Airo International Research Journal
Volume XII, ISSN: 2320-3714
August, 2017
Impact Factor 0.75 to 3.19

ज्ञान-विज्ञान विमुक्तये
UGC Approval Number 63012

A STUDY OF CLOUD RISK AND GOVERNANCE FRAMEWORK

Diwakar Ramanuj Tripathi
Research Scholar Kalinga
University Dr.Rupak Sharma
Asst. Prof.

ABSTRACT

The development of collaborative business process relies mostly on software services spanning multiple organizations. Therefore, uncertainty related to the shared assets and risks of Intellectual Property infringement form major concerns and hamper the development of inter-enterprise collaboration. This paper proposes a governance framework to enhance trust and assurance in such collaborative context, coping with the impacts of Cloud infrastructure. First, a collaborative security requirement engineering approach analyzes assets sharing relations in business process, to identify risks and uncertainties and, therefore, elicits partners' security requirements and profiles. Then, a 'due usage' aware policy model supports negotiation between asset provider's requirements and consumer's profiles. The enforcement mechanism adapts to dynamic business processes and Cloud infrastructures to provide end-to-end protection on shared assets.

KEYWORDS: End-to-end security, governance, framework, policy, risk and uncertainty, collaborative business process.

INTRODUCTION

With the development of knowledge and service economy, enterprises focus more on their core business while building business federation strategy to provide a better service for their clients. Accordingly, corporate Information Systems are developing toward collaborative paradigm, using different software components. This allows new opportunities for business development, taking advantage of new computing paradigm as Service Oriented Architecture and Cloud Computing. These phenomena suggest a collaborative IT-based service ecosystem trend, where enterprises use the dynamic organization offered by service composition to set flexible business processes and enhance enterprise assets value.

Nevertheless, security risks and uncertainty related to the intellectual property due to shared assets are seen as a major challenge for enterprises to participate incollaborative business process [1]. Security engineering in such complex and dynamic collaborative contexts should offer end-to-end security governance concerning partners' shared assets value. This involves a multi-layered viewpoint ranging from security requirements engineering phase to security configuration and enforcement phases, paying attention to the challenges of interoperability and virtualization which stem from collaborative IT infrastructure.Security engineering in a collaborative context is a multi-folded task among business process model and analysis, risks assessment and management,

collaborative authorization and virtualization-aware security auditing. After presenting the IS context and risk analysis and management methods, we focus on the implementation level, paying attention to security policy and to cloud security particular models.

SECURITY GOVERNANCE FRAMEWORK FOR CLOUD COMPUTING

During the last few years, both organisations and individuals have started paying attention to the explosive growth and adoption of cloud computing services. This new paradigm encompasses access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort [1]. Users may benefit from the flexibility and elasticity of on-demand cloud services, especially at present when economic restrictions require IT departments to achieve more objectives with less resources. When these kinds of services are aligned with well-defined strategic initiatives and objectives, they make valuable contributions to an enterprise [2]. However, the many benefits provided by cloud computing are also accompanied by the appearance of new risks [3], in addition to the continued presence of all the security issues that may affect its underlying technologies [4]. The independence of the cloud service delivery model signifies that security management is necessary if its adoption is to be fostered [5]. Cloud computing extends computing resources across the corporate perimeter, resulting in control being lost over its information assets. A security governance function therefore needs to be established for the managementlevels, with a clear security strategy [6]. Regardless of the cloud model adopted, security and governance must lead and guide the adoption of cloud services [7]. Security policies and measures involve a third party when moving services to cloud computing, and this loss of control emphasizes the need for security governance within the enterprise and for the transparency of cloud providers [8, 9]. Security governance, as part of the company's corporate governance, is the most suitable path by which to gain control of security processes and guarantee an alignment with business strategies [10].

An Information Security Governance (ISG) framework that tackles all the security issues in the cloud environment in a uniform manner is not currently available. Although there are many technological approaches that can improve cloud security, there are currently no comprehensive solutions [11]. Our previous research shows that existing efforts that attempt to deal with cloud computing security do not detail the governance aspects. In this paper we therefore propose a first approach to a security governance framework that considers the particularities of cloud deployments (ISGcloud). The ISGcloud framework compiles existing published guidance works on the field, and groups them homogeneously to provide a model that is capable of delivering an ISG process for the cloud services. ISGcloud is led by standards, resulting in an alignment with actual best practices. With the use of standards we aim to increase the quality and reliability of the results and simplify the governance process while guaranteeing the security of the cloud service and promoting the reuse of resources. The perspective followed in our approach is process oriented, thus facilitating its inclusion in any organisation. In order to deploy security governance, we have chosen the model published in the ISO/IEC 38500 standard, which states that directors should perform governance

by using three main processes: Evaluate Direct and Monitor. The Evaluate-Direct-Monitor cycle will therefore become a core process of our framework. We also propose the addition of a fourth process, namely Communicate, owing to the relevance of disseminating security knowledge within the organisation, particularly as regards the adoption of new services such as those of cloud computing. In addition to the four core processes highlighted, we consider that it is paramount to identify a cloud service lifecycle as part of our objective of defining an ISG deployment. The relationship between the cloud client and its provider, as with any other outsourcing service, leads to new risks throughout its lifecycle phases that must be managed in order to guarantee the service's success. The ISO/IEC 27036 standard despite being in its draft stage outlines security controls to be addressed in an outsourcing lifecycle. We have adapted this standard to a generic cloud computing lifecycle in order to identify the steps in the processes.

NEW CLOUD GOVERNANCE FRAMEWORK

The changes being driven by Cloud Computing and the growing sophistication of attackers do represent new challenges. We solve these challenges by creating the Cloud Governance Framework to control people, data, applications and infrastructure. Our security framework provides a more integrated, intelligent approach to Cloud Governance. An intelligent framework must improve itself continuously; it has to have a feedback and service improvement process. We develop a new framework with five stages to achieve this goal (Figure 1). It also solves the weakness of organization strategy alignment. The stages are:

- Strategic trigger
- Define and align
- Build and implement
- Deliver and measure
- Operate and feedback

Strategic trigger is the first stage. It is the event that initiates the need to use the Cloud computing.

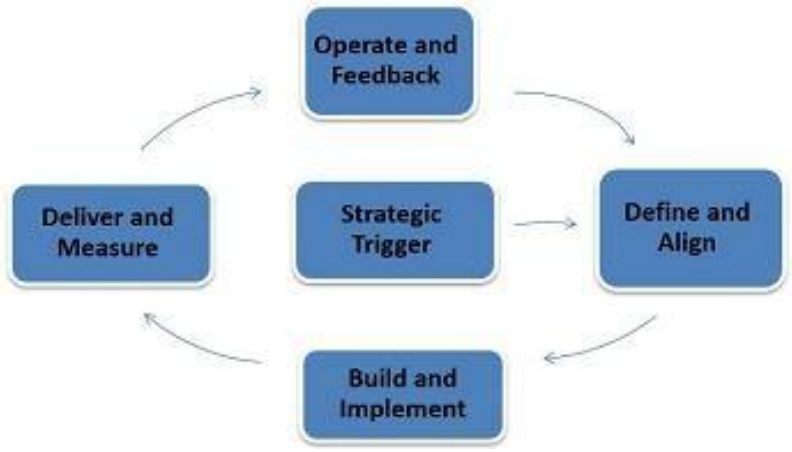

Figure 1: New Cloud Governance Framework

Business need is the main trigger for using the Cloud services. Other trigger may be gaining market share due to strong competition in market. The company needs a competitive edge. We use Cloud services to comply with a standard or a government rule. The major trigger is the technical need. An SP delivering services needs technically a Cloud service; for example, E-mail services. This stage contains four processes. Business process management policy defines interrelations between Cloud-based services. It analyses the business and considers the service process reuse. Service discovery finds and discovers the existing services and available technologies for new services. Capacity planning reviews the existing environment and future business extensions to plan the best way technically and financially to achieve business goals. Exit policy is mandatory. Business needs changes to cope with the market. It may require ending the Cloud service. Exit the Cloud service is more complicated than joining and entering it. A well-defined plan is mandatory before starting to use Cloud service. Define and align stage is the planning phase of adopting the Cloud service or transforming the existing environment to the Cloud. It ensures that the Cloud services are aligned to the business needs and actively supports them. Organizations using a Cloud require their service to be successful. If processes and services are implemented, managed and supported in the right way, the business will be more successful. This means cost reduction, revenue increase, and achieving its business objectives. It is the most important phase helping the decision makers with the economic and technical preparations for Cloud services.

This stage contains six Processes. Data Policy defines data's physical and logical model, in addition to data performance and stability. Service policy builds a service dictionary. It analyses theintegration and separation of the service based on deployment model. Policy management determines and reviews the service policy. Moreover, it reviews the violation and solves the policy conflicts in order to prevent further problems. Risk management defines risks when moving to the Cloud. It plans a mitigation process and determines residual risks. Risk plan has to be reviewed with the organization and provider policies. Jurisdiction is an important process. Law and regulations vary from country to another. Organizations must review country laws where data is to be stored and processed. Integration is a mandatory process if you have an existing infrastructure. It plans the integration between the existing environment and the Cloud service.Build and implement stage covers issues related to people, processes and infrastructure technology. It ensures cost-effective and the high quality provision of Cloud service necessary to meet business needs. The blurred lines between the traditional technology and Cloud services management means that an updated approach to managing Cloud implementation is needed. This stage contains eight processes. Authentication determines the authentication mechanism that will be used in the Cloud and between organization systems and Cloud. Authorization is the level of access that will be granted to users from the organization side and from the provider side as well. Metadata repository is the storage of policy. It considers the location of polices and roles. Asset management monitors and maintains things of value to an organization. It manages the logical and physical assets and even human assets. Configuration management and

documentation establishes and maintains performance, functional and physical attributes. It also establishes and maintains configurations within Cloud service throughout its life. Roles and responsibility is a dictionary, which determines the roles and the responsibility of each contributor in the Cloud service. Privacy considers the data encryption and the location privacy. Access takes care of the access policy in the Cloud because of using shared resources.

CONCLUSION

A Cloud system has different deployment models and architecture. Although it offers an economy of scale solution to the market, it creates new risks andchallenges in the IT environment. In this paper, we introduce our new Cloud Computing governance model that represents a perspective combination of theoretical and practical implementation. We identify the gap using CCM, and then identify controls related to each process and its effect using CCM. We add, modify and update the missing corners in the model. We create a new governance framework. It is a five stages framework with a service feedback. Each stage has few processes. Each process contains controls. Each control has inputs, outputs, and tools to activate and measure it. The framework is suitable for all Cloud deployment models. Our security governance framework aims at providing comprehensively management on the business operations of organizations in a collaborative process, helping them to clearly identify the risks of intellectual property infringement when their business value flows through the whole virtual-enterprise architecture. In sum, designed in a layered and modular way, our framework could be used in a wide range of industrial inter-organizational business contexts, giving enterprises more grasp ofthe risks related to the assets they provide, promoting the successes of business federation.

REFERENCES

[1]. Linda, B. B., Richard, C., Kristin, L., Ric, T., Mark, E.:The evolving role of IT managers and CIOs–findings from the 2010 IBM global IT risk study. Technical report, IBM (2010)

[2]. Su, Z., Biennier, F.: An architecture for implementing 'collaborative usage control' policy - toward end-to-end security management in collaborative computing. In: ICEIS2012, (submitted).

[3]. Hug, C., Front, A., Rieu, D., Henderson-Sellers, B.: A method to build information systems engineering process metamodels. J. Syst. Software. 82(10), pp. 1730 – 1742 (2009)

[4]. Ducq, Y., Chen, D., Vallespir, B.: Interoperability in enterprise modelling: requirements and roadmap. Adv. Eng. Inf. 18(4), pp. 193 – 203. (2004)

[5]. Su, Z., Biennier, F.: Toward comprehensive security policy governance in collaborative enterprise. In: APMS 2011, IFIP WG5.7 (2011)

[6]. Maamar, Z., Benslimane, D., Thiran, P., Ghedira, C., Dustdar, S., Sattanathan, S.: Towards a context-based multi-type policy approach for web services composition. Data & Knowledge Engineering. 62(2), pp. 327 – 351. (2007)

[7]. Su, Z., Biennier, F.: A collaborative-context oriented policy model for usage-control in business federation. In: 2011 IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering.pp.201 – 204. (2011).

[8]. Bussard, L., Neven, G., Preiss, F.-S.: Downstream usage control. In: Proc. 11th IEEE International Symposium on Policies for Distributed Systems and Networks. pp. 22–29, IEEE Computer Society, Washington (2010)

[9]. Ma, C., Lu, G., Qiu, J.: An authorization model for collaborative access control. Journal of Zhejiang University - Science C. 11(9), pp. 699–717. (2010)

[10]. Wilson, P.: Positive perspectives on cloud security. Information Security Technical Report. 16(3-4), pp. 97 – 101. Elsevier (2011)

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification / Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/ Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Diwakar Ramanuj Tripathi