Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 3, March 2021, pg.66 – 71

A STUDY on SECURITY ISSUES in SaaS CLOUD COMPUTING

Adarsh G Prabhu[1]; Adithya Narayanan MV[2]; Claijo Kurian[3]
[1]Student, Dept. of Computer Applications, SNGIST ASC, MG University, India
[2]Student, Dept. of Computer Applications, SNGIST ASC, MG University, India
[3]Asst. Professor, Dept. of Computer Applications, SNGIST ASC, MG University, India
[1] adarshgprabhu21@gmail.com; [2] adithyanarayanan5856@gmail.com; [3] claijokurian@gmail.com
DOI: 10.47760/ijcsmc.2021.v10i03.008

Abstract — Cloud Computing is an Internet-based delivery of computing services, which include shared resources, software and data storage that are provided to the computing devices on demand. Cloud computing is very popular in distributed computing as well as used in our everyday. Cloud Services are provided on a leased basis and are mainly delivered by a third-party source which owns cloud infrastructure. Software as a Service (SaaS) is a software licensed delivery model that provides software through cloud. Saas has a feature of multi tenancy that virtually provides all the services at individual basis but physically all users can make use of the service at same time. In Recent Years, Saas has an increasing number of countries attention that promote SaaS Market. Even though SaaS provides attractive features, the Security Challenges are the main factor that makes SaaS in a critical situation. The Major Security Issues faced by SaaS include Data Confidentiality, Availability, Data Breaches, etc. In this paper we attempt to describe about SaaS Cloud Computing and Its Security Challenges.
Keywords — Cloud Computing, Software as a Service, Security Issues in SaaS, Data Segregation

I. INTRODUCTION

The term cloud is a historical metaphor used for the Internet and its usage was to represent the transportation of data from a carrier who owned the cloud o a repository at the other end of the cloud. Its concept was dated back as early as 1961 when Professor John McCarthy pointed out that "computer time-sharing technology might lead to a future where computing power and even specific applications might be sold through a utility-type business model"[3]. This idea was admired in the late 1960s, but by the mid-1970s the idea faded away. However, after a millennium, the concept has been modernized. It was during this time of modernization that the term cloud computing began to arise in technology circles. In a presentation entitled “Effectively and Securely Using the Cloud Computing Paradigm,” held in the National Institute of Standards and Technology (NIST) Information Technology Laboratory at October 2009 by Peter Mell and Tim Grance, cloud computing is defined as follows: "Cloud computing is a model for enabling suitable, on-demand network access to a shared pool of customizable and dependable computing resources that can be rapidly supplied and released with slightest consumer management effort or service provider interaction". In simple terms, it’s an on-demand distribution of computing resources over the internet ie; storing and accessing

data and information over the internet instead of computer hardware. Cloud Computing is getting high in favor day by day. Cloud Computing is capable to help organizations to expand and also safely transmit data from physical locations to the 'cloud' that can be accessed from anywhere[3]. There exist a number of characteristics in Cloud Computing that make it one of the rapid-growing industries at present. The adjustability offered by Cloud services has increased its deployment across industries. This cloud model is a collection of more than one characteristics three service models and four deployment models.
Fig 1. shows the characteristics of Cloud Computing. The 5 vital characteristics are:

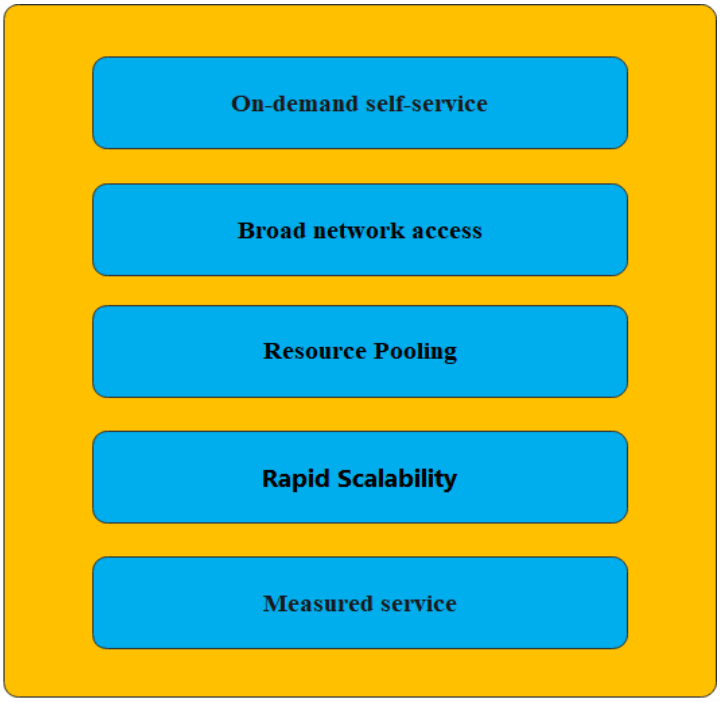

Fig. 1 Characteristics of Cloud Computing.

1.1 On-demand self-service
It is one of the notable and crucial features of Cloud Computing .It allow the client to always monitor the server uptime, abilities and granted network storage[8].This is a basic characteristic of Cloud Computing. Here, a client can also control the computing capacity as per his needs.

1.2 Broad network access
The big part of cloud characteristics is that its capacities are accessible all over. The customer can access or transfer the data to the cloud from any place within a device with a network connection. The resources are hosted in the private cloud. Cloud providers detect and guarantee different measurements that consider how clients access cloud resources and data through latency, access time, data throughput, etc.

1.3 Resource pooling
One of the indispensable characteristics of Cloud Computing[8]. Here, the cloud service provider can share resources among some clients, providing everyone with a dissimilar set of services as per their demands. It is a multi-client master plan that can be applied to data storage services, processing services, and bandwidth-provided services. The real-time processing in allocating resources to the administration process does not clash with the client's experience.

1.4 *Rapid scalability*
A key characteristic and benefit of cloud computing. This cloud typically enables low-cost running of tasks that need a huge number of servers but only for a short period of time. Clients with huge workloads, can run very cost-effectively because of the rapid scalability of Cloud Computing[3].

1.5 Measured service

It is the best choice for organizations. Measuring service is obliged for both cloud providers and their clients[8]. It enables both the provider and the customer to monitor and report what services have been used and for what purpose. This assists in monitoring billing and guarantees the best usage of resources.

The 3 service models are as follows:

A. Software as a Service (SaaS)

It is a "one-to-many" software delivery model that gives access to applications over the network service. The users can either install anything on their place or have to pay a substantial up-front cost to buy the software and the needed license[1]. They are naturally multi-tenant. The users don't have to control the fundamental cloud base including network, servers, operating systems, storage, etc. Updation is done automatically and it's Platform independent. The most popularly used saas are: Google, Google Drive, Microsoft Office 365, etc.

B. Platform as a Service (PaaS)

PaaS is a development and deployment platform for running applications in the cloud It is made up of a programming language environment, an operating system, a web server, and a database. The users will manage data and the application resources while the other resources are managed by the vendor. PaaS is scalable and low in cost as well as Domain for developers[5]. Popular PaaS providers are: Windows Azure, Heroku, Google App Engine, etc.

C. *Infrastructure as a Service (IaaS)*

Most popular and grown market section of cloud computing. IaaS hires processing, storage, network capacity, and other basic computing resources. Its service offers the computing architecture and infrastructure as well as virtual computing resources so that various users can access them. Its mainly used by system Admins. Popular IaaS used will be - Amazon EC2,GoGrid etc.

The 4 deployment models are as follows:

A. Public cloud

The public cloud is defined as computing services supplied by third-party providers through a public network, making the services obtainable to anyone who wants to utilize or buy them. Any customer can easily sign in with the cloud that may be free of cost or bought on-demand, allowing consumers to pay only per usage. Historically, the public cloud where the first class of cloud that was put into action. Some of the most popularly used public clouds are: Google Drive, Gmail, Microsoft Azure, etc.

B. Private cloud

Private cloud is an internal or corporate cloud offering computing services through the Internet only to selected users instead of the general public, private cloud consists of self-service, scalability, and elasticity - with the extra control and customization accessible from dedicated resources. Additionally, private clouds provide a high level of security and privacy to ensure operations and sensitive data are not accessible to third-party providers. Some of the most popularly used private clouds are: HP Data Centers, Microsoft, Ubuntu, etc.

C. Hybrid cloud

A hybrid cloud is a combination of both the public as well as the private cloud. It is a heterogeneous distributed system because the private cloud integrates additional resources from one or more public clouds. It's more flexible to use and is of less cost than private cloud by helping the organization to save cost. Due to the critical activities provided by the private cloud, we can say that it is secure. Some of the most popularly used Hybrid clouds are: Amazon, Microsoft, Google, etc.

D. Community cloud

A community cloud is a cloud base that allows systems and services to be available by a group of organizations to share information[9]. It is owned, managed, and operated by one or more companies or a combination of them in the community. Since the whole cloud is shared between organizations it's cost-effective and is flexible and scalable because it's compact to every user. When it comes to security it is less secure than private and more secure than public. Some of the used community clouds are: Multiple government departments, U.S Federal agencies, etc.

II. SECURITY ISSUES IN SAAS

Software as a Service (SaaS) is cloud deployment model which provides application services on demand such as conference applications and business application like ERP, SCM, and CRM. In the SaaS model, the client depends on the cloud service provider for security. In SaaS, the user's data is stored at the vendor's or provider's end and this raises many security concerns and trust issues. SaaS is sure likely to remain a superior cloud service model for the near future and the area where the most critical need for security measures and oversight will reside[3]. Fig 4, shows the most common security issues faced by users in the SaaS model.

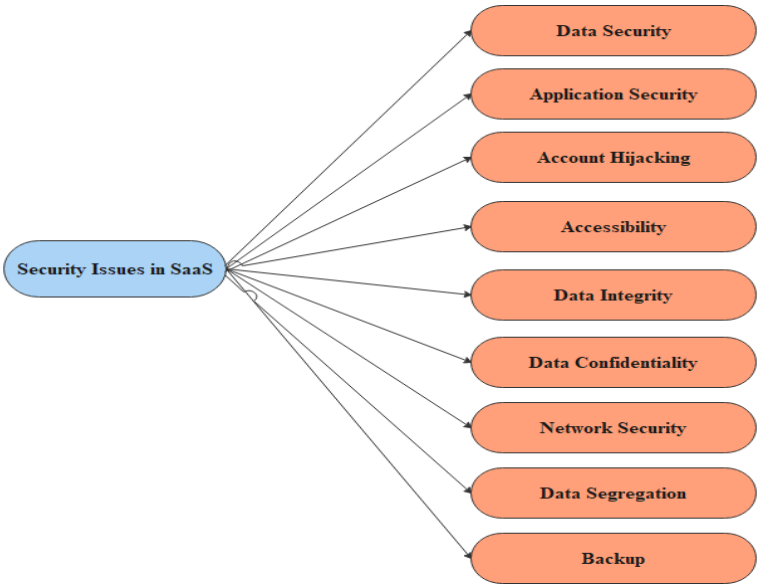

Fig 2. Security Issues in SaaS Model.

2.1 Data Security

Data Security is the most crucial challenge for any cloud model. Saas users have to rely on the security features given by their cloud service providers to ensure the data is protected. In the Saas service model, the data is stored in the provider's data centers and firewalls are used to protect this sensitive information. Furthermore, these providers need to raise additional security against data breaches caused either done by malicious software or employees[7]. It is the Cloud service provider's responsibility to ensuring a secure cloud environment.

2.2 Application Security

Cloud Applications are mainly delivered through web browsers. Hackers often use web means for attacking user's computers for doing malicious activities such as stealing private information[1]. Lack of security in the web application may create Saas applications vulnerable.

2.3 Accessibility

One of the major merits of Software as a Service is that it can be accessed where ever there is internet connectivity through mobile devices and computers. Even though it increases the convenience of the user but it also poses a great risk[7]. The Cloud Security Alliance(CSA) has released a report regarding mobile computing and its threats such as malicious malware that can steal information, insecure networks, proximity-based hacking, and flaws in the device operating system.

2.4 Data Integrity

Data Integrity guarantees that data is uncorrupted and can only be accessed and modified by an authorized person. It is defined as "a level to which a collection of data is complete, consistent and accurate". Maintaining data integrity is critical to ensure data can be used for making a good choice and deliver a top-quality product. Data Integrity can be achieved by ensuring data meets the principle of ALCOA (Attribute, legible, contemporaneous, original, and accurate).

2.5 Data Confidentiality

Data Confidentiality is defined as preventing the disclosure of information intentionally or unintentionally. The cloud storage environment includes intellectual property rights sites, hidden channels, traffic analysis, encryption, and capture[1]. Cloud computing involves sharing or storing information on remote servers owned or used by others while accessing the Internet or other communications. There are variations in cloud computing services. including data storage sites, video sites, tax preparation sites, health recording websites, and much more. All contents of a user storage device can be stored with one cloud provider or with multiple cloud providers. Privacy and confidentiality are essential whenever an individual, business, government agency, or other organization shares information in the cloud.

2.6 Account Hijacking

There might be a risk that users' accounts might get hijacked or stolen through malicious and unauthorized acts by hackers. They might do this for personal gain, manipulate user data or provide false information. In SaaS, anyone can register as a cloud service user so the chance of an account getting stolen is very high[7].

2.7 Network Security

In the SaaS cloud model, the sensitive information is available from enterprises through the Saas application and they are stored at the SaaS provider's end. These sensitive data are accessed through the network and therefore needed to encrypt the data flow in the network to avoid leaking of data. The common encryption techniques used for network traffic include Secure Socket Layer(SSL) and Transport Layer Security(TLS).

2.8 Data Segregation

Multi-tenancy is a crucial component of cloud computing. Due to multi-tenancy, multiple users can store their data by using the applications provided by SaaS Provider. In these cases, the data of multiple users will be stored at the same location. Because of this Intrusion of private data of a user by another user becomes possible[4]. It can be overcome by injecting client code. A SaaS model should therefore ensure a clear limitation for each user's data. This restriction must be ensured not only at the physical level but also at the application level. The service should be efficient enough to segregate data from different users.

2.9 Backup

It is the SaaS provider's responsibility to ensure that all the sensitive data is backed up regularly in order to smooth the recovery process in case of any failure. The traditional backup methods were used for applications and data centers that were primarily designed for web and consumer applications but they are not optimal backup methods for cloud applications[6]. Also, it is necessary to use a strong encryption method to store backup data to avoid unexpected leakage of sensitive data. Some cloud service providers like Amazon do not provide this encryption by default. So, Users have to independently encrypt data to restrict unauthorized access from others.

III. CURRENT SECURITY SOLUTIONS

In terms of the security of cloud computing, there are numerous researches and tests happening around us. Many organizations are developing several applications and security standards for cloud security. Among them, the Cloud Security Alliance(CSA) is gathering solution providers and individuals to enter into a discussion about the current and future best measures for data assurance in the cloud system. CSA is a non-profit organization with the objective to promote the use of best practices for providing security assurance in the cloud environment[1]. The optimal and simplest security solution for SaaS applications is to develop a development framework that has tough security architecture.

To avoid the access of data from other users, applying cryptography on data that makes data totally unuseable and normal encryption can complicate availability. Before uploading data into the cloud the users are recommended to verify whether the data is stored on backup drives and that keywords in files remain unmodified. The data can be secured with digital signatures with the RSA algorithm. It is claimed that RSA is the most recognized cryptographic algorithm and is capable of securing data in the cloud environment[7]. Another approach for securing data during processing is resource isolation, i.e., by isolating the processor caches in virtual machines and isolating those virtual caches from the hypervisor cache. CSA has issued a report called Identity and Access Management Guidance, which issues a list of best practices for identity and secure access management[5].

IV. CONCLUSION

In this paper, we tried to present an overview of Cloud computing, Software as a Service, and its security issues. Cloud computing is a very broad concept in the field of information technology, even though it provides many great advantages but it also poses numerous security issues. Cloud doesn't have stable security for all the security issues and these security concerns are the reason that keeps new users away from the cloud. Users are concerned about their privacy and security when comes to cloud usage.

REFERENCES

[1]. Navneet Singh Patel and Rekha B.S, *Software as a Service (SaaS): Security issues and Solutions*, International Journal of Computational Engineering Research *(*IJCER*)*, Vol.4 Issue 6, June 2014.

[2]. Jon Brodkin**,***5 problems with SaaS security*. [Online]. Available: https://www.networkworld.com/article/2219462/5-problems-with-saas-security.html.

[3]. John W. Rittinghouse and James F. Ransome, *Cloud Computing Implementation, Management, and Security*,Taylor and Francis Group LLC,2010.

[4]. Aized Amin Soofi,M.Irfan Khan,Ramzan Talib and Umer Sarwar, *Security Issues in SaaS Delivery Model of Cloud Computing*, International Journal of Computer Science and Mobile Computing (IJCSMC),Vol. 3, No.3, pg.15 – 21,March 2014.

[5]. Cloud Security Alliance, *Guidance for Identity & Access Management*,Sept. 2012, Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf.

[6]. Ronald L. Krutz and Russell Dean Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*,ISBN: 978-0-470-58987-8

[7]. Keiko Hashizume,David G Rosado,Eduardo FernándezMedina and Eduardo B Fernandez, *An analysis of security issues for cloud computing*, Journal of Internet Services and Applications ,Vol. 4 No. 5,2013.

[8]. Isha Upadhyay, *Top 10 Major Characteristics of Cloud Computing*. [Online]. Available: https://www.jigsawacademy.com/blogs/cloud-computing/characteristics-of-cloud-computing/

[9]. Dejan Tucakov, *What is Community Cloud? Benefits & Examples with Use Cases*. [Online]. Available: https://phoenixnap.com/blog/community-cloud

