pay based on the usage. Trough cloud computing the user can decrease the cost and can use the resource at any time.

There are three types of cloud as shown in fig1
i)Public cloud
ii)Private cloud
iii)Hybrid cloud

Public cloud:

Public cloud or external cloud is one in which the resources are leased on self service basis over the internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.

Private cloud:

Private cloud or internal cloud is used to describe the offerings of private network.

Hybrid cloud:

Hybrid cloud is one which contains multiple internal or external clouds. AMES is based on platform as a service. Platform as a service (PaaS) is a category of cloud computing services that provides a computing platform and a solution stack as a service. Along with software as a service (SaaS) and infrastructure as a service (IaaS), it is a service model of cloud computing. In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities.

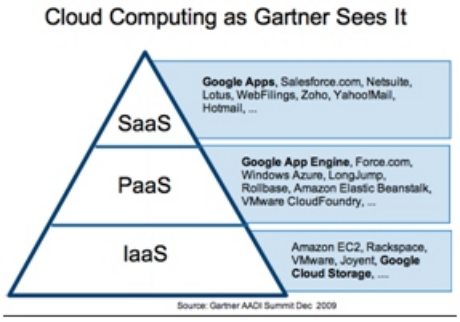


Fig 1 : Types of services

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

Figure 2 shows the architecture of a typical cloud at a high level. An end user Bob connects to the cloud via a portal from his browser. Alternatively, a user Alice can choose to directly connect to the cloud manager via a command line interface similar to that used in EC2. A cloud provides three types of resources: a collection of virtual machine (VM) images, a set of computer servers on which the VM images can be run, and optionally a storage pool to store persistent user data.ASAN is a specialized high speed network of storage devices and switches connected to computer systems. The users will make the request and the cloud manager will authenticate the user and he keep track of the users and their request and due to the streaming techniques and AMoV will adjust the streaming flow with a video coding technique will adjust the flow and increase the quality.ESov monitors the social network interactions.

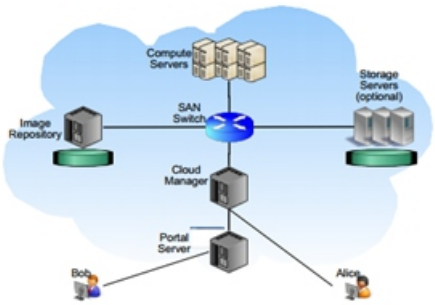


Fig 2:cloud architecture

Google, Twitter, Facebook and Flickr are all examples of SaaS, with users able to access the services via any internet enabled device. Enterprise users are able to use applications for a range of needs, including accounting and invoicing, tracking sales, planning, performance monitoring and communications (including webmail and instant messaging).SaaS is often referred to as software-on-demand and utilising it is akin to renting software rather than buying it.

With traditional software applications you would purchase the software upfront as a package and then install it onto your computer. The software's licence may also limit the number of users and/or devices where the software can be deployed. Software as a Service users, however, subscribe to the software rather than purchase it, usually on a monthly basis. Applications are purchased and used online with files saved in the cloud rather than on individual computers.

There are a number of reasons why SaaS is beneficial to organisations and personal users alike:

1.No additional hardware costs; the processing power required to run the applications is supplied by the cloud provider.
2.No initial setup costs; applications are ready to use once the user subscribes.
3.Pay for what you use; if a piece of software is only needed for a limited period then it is only paid for over that period and subscriptions can usually be halted at any time.
4.Usage is scalable; if a user decides they need more storage or additional services, for example, then they can access these on demand without needing to install new software or hardware.
5.Updates are automated; whenever there is an update it is available online to existing customers, often free of charge. No new software will be required as it often is with other types of applications and the updates will usually be deployed automatically by the cloud provider.
6.Cross device compatibility; SaaS applications can be accessed via any internet enabled device, which makes it ideal for those who use a number of different devices, such as internet enabled phones and tablets, and those who don't always use the same computer.
7.Accessible from any location; rather than being restricted to installations on individual computers, an application can be accessed from anywhere with an internet enabled device.
8.Applications can be customised and whitelabelled; with some software, customisation is available meaning it can be altered to suit the needs and branding of a particular customer.

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

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

benign service providers may include security holes that can be exploited by attackers.

DISADVANTAGES OF EXISTING SYSTEM:

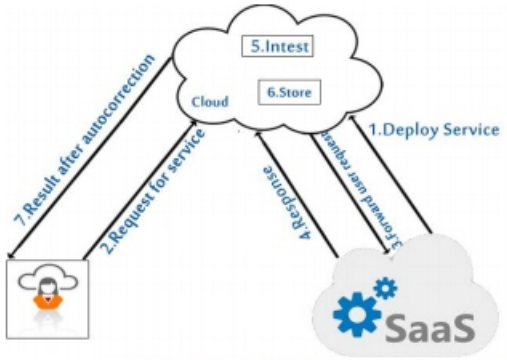
•Those techniques often require special trusted hardware or secure kernel support.
•Which makes them difficult to be deployed on large-scale cloud computing infrastructures.

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.

ADVANTAGES OF PROPOSED SYSTEM:

•A scalable and efficient distributed service integrity attestation framework for largescale cloud computing infrastructures.
•A novel integrated service integrity attestation scheme that can achieve higher pinpointing accuracy than previous techniques.
•A result autocorrection technique that can automatically correct the corrupted results produced by malicious attackers.
•Both analytical study and experimental evaluation to quantify the accuracy and overhead of the integrated service integrity attestation scheme.



Over all architecture of the proposed method

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 perfunction 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.

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.

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

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] 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.

[3] 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.

[4] 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.

[5] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-ofthe-art and Research Challenges," in Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, Apr. 2010.

[6] D. Niu, H. Xu, B. Li, and S. Zhao, "Quality-Assured Cloud Bandwidth Auto-Scaling for Video-on-Demand Applications," in IEEE INFOCOM, 2012.

[7] Z. Huang, C. Mei, L. E. Li, and T. Woo, "CloudStream : Delivering High-Quality Streaming Videos through A Cloud-based SVC Proxy," in IEEE INFOCOM, 2011.

[8] B. Aggarwal, N. Spring, and A. Schulman, "Stratus : EnergyEfficient Mobile Communication using Cloud Support," in ACM SIGCOMM DEMO, 2010.

[9] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing : Architecture , Applications , and Approaches," in Wiley Journal of Wireless Communications and Mobile Computing, Oct. 2011.

[10] Gentry Craig. "A fully homomorphic encryption scheme".Ph.D. thesis, Stanford University; 2009. <http://crypto.stanford.edu/craig/craig-thesis.pdf>[retrieved 21.04.11].

[11] http://en.wikipedia.org/wiki/Software_as_a_service