International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Reputation Attacks Detection for Effective Trust Management in Cloud Environment

G. Kowselya, T. Aravind

Muthayammal Engineering College, Rasipuram, Rasipuram, Tamil Nadu, India

ABSTRACT

Cloud Services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service .model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

Keywords : CloudArmor, Trust Management, Attacks Detection, Cloud Services Introduces, Cloud Computing

I. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud Computing ,as a new technology paradigm with promising further, is becoming more and more popular nowadays. It can provide users with unlimited computing resource. Enterprises and people can outsource time-consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. In recent years, outsourcing computation has attracted much attention and been researched widely.

It has been considered in many applications including scientific computation, linear algebraic computations, linear programming computations and modular exponentiation computations. Besides, cloud computing can also provide users with unlimited storage resource. Cloud storage is universally viewed as one of the most important services of cloud computing.

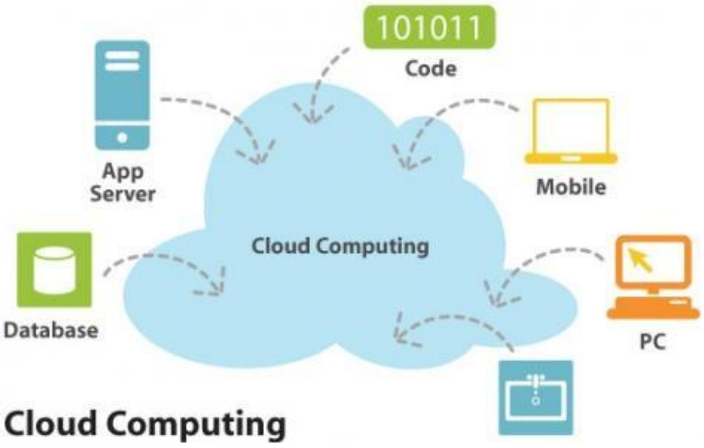

Figure 1. Cloud Computing Architecture

Although cloud storage provides great benefit to users, it brings new security challenging problems shown in fig 1.1. In recent years, many auditing protocols for cloud storage have been proposed to deal with this problem. These protocols focus on different aspects of cloud storage auditing such as the high efficiency, the privacy protection of data, the privacy protection of identities, dynamic data operations, the data sharing.

CSEIT1722290 | Received : 10 April 2017 | Accepted : 20 April 2017 | March-April-2017 [(2)2: 884-887]

1.2 CLOUD COMPONENTS

A Cloud system consists of 3 major components such as clients, datacenter, and distributed servers. Each element has a definite purpose and plays a specific role.

1.2.1 Clients

End users interact with the clients to manage information related to the cloud. Clients generally fall into three categories.

- **Mobile:** Windows Mobile Smartphone, smartphones, like a Blackberry, or an iPhone.
- **Thin:** They don't do any computation work. They only display the information. Servers do all the works for them. Thin clients don't have any internal memory.
- **Thick:** These use different browsers like IE or Mozilla Firefox or Google Chrome to connect to the Internet cloud.

Now-a-days thin clients are more popular as compared to other clients because of their low price, security, low consumption of power, less noise, easily replaceable and repairable etc.

1.2.2 Datacenter

Datacenter is a collection of servers hosting different applications. An end user connects to the datacenter to subscribe different applications. A datacenter may exist at a large distance from the clients. Now-a-days a concept called virtualization is used to install software that allows multiple instances of virtual server applications.

1.3 TYPES OF CLOUDS

Based on the domain or environment in which clouds are used, clouds can be divided into 3 categories:

- **Public Cloud :** A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space. Eg: online photo storage services, e-mail services, or social networking sites.
- **Private Cloud:** In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party.
- **Hybrid Cloud :** In a hybrid cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider. A hybrid cloud is a combination of different methods of resource pooling (for example, combining public and community clouds).

1.4 CLOUD SERVICE PROVIDER

Choosing a cloud provider each provider serves a specific function, giving users more or less control over their cloud depending on the type. When you choose a provider, compare your needs to the cloud services available. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider.

II. LITERATURE REVIEW

2.1. Privacy, Security And Trust Issues Arising From Cloud Computing

AUTHORS : S. Pearson and A. Benameur

Cloud computing is an emerging paradigm for large scale infrastructures. It has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on the budgeting of IT budgeting but also affect traditional security, trust and privacy mechanisms. Many of these mechanisms are no longer adequate, but need to be rethought to fit this new paradigm. Assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.

2.1.1 TRUST ISSUE

The speed and flexibility of adjustment to vendor offerings, which benefits business and motivates cloud computing uptake, brings a higher risk to data privacy and security. This is a key user concern, particularly for financial and health data, and the associated lack of trust can be a key business inhibitor for cloud computing in domains where confidential or sensitive information is involved. Since customers lack control of cloud resources, they are not in a good position to utilize technical mechanisms in order to protect their data against unauthorized access or secondary usage or other forms of misuse. Instead, they must rely on contracts or other trust mechanisms to try to encourage appropriate usage.

2.1.2 Lack of Customer Trust

When it is not clear to individuals why their personal information is requested, or how and by whom it will be processed, this lack of control and lack of visibility of the provider supply chain will lead to suspicion and ultimately distrust. There are also security-related concerns about whether data in the cloud will be adequately protected. As a result, customers may hold back from using cloud services where personally identifiable information is involved, without an understanding of the obligations involved and the compliance risks faced, and assurance that potential suppliers will address such risks. This is particularly the case where sensitive information is involved, for example financial and healthcare information.

2.1.3 Weak Trust Relationships

Trust relationships at any point in the cloud service delivery chain may be weak, but exist in order that a service can be provided quickly. Significant business risk may be introduced in a way that is not transparent when a cloud transaction is initiated, due to loss of control in passing sensitive data to other organizations and the globalised nature of cloud infrastructure. Organizations that contract out key business processes may not even know that contractors are sub-contracting, or even if they do, contract requirements regarding data protection measures may not be propagated down the contracting chain.

2.2 Trust Mechanisms For Cloud Computing AUTHORS: J. Huang and D. M. Nicol

Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. The paper with a survey of existing mechanisms for establishing trust, and comment on their limitations. The address those limitations by proposing more rigorous mechanisms based on evidence, attribute certification, and validation, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the cloud.

2.2.1 Reputation Based Trust

Trust and reputation are related, but different. Basically, trust is between two entities; but the reputation of an entity is the aggregated opinion of a community towards that entity. Usually, an entity that has high reputation is trusted by many entities in that community; an entity, who needs to make trust judgment on an trustee, may use the reputation to calculate or estimate the trust level of that trustee.

3.2 PROPOSED SYSTEM

The Proposed design and the implementation of Cloud Armor (Cloud consumers credibility Assessment & trust management of cloud services): A framework for reputation-based trust management in cloud environments. In Cloud Armor, trust is delivered as a service (TaaS) where TMS spans several distributed nodes to manage feedbacks in a decentralized way.

3.2.1 Advantages

- Easy to finding the attacks (collusion and Sybil attacks).
- Store data in multiple clouds

3.3. SYSTEM REQUIREMENTS

3.3.1 Hardware Requirements

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 14' Colour Monitor.
Mouse	: Optical Mouse.
Ram	: 512 Mb.
Keyboard	: 101 Keyboards.

3.3.2 Software Requirements

Operating system	: Windows XP.
Coding Language	: ASP.Net with C# 2010
Data Base	: SQL Server 2008.

III. CONCLUSIONS AND FUTURE WORK

The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors. There are a few directions for our future work. To combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

IV. REFERENCES

[1]. S. M. Khan and K. W. Hamlen, “Hatman: Intra-Cloud Trust Management for Hadoop,” in Proc. CLOUD’12, 2012.

[2]. S. Pearson, “Privacy, Security and Trust in Cloud Computing,” in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.

[3]. J. Huang and D. M. Nicol, “Trust Mechanisms for Cloud Computing,” Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

[4]. K. Hwang and D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” IEEE Internet Computing, vol. 14,no. 5, pp. 14–22, 2010.

[5]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwin- ski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Communications of the ACM, vol. 53,no. 4, pp. 50–58, 2010.

[6]. S. Habib, S. Ries, and M. Muhlhauser, “Towards a Trust Man- agement System for Cloud Computing,” in Proc. of TrustCom’11, 2011.

[7]. I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, “Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds,” in Proc. of CLOUD’10, 2010.

[8]. W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrst- edt, “A Trust Management Framework for Service-Oriented Environments,” in Proc. of WWW’09, 2009.

[9]. T. H. Noor, Q. Z. Sheng, and A. Alfazi, “Reputation Attacks Detection for Effective Trust Assessment of Cloud Services,” in Proc. of TrustCom’13, 2013.

[10]. T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “Trust Management of Services in Cloud Environments: Obstacles and Solutions,” ACM Computing Surveys, vol. 46, no. 1, pp. 12:1 - 12:30, 2013.