Self Configuring Security ensuring Trust in Cloud Computing

M Sashi Kumar[#], S Vinay Kumar[#], V Sai Vamsidhar Rao[#]
[#]*Asst. Professor, Dept of CSE, Vasavi College of Engineering*

Abstract

Establishing strong security would often require large IT resource and also result in difficulty of usage. To enhance security while reducing the spending on IT & improving the ease of use, we require a security mechanism which can configure itself, as requested, for services offered in a Cloud environment. The architecture is driven by security policies based on these inputs,

1. *Network access risk.*
2. *Compute Type.*
3. *Security level.*

With these inputs in place, the security policies can generate security parameters which in turn are used to configure mechanisms to alter security (including algorithms and protocols) at every domain for protection of specific security services. This architecture can realize varied security requirements from users and services in cloud computing in turn building trust for the end users via Security at their ease & also data control.

1. Introduction

Cloud computing has been defined by NIST as a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. The term itself is often used today with a range of meanings and interpretations [2]. Three widely referenced service models have evolved:

• **Software-as-a-Service** (SaaS) enables a software deployment model in which one or more applications and the computing resources to run them are provided for use on demand as a turnkey service. It can reduce the total cost of hardware and software development, maintenance, and operations.

• **Platform-as-a-Service** (PaaS) enables a software deployment model in which the computing platform is provided as an on-demand service that applications can be developed upon and deployed. It can reduce the cost and complexity of buying, housing, and managing hardware and software components of the platform.

• **Infrastructure-as-a-Service** (IaaS) enables a software deployment model in which the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be founded.

Cloud computing has been developed by various successful commercial organizations, such as Amazon EC2/S3, Google Apps, and Force.com. Security has been and is the biggest challenge to cloud computing [3]. It is hard for the users to believe in cloud computing due to invisibility of the user's data storage and how are they protected. Research says that as of now there is no way to know if the cloud providers properly purged a client's data, or whether they have saved it for some unidentified reason. Currently, the study on cloud security still lies in the preliminary study. For data storage, a TPA (Third Party Auditor) is proposed to verify the integrity of the dynamic data stored in the cloud. In trust management field, some experts considered that multiple security policies should be used in user's authentication and identity management, and those policies must be able to avoid intrusion of data by unauthorized users [4].

Amazon administrators do not have privilege to access customers' instances and customers' operating systems. If it is necessary for an administrator to access the customers' resource, all such accesses must be logged and routinely audited [4]. However, these researches focus on specific security threats and provide individual security solutions. In fact, various services share the same cloud computing platform and their security requirements are always different. Few of them are services with public information which only needs essential security and few others are services with sensitive information which needs strong security. To the best of my knowledge there are no specific security architectures to satisfy such a varied security requirements.

2. Self Configuring Security Requirements

High Security aspects are often honoured in various services example E-banking; at the same time there are services which can be optional example web search to the users. Security parameters even differ for a specific service for two different users depending on the sensitivity of the information. The solution for these issues can simply be the usage of a highly complicated and secure algorithm popularly used to safeguard all services in the network. Potentially, this might not be effective way for cloud service providers to use the same security mechanism throughout the services since it consumes a lot of IT resources every time. It would not be a solution to consume resources for security itself, as we counteract the advantage of cloud computing platform wasting the available resources.

There are few ways to identify the amount of security strength (a measure for the amount of effort & time spent to break a security algorithm and protocol) like Single factor & Multi factor authentication. Each of them defines the number of passwords, passphrases, RSA SecurID or Biometric Information. It is evident that multifactor authentication is strong when compared to single-factor but reduces the ease of use at the user level and may not lure the customers. Thus, using the highest security strength for all services in cloud computing is not feasible. Therefore, services on cloud computing require self-configuring security solution with automatic adjustment of security strength which means the level of security is identified depending on factors earlier identified: Network access risk, service type. I would propose to achieve a self configuring security architecture which can protect the services in cloud computing with the three security domains at Network Layer, Compute Layer & Storage Layer. This architecture can reduce IT resource consumption on security and increase ease of use for end users.

3. Security Domain

A security domain is the determining factor in the classification of an enclave of servers/computers. A network with a different security domain is kept separate from other networks. A security domain is considered to be an application or collection of applications that all trust a common security token for authentication, authorization or session management. Generally speaking, a security token is issued to a user after the user has actively authenticated with a user ID and password to the security domain. Before we design security architecture for specific network systems, we always need to divide the network and system into several security domains which can simplify the deployment of security solutions based on the architecture. Here, the security domain is a scope statement of security policy which has similar security mechanisms. We can build the security architecture into three security domains and each of them uses the same security policy. Regarding lifecycle of data for an application, it always stays in one of three main statuses: data in network transmission, data in compute platform and data in storage. Every status needs different security mechanisms, i.e., security algorithms and protocols, to protect the data. Since self configuring security depends on differentiated configuration of security mechanisms, and every data status needs a composition of security mechanisms, it is reasonable to design security domains for clouding computing according to the three data statues. Therefore, three security domains are proposed with Network Security Domain, Compute Security Domain and Storage Security Domain.

Figure 1 shows the security domains in cloud computing architecture. Security Policy Administrator is responsible for the management of cloud computing determining which security policy is to be used to give on the fly security. The network security domain refers to the protection where data is in transmission status. Its main threats include fabricating identity, middle attack and types of denial-of-service attacks. Security mechanisms such as encryption, intrusion detection and traffic clean are necessary. For example, secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols and IPSec are often used in this domain.

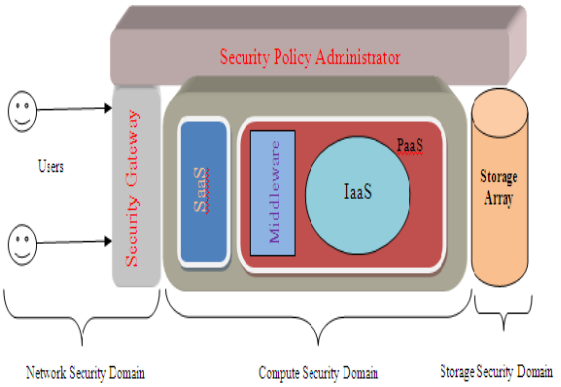

Figure1. Security Policy Administrator

Security Gateway is one of the important entities which mediate all communication to and from system, enabling more refined control through access control mechanism. If it is a malicious (e.g. Distributed Denial of Service (DDos) Attack [5]), Security Gateway can limit or even turn off the communication immediately preventing effectively. If the requirement is legal, connection is established with security protocol (e.g. SSL/IPSec), which is in case of middle attack and information leakage.

The Compute Security Domain means that data are protected in service platform including SaaS, PaaS and IaaS. Its main threats include weak credentials, insecure protocols, application flaws, Default application Configurations, Insecure permissions on Cloud Data, Vulnerabilities in underlying OS services, Remote Management, DNS Implementation flaws respectively. Meanwhile, in order to protect legal services out of illegally control and interruption of process by Hackers, all the actions from users can be monitored by IDS/IPS. System can also use Honeypot technology to capture malicious actions at intervals. In order to avoid virus infection and hijack attack from other users, each user's services supplied by SaaS PaaS and IaaS run in independent sand table environment.

The Storage Security Domain refers to protection of data in storage status. Its main threats include unauthorized access, change or steal of data & legal issues. Security mechanisms such as encryption, access control and integrity are necessary. Sensitive data is encrypted and marked with different access levels. It is also critical important to use backup (e.g. Redundant Array of Independent Disk (RIAD)) and data recovery techniques to protect data. It is still not evident to say the data where the data is saved geographically & in which data center. Security even needs to be dealing with data being saved under the jurisdiction of the government and also needs to confirm that the data is permanently removed from the storage space without leaving a trace of it in the HDD.

4. Security Architecture

The proposed architecture is shown in Figure 2. The architecture is divided into three levels with input layer, policy layer and layer of security mechanism. The input layer has three inputs, i.e., security level, type of service and risk of access network. The policy can further be divided into few layers of policies each of which correspond to the three security domains respectively. The layer of security mechanism represents all the security mechanisms in every security domains. The task of security policy manager is to produce security parameters according to inputs. These security parameters are used to drive security mechanisms to protect specific service. For example, IPSec is used by cloud computing in network security domain. The security parameters of Security Association drive the IPSec to protect data flow in the network security domain.

a) In the input layer, the security level is the application of a computer system to process information with certain sensitivity, permit simultaneous access by users with certain security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization. Normally, to keep the same security level, the higher risk environment of a system needs the stronger security strength of security algorithms. As one of inputs, the security level is always configured by user according to security requirement for specific service from user. There is the minimum security level for every service which is determined by operator of cloud computing. It can guarantee the essential security for all the service in cloud computing. User can only configure security level higher than the minimum security level. He can also neglect the setting and the service is protected by the minimum security level.

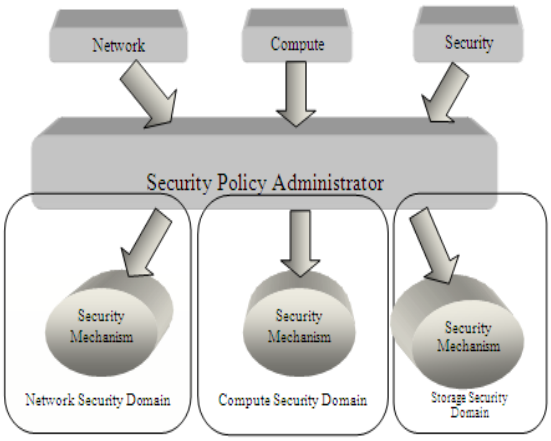

Figure 2. Security Architecture

b) The type of service is necessary because different types of service always need different composition of security mechanisms. For example, multimedia service is sensitive to time delay and allows certain packet loss. Integrity is not required by the type of service. However, if the service is file transmission, the integrity is one of important security mechanisms to protect the service.

c) The risk of access network depends on the network that the terminal accesses. As we know, most of attacks come from access network. There are various access networks for terminal to connect, such as 3G access network, public WiFi access network and wire access network in office, etc. For example, the risk is relative high if user uses public WiFi access network, while it is relative low if the user uses wire access network in office. Since every of the three inputs can affect strength and composition of security mechanisms, the Security Policy is used to measure the affection and produces a composition of security parameters as outputs which drive the security mechanisms to protect service with certain strength.

Advantages of this new approach can be:

- The Security Domains would face their own type of security threats and is deployed with the required security mechanisms by employing an individual security policy unit.

- The division of security domains can greatly benefit the situation with multiple operators.
- Once a specific service is ordered, the inputs with type of service and risk of access network can be automatically determined by platform and kept static. Only the input of security level is configured by user. By this means, the inputs are feasible, manageable and configurable.
- Security mechanisms in existing network can be included into this architecture without fundamental change. It can fully utilize existing network resource and save investment when cloud computing is deployed.
- The execution result could be fed back to billing module to support security provisioning as a service and make security as a value-added service.

5. Application Scenario

Figure 3 shows an example to illustrate application of the on-demand cloud security architecture. Alex Bob & Charley work in an organization. Charley gets connected to the office network from a hotel while Alex & Bob are currently working. Charley is supposed to get connected to a video conference with Bob & textual conversation with Alex to discuss business issues. Charley also needs to share few confidential documents which are uploaded into the cloud storage with Alex & Bob. Once they confirm the read of the documents, Charley would like to erase the documents with the acknowledgement of Alex & Bob. Charley being the initiator of the conference, he configures high security level for the video conference and text conversation. We have few concerns which can confirms Trust is

Authentication: This would be handled by the Compute Security Domain to protect the video conference and text conversation.

Confidentiality: This would be handled by the Network Security Domain to protect the video conference and text conversation.

Integrity: This would be handled by the Network Security Domain to protect the text conversation.

Data Security: This would be handled by the Storage Security Domain to encrypt the data flow

Data Deletion: A metadata is created for every object stored on the cloud would be the reference using which the user can confirm the deletion of the data. The data is stored only after being encrypted. This results in an unreadable data stored anywhere in the data centers ensuring security, and with the user action being delete through the type of service, the unique metadata resulting objects are deleted across the data centers confirming deletion.

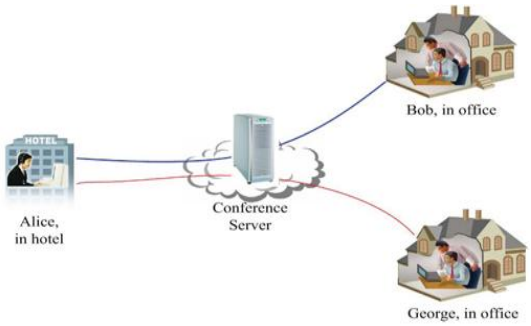

Figure 3. Application of On-Demand Cloud Security Architecture

Since Charley is located in a public area, he faces more security risk than Alex and Bob in office. By this means, the cloud computing will configure stronger security for Charley who is in a more insecure environment than Alex and Bob. Therefore Charley should be authenticated by cloud computing platform with multi-factor authentication in service security domain and data flow in network security domain should be encrypted with IPSec. With both Alex & Bob, only simple authentication in service security domain, such as password is necessary and data flow in network security domain can be plaintext since their risk of access network is low.

6. Conclusion

Security on demand for the end users would certainly define Trust, as one could understand the way things are being organized in the Cloud. The self configuring security architecture would not only ensure ease of use but also mitigate the usage of IT resources. The architecture is divided into 3 layers handling the input type from the user in the forms of security level, network access risk and the type of services. The next layer was determining the security policies for the security mechanisms in every security domain according to the input layer. The final layer deals with the security mechanisms which protect specific services based on the parameters from the second layer. Furthermore, the execution can be monitored and is fed back to billing centre which can add on as a service for the service provider. Trust finally can be proven when the user has complete belief on how secure his data got transmitted, how secure is his data and how securely has he deleted it when not needed.

References

[1] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, National Institute of Standards and Technology, October 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing.
[2] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009.

[3] H. Takabi , J.B.D. Joshi, and G.J. Ahn, “Security and privacy challenges in cloud computing environments”, Computer, vol. 8, no. 6, 2010, pp. 24-31.
[4] G.Pallis, “Cloud computing the new frontier of Internet computing”, IEEE Internet Computing, vol. 14, no. 5, 2010, pp. 70-73.
[5] Quingtao Wu, “An adaptive control mechanism for mitigating DDoS attacks”, Automation and Logistics, 2009. ICAL '09. IEEE International Conference on 5-7 Aug. 2009.