International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Security Rudiments for SaaS Application Development and Deployment

Anand Singh

Kantipur City College, Kathmandu, Nepal

Abstract: ***Cloud computing is an embryonic paradigm with varying meanings, but an industry wide acknowledged definition standardized by National Institute of Standards and Technology (NIST) delineates cloud computing as a model for facilitating ubiquitous, well-situated, on-demand network access to a shared puddle of configurable computing resource (e.g., servers, storage, networks, applications and services) that can be speedily provisioned and released with negligible management endeavour or service provider interaction. This research work identifies and reviews the security measures of cloud computing.***

Keywords: Cloud Computing, Cloud Security, Software-as-a-Service, Web data security

1. Introduction

The foremost inclination for service infrastructures in the IT province is called cloud computing, a way of computing that permits users to access information services. Cloud providers trade their services on cloud resources for funds [9]. In the cloud software stack, National Institute of Standards and Technology (NIST) has standardized cloud computing as it has three distinct levels: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Each layer has different levels of abstraction from the physical hardware from which the software runs on top of.

Cloud computing is a disseminated computational model over a large puddle of shared-virtualized computing resources (e.g., storage, memory, processing power, applications, network bandwidth and services), where customers are provisioned as well as de-provisioned recourses as they require. Cloud computing represents a vision of providing computing services as public utilities like water and electricity. The structural design of cloud computing can be split in front-end and back-end. The front-end characterizes cloud applications, customers or organizations that use the cloud services. The back-end is a giant network of data centres with numerous diverse system programs, applications, and data storage systems. It is metaphorically supposed that, cloud service providers (CSPs) have almost unbounded computation power as well as storage capacity. Figure 1 illustrates the conceptual scaffold of cloud computing architecture with its two main parts.

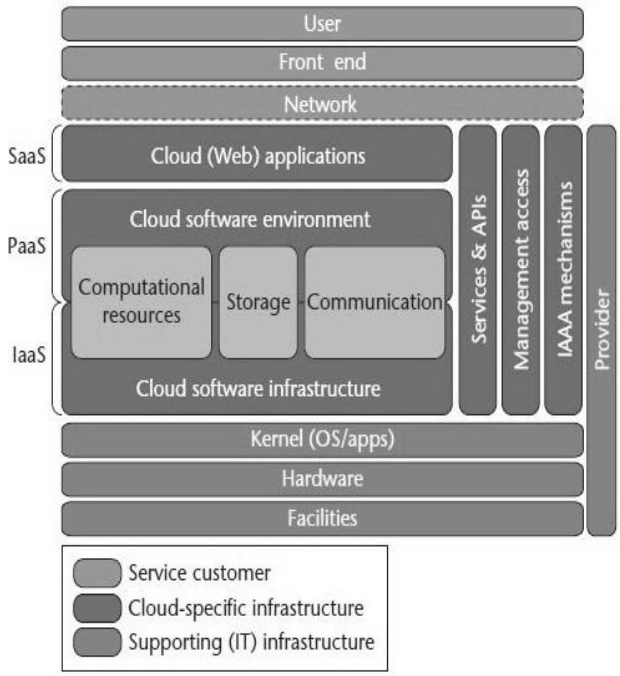

Figure 1: Conceptual framework for Cloud Computing architecture

2. Cloud Security

As promising as it is, cloud computing also faces various security issues, which include data segregation, access of perceptive data, privacy, policy integration, authentication, identity management, bug exploitation, recovery, accountability, management console security, malicious insiders, visibility under virtualization, account control, and multi-tenancy issues.

There are numerous security challenges for cloud computing because it includes numerous technologies, which comprise operating systems, networks, databases, virtualization, resource scheduling, transaction management load balancing, memory management and concurrency control. Consequently, security issues for these systems and technologies are applicable to cloud computing [10].

2.1 Security Issues in Cloud Model

The security of the cloud is ensured in many levels, but the scope of intrusions makes it necessary to understand the factors that affect cloud security to ensure that it is a usable system of advanced data processing by all industries and the resistance that is faced by some sectors towards cloud computing is broken down[1].

Three delivery models are utilized by cloud computing by which diverse types of services are offered to the end user. The three delivery models are the SaaS, PaaS and IaaS which give infrastructure resources, application platform and software as services to the end user.

3. Security Issues in Saas

In SaaS, the user has to rely on the provider for appropriate security measures. The provider must accomplish the effort to maintain diverse users from access each other‟s data. So it becomes complicated to the user to guarantee that right security measures are in place and also complex to get assertion that the application will be accessible when required[2]. With SaaS, the cloud client will by definition be substituting new software applications for old ones. As a result, as mentioned by Adrian et al[3], the focal point is not upon portability of applications, but on safeguarding or enhancing the security functionality provided by the legacy application and realizing a unbeaten data migration.

The SaaS software vendor can host the application on its own private server farm or set up it on a cloud computing infrastructure service provided by a third party provider for instance Amazon, Google, etc. The use of cloud computing coupled with the pay-as-you-go (grow) approach, assists the application service provider to diminish the investment in infrastructure services and enables it to concentrate on providing improved services to clients.

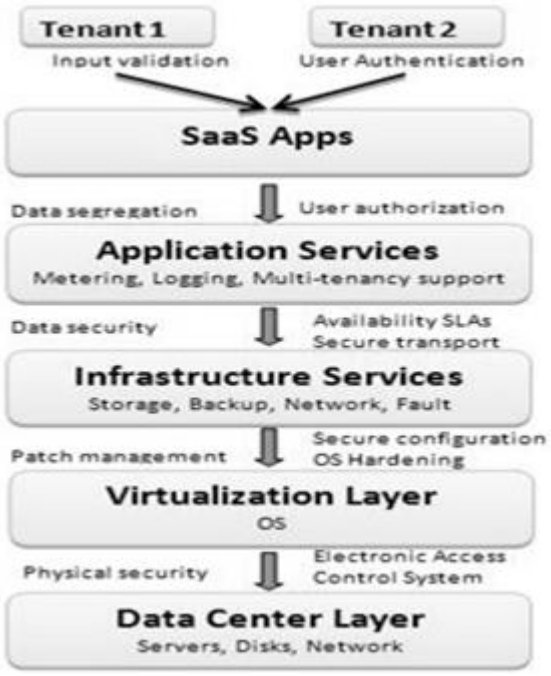

Figure 2: Layered Security for the SaaS stack

The encrusted stack for an archetypal SaaS vendor and decisive aspects that must be covered across layers in order to guarantee security of the enterprise data is exemplified in Figure 2.
The following key safety rudiments should be vigilantly considered as an essential part of the SaaS application development and deployment process:

3.1 Data security

In a conventional on-premise application deployment model, the perceptive data of each enterprise continues to be inherent within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. Nevertheless, in the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must espouse extra security checks to guarantee data security and avoid breaches due to security vulnerabilities in the application or through malevolent employees. This entails the use of tough encryption techniques for data security and fine-grained authorization to manage access to data.
Malevolent users can exploit weak points in the data security model to get unlawful access to data. The following assessments test and corroborate the safety of the enterprise data stored at the SaaS vendor.

- Cross Site Request Forgery (CSRF)
- Access control weaknesses
- Cross site scripting (XSS)
- Concealed field manipulation
- OS and SQL Injection Flaws
- Cookie manipulation
- Insecure storage
- Insecure configuration

3.2 Network security

In a SaaS deployment model, perceptive data is attained from the enterprises, processed by the SaaS application

and accumulated at the SaaS vendor end. All data flow over the network needs to be protected in order to avert seepage of perceptive information. This engrosses the use of strapping network traffic encryption methods such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

Nevertheless, malevolent users can exploit weaknesses in network security configuration to snuffle network packets. The following assessments test and corroborate the network safety of the SaaS vendor.

- Insecure SSL trust configuration
- Network penetration and packet analysis
- Session management weaknesses

Any vulnerability noticed during these tests can be exploited to capture active sessions, gain access to user credentials and perceptive data.

3.3 Data locality

In a SaaS representation of a cloud milieu, the clients utilize the applications offered by the SaaS and process their business data. But in this situation, the client does not identify where the data is getting stored. In numerous cases, this can be an issue. Due to conformity and data seclusion laws in different countries, locality of data is of utmost significance in numerous enterprise architecture[4].

3.4 Data veracity

Data veracity is one of the most significant rudiments in any system. Data veracity is simply accomplished in a standalone system with a sole database. Data veracity in such a system is maintained via database constraints and transactions. Transactions should follow ACID properties (Atomicity, Consistency, Isolation and Durability) to guarantee data veracity. Most databases support ACID transactions and can conserve data veracity.

Next in the complexity chain are the disseminated systems. In a disseminated system, there are manifold databases and manifold applications. In order to preserve data veracity in a disseminated system, transactions across multiple data sources require to be handled perfectly in a reliable manner. This can be made using a central universal transaction manger. Each application in the disseminated system should be able to partake in the universal transaction via a resource manager. This can be achieved using a 2-phase commit protocol as per XA standard.

3.5 Data segregation

Multi-tenancy is one of the chief characteristics of cloud computing. As a outcome of multi-tenancy numerous users can store their data using the applications offered by SaaS. In such circumstances, data of diverse users will exist at the same location. Infringement of data of one user by another becomes feasible in this environment. This infringement can be done either by hacking through the loophole in the application or by injecting client code into the SaaS system. A customer can write a masked code and inject into the application. If the application executes this code without authentication, then there is a high prospective of intrusion into other‟s data. A SaaS representation should hence guarantee a clear boundary for each user‟s data. The boundary must be guaranteed not only at the physical level but also at the application level. The service should be sharp sufficient to segregate the data from other users.

A malevolent user can utilize application vulnerabilities to handcraft parameters that evade security checks and access perceptive data of other tenants. The following assessments test and authenticate the data segregation of the SaaS vendor in a multi-tenant deployment:

- SQL Injection flaws
- Data validation
- Insecure storage

Any vulnerability discovered during these tests can be exploited to get access to perceptive enterprise data of other tenants.

3.6 Data access

Data access concern is primarily related to safety policies provided to the users while accessing the data. In a emblematic situation, a small business organization can utilize a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These safety policies must be adhered by the cloud to evade infringement of data by illegal users which is stressed by Bowers et al[5]. The SaaS model must be flexible sufficient to integrate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment[7].

3.7 Authentication and authorization

Most of companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of small and medium-sized companies, a segment that has the uppermost SaaS acceptance rate, Active Directory (AD) seems to be the most admired tool for managing users (Microsoft White Paper 2010[6]). With SaaS, the software is hosted outside the corporate firewall. Many times customer credentials are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. This means SaaS clients must memorize to remove/disable accounts as employees depart from the company and create/enable accounts as come onboard. In essence, having manifold SaaS products will increase IT management operating cost. For instance, SaaS providers can offer delegates for the substantiation process to the clients internal LDAP/AD server, so that companies can preserve control over the management of users.

3.8 Data secrecy issue

Cloud computing entails the sharing or storage by users of their own information on remote servers owned or operated by others and accesses through the Internet or other connections. Cloud computing services subsist in numerous variations, comprising video sites, tax preparation sites, data storage sites, personal health record websites etc. The entire stuffing of a user‟s storage device might be stored with a sole cloud provider or with numerous cloud providers. When an individual, a business, a government agency, or any other entity shares information in the cloud, privacy or secrecy questions are raised[5].

3.9 Web application security

SaaS is software deployed over the internet and/or is deployed to run behind a firewall in local area network or personal computer. The chief characteristics embrace Network-based access, and management of commercially available software and managing activities from central locations rather than at each customer‟s site, enabling clients to access application tenuously via the Web. SaaS application development may utilize different kinds of software components and frameworks. These tools can diminish time-to-market and the charge of translating a conventional on-premise software product or building and deploying a novel SaaS solution. Examples embrace components for subscription management, web application frameworks grid computing software, and complete SaaS platform products.

3.10 Data breaches

Since data from diverse clients and companies lie together in a cloud environment, breaching into the cloud environment will potentially assault the data of all the users. Thus the cloud becomes a soaring value target[7]. In the Verizon Business breach report blog[8], it has been said that outside criminals pose the utmost menace (73%), but attain the least impact (30,000 compromised records), resulting in a Psuedo Risk Score of 67,500. Insiders pose the slightest menace (18%), and attain the greatest impact (375,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Partners are middle in both (73.39% and 187,500) resulting in a Pseudo Risk Score of 73,125. Though SaaS advocates assert that SaaS providers can offer superior security to customers‟ data than by usual means, Insiders still have admittance to the data but it is just that they are accessing it in a dissimilar way. Insiders do not have straight access to databases, but it does not diminish the menace of insider breaches which can be a massive impact on the security. The SaaS providers‟ employees have access to a lot more information and a single confrontation could expose information from numerous customers. SaaS providers must be compliant with Payment Card Industry – Data Security Standards (PCI DSS) in order to host merchants that must comply with PCI DSS.

3.11 Vulnerability in virtualization

Virtualization is one of the major apparatus of a cloud. But this poses chief security risks. Guaranteeing that diverse instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely in today‟s situation. The other concern is the control of administrator on host as well as guest operating systems. The present virtual machine monitor does not proffer perfect isolation. A lot of bugs have been located in all popular VMMs that allow absconding from Virtual Machine. VMM should be „root secure‟, meaning that no dispensation within the virtualized guest environment allows interference with the host system.

3.12 Availability

The SaaS application requires guaranteeing that enterprises are offered with service around the clock. This engrosses making architectural changes at the application and infrastructural levels to attach scalability and elevated accessibility. A multi-tier architecture needs to be acknowledged and supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software breakdown, as well as to denial of service (DOS) attacks, needs to be built from the ground up within the application.

At the same time, an appropriate action plan for Business Continuity (BC) and Disaster Recovery (DR) requires to be considered for any spontaneous emergency. This is necessary to guarantee the safety of the enterprise data and negligible downtime for enterprises.

3.13 Backup

The SaaS vendor requires ensuring that all perceptive enterprise data is repeatedly backed up to ease quick recovery in case of adversity. Also the use of brawny encryption technique to protect the backup data is recommended to avoid unplanned seepage of perceptive information.

In the case of cloud vendors such as Amazon, the data at reside in S3 (Simple Storage Service) is not encrypted by default. The users require to independently encrypt their data and backups so that it cannot be accessed or tampered by illegal parties [10].
The following assessments test and authenticate the security of the data backup and recovery services provided by the SaaS vendor.

- Insecure storage
- Insecure configuration

4. Conclusion

Cloud computing security is an embryonic sub-domain of information security, computer security, and more generally network security. Cloud security is not to be mystified with security software offerings that are “cloud-based”. The scale of the cloud security spans across all the three service delivery models deployed in any of the four cloud deployment models (private, public,

hybrid and community cloud) and exhibiting the five essential characteristics of the cloud. This paper analyses the questions related to application and data security which falls under the SaaS layer.

References

[1] Cong, W., Qian, W. and Kui R., "Ensuring Data Storage Security in Cloud Computing", Cryptology ePrint Archive, Report, http://eprint.iacr.org/, 2009.
[2] Choudhary, V. "Software as a Service: Implications for Investment in Software Development", In International Conference on System Sciences, pp. 209, 2007.
[3] Adrian, S., Alex, H., Alexander, M., Alexander W., Anish M., Anthony and Licciardi. "Security Guidance for critical areas of focus in cloud computing", Cloud Security Alliance, Vol.2.1, p25, 2009.
[4] Softlayer, "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, 2009.
[5] Bowers, K.D., Juels, A. and Oprea, A. "HAIL: A High-Availability and Integrity Layer for Cloud Storage", Cryptology ePrint Archive, Report 2008/489, http://eprint.iacr.org/, 2008.
[6] Microsoft White Paper, "MS Strategy for Lightweight Directory Access Protocol", http://technet.microsoft.com/en-us/library/ cc750824.aspx,2010
[7] Kaufman, L.M. "Data Security in the world of cloud computing", Security and Privacy, IEEE Vol. 7, No. 4, pp. 61-64, 2009.
[8] Russ, Cooper. "Verizon Business Data Breach security blog", http://securityblog.verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/,2008
[9] Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S., Cloud computing features, issues, and challenges: a big picture. IEEE International Conference on Computational Intelligence and Networks (CINE), pp. 116-123, 2015
[10] Hendre, Amit, and Karuna Pande Joshi. "A semantic approach to cloud security and compliance." IEEE 8th International Conference on Cloud Computing. pp. 1081-1084, 2015.