International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Brief Survey on Cloud Security Risk Assessment for Autonomous Agents Security Issues

S. Shanmugapriya[1], R. Ramya[2]
[1]*PG Scholar, Dept. of Computer Science & Engineering, A.V.C. College of Engineering, Mayiladuthurai, India*
[2]*Assistant Professor, Dept. of Computer Science & Engg., A.V.C. College of Engineering, Mayiladuthurai, India*

***Abstract*: Cloud computing is introducing many huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications. Cloud federations allow Cloud Service Providers (CSPs) to deliver more efficient service performance by interconnecting their Cloud environments and sharing their resources. However, the security of the federated Cloud service could be compromised if the resources are shared with relatively insecure and unreliable CSPs. A federation formation algorithm that enables CSPs to cooperate while considering the security risk introduced to their infrastructures, and refrain from cooperating with undesirable CSPs. According to the stability-based solution concepts that use to evaluate the game, the model shows that CSPs will be able to form acceptable federations on the fly to service incoming resource provisioning requests whenever requires.**

***Keywords*: Cloud Computing, Cloud Consumers, Cloud Federations, Cloud Service Providers, Unreliable CSP, Stability based Solution.**

1. Introduction

The Cloud Computing paradigm advocates centralized control over resources in interconnected data centers under the administration of a single service provider. This approach offers economic benefits due to supply-side economies of scale, reduced variance of resource utilization by demand aggregation, as well as reduced IT management cost per user due to multi-tenancy architecture [1].

These benefits have contributed to the increasing industry acceptance of Cloud services, which are seen as more affordable and reliable alternatives compared to traditional in house IT systems and services. However, downsides of the Cloud Computing paradigm are surfacing. Surveys show that potential customers hesitate to outsource their business applications and data into the cloud [2]. Besides security concerns, application users are afraid of losing ownership and control. The lack of standardized service interfaces, protocols and data formats is a portent of vendor lock-in [3].

This problem can lead to underinvestment, an economically inefficient situation, and therefore deserves our attention. We suggest the concept of Cloud Federation to enable the design of flexible and interoperable Cloud-based software, thereby lowering the adverse effects of vendor lock-in. We further discuss Cloud Federation as a key concept allowing the development of new types of applications.

2. Literature survey

A. A novel intrusion severity analysis approach for Clouds

Junaid Arshad (2013) proposed that cloud computing presents exciting opportunities to foster research for scientific communities; virtual machine technology has a profound role in this. Among other benefits, virtual machine technology enables Clouds to offer large scale and flexible computing infrastructures that are available on demand to address the diverse requirements of scientific research.

However, Clouds introduce novel security challenges which need to be addressed to facilitate widespread adoption. This paper is focused on one such challenge intrusion severity analysis. In particular, we highlight the significance of intrusion severity analysis for the overall security of Clouds. Additionally, we present a novel method to address this challenge in accordance with the specific requirements of Clouds for intrusion severity analysis. We also present rigorous evaluation to assess the effectiveness and feasibility of the proposed method to address this challenge for Clouds.

B. A Review on Reactive Security in Cloud Computing

Manisha Yadav, Suman Aggarwal (2016) proposed that the use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un-trusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.

A movement towards "multi-clouds", or in other words,

"inter-clouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions.

It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

As a matter of fact, we can understand that in any resource we have less threat from invasion rather more threat from inside. Consequently, the focus of this project is to demonstrate the reactive or passive measure of security in cloud computing ensuring that the trusted resource can share the data/communication even they are under the umbrella.

C. An Overview of the Security Concerns in Enterprise Cloud Computing

Anthony Bisong1 and Syed (Shawon) M. Rahman (2011) proposed that Deploying cloud computing in an enterprise infrastructure bring significant security concerns. Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. We believe enterprise should analyze the company/organization security risks, threats, and available countermeasures before adopting this technology.

In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management.

D. Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption

Aderemi A. Atayero, Oluwaseyi Feyisetan (2011) proposed that the prominence of the place of cloud computing in future converged networks is incontestable. This is due to the obvious advantages of the cloud as a medium of storage with ubiquity of access platforms and minimal hardware requirements on the user end. Secure delivery of data to and from the cloud is however a serious issue that needs to be addressed.

We present in this paper the security issues affecting cloud computing and propose the use of homomorphic encryption as a panacea for dealing with these serious security concerns vis-à-vis the access to cloud data.

E. Trust in the Cloud

Imad M. Abbadi, Andrew Martin (2011) proposed that Cloud infrastructure is expected to be able to support Internet scale critical applications (e.g. hospital systems and smart grid systems). Critical infrastructure services and organizations alike will not outsource their critical applications to a public Cloud without strong assurances that their requirements will be enforced. Central to this concern is that the user should be provided with evidence of the trustworthiness of the elements of the Cloud. Establishing Cloud's trust model is important but the Cloud's infrastructure complexity and dynamism makes it difficult to address. Establishing trust in the Cloud is one of the key objectives of the EU funded TClouds (Trustworthy Clouds) project. In Clouds we focus on building trust models that provide various levels of transparency in the context of technical complexities and trust establishment. These trust models are not only beneficial to a Cloud's users, but also to Cloud providers, collaborating Clouds-of-Clouds, and external auditors. In this paper we explore this problem, and summarize some of the recent results from the TClouds project in context of trust establishment.

F. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility

Rajkumar Buyya (2009) proposed that with the significant advances in Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community.

To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Hence, in this paper, we define Cloud computing and provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). We also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation.

In addition, we reveal our early thoughts on interconnecting Clouds for dynamically creating global Cloud exchanges and markets. Then, we present some representative Cloud platforms, especially those developed in industries, along with our current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology. Furthermore, we highlight the difference between High Performance Computing (HPC) workload and Internet-based services workload.

We also describe a metanegotiation infrastructure to establish global Cloud exchanges and markets, and illustrate a case study of harnessing `Storage Clouds' for high performance content delivery. Finally, we conclude with the need for convergence of competing IT paradigms to deliver our 21st century vision.

G. The Cloud Grid approach: Security analysis and performance evaluation

Valentina Casola (2013) proposed that both cloud and grid are computing paradigms that manage large sets of distributed resources, and the scientific community would benefit from

their convergence. This paper proposes a novel computing model, cloud grid, able to achieve full cloud and grid integration.

After presenting its three-layer architecture, the security issues involved are analyzed, proposing a solution based on fine-grained access control mechanisms and identity federation that allows cooperation and interoperability among untrusted cloud resources. The overhead introduced by the multiple-layer architecture and by the security system are measured by extensive testing on a prototype implementation, and a trade-off analysis between security and performance is presented.

H. Virtual machine provisioning through satellite communications in federated Cloud environments

Antonio Celesti (2012) proposed that Cloud federation offers plenty of new services and business opportunities. However, many advanced services cannot be implemented in the real Cloud market due to several issues that have not been overcome yet. One of these concerns is the transfer of huge amount of data among federated Clouds. This paper aims to overcome such a limitation proposing an approach based on satellite communications. By comparing performance in data delivery on the Internet and satellite systems, it is evident that satellite technologies are enough ripe to be competitive against systems with a wired infrastructure.

Thus, we propose to make use of satellite transmission to implement fast delivery of huge amount of data. Through the discussion of a use case, where a WEB TV company offers a streaming service, we show how to practically apply the proposed strategy in a real scenario, specifying the involvement of Cloud providers, Cloud users, satellite companies and end-user clients.

I. Study on the security models and strategies of cloud computing

Jianhua Che, Yamin Duan (2011) proposed that Cloud computing is introducing many huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications.

In this paper, to facilitate customers to understand the security status quo of cloud computing and contribute some efforts to improving the security level of cloud computing, we surveyed the existing popular security models of cloud computing, e.g. multiple-tenancy model, risk accumulation model, cube model of cloud computing, and summarized the main security risks of cloud computing deriving from different organizations. Finally, we gave some security strategies from the perspective of construction, operation and security incident response to relieve the common security issues of cloud computing.

J. Data Security and Privacy Protection Issues in Cloud Computing

Deyan Chen, Hong Zhao (2012) proposed that it is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud.

The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remains the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.

3. Proposed system

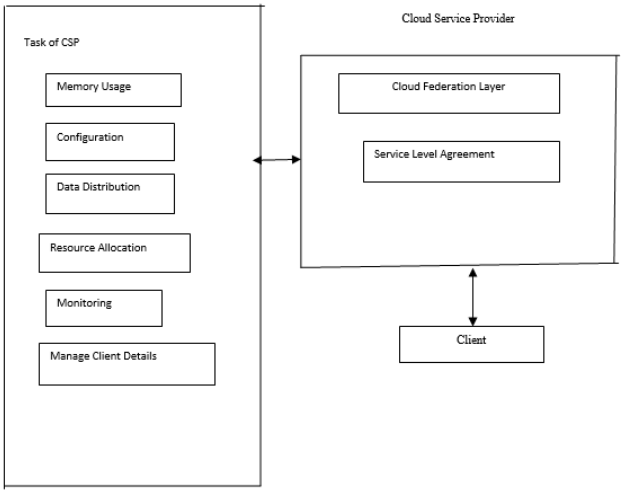

Fig. 1. System Architecture

Cloud federation comprises services from different providers aggregated in a single pool supporting three basic interoperability features - resource migration, resource redundancy and combination of complementary resources resp. services. Migration allows the relocation of resources, such as virtual machine images, data items, source code, etc. from one service domain to another domain. While redundancy allows concurrent usage of similar service features in different domains, combination of complementary resources and services allows combining different types to aggregated services.

Service disaggregation is closely linked to Cloud Federation as federation eases and advocates the modularization of services in order to provide a more efficient and flexible overall system. The security risk that a CSP can introduce to the federation when joining its members was not considered in the previous federation formation models.

The security risk level of the federation members should be efficiently assessed before the formation of the federation. The formation of Cloud federations represents a decision making situation that can be mathematically modeled as a combinatorial optimization problem.

4. Conclusion

The process of collecting real information about CSPs' security risk levels to complete the evaluation of the performance of the proposed model based on a real data. This model enables CSPs to form federations in each other, and refrain from joining undesirable federations where they either do not trust their members, or they feel that their security risk levels are unacceptable. Cloud Federation is a concept, which has a large potential and might have an enormous influence on the way computing resources and applications will be handled, developed and used. It is a further step of providing computing resources in a utility-services-like way, similar to other services, e.g., electricity or water. However, the evolution of Cloud Computing and related concepts and technologies is extremely dynamic and it is very difficult to make long-term prognoses. We believe anyhow, that this article can be a substantial contribution to future works on Cloud Federation.

5. Future enhancement

This review could serve as a theoretical basis for future research, showcasing the current major security issues as well as theoretical solutions. Future research should focus on practical case studies in order to validate the theoretical solutions discussed and presented in this review. Aside from this more research should be done in order to better understand the attitudes of cloud computing consumers as well as cloud service providers when it comes to security. Finally, future research should strive to better understand the way the different deployment methods and service models affect the overall security of a system.

References

[1] Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114.
[2] Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
[3] Arshad, J, Townsend, P. and Xu, J. (2013). A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428.
[4] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
[5] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45.
[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.
[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401.
[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93.
[9] Che, J. Duan, Y, Zhang, T. and Fan, J, Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593.
[10] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651.