International Journal of Advanced Research in Engineering Technology & Science

ISSN: 2349-2819

Email: editor@ijarets.org Volume-9, Issue-8 August – 2022 www.ijarets.org

STUDY ON SECURITY DIFFICULTIES IN THE GENERAL SAAS APPLICATIONS

Sanober Zia,

Research Scholar, School of Technology and Computer Science,

Glocal University Mirzapur Pole, Saharanpur (U. P.)

Dr. Aaruni Goel,

Research Supervisor School of Technology and Computer Science,

Glocal University Mirzapur Pole, Saharanpur (U. P.)

ABSTRACT

Cloud computing provides its users the ability to access computing resources in a convenient and on demand basis. Cloud offers the hardware, platform and software

applications via its IaaS (Infrastructure As a Service), PaaS (Platform As a Service) and SaaS (Software As a Service) models.Although, the number of users and thecloud computing applications are growing at a faster rate, security remains the biggest challenge in the wide-spread adoption of the cloud computing. Security issues are more significant in the SaaS environments because of the high adoption rate and the number of applications. In this paper, the security issues in the popular SaaS applications have been presented along with the implementation challenges to the secure environments. Tools and technologies are continuously evolving to provide better security, to the cloud users. Prominent security applications have been outlined in this paper.

Keywords: *Cloud Computing, Security, Risk Management*

1. INTRODUCTION

Cloud computing [1] is a new computing paradigm in which the computer resources (software and hardware) are delivered as a service to the users on metered basis (i.e. pay as you use) generally over the Internet.The users pay for what and how much they use the services made available by service provider. The users of the cloud services are generally called the tenants of the clouds. The word cloud was taken from the cloud symbol that is generally used in flowchart and diagram used for Internet. Cloud computing has become a significant technology trend, and many experts expect that cloud computing will reshape information technology(IT) processes and the IT marketplace. With the cloud computing technology, users use a variety of devices, including PCs, laptops, smart phones and PDAs to access programs, storage, and application – development platforms over the Internet, via services offered by cloud computing providers. Advantages of the cloud computing technology include cost savings, □□high □□availability, and easy scalability [5],[6],[7].

Layered Paradigm of cloud

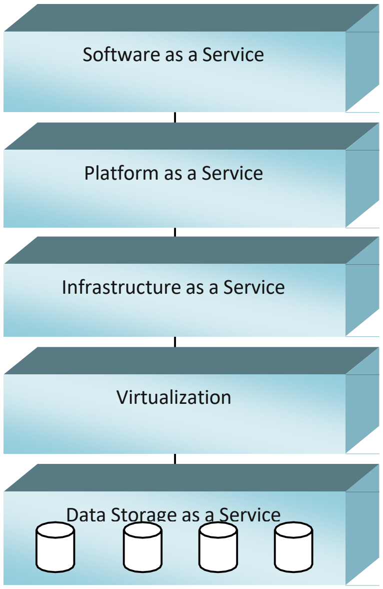
We can view Cloud computing [1] as a collection of services, which can be represented as a layered cloud computing architecture, as shown in Fig.1. These services include software as a service, platform as a service, infrastructure as a service and data storage as a service.

Software-as-a-Service(SaaS)-

Software As a Service refers to the services offered through cloud computing usually include IT services,which is shown on top of the service stack. These applications include business processes, industry application, collaboration and other similar application. SaaS allows users to run applications remotely from the cloud as they are running applications on their own computers [2],[5].

Platform-as-a-Service (PaaS)-

PaaS evolved from Software as a Service (SaaS), which uses the Internet to host software applications. Platform As a Service gives the capability to the consumers to run their own created applications and other tools on service provider's platform. The services provided in this category include middleware, database, development tooling, java runtime, web application runtime etc. Consumers have the control over their applications but cannot control operating system, storage and other underlying infrastructure of the cloud [2],[6].



Infrastructure-as-a-Service(IaaS)-

Infrastructure As a Service refers to the services which give consumers the capability to use and manage operating system, storage, network and other resources available on the cloud but do not have control on underlying cloud infrastructure [2],[10]. Characteristics of IaaS include:

□ Automated administrative tasks

□ Dynamic scaling

□ Platform virtualization

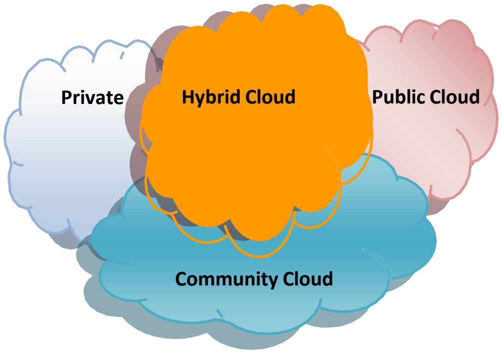
□ Internet connectivity

The data - Storage-as-a-Service (d SaaS)- Data Storage As a Service is the service which provides storage to the consumer and also includes bandwidth requirements for the storage [2]. You can think of the DaaS model as new methods for accessing data within existing data centers. It often provides new architecture designs, like private clouds inside a public cloud. Data is usually located in relational databases inside corporate data centers. Because data is easily accessible, customers can take immediate action and do not require in-depth understanding of actual data

Cloud Deployment models

There are mainly four types of cloud: (i) private cloud, (ii) public cloud, (iii) hybrid cloud and (iv) community cloud as shown in Fig.2.

Fig.2 Cloud Deployment Models



Private cloud (or internal cloud) [1],[2],[5] refers to cloud computingon private networks. Private clouds are built for the exclusive use of one client, providing full control over data,security, and quality of service.Private clouds can be built and managed by a c ompany's own IT organization or by a cloud provider.

In the public cloud (or externalcloud) computing resources aredynamically provisioned over the Internet via Web applications or Web services from an off-site third-party provider. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks [1],[2].

A hybrid cloud environmentcombines multiple public and private cloud models. Hybrid clouds introducethe complexity of determining how to distribute applications across both a public and private cloud [1],[2].

In Community cloud, the cloud infrastructure is shared by severalorganizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations

). It may be managed by the organizations or a third party and may exist on premise or off premise [1],[2].

Cloud burst

Cloud burst is a quality of service (QoS) metric used to gauge cloud solution scalability and measure software application capability andperformance on hosted cloudplatforms. Cloud application andservice vendors provide benchmark performance ratios for total leased infrastructure and ensure maximized application hosting. However, a well- designed, scalable, flexible andreliable architecture easily handles network traffic and computing requirements, while a poorly-designedarchitecture will falter when subjected to resource-hungry applications.

Cloud burst can be either a positive and negative phenomenon that definesa cloud infrastructure's ability to handle traffic and computing surges. A positive cloud burst refers to a cloud-based application or infrastructure platform that efficiently and capably manages cloud-hostedapplication scalability. A negative cloud burst refers to a cloud-based application or infrastructure's inability to efficiently manage resource requirements.

1. SaaS

Software as a Service (SaaS) [2],[3] is a software deployment model whereapplications are remotely hosted by the service provider and made available to consumers on demand on metered basis, over the Internet. Enterprises can take advantage of the SaaS model to reduce the IT costs associated with traditional on-premise applications like hardware, patchmanagement, upgrades, etc. On demand licensing can help consumers adopt the "pay-as-you-go/grow" model to reduce their up-front expenses for IT purchases. SaaS lets software vendors control and limit use, prohibits copies and distribution, and facilitates the control of all derivative versions of their software. SaaS centralized control often allows the vendor to establish an ongoing revenue stream with multiple tenants. The tenants are provided a protected sandbox view of the application that isisolated from other tenants. Each tenant can tune the metadata of the application to provide a customized look and feel for its users. The SaaS software vendor may host the application on i ts own private server farm or deploy it on a cloud computing infrastructure serviceprovided by a third party provider (e.g. Amazon, Google, etc.). The useof cloud computing coupled with the pay-as-you-go (grow) approach helps the application service provider reducethe investment in infrastructureservices and enables it to concentrate on providing better services to customers. SaaS is most often subscription-based and all ongoingsupport, maintenance, and upgrades are provided by the software vendor aspart of the service. Applicationcustomization capabilities, if availableat all, are generally provided to all customers in a consistent manner.From the perspective of the software vendor, the SaaS model provides stronger protection of its intellectualproperty, operational control of the environment running the software, andgenerally a repeatable revenue stream from the service subscription fees. Software vendors have varyingcapabilities and applications can comein varying flavors but SaaS applications most typically support many unique customers using a single instance of that application, also known as multi-tenancy. SaaS requires more care around security than any of other available delivery models. The current best security practices associated with application development involve a l ayered approach. Regardless of the software delivery model, security cannot be implemented at a s ingle "make or break" point. Instead, security must be layered into the network, the servers, the code and the database. Security comes in the form of both active prevention and, more recently, intrusion detection. SaaS is a n atural evolution of software. The old model of getting physical DVDs and installing on local servers had been theonly realistic solution for many years. In fact, the client-server model is still required for many scenarios. Thatsaid, in recent years a number of developments have allowed SaaS tocome mainstream. One factor is bandwidth -- the Internet is simply faster than it was a decade ago. Other major factors include the evolution of both virtualization and tools in big data. All these advances have made it much easier for providers to scale and manage their own infrastructure andthus provide SaaS solutions. SaaS is used in a number of common business areas, including customer relationship management, document management, accounting, human resource (HR) management, service desk management, content managementand collaboration, among others.

There are a f ew major characteristics that apply to most SaaS vendors:

□ Updates are applied automaticallywithout customer intervention

□ The service is purchased on asubscription basis

□ No hardware is required to beinstalled by the customer

SaaS Examples

□ SalesForce CRM (CustomerRelationship Management)

□ Google Apps

□ DeskAway

□ Impel CRM

Wipro w-SaaS

2. Security Issues

Cloud infrastructures [3], [20] are just another computer network. This means that Clouds will have the same security issues any networkinfrastructure will have as intrusion detection and prevention etc. It is upto the Cloud vendor to determine the level of security required. The following key security elements should be carefully considered as an integral part of the SaaS application:

Selection of SaaS Deployment Model

The SaaS security challenges differ depending upon the deployment model being used by the vendor (i.e public cloud or private cloud). SaaSvendors may choose to deploy the security solution either by u sing a public cloud vendor or host itthemselves. Dedicated public cloud providers such as Amazon help to build secure SaaS solutions by providing infrastructure services thataid in ensuring perimeter and environment security. This involves the use of firewalls, intrusion detection systems, etc. A self-hosted SaaS deployment, however, requiresthe vendor to build these services and assess them for securityvulnerabilities.

Data Security

In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the enterprise data is stored outside theenterprise boundary, at the SaaS vendor end. Consequently, the SaaSvendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. Thisinvolves the use of strong encryption techniques for data security and fine- grained authorization to control accessto data.

Network Security

In a SaaS deployment model, sensitivedata is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All dataflow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer [SSL] and the Transport Layer Security [TLS] for security.

Regulatory Compliance

The SaaS deployment needs to be periodically assessed for conformance to regulatory and industry standards. Data privacy has emerged as an other significant challenge. Differentcountries have their distinct privacy regulations about how data needs to besecured and stored. These might leadto conflicts when the enterprise data ofone country is stored in data centers located in another country.

Data Segregation

In a mature multi-tenant SaaS architecture, the application instances and data stores may be shared across multiple enterprises. This allows theSaaS vendor to make more efficient use of resources and helps achieve lower costs. At the same time, sufficient security checks need to be adopted to ensure data security and prevent unauthorized access to data of one tenant by users from other tenants.This involves hardening the data store as well as the application to ensuredata segregation. In case the SaaS application is deployed at a third partycloud vendor, additional safeguards need to be adopted so that data of an application tenant is not accessible to other applications.

Availability

The SaaS application needs to ensure that enterprises are provided withservice around the clock. This involves making architectural changes at the application and infrastructurallevels to add scalability and high availability. A multi-tier architectureneeds to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs tobe built from the ground up within the application. At the same time, an appropriate action plan for business continuity and disaster recovery needs to be considered for any unplanned emergencies. This is essential to ensure the safety of the enterprise dataand minimal downtime for enterprises.

Backup

The SaaS vendor needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters. Also the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information. The users need to separately encrypt their data and backups so that it cannot be accessed or tampered with by unauthorized parties.

3. Implementation ChallengesIdentity Management

Cloud providers [4] themselves aren't always sophisticated about integrating their platforms with identity services that exist behind the enterprise firewall. There are some third-party technologies that let IT extend role-based access controls into the cloudwith single sign-on Identity and accessmanagement in the cloud has a long way to go, according to the Cloud Security Alliance, an industry group. This is a field that is still in the early stage “Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today," according to research from the Cloud SecurityAlliance. While an enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a n ecessary prerequisite for strategic use of on-demand computing services

Cloud Computing Standards

There are few standard are available for cloud security but they are not as strong as we expect. For example ISO 27001 (an information security specification published by the International Organization for Standardization in Switzerland) is not perfect but it's a step in the right direction," Experts says. "It's the best one out there, but that doesn't mean it's sufficient." There's no guarantee that your data will be safe with an ISO 27001-compliant vendor, however.Google, like other vendors, have strict privacy policies for their employees. But those policies reportedly did not prevent Barksdale from accessing Google Voice call records and Gmail and Google Chat accounts of several Google users, and he was subsequently fired.

Security Analysis

The ability to analyze the security of SaaS applications [4],[17] is more limited than the ability to analyze the security of in-house systems, but that shouldn't prevent customers from demanding proof of vendor claims. Cloud vendors argue that they are more able to secure data than a typical customer, and that SaaS security is actually better than most people think. But some customers find this hard to believe because SaaS vendors tend to be rather secretive about their security processes. In particular, many cloudservice providers release very few details about their data centers and operations, claiming it wouldcompromise security. Howevercustomers and industry analysts are getting fed up with all the unanswered questions and hush-hushnondisclosure agreements.

Risk Analysis

One major benefit of software-as-a- service is that business applications can be accessed wherever there is Internet connectivity which also poses new risks. Coupled with the proliferation of laptops and smart phones, SaaS makes it even more important for IT shops to secure endpoints. Maintaining control over e-mails and documents is easier when those files are stored on your local servers, rather than in the cloud. Enterprises that make use of SaaS need to implement policies to control connectivity.

Data Centre Locations

In highly virtualized systems, data andvirtual machines can move dynamically from one country to another in response to load balancing needs and other factors. There's nothing stopping you from moving a VM from one place in the world to somewhere else, and more importantly, there's no w ay to auditthat at any sort of scale.

Continuously Evolving Nature

User requirements are continuously evolving, as ar e the requirements for interfaces, networking, and storage. This means that a “cloud,” especially apublic one, does not remain static and is also continuously evolving.

4. Security-as -a Service

Security-as-a-service (SaaS) [19],[20] is an outsourcing model for security management. Typically, Security as a Service involves applications such as anti-virus software delivered over the Internet but the term can also refer to security management provided in- house by an external organization. Security-as-a-Service offers a number of benefits, including:

- Constant virus definition updates that are not reliant on user compliance.
- Greater security expertise than is typically available within an organization.
- Faster user provisioning. Outsourcing of administrative tasks, such as log management, to save time and money and allow anorganization to devote more time to its core competencies.
- A Web interface that allows in-house administration of some tasks as w ell as a v iew of the security

environment and on- going activities.

Cloud computing, hosted services and applications on demand haveredefined how users interact with data,but security solutions are still stuck in the past, hindered by arcane architecture and localized thinking.The market demands a b etter way to implement and manage security, whileeliminating the liabilities of the past and looking to the future. The time is now to evolve security to meet the needs of the Web 2.0 w orld and that evolution will come from the adoptionof Software as a Service (SaaS) based security solutions that eliminate the disadvantages of traditional security products. Security as a Service is showing strong promise, not only as a means of closing existing tactical gapsin security management, but as a new way to approach or extend security strategy. One of the examples ofSecurity as a service is McAfee.McAfee is providing McAfee Security as a S ervice to the organization or industries over Internet. McAfee Security-as-a-Service solutions are designed to provide organizations witha comprehensive set of securityproducts built in a Software-as-a-Service (SaaS) model [22]. This strategy takes advantage of McAfee's core strength in threat prevention, adiverse SaaS portfolio, and ourindustry-leading Global Threat Intelligence, powered by McAfee Labs. McAfee Security-as-a-Service solutions are available over theinternet, managed by McAfee and provided on a subscription basis. By running security as a cloud-basedsolution, you can reduce your capital investment, eliminate onsite administration, and reallocate IT resources to projects better aligned to your initiatives. And with McAfee Security-as-a-Service solutions, youget immediate, up-to-the-minute threatprotection to ensure your data, systems, and networks are instantly and always secure. Easy on t he budget, McAfee Security-as-a-Service solutions deliver peace of mind. The volume and complexity of Web, email, and data security threats today pose a huge security challenge for organizations, and many lack the resources to address these threats effectively. The growing number of mobile workers, economic constraints, and regulatory compliance compound the security dilemma. Security professionals are left wondering whereto turn for the right solution. One technology that is meeting these challenges head on is Security-as-a-Service (SaaS). SaaS is increasing in popularity as an effective and lowertotal-cost delivery platform. Organizations of all sizes are now looking to SaaS to reduce the cost of deploying and managing Web and email security across their headquarters, branch offices, andmobile workforce. Advances in cloud computing and the increased capacity and functionality of cloud-based services have led to a significantincrease in the adoption rate for SaaS [23]. Despite this upward trend, some organizations remain reluctant toadopt SaaS due to concerns that it does not provide the same coverage, reliability, and control as on-premise platform-based solutions. But an effective SaaS solution is entirelycapable of addressing these concerns. The introduction of a hybrid deployment model that has unified administration is an example of such asolution. This model enables the simultaneous deployment of on-premise and cloud-based services atdifferent points in the enterprise, providing comprehensive protectionalong with control via a single management interface [23].

5. CONCLUSION

Cloud computing is the powerful technology for delivering computing services like application software, storage, network bandwidth and computing power to the consumes on an as needed basis. This has been evolving and continues to evolve. The Software as a Service (SaaS) modeloffers customers significant benefits, such as improved operationalefficiency and reduced costs. However, to overcome customer concerns about application and data security, vendors must address above issues. Cloud computing is a new technique but security challenges are old one. We u se almost the same techniques of security in cloud computing as w e are using intraditional networks but difference is that cloud is a multi-tenant environment with more than one company sharing the same cloud service provider. Because of multi- tenant risk are severe and difficult to manage. Examples of previous "cloud computing" capabilities include hostedmainframes (more than 40 years), hosted file and mail servers (AT&T, IBM in the early 90's), and software services like SalesForce.com. The security of the cloud should be equalto the most risky client that theprovider has. The number of on demand application and usersincreases today so raises the security issues. So security should be placed onboth end (at service provider end and consumer end).

REFERENCES

[1]. F. Douglis, "*Staring at Clouds*",IEEE Internet Computing, pp. 4 - 6, June 2009.

[2]. G. Ling, D. Fu, J. Zhu and G. Dasmalchi, "*Cloud Computing: ITas a Service*", IEEE Computer Society, pp. 10 – 13, April 2009.

[3]. J. W. Rittinghouse and James F. Ransome, *Cloud Computing : Implementation, management and Security*. CRC Press, 2010. pp.26- 37.

[4]. http://www.saas- tenant.com/white-paper/Securing- SaaS-Applications.htm [Accessedon Nov 27, 2012]

[5]. http://www.networkworld.com/ne ws/2010/092710-software-as- service-security.html?page=1 [Accessed on Dec 16, 2012]

[6]. J. Chen, Y. Wang and X. Wang, *"On Demand SecurityArchitecture for Cloud Computing"*, Research Feature, Computer, IEEE ComputerSociety, pp. 73 78, July 2012.

[7]. R. L. Krutz and R. D. Vines, *Cloud Security:* A Comprehensive Guide to Secure Cloud Computing, W ileyP ublishing Inc. pp.62-85.

[8]. B. R. Kandukuri, R. Paturi V and A Rakshit. "*Cloud Security Issues":* IEEE International Conference on S ervices computing,2009. pp.517-520.

[9]. *Security Guidance for Critical Areas of Focus in CloudComputing V2.1*, Cloud SecurityAlliance (CSA), 2009. pp.14-19.

[10].*Cloud Computing Security*. A Trend Micro White Paper, May 2010. pp.2-10.

[11].*Introduction to cloud computing*, White Paper, Dialogic. pp.4-9. [12].U. Somani, et al., "*Implementing Digital Signature with RSAEncryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing"*, 1stInternational Conference on Parallel, Distributed and Grid Computing (PDGC - 2010). pp.212-213.

[13].W. Juang and Y. Shue. "*A Secure and Privacy Protection Digital Goods Trading Scheme in Cloud Computing"*.IEEE 2010.p.288.

[14].C.N. Hoefer and G. Karagiannis, *Taxonomy of cloud computing services*, IEEE.pp.1345-1348.

[15].*Cloud Computing: Silver Liningor Storm Ahead?* Volume 13 Number 2, Spring 2010. pp.4-8.

[16].DRAFT**:** *Cloud ComputingSynopsis and Recommendations.* NIST, U.S. Department of Commerce, Special Edition 800-146. pp.9-10.

[17].DRAFT**:** *Guidelines on Security and Privacy in Public Cloud Computing.* NIST, U.S.Department of Commerce, Special Edition 800-144. pp.11-15.

[18].D. Balfanz, S. Kirsch, R. Chow, S Matsumoto, O. Eisen, J.Molina, M. Jakobsson and P. V. Oorschot, *"The future of Authentication"*, AuthenticationTechnologies, IEEE Security and Privacy, IEEE Computer andReliability Societies, pp. 22-27, January/February 2012.

[19].J. M. Myerson, *The role of Software as a Service in cloud computing*, Developer works,IBM, 07 April 2009. pp.6-7.

[20].http://searchsecurity.techtarget.com/definition/Security-as-a- Service. [Accessed on 02, Feb2013].

[21].https://www.barracudanetworks.com/docs/White_Papers/Barracuda _Web_Security_Flex_WP_SaaSI mprovesSecurity.pdf. [Accessedon 02, Feb 2013].

[22].https://www.mcafeeasap.com/downloads/Docs/sb_saas_0410.pdf.[Accessed on 30, March 2013].

[23].http://www.websense.com/assets/ white-papers/whitepaper-seven- criteria-for-evaluation-security-as- a-service-solutions-en.pdf. [Accessed on 30, March 2013].