Future Generation Computer Systems 57 (2016) 24–41

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Cloud computing adoption framework: A security framework for business clouds

Victor Chang [a,*], Yen-Hung Kuo [b,*], Muthu Ramachandran [a]

[a] School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK
[b] Data Analytics Technology & Applications, Institute for Information Industry, Taiwan, ROC

HIGHLIGHTS

- We demonstrate CCAF multi-layered security.
- We explain the mappings between CCAF multi-layered architecture and core technologies
- We performed penetration testing and SQL injection on CCAF multi-layered security.
- Results and analysis by CCAF are better than those produced by the other tools.
- CCAF multi-layered security blends with policy, services and business activities.

ARTICLE INFO

Article history:
Received 11 July 2015
Received in revised form
9 September 2015
Accepted 27 September 2015
Available online 19 October 2015

Keywords:
Cloud computing adoption framework (CCAF)
OpenStack
CCAF multi-layered security
Security for business clouds

ABSTRACT

This article presents a cloud computing adoption framework (CCAF) security suitable for business clouds. CCAF multilayered security is based on the development and integration of three major security technologies: firewall, identity management, and encryption based on the development of enterprise file sync and share technologies. This article presents the vision, related works, and views on security framework. Core technologies have been explained in detail, and experiments were designed to demonstrate the robustness of the CCAF multilayered security. In penetration testing, CCAF multilayered security could detect and block 99.95% viruses and trojans, and could achieve $\geq$85% of blocking for 100 h of continuous attack. Detection and blocking took $<$0.012 s/trojan or virus. A full CCAF multilayered security protection could block all SQL (structured query language) injection, providing real protection to data. CCAF multilayered security did not report any false alarm. All F-measures for CCAF test results were $\geq$99.75%. The mechanism of blending of CCAF multilayered security with policy, real services, and business activities has been illustrated. Research contributions have been justified and CCAF multilayered security can be beneficial for volume, velocity, and veracity of big data services operated in the cloud.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Security, trust, and privacy always remain challenges for organizations that adopt cloud computing and big data. Although there are demands for businesses to move their data to the cloud and centralize management for data centers, services and applications are designed to reduce cost and increase operational efficiency. System design and deployment based on current security practices should be simultaneously enforced to ensure compliance of all data and services with up-to-date patches and policies. A risk-based approach to the development of a security program that recognizes (and funds) appropriate controls will ensure protection of all users and confidentiality, integrity, and availability of data.

Some researchers have adopted a framework approach that allows organizations to follow guidelines, policies, and standards. For example, Zhang et al. [1] propose a usage-based security framework (UBSF), which can consolidate guidelines and policies with their framework, architecture, and digital certificates. Takabi et al. [2] describe a comprehensive security framework via a model that explains the method of working with different service integrators and service providers. Zia and Zomaya [3] present a wireless sensor network model with algorithms and a software engineering approach. All these frameworks have recommendations

[*] Corresponding authors.
E-mail addresses: V.I.Chang@leedsbeckett.ac.uk (V. Chang), keh@iii.org.tw (Y.-H. Kuo).

http://dx.doi.org/10.1016/j.future.2015.09.031
0167-739X/© 2015 Elsevier B.V. All rights reserved.

on guidelines to use. However, there are no details on the actual use of these proposals and also no clear evidence of adoption of these proposals to business clouds, whose requirements include ease of use, adaptability, best practice compliant, and support by large-scale experiments such as penetration testing to validate robustness of such proposals [4,5]. Indeed, without such a clear ''line of sight'' between conception and implementation, such frameworks are unlikely to achieve operational status.

The cloud computing adoption framework (CCAF) has been developed to meet the requirements of business clouds and ensure that all implementations and service deliveries overcome all the technical challenges. Real-life case studies show how different cloud computing designs and their development and service delivery overcome both technical and organizational challenges. In the first example, CCAF was the framework used to develop cloud storage and bioinformatics solutions for biomedical scientists based in the United Kingdom at Guy's Hospital and King's College London [6]. This framework ensured the deliveries of storage services to back up thousands of terabyte-sized medical data. Bioinformatics services can simulate DNAs, proteins, genes, tumors, and organs of the human body. The use of this security is limited to authentication, encryption, and users with authorized access. In the second example, CCAF is used to provide guidelines for financial modeling, so that the best practice and call prices can be computed with respect to the change of risks. Advanced computational techniques have been used to calculate risks and market volatility [7]. Security is limited to password authentication and users with authorized access and biometrics checks for financial simulations. In the third example, investigations of hacking methods have been studied and made as part of prototype requirements. User requirement and literature review have identified factors for a successful implementation. All the collected and synthesized data have been instrumental in the development of CCAF Version 1.1, which emphasizes on the security policies, recommendations, techniques, and technologies to be updated in the framework [8]. In the aforementioned examples, a more comprehensive cloud security solution is required to ensure robustness and resistance of the services to attack, hacking, and unauthorized attempts to gain access. More experiments and simulations are required to validate the robustness and effectiveness of the proposed security framework. This motivates us to consolidate our CCAF framework by providing a holistic approach involved with service integration, OpenStack security, and multilayered security to enhance security for business clouds. An integrated security framework is proposed for business clouds to have the multilayered security in place and the large-scale penetration testing and experiments to validate the robustness and effectiveness of our approach. All these proofs of concepts and lessons learned are important to big data in the cloud as follows. First, it ensures that all the cloud services are safe and secure, including the incoming and outgoing data of the organizational data centers hosted on hundreds and thousands of virtual machines (VMs). Second, it ensures that large amount of data and large data sets can be processed and analyzed safely in the cloud, which also explains the necessity of large-scale penetration testing to validate the framework.

The organization of this article is as follows: Section 2 presents the literature for security. Section 3 describes our core security technology for enterprise file sync and share (EFSS), including the architecture and layered components. Section 4 explains the multilayered approach with core technologies and results from large-scale experiments for penetration testing, SQL (structured query language) injection, and data scanning. Section 5 illustrates topics of discussion, and Section 6 summarizes conclusion and future work.

2. Literature

The following are the different types of security frameworks proposed so far. Zhang et al. [1] propose their UBSF for collaborative computing systems. They explain their motivation, techniques used, architecture, and conditions for experiments. The decision on the use of UBSF is made based on subjects, objects, authorization, obligations, and conditions. With support from literature and hypotheses, they explain their model's mechanism of work in collaborative ways. The usage-based authorization architecture uses sensors, directory service, policy decision point (PDP), and usage monitor (UM) to functions. Steps have been described to justify the effective function of UBSF. In order to assist UBSF, Zhang et al. [1] include a prototype system architecture. They use OpenLDAP and OpenSSL to enforce security. They have three types of digital certificates: user, attribute repository (AR), and resource provider (RP). They explain the use of these certificates in their workflow of security processes. They also adopt extensible access control markup language (XACML) to enforce policy specification, which aligns with the UBSF approach for security. Ko et al. [9] investigate trust for cloud computing and propose a TrustCloud framework that focused on accountability. It has three layers: (1) system layer that covers all the underlying hardware and platform; (2) data layer that contains the data for the work; and (3) workflow layer that uses workflow to execute all the services and requests. In addition, two nonfunctional layers are associated with these three layers. The first layer is laws and regulations, which ensures all services follow the legal requirements of the country in which the service was delivered. The second layer is policies, which are the consolidated service-level agreements and the best practice approach. This framework is considered as a conceptual framework focused on the recommendations and best practice, as they do not include quantitative analyses, computational demonstrations, and case studies. Pal et al. [10] present their cloud security that has emphasized on the architecture and steps of interactions between different services. They explain the role of each major user, their agents, and all the 15 steps involved. They use unified modeling language (UML) diagram to justify their approach and architecture to explain the relationship between the user, provider, proxy server, user agent, and provider agent. They present two algorithms and experimental results. They validate their approach using ''trust value updation''. However, their assumption is based on the probabilities of 0.8 and 0.2 of having a trusted and nontrusted user, respectively. There is no evidence supporting this, and they do not use any reference or survey to justify their research. This also depends on the sample size, demographics, and the country in which the research was conducted. The National Institute of Standards and Technology (NIST) [11] framework provides a common language for establishing cybersecurity. The core NIST framework provides a set of activities to identify, protect, detect, respond, and recover without more specific examples and case studies implementing a full-security solution. However, our work on CCAF extends to detailed activities and implementation on security for cloud computing and big data.

All these examples have security framework. However, the proposals described above do not demonstrate their contributions to business clouds. In other words, when businesses adopt cloud computing solution, they should be able to provide architecture, approaches for their framework, and steps and experiments to support the robustness and validity of the framework. Our proposal on CCAF provides details on core technologies in Section 3, and the theoretical framework mapping of core technologies is shown in Section 4 with experimental results validating our framework. Key topics, including security policy, business and security alignment, framework and core technology integration, relation of the big data in cloud, and overall contributions with limitation, are discussed

Download English Version:

https://daneshyari.com/en/article/425163

Download Persian Version:

https://daneshyari.com/article/425163

Daneshyari.com