International Journal of Advanced Technology and Innovative Research

www.ijatir.org

ISSN 2348–2370
Vol.07,Issue.13,
September-2015,
Pages:2597-2602

Scalable and Feasible Data Distribution in SaaS Clouds

J. V. S. R. A. VINDHYA[1], A. VANATHI[2]

[1]PG Scholar, Dept of CSE, Aditya Engineering College, Surampalem, East Godavari(Dt), AP, India,
E-mail: vindhyaswi@gmail.com.

[2]Associate Professor, Dept of CSE, Aditya Engineering College, Surampalem, East Godavari(Dt), AP, India,
E-mail: vanathi.andiran@aec.edu.in.

Abstract: In cloud computing, data is distributed via huge clouds lack of efficiency and security issues will arise .There are many application service provides to deliver their applications in a large group of cloud systems. SaaS However, due to their sharing nature, lack of security issues will arise and there is a chance of malicious attackers to easily attack on certain data service functions. This paper presents, IntTest, a novel effective service integrity attestation scheme it replaces the corrupted results produced by the attackers with good results. It also provides auto correction technique to correct the corrupted data. IntTest needs when popular service function attacks occurs we need to support for time stamp conditions for large scale cloud systems. On production cloud computing infrastructure using IBM system to implement a type of the IntTest model and tested. By the result of this, IntTest achieves higher attack pinpoint accurately than the previous schemes. IntTest did not need specific components and internal structure and also it inflicts an application to be impacted with a small performance, which causes it feasible for large group of cloud systems.

Keywords: Secure Distributed Data Processing, Distributed Service Integrity Attestation.

I. INTRODUCTION

The Cloud Computing is an advanced technology, means that helps users to access data, store the data, programs and applications through Internet instead of utilizing hard drive of a computer. This Cloud computing has greater flexibility and availability at lower cost. The deployment models employed by a cloud computing are the Public Cloud, the Community Cloud, the Private Cloud and the Hybrid Cloud.

Private Cloud: The cloud infrastructure can be managed completely by an organization and can also maintain by a third party or a cloud. It offers increased security because of its private nature.

Public Cloud: A public cloud allows systems and services can be easily access to the common public or a group of industries and also maintain by companies which sells the facilities provided by the cloud.

Community Cloud: It is a multi-tenant infrastructure that can be accessible by the various organizations from a certain group that have to share common concerns.

Hybrid Cloud: This cloud is the combination of private and public clouds. However, the critical and non-critical activities are performed using private cloud and public cloud. There are different types of cloud service providers like Software as a Service, Infrastructure as a Service and Platform as a Service. Let us discuss about SaaS Cloud system. The Software as a Service is a progressively prevailing delivery model for distributing the software, in which software is authorized on a subscription basis and is hosted centrally. SaaS service are suffered from many malicious attacks hence they need security. Below are the various frameworks proposed to provide security.

By taking an integrated approach, IntTest can not only pinpoint attackers more efficiently but also can suppress aggressive attackers and reduces the chance of damage caused by the colluding attacks. Moreover, IntTest provides result auto correction technique that can automatically replace corrupted results of data processing made by the attacker with fine results produce by the trusted service provider. This paper specifies the following contributions:

- In large scale cloud computing infrastructures, it provides an efficient and feasible integrated service distribution attestation framework.
- The effective scheme of IntTest attains pinpointing of an attacker accurately than the earlier approaches.
- We describe an auto correction method, which will automatically correct the corrupting results provided by the malicious attackers.
- We conduct an experimental evaluation and analytical study for quantifying the overhead and accuracy of this integrated service integrity attestation scheme.

II. RELATED STUDY

In recent years many integrity attestation schemes have been developed for software as a service clouds. For example the BIND technique, AdapTest technique, RunTest technique etc. but all of these are having some problems some of them needs secure kernel support and special trusted hardware components. The BIND (Binding Information and Data) technique is a verification method of integrity services that are provided by the software as a service cloud system. It was a fine grained attestation framework and can provide the verification through a secure kernel or by a third party. This technique uses the following steps: 1) attestation annotation mechanism 2) sandbox mechanism 3) verification of authenticator through hash. BIND method uses the Diffee- Hellman key exchange for the purpose of integrity attestation. Another existing technique is TEAS (Timed Executable Agent System) this is used to protect the integrity for cloud computing platform. In this TEAS method, an agent generation and verification algorithm is used.

Another one existing technique is the runtest, it is a scalable runtime integrity attestation framework. It provides a light weight application level attestation method to assure the integrity of data flow processing in cloud. This will identify the untruthful data flow processing and will pinpoint malicious data processing service provider and at last it will detect behavior of the attackers. This RunTest will provide the benign service providers and will determine the malicious behaviour of the attackers. But the disadvantage is its low performance. The AdapTest is another existing technique, it provides a new adaptively runtime data driven service integrity attesting model. This method will radically decrease the attestation overhead and the detection of delay can also shorten. It treats all components as black boxes. It also reduces the attestation overhead and the detection of malicious attackers or service providers will be high when compared to other techniques. All the above methods that are used in the existing papers are having some disadvantages. And to overcome that disadvantages this IntTest is using. And by using this IntTest it will provides more integrity and it will provide more accuracy in pinpointing the malicious attackers and service providers. Also it can provides a result auto correction method and will correct the bad results and replace it with good results.

III. REVIEW OF EXISTING FRAMEWORKS

A. Integrity of Dataflow Processing

This paper proposes Runtest [1] to assure integrity of dataflow processing for multitenant cloud systems.When inconsistent results are detected run test can dynamically verifies the data processing results and also identify the service providers who are malicious in a large group of cloud computing infrastructure by providing application level attestation methods. This proposed scheme of runtest is an effectual and in cloud infrastructure, it exploits a slight performing effect for dataflow processing.

Advantages: Low overhead, cost effective, guaranteed integrity processing, light-weight process application.

Drawbacks: Input deterministic, Presence of Security Loop holes.

B. Privacy Proxy

We are proposing a lightweight and scalable layout. It utilizes the privacy proxy for achieving privacy for a data. This paper [2] also proposes the use of service level agreements (SLA's) for the user benefits. There are two design principles like:

Direct Disclosure: It determines by whom a personal data can be accessed. ii) Minimal disclosure: A strong control for accessing personal data in number of time intervals. Privacy Proxy Service (PPS) was determined as entrusted third party for communication among the composite services and a customer. The PPS important task is temporarily stores the personal data items of customer and also regulates the accessing for that data. This design offers the following properties:

- Each PDI (personal data item) can be store separate.
- Every PDI have to be stored with in a time limit only.
- A unique key is used to identify any PDI, later it is refer as a ticket.
- Tickets are not linkable. There are three interaction phases: Negotiation, Storage and Retrieval. During storage phase, PDI can be stored in PPS by the customer and for each PDI, a ticket also return. In retrieval phase, the services that are related to business can communicate through PPS only (no interaction of intermediary service).However this design did not prevent the services from colluding.

Advantages: Scalable, light weight, uses SLA's, transparent, no need to modify existing service and underlying infrastructure, less impact on overall performance.

Drawback: Doesn't prevent service from colluding hence cannot keep the overhead at minimal. SLA negotiations are not dynamic.

C. Placement and Extraction method for Exploring Information Leakage

This paper [3] aims at the practicability of rising cross VM attacks in existed third party computing clouds. There are two main steps while considering the attacks they are placement, extraction. A Placement refers the arrangement of placing their malignant virtual machine on the identical physical machine similarly to target the customer. The word Extraction refers to extract the secret information through a cross VM attack. This mainly occurs because of sharing physical resources. Here there are two kinds of attackers being considered – first is those who are casting a vast net and have interest to attack on some well-known hosting service and second is those who have focus to attack on a certain targeted service. Amazon's Elastic Compute Cloud (EC2) service is taken as example here. Network Probing can be used in the EC2 system to better understand the VM placement and a hard-disk-based covert channel can also be used between the instances of EC2 to achieve the coresident or determining coresidence. Brute force placement is the technique that is being used earlier, later this was replaced by the new one that assumes a attacker may create instances comparatively early when after the setting up a target victim. Then an attacker can engage within the instance flooding that possibly runs lot of instances parallel in the proper availability zone with appropriate type. Another kind of attack is cryptographic cross-VM attacks. But these kinds of attacks are very difficult to realize. Co-residence detection can also detected by analysing variations in the load because of publicly available service that runs on the target.

Advantages: It helps to determine where an instance is located in the cloud infrastructure and also uses the Binding techniques to minimize the information leakage.

Drawbacks: Methods used for inhibiting side channel attack has two drawback-high overhead, nonstandard hardware, application specific and are not sufficient for mitigating risk, keystroke attacking can be applied only when attackers and victim shares the same core.

D. Stateful Dataflow Processing Services

This paper [4] proposes a framework, Robust Service Integrity Attestation (ROSIA). In large-scale cloud system, it can efficiently pinpoint the malicious service and also verifies integrity for stateful processing services of dataflow. ROSIA support stateful dataflow Services and hence achieves robustness. This framework performs integrity attestation thru examine the relationship between the consistent and inconsistent. It also attains higher attacker detections with accurateness, also reduce the chances of damages initiated by malicious attackers. This proposes two of the methods for attesting the stateful functions. One of the methods is indirect state recovery, this depends on replayed order of historical data input in some way to get the existed state. Another method is difference check, it derives consistent relationship among two stateful service components to compare the variation in the result produced by two consecutive data inputs. The basic idea behind this is Replay-based Consistency Check.

Advantage: This framework supports both the stateful and stateless service functions and imposes low overhead.

Drawbacks: The service providers who are malicious can escape from the detection and try a clique formation in Per function consistency graph.

E. Integrity Protection

This paper [5] propose a Software based integrity verification is through Timed Executable Agent Systems(TEAS).TEAS typically consists of pieces of computer code an agent designed to run on a client whose integrity is being ascertained. Since the client will be asked to execute code unknown to it, the agent must be signed by sending host to signify that it comes from a trusted entity up on receipt of a TEAS agent, the client must execute it immediately and return any results. Data integrity in cloud system is a challenge issue and to produce services towards users with in the time is also a difficult issue.

Advantages: The implementation of integrity of computing platform using time executable agent systems. This works on integrity of data protection in both offline and online services.

Drawbacks: Data integrity in cloud system is a challenging issue and to produce services towards users with in the time is also a difficult.

IV. PROPOSED METHODOLOGY

The basic concepts of SaaS clouds are the service oriented architecture and software as a service. This will allow the service providers of application to distribute the applications in an infrastructure of cloud computing. In the proposed method, we are introducing a new concept called IntTest. The main goal of IntTest is, it pinpoint all the malicious service providers. IntTest will treat all service providers as the black boxes. This doesn't 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 definite malicious attacker. In this, let us imagine that the malign nodes are not having any knowledge about the other nodes except those which they are directly interacting. In this proposed system we are making some assumptions. First of all we are assuming that the number of service components is less than the total number of benign service providers in the entire cloud. This assumptions is very important because without this assumption, it would be difficult for any attack detecting scheme to work successfully. The second assumption is the data processing services are deterministically important. It means, for a similar input that is given by a benign service component will always produce the same output. And finally we assume that the inconsistency caused by hardware or software faults can be excluded from malicious attacks. The following figure shows the overall architecture of the proposed system. In this the user give request to cloud the service will be deployed in the cloud the cloud will forward the user request to the SaaS and the response will be send to the cloud by the SaaS. And then the IntTest process will be done. After that the result auto correction will be done. After that the result will be send to the user by the cloud. The architecture shows this IntTest module in detail shown in Fig.1.

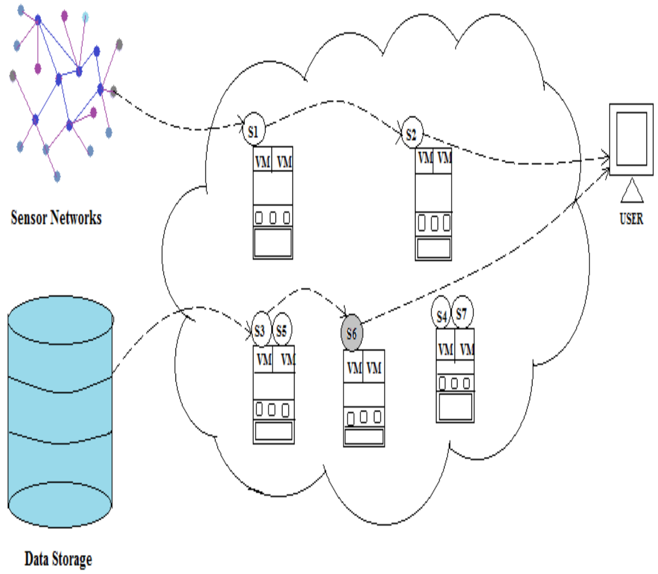


Fig.1. Service Integrity in Cloud.

V. MODULES

In this section we present the main modules in the proposed system shown in Fig.3. Mainly it consists of three modules that are described below.

A. Baseline Attestation Scheme

IntTest is used to detect the service integrity attack and pinpoint the malicious service providers. For that first we have to derive the consistency and inconsistency relationship between service providers. Consider the following fig.2 it shows the consistency check method. In that p1, p2 and p3 are the service providers. All of them offer 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.

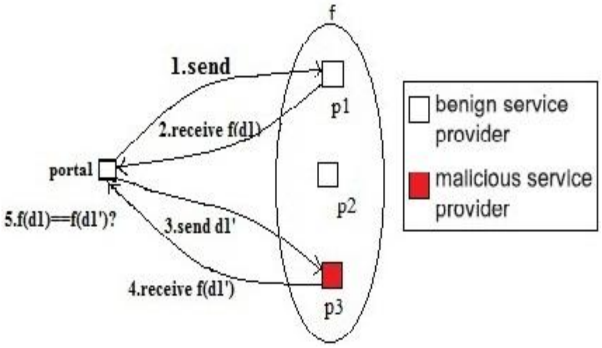


Fig.2. consistency check.

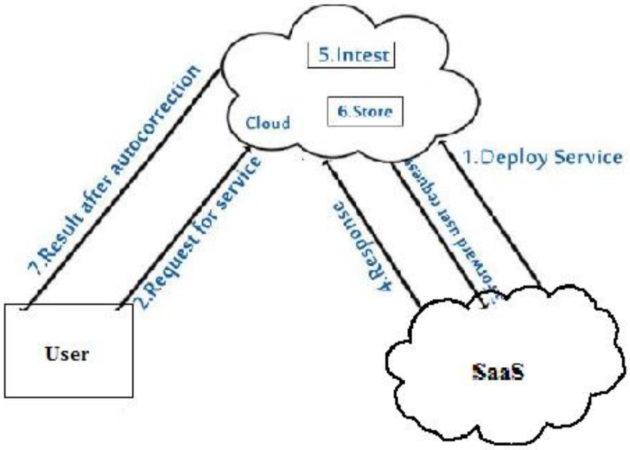


Fig.3. overall new proposed method.

B. 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 trusted service providers will always keep consistent with each other and will have to form a clique in terms of consistent links. The colluding attackers can try to escape from being detected. Then next we must examine the per-function in consistency graph too.

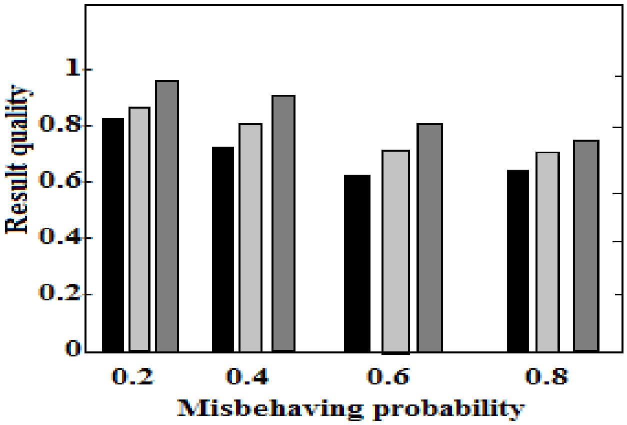
Step 2: Inconsistency analysis: This inconsistency graph will contain only the inconsistency links, this may exist in different possible combinations of the benign node and the malicious node set. First we have to suppose that in the cloud system, the malignant service providers are not to be more that of 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.

C. Result Auto Correction for Attacks

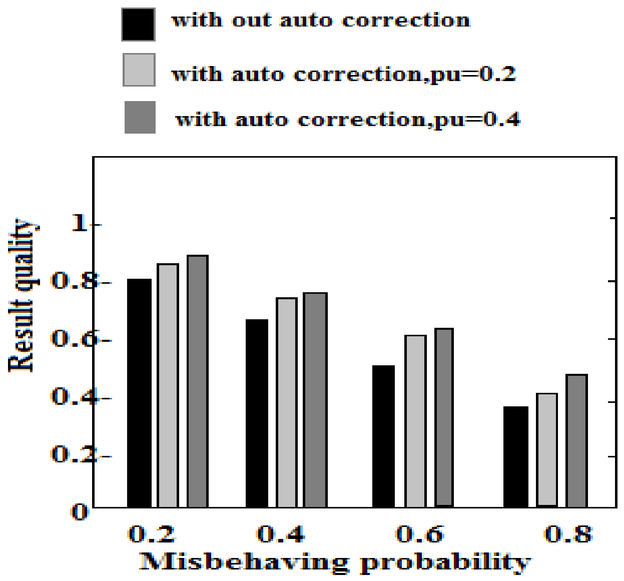
IntTest can not only pinpoint malicious service providers but also it will autocorrect the corrupted data processing results with good results to improve the result quality of the cloud data processing service. Without our attestation scheme, once if an original data input is changed by any malicious 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. 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.

VI. RESULTS

In this paper, IntTest will achieve shorter detection time and delay time for detecting the malicious nodes and replace the corrupted results with good data result. IntTest will detect those attackers that only misbehave in service functions where they can take



(a) 20% non-colloding attackers



(b) 40% colluding attackers

Fig.4. Result quality detection and auto correction performance under non colluding attacks and colluding attackers.

We can compare the result quality without auto-correction and with auto-correction and also investigate the impact of the attestation probability. The fig.4a and 4b shows the result quality under non-colluding attacks with 20 percent malicious nodes and colluding attacks with 40 percent malicious nodes, respectively.

VII. ENHANCEMENT

Firstly, before making any transaction in cloud the user should authenticate independently to provide security by this only, the authorized user can able to access data. For this, the cloud will maintains the sensor modules which allow the authorized users to upload and download the data files without any occurrence of malicious attacks to the server.

VIII. CONCLUSION

A novel effective integrated service integrity attestation graph analysis scheme is presented for multitenant software-as-a-service cloud system. IntTest uses a replay based consistent check for verifying 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. A wide survey of the different frameworks for providing security to SaaS has been carried out and pointed out their advantages and drawbacks. We need to further improve those frameworks or develop some efficient novel methods.

IX. FUTURE WORK

In future the efficiency, reliability and accuracy of the cloud system will be increase through the implementation of the NaaS (Network as a Service) service model that can incorporates the modern offers provide by the cloud computing for accessing the network infrastructures more securely by the tenants. Furthermore, tenants can efficiently execute advanced network services, such as redundancy removal and smart caching.

X. REFERENCES

[1] Juan Du, Wei Wei, Xiaohui Gu, and Ting Yu, “Runtest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures,” Proc. ACM Symp. Information, Computer and Communication Security (ASIACCS), 2010.

[2] Zhendong Ma, Jurgen Manglery, Christian Wagner, Thomas Bleier Austrian Institute of Technology, “Enhance Data Privacy In Service Compositions Through A Privacy Proxy”, Proc. Sixth Int’l Conf. Availability, Reliability and Security, Pages 615-620, 2011.

[3] Thomas Ristenpart Eran Tromer Hovav Shacham Stefan Savage, ”Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds” Proc. ACM conference on Computer and communications security,2009.

[4] Juan Du, Xiaohui Gu, Ting Yu, ”On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems”, Proc. ACM Conf. Computer and Communications Security (CCS), pp. 672-674, 2010.

[5] Juan Garay and Lorenz Huelsbergen, “Software Integrity Protection Using Timed Executable Agents,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2006.

[6] Wei Xu, V.N.Venkatakrishnan, R.Sekar and I.V.Ramakrishnan, Department of Computer Science,”A Framework for Building Privacy-Conscious Composite Web Services”, International conference on web services, pp.655-662, Sept.2006.

[7] Juan Du, NidhiShah and Xiaohui Gu, “Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems,” Proc. International Workshop Quality of Service (IWQOS), 2011.

[8] Juan Du, Daniel J. Dean, Yongmin Tan, Xiaohui Gu and Ting Yu, ”Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds”, Proc.IEEE Transactions On Parallel And Distributed Systems, vol.25, no.3, march 2014.

[9] S.Berger, Caceres, K.Goldman, D.Pendarakis, ”Security for the cloud infrastructure: Trusted virtual data center implementation”, proc. IBM Journal of Research and Development archive, Volume 53 Issue 4, July 2009 , Pages 560-571.

[10] X.Gu et al.,“QoS-Assured Service Composition in Managed Service Overlay Networks,” Proc. 23rd international Conf. Distributed Computing Systems (ICDCS ’03), pp. 194-202, 2003.

[11] L. Alchaal, V.Roca and M. Habert, “Managing and Securing Web Services with VPNs,” Proc. IEEE Int’l Conf. Web Services, pp. June 2004.

[12] H Zhang, M Savoie, S Campbell, S Figuerola, “Service-Oriented Virtual Private Networks for Grid Applications,” Proc. IEEE Int’l Conf. Web Services, pp. 944-951, July 2007.

[13] Gargi Joshi,Dr.D.Y.Patil,"Anomaly Extraction and Mitigation using Efficient-Web Miner Algorithm",proc. International Journal of Computer Applications ,Volume 100– No.2, August 2014.

[14] 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.

Author's Profile:

Mrs. A.Vanathi, Received her B.E in CSE from Bharadhidasan University, Trichy, T.N, India and M.E., in CSE from Anna University Chennai, TN, India. She is currently Pursuing Ph.D in Acharya Nagarjuna University, Guntur. She was a lecturer, Assistant Professor and currently working as an Associate professor and Head Of the Department CSE, Aditya Engineering College, Surampalem, AP, India. Her research interests include Information Security and Mobile Computing. She is a Lifetime Member of CSI and ISTE.

J.V.S.R.A.Vindhya obtained B.Tech Degree in Information Technology in Lenora EngineeringCollege, Affiliated to Jawaharlal Nehru Technological University Kakinada in the year 2011 and pursuing M.Tech Degree in Computer Science Engineering in Aditya Engineering College, Affiliated to Jawaharlal Nehru Technological University Kakinada, India.