CLOUD SECURITY MODEL CSM 2.0: AN AUTONOMIC CLOUD SECURITY GATEWAY

Tamaike Brown
Department of Computer Science, North Dakota State University, Fargo, ND 58102, USA
Tamaike.brown@ndus.edu

Abstract

The use of Cloud Services is on the rise in this era of information technology age. It is perhaps the most important area, which has significant technical challenge of our time to have these services provide secured use and is simultaneously be safe for everyday users. Cloud Security is now the key preventive feature on what these services are able to provide us within a Cloud. In this research work, we are proposing to make the Cloud a virtual place where insecure services is the inconsistency, not the standard, and the Cloud Secured Services Venture, and it can be referred as CSSV 1.0. It is vital that the use of cloud is to be secured to prevent any security breaches for both users as well as service providers. In this research paper, we present a test of Cloud Security Architecture using Cloud Security Model (CSM 2.0). This model is based on Layered Architecture and looks into a Cloud domain through the resource autonomic management by containing a consumer login service, which needs to adhere the procedures and protocols provided by the service/service provider.

Key Words: Autonomic Computing, Cloud Computing, Data Communications, Service, SOA, Software Engineering, System, QOS

I. Introduction

IBM started the autonomic computing initiative in 2001, to create a self-managing computing system, which can handle increasingly complex tasks while making sure that rest of it is intact and checked. Autonomic computing involves systems design to also run self-diagnostics and checks and to compensate for any irregularities or glitches that may appear during any task performance. Whereas Cloud Computing is the computing on-demand and relies on several autonomic computing features and autonomic components. It is more of a virtual computing on-demand interface, in which the user's environment of work is not actually connected to a single computing device; rather it involves the use of computing infrastructure as hardware as a service (HaaS) and software as a service (SaaS) from a remote location. Cloud refers to the stipulation of different services required by users' on-demand in the form of computational resources as a combination of services. The services are designed and developed using service-oriented architecture or SOA. Any software application that requires frequent modification needs to be separated from the servicing applications, which is consistent and rarely needs to be updated. Service Oriented Architecture (SOA) is the application of this understanding on the knowledge management of a business.

SOA evolved in stages over the last few decades, since industrial automation increased. The services we use today process requests as input and produce output for customers, other systems or services. These systems or services orchestrate the data when generating messages among each other and to us as the user. The operational users of these services can monitor or manage many requests simultaneously. These operations can also be performed by a mediator service designed to follow the agreed policies and procedures among each of these services. Each service is owned and governed by a business entity and works within a certain body of rules, defined by the policymakers.

SOA provides a service data abstraction. This abstraction can be understood as a services messaging metadata, which can be in the shape of XML, XSD or other set industry standards providing interoperability to a user's request. The messaging between services is encapsulated for information-hiding purposes.

SOA eases the development of ever-changing applications that compare data with stationary applications while maintaining a decoupled relationship between these applications on a simultaneous basis as well as maintaining quality of service (QoS). SOA brought in a fresh approach for business information technology departments, making it easy to assemble and configure IT components like building blocks that can be combined to provide easy and fast solutions creation. For example, a bank provides a line of credit by checking a consumer's credit; an automotive parts seller checks the inventory; a shipping company maintains the shipping status for delivery to consumers, etc. SOA provides the framework to work modularly in the Cloud. Due to this flexibility, any business can adapt SOA and assemble its services as needed.

As the world has become a global village using latest Cloud computing, there is a significant need for businesses to fulfill consumer needs by providing services globally. This pursuit presents some challenges as given below:

- Flexibility is required.
- Increasing demand of standardized services with seamless experience for consumers.
- Reduction in operational cost of these services by getting satisfactory results due to improved efficiency, which means users control their business, rather than technology.
- Services are mostly distributed.
- Getting regulatory approvals.
- Getting rigid information systems wrappers developed to get the services combined at one framework.
- Efficient use of existing resources.
- Services are heterogeneous.
- The patterns of services interaction are unpredictable
- The service(s) "front end" is less useful for testing purposes due to decoupled implementation on the backend.

II. Background

Cloud has services serving users, and services are based on SOA, which is an adaptable and flexible approach—not a technology. SOA facilitates the utilization of reusable IT components to create new solutions over an existing framework of components. SOA provides platform-independent coupling of service components. This coupling can involve diversely developed service components in various languages, which can be maintained on several operating systems. The logical or functional separation of service components is provided by SOA. This separation allows software designers and developers to modify, test or redevelop and run these components on different servers before initiating them into a new lineup.

A. **SOA and related work:** According to Schreiner and Lamb [2], systems of the future will be based on the concepts of SOA. Service applications will be composed of a number of individual services running in the Cloud. As illustrated by Erl [3], service component application logic can be divided into two levels: a service interface, where loosely coupled services are available with their implementation and technology platform; and a service-using application level in which service application logic is developed and deployed on different technology platforms. These services communicate via open protocols.

B. **Autonomic System:** A human body is controlled by a human autonomic nervous system. This control is incredible in managing ever changing and unpredictable circumstances, in which a human can be involved. There is normally no humans' interference and even consciousness is required to exert any actions. Autonomic computing is primarily inspired by the functionality of human autonomic nervous systems, to design and build computing systems that function as a human autonomic

nervous system controls the human body. Essentially the autonomic computing paradigm is to provide self-managing mechanisms to computing, without any user's intervention. IBM has instantiated self-managing mechanisms into four specific capabilities, i.e., self-configuration, self-optimization, self-healing and self-protection [4].

III. Related Work on Cloud Security Issues

As per Schneier, et. al, "Security is not a product - it's a process. [5] Service security in the Cloud is not only a quality attribute, it is also regulated by governmental laws. There are several laws that can be identified to understand the need for Cloud security from the perspective of service providers, and from the perspective of the users. Some of the computer related crimes that are addressed by Criminal Laws [6] are:

- Unauthorized access
- Exceed authorized access
- Intellectual property theft or misuse of information
- Child pornography
- Theft of services
- Forgery
- Property theft (i.e., computer hardware, chips, etc.)
- Invasion of privacy
- Denial of service
- Computer fraud
- Viruses
- Sabotage (data alteration or malicious destruction)
- Extortion
- Embezzlement
- Espionage
- Terrorism

Cloud computing needs security of the cloud tested at an extensive level. To test any of the cloud service we need to know the base architecture of the Cloud security service(s). The base knowledge of Software architecture is a vital part to understand, that is the main core of software engineering. The Security of Cloud is an essential attribute, and is critical in making sure that there is no unauthorized access is allowed of any kind to the Cloud using by a corporation or even an individual. The Cloud service providers must consider, security of the service that they are about to provide to a consumer in the design process on earlier basis in system requirements engineering phase. This needs to be taken as a compulsory initiative at every architectural level in the service design, using SOA.

Service-Oriented Architectures (SOA) presents an advanced architectural concept with significance. Dorner et al. [7] have brought forward a few considerations of SOA in terms of End User Development (EUD). They analyzed the development of adaptable systems as a potential for SOA, proposing challenges that need to be solved to get an effective EUD. The authors' analysis is based on requirements for EUD systems and empirical studies, taken from earlier research work [8]. Dorner et al. have suggested in their study, that SOAs can be extended with structures for in-use modifications; the design of user-adaptable next-generation systems is also possible. EUD can also be suited develop Cloud service for the purpose of securing end-user as well.

With SOA-provided flexibility, the new tailorable systems can be produced, and platform independence can also be achieved. Services designed using SOA are

formulated software applications, and this formulation is closer to business domains. Research has also indicated that the call for additional metadata of service descriptions is growing quickly, and the amount of data collected from experiences with a service needs to be stored for analysis of service and its future use. This data handling in terms of storage locations and synchronization raises issues and serious concerns about service performance. The service can have performance issues in terms of message communication to and from the user to the service provider due to this additional contextual information. Research has found that requirements of EUD of a service may involve extending protocol and server structures of SOA standards.

Cloud computing embeds almost all known computing devices as well as several of software, such as SaaS (Software as a Service) [1], PaaS (Platform as a Service) and several Operating Systems. It also utilizes as many data communication networks, such as local area networks (LANs), metropolitan area networks (MANs) and wide area networks (WANs). A recent survey by Cloud Security Alliance (CSA) & IEEE indicates the eagerness of corporate sectors to adopt cloud computing, major bottle neck is the security is needed both to hasten cloud adoption, while making sure to achieve regulatory drivers coverage for their daily activities. It is vital for organizations to look critically at security models to examine the confidentiality issues for their business critical tactless applications.

Due to several such gaps, it is yet not possible to provide guarantees that corporate data in the "cloud" is secured, if not impossible, as they provide different services like SaaS, PaaS, and IaaS. Each service has its own security issues [9].

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 [10].

IV. Proposed Cloud Security Model

It is vital that the use of cloud is to be secured to prevent any security breaches for both users as well as service providers [11]. In this research paper, we present a Cloud Security Architecture using Cloud Security Model (CSM 2.0) to make sure that both data

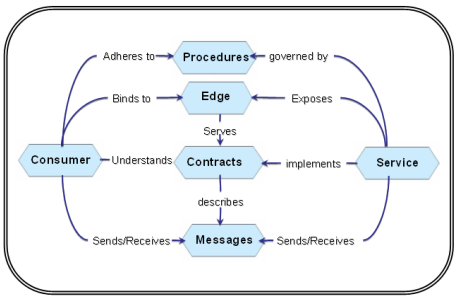

Figure 1: Cloud Security Model – CSM 1.0

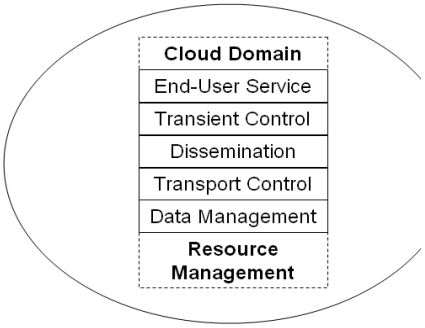

Figure 2: Cloud Security Architecture

and user requiring this data is protected under the federal law of ITAR/EAR [12][13]. This model is based on Layered Architecture and looks into a Cloud domain through the Resource Management as shown in the given figure.

The proposed architecture can be understood by the following Figure 2. CSM 1.0 contains a consumer login service, which needs to adhere the procedures and protocols provided by the service/service provider, Figure 1. Every service has an end-point; we call it Edge, which is to bind the consumer to use the service on the basis of contract accepted by both consumer and service provider. Communication among user or consumer is the key transient control between both for transparent use of the service(s). These procedures and processes are depicted in Figure 3.

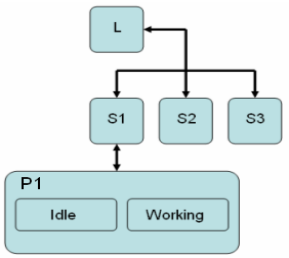

Figure 3: A functional example of an SRD

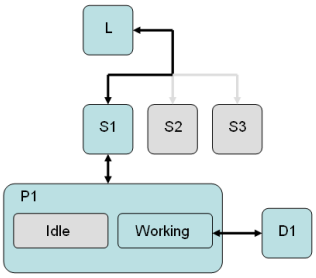

Figure 4: A working service prototype

The processing operator **P1** connects and relates elements to show the logical flow to construct a block in order to illustrate the performance of a desired system. The performance of a system is illustrated in two foremost ways, expressed by the combination of communicational links and conditional operators. A processing operator can have several inner processing operators related to each other directly or indirectly; one or several of these processing operators can be used to serve some other block of the system on a simultaneous basis. Let us assume the notations as shown below:

- L = List of Services
- S1 = Service 1
- P1 = Process Operator 1
- P1.1 = Idle Service
- P1.2 = Working

L is a **list of services** available in the Cloud containing a combination of **S1**, **S2** and **S3** (the **services** provided by a service provider) and **D1** (a service provided by a data centre in the Cloud). There can be two major processes a service can be in—0 and 1. The service is **Idle** or **Working**. The use of CSM 1.0 protocols provides us a secured way to use any further services from this point onwards.

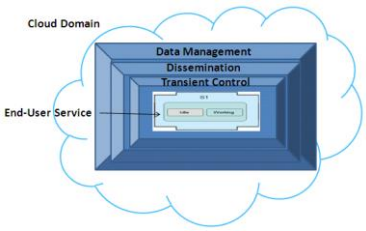

Figure 5: Three layered Cloud Security Model 2.0

Let us consider the service S1 is a Security Check Point 1 and the user's authentication is clarified for further processing. The service might be idle due to no job being needed to be done at this moment in time. The working service might also be idle, as there can be a delay in receiving some messages for next level of authentication combining user's as well as service provider's authentication for other services or a data centre of some kind. P1.1 and P1.2 can further be drilled down. The Figure 4 shows a prototype of getting required information for the service user of **L** from data center service **D**.

The service **S1** as shown in Figure 5 is the actual service built as an application block. This service block S1 connects with another service, **D1,** which is a service provided by a data centre in the Cloud and is assigned with first encrypted key **K1**, upon third level of authentication key **K3,** which is to be assigned by Dissemination level as the main locked layer key **K2** to issue clearance to get the required data for the user of service **L**. The processing block as shown in earlier Figure 4.4 can be seen as an independent processing operator connecting two services by communication of the requestor's requirement, and the operator gets the resultant data set(s) and delivers it to the requestor.

Let us look into further details of these services; **L** is a listing service of several services. For simplicity's sake, we will take the service **L** as given below:

- Detailed display of services available by a provider has applied CSM 1.0 protocols.
- Facilitates user's request as input to get a resultant data set at each entry and exit point of the service.

The service **S1** provides the following features:

- Generates a query on the request input once cleared from CSM 1.0 protocols.
- Stores the data for future feedback for service designer
- Manages bandwidth rates of data set receiving
- Delivers the data set(s) to service **L** upon clearing from CSM 1.0 protocols.

The service **D1** provides the following features:

- Receives query from **S1** cleared by CSM 1.0 protocols.
- Processes the resultant data set(s)
- Delivers to **S1** upon clearance from CSM 1.0 protocols.
- Stores the query for future use for some other user.
- Stores query snapshot for feedback for service designer.
- Self-manages the storage usage.
- Manages bandwidth rates of every query.
- K1 contains detail of data center originating IP address, as well as physical address with service provider's name and company license info.
- K3 contains detail of requestor/user's originating IP address.

- The main process of K2 is to confirm that both user and data provider are with ITAR/EAR defined boundaries;

In SRD, a database is also considered a service. Here are a few real-life examples given below to understand the use of database services to the users on an everyday basis:

- An owner/operator of a transport company can use the service **S2** using CSM 2.0 protocols to enhance his business by maintaining and adding the data associated with his customer organizations. This database service will keep a record of load pick-up and delivery dates for all the customers (organizations) provided by the transport company. If this transport company is planning a special pre-summer promotion, the database service will be able to generate results of the customers to target for advertising to increase business.
- A chief organizer of ABC party can take advantage of the same database service **S2** using CSM 2.0 protocols for a fundraising event. The mailing list generated by the database service is made up of a wide range of organizations with contact person's data of every organization arranged as per the area or city, town or a state. These people can be invited with reference to the transport company's owner for a fundraising dinner for the ABC party for election.

In the case of a merger between the manufacturer of a certain product, such as a printing company, and the transport company, the service S2 using CSM 2.0 protocols can be used to inform customer organizations of the newly available services of printing for clients to go with the transportation services as well.

The use of CSM 2.0 will prevent unauthorized access of any data hosted within US borders critical to the ITAR/EAR munitions list to any of the users of both merged concerns as given in the above example to access restricted documentation from outside of the country, except been exempted to get access to under the given provisions of the law.

V. Conclusion

As described in the paper, though there are tremendous advantages in using cloud-based systems, there are yet many realistic problems which have to be solved. Cloud is a union of several hardware and software platforms. There are several hybrid technologies being utilized to provide the services in the cloud by many service providers. This paper sheds light on few of the several issues dealing with Cloud and specifically the security issues and research work done to find suited solutions to resolve security problems. It also encompasses a proposal of Cloud Security Architecture based on Layered Architecture approach. This approach is presented as Cloud Security Model and is named CSM 2.0, with expansion of three services with an addition of encrypted internal keys to find the source of request and destination, which needs more future enhancements and modifications with the incorporation of systems functional testing. CSM 2.0 has potential to be enhanced to achieve a favorable methodology to resolve the issues related to Cloud Security, reliable availability of the desired results from the effective use of Cloud's available resources.

VI. References

[1] A. F. Mohammad, E. S. Grant; Cloud Computing, SaaS and SOA 3.0: A New Frontier. Cloud Computing and Virtualization 2010 International Conference, Singapore May 2010

[2] R. Schreiner, U. Lang; Protection of complex distributed systems. Proceedings of the 2008 workshop on Middleware security. Pages 7-12. 2008.

[3] T. Erl. Service-Oriented Architecture: Concepts, Technology, and Design. Prentice Hall PTR, 2005.

[4] IBM, 2001. IBM autonomic computing manifesto, 2001 http://www.research.ibm.com/autonomic/manifesto/.

[5] Schneier Bruce, Secure System Engineering Methodology, http://www.counterpane.com/; Accessed on April 15, 2011

[6] H. P. Tipton and M. Krause, Information Security Management 4th edition, Auerbach, United States of America, 2000

[7] C. Dörner, V. Pipek, M. Weber, V. Wulf. End-user development: new challenges for service oriented architectures. in Proceedings of the 4th international workshop on End-user software engineering, pp. 71-75, May 2008

[8] F.P.J. Brooks. No silver bullet: essence and accidents of software engineering, IEEE Press, pp.10-19, 1987

[9] B. R. Kandukuri, V.R. Paturi, A. Rakshit. Cloud security issues.In: IEEE international conference on services computing, p.517–20. 2009

[10] V. Choudhary. Software as a service: implications for investment in software development. In: International conference on system sciences,p.209. 2007

[11] A. F. Mohammad, R. Marsh, E. S. Grant. Cloud Security Model using SOA 3.0 - CSM 1.0: A New Frontier. 2nd International conference on Cloud Computing and Virtualization 2011, Malaysia, April 2011

[12] http://www.pmddtc.state.gov/regulations_laws/itar_official.html; Accessed on April 19, 2011

[13] http://www.gpo.gov/bis/ear/ear_data.html; Accessed on April 19, 2011