# Advanced Security Framework Model for Cloud Computing Environment

Hae-Gill Choi [1], Sung-Ho Sim [2]

[1.] Department of Digital Media Engineering, Kyunghee Cyber University. Hoegi-dong, Seoul, 130-701, Korea
[2.] Department of Liberal Education, Semyung University, Korea
[1.] hgchoi@khcu.ac.kr, [2.] shshim@semyung.ac.kr

**Abstract:** Cloud computing technology is a new trend of IT (Information Technology) . In this environment, all users can share their information and experience very easily. However it is hard to keep their own information such as a private data. Actually, cloud computing can be open their data and is difficult to protect the user data from the access or attack to the system. In this paper, we propose security framework model for cloud computing environments. In order to make this framework, we make a structure for each module in 3 layers, PaaS, IaaS and SaaS.

[Kharkwal G, Mehrotra P, Rawat YS. **Taxonomic Diversity of Understorey Vegetation in Kumaun Himalayan Forests**. *Life Sci J* 2017;11(7s):136-139] (ISSN:1097-8135). http://www.lifesciencesite.com. 25

**Keywords:** Security model; Security framework; Cloud computing; Cloud computing environment

## 1. Introduction

Cloud computing is positioning itself as a new and promising platform for delivering information infrastructure and resources as IT services. Customers can then access these services to execute their business jobs in a pay-as-you-go fashion while saving huge capital investment in their own IT infrastructure [1]. The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood, many of the major players will be tempted to holdback [3]. According to a recent IDCI survey, 74% of IT executives and CIO's cited security as the top challenge preventing their adoption of the cloud services model [2]. Customers often have concerns about whether their privacy can be protected when facilitating services in the cloud, since they do not have much control inside the cloud. Correspondingly, privacy protection has become a critical issue and one of most concerning. Without it, customers may eventually lose the confidence in and desire to deploy cloud computing in practice [1]. So some researchers notice that cloud computing should provide key elements of the necessary architectural change to segregate clients from mass data and applications [4]. Examples is, with the emergence of cloud computing, multi-billion dollar organizations like IBM, Amazon, Google and Ebay have already invested in cloud technology. If extortionists threaten to bring down their Cloud System with a Distributed Denial of Service (DDoS) attack, which is for this paper means many nodes systems attacking one node all at the same time with a flood of messages, it is usually better for a corporation to pay the ransom than see their systems go offline (Fowler, 2009). However, it is not only extortionists that can exploit cloud computing. For example, Amazon or Ebay competitors could also use known vulnerabilities to interrupt the normal operations of their cloud system so their customers move onto the next business that can provide them with the service they require. Renting out its sky-high computer infrastructure from Amazon, this actual example happened to the BitBucket.com cloud, who according to the report, went down for 19h. X-DoS and its distributed version, Distributed XML-based DoS (DX-DoS) occurs when an XML message is sent to a Web Server or Web Service with malicious content to use up all their resources. One example of an X-DoS attack is called a Coercive Parsing attack, which manipulates the Web Service Request when a Simple Object Access Protocol (SOAP) is parsed to it so that it can transform the content to make it accessible to applications. The Coercive Parsing attack uses a continuous sequence of open tags so that the CPU usage on an Axis2 web server becomes exhausted [5].

In this paper, we propose advanced security framework model for cloud computing environment. Generally cloud computing technology has 3 main factors, PaaS (Platform as a Services), IaaS (Infrastructure as a Services) and SaaS (Software as a Services). So this framework has 3 layers for them, and each module for security is in 3 layers.

## 2. Cloud computing environment with security

Cloud computing is attracting more and more users. In addition to the common customers

from industry, researchers out of the scientific fields are also joining the Cloud world. The reason for the success of Cloud computing lies in its easy-to-use computing model and the benefits it brings to the users. We see the following features from Cloud computing [9]:

- Elasticity. Cloud computing provides users with the flexibility in the amount of requested resources, e.g. size of the storage and number of the processors/machines. This feature is rather helpful for scenarios like "Web service operators need to add or remove servers depending on the number of users".
- Economy. In Cloud computing, customers pay only what they used. For small companies or research groups, the cost for using Cloud resources can be much cheaper than investing and maintaining an own local system.
- Reliability. Cloud systems are fault tolerant and the services on them are highly available.
- On-demand. Cloud computing provides users with customized environments that are tailed to individual requirement. This feature is more user friendly than Grid computing where the application has usually to be adapted to the target architecture.

A majority of the cloud computing definitions, including on-demand, pay-by-use model, virtualized and dynamically-scalable, have the characteristics of cloud computing. And it applies novel diverse computing types, such as SaaS (Software as a Service), PaaS (Platform as a Service), utility computing, web services in the cloud, MSP (Managed Service Providers), service commerce platforms, and Internet integration. Furthermore, these computing types are based on new payments, new deployments and new updated/maintained mechanisms [6]. Also cloud computing offers the opportunity to store a huge amount of data relatively cheaply. Using the cloud, users can access the services or applications regardless of their location or computing device/platform they use. However, despite all these benefits the cloud has to offer, privacy and security issues are still major challenges of cloud computing. There are many security issues to consider, including: fine grained access to cloud resources, privacy protection of data in the cloud, and auditing of cloud operations. Some threat models assume that the cloud provider cannot be trusted, and therefore propose storing only encrypted data in the cloud. Others assume that the cloud provider can be

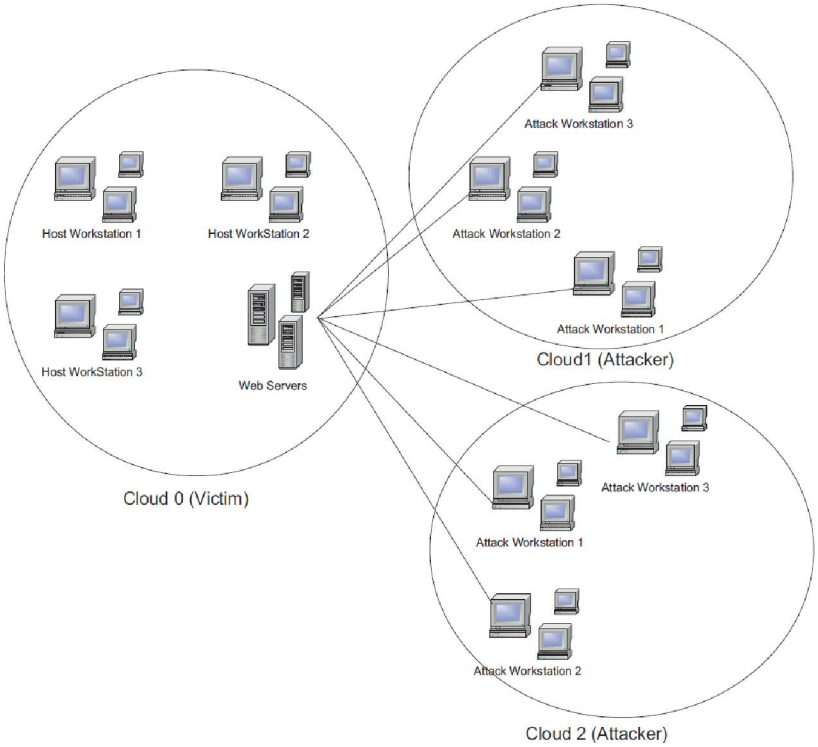


Figure 1. Distributed XML-based Denial of Service attack in cloud environment

trusted, and that the threats come primarily from outside attackers and other cloud users [7]. In ths contents, Imad and Andrew [8] notified three examples as below.

- A Cloud user (that is, the trustor) wants to establish 'trust' in the ability of the trustee (i.e. Cloud infrastructure and Cloud provider) to provide some service S, and to enforce an agreed policy P, when both the trustor and the trustee have behaviour B.
- Similarly, the trustor could be a Cloud provider or a collaborating Clouds-of-Clouds who want to establish 'trust' in the ability of the trustee (the Cloud infrastructure, or the collaborating Cloud provider and its infrastructure) to provide some service S, and to enforce an agreed policy P, when both the Trustor and the Trustee have behaviour B.
- When the trustor is a customer of a Cloud user, and the customer wants to establish 'trust' in the ability of the trustee (i.e. Cloud user resources which are hosted at the Cloud infrastructure) to provide some service S, and to enforce an agreed policy P, when both the Trustor and the Trustee have behaviour B.

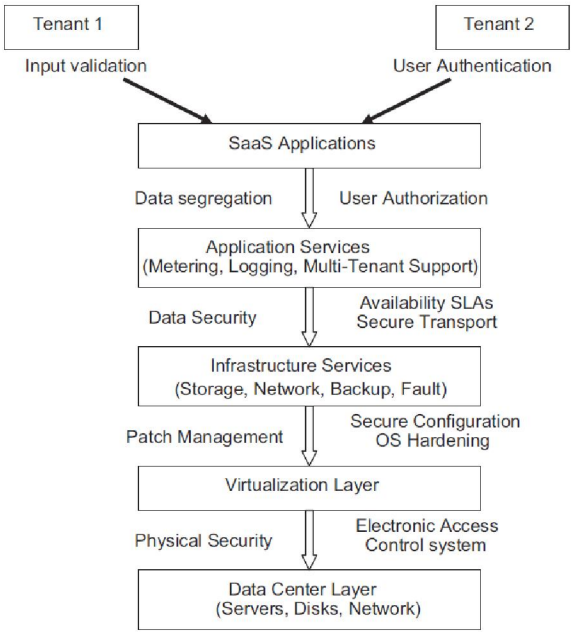


Figure 2. Security workflow for the SaaS by S. Subashini, V. Kavitha [2]

Ashley et al. [5] depicted service attack in cloud computing environment as shown in Figure 1. I the picture shows the attacker uses multiple hosts to attack the victim with X-DoS attacks in Distributed XML based Denial of Service(DX-DoS).

Actually, in side of software has very weak for security and protect from the other access or attack. In SaaS, the client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data. So it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed. With SaaS, the cloud customer will by definition be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration. So, S. Subashini, V. Kavitha [2] proposed Security workflow for the SaaS as shown in Figure 2.

## 3. Security Framework for Cloud Computing

In this contents, we propose advanced security framework for cloud computing environment. Especially we design each module in three layers, SaaS, PaaS, and IaaS. Figure 3 shows proposal structure for security cloud computing by three layers.

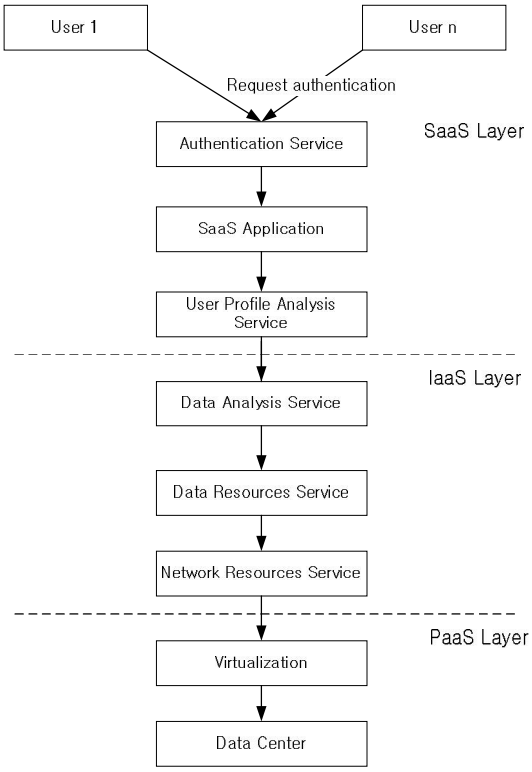


Figure 3. Proposal workflow for security cloud computing

This structure has each service module in three layers as below.

- SaaS Layer
  Authentication Service: Authentication for user login
  SaaS Application: Service application for user authentication.
  User Profile Analysis Service

- IaaS Layer
  Data Analysis Service: Data analysis for user authentication, access to service and their information.
  Data Resources Service: To store and manage user information and authentication data.
  Network Resources Service: To manage network resources.

- PaaS Layer
  Virtualization: System and resources virtualization.
  Data Center: Security data group and mart include big data.

**4. Conclusion**

This paper proposed an advanced security framework model in cloud computing environment. The framework has 3 layers for SaaS, IaaS, and PaaS, and each module for security has in 3 layers. In SaaS Layer, it has Authentication Service for Authentication for user login, SaaS Application for Service application for user authentication, and User Profile Analysis Service. In IaaS Layer, Data Analysis Service for user authentication, access to service and their information, Data Resources Service for store and manage user information and authentication data, and Network Resources Service for manage network resources. In PaaS Layer, Virtualization for System and resources virtualization, and Data Center for Security data group and mart include big data.

We expect this research will contribute next and future cloud computing security model.

4/28/2014

**Corresponding Author:**
Dr. Sung-Ho Sim
Department of Liberal Education,
Semyung University, Korea
E-mail: shshim@semyung.ac.kr

**References**

1. Gaofeng Zhang, Yun Yang, Jinjun Chen, A historical probability based noise generation strategy for privacy protection in cloud computing, Journal of Computer and System Sciences
2. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (2011) 1–11
3. Viega. Cloud computing and the common man. Computer 2009; 42(8): 106–8.
4. P.G. Dorey, A. Leite, Commentary: Cloud computing e A security problem or solution?, (2011), doi:10.1016/j.istr.2011.08.004
5. Ashley Chonk, Yang Xiang, Wanlei Zhou, Alessio Bonti, Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, Journal of Network and Computer Applications, (2010), doi:10.1016/j.jnca.2010.06.004
6. Yishui Zhu, Roman Y. Shtykh, Qun Jin, A human-centric framework for context-aware flowable services in cloud computing environments, (2012), doi:10.1016/j.ins.2012.01.030
7. David W. Chadwick, Kaniz Fatema, A privacy preserving authorisation system for the cloud, Journal of Computer and System Sciences, (2012) doi:10.1016/j.jcss.2011.12.019
8. Imad M. Abbadi, Andrew Martin, Trust in the Cloud, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.006
9. Jie Tao, Holger Marten, An Intuitive Framework for Accessing Computing Clouds, International Conference on Computational Science, ICCS 2011, Procedia Computer Science 4 (2011) 2049–2057.