International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

Vol. (1), No. (2) December, 2022 الإصدار (1)، العدد (2)

"Critical Requirements Engineering for Software-as-a-Service"

Nesma El-Sokkary
M.Sc. of Information Systems, Cairo University, Egypt
nesma.elsokary@gmail.com

Walaa H. El-Masry
M.Sc. of Information Technology, Cairo University, Egypt
welmasry1611@gmail.com

Abstract:

In the Software evolution, the requirements phase is the first and most critical software engineering task. This phase is a stakeholders-dominated phase and is based on the transformation of the ideas or views into a documented requirement. Fulfillment the stakeholder's requirements in a clear and unambiguous manner is the first essential step to achieve a high-quality- product. With the Software-as-a-service (SaaS) business model, where the target is recurrent releases and continual delivery of improved services, the associated requirements become even more important. Now, more than ever it shows the importance of real communication and discussion, focusing always on the most important issues and most important stakeholders only. Furthermore, keeping the vision up to date and clear for the whole duration of a system development project. In this paper, we attempt to answer the question "What are the specific requirements that should get priority during the requirements Engineering of SaaS?"

Keywords:

Cloud Computing; Software-as-a-Service; Requirements Engineering; Stakeholders.

1- Introduction

Cloud computing is the most brilliant innovation of technology of the 21st century because of its importance in every field you can imagine. Cloud is becoming a top item in the C- suite agenda as companies are seeking to transition of a piece- meal approach to a more comprehensive end-to-end digital transformation with Cloud at its core. Tomorrow's winners, who can cope with this change rapidly, make the best choices and take part with the appropriate partners to increase their own capabilities. Cloud transition requires speed, new thinking, and involving in different levels of skills and investments to achieve end-to-end digital transformation. Now, more than ever, cloud technology is vital to help companies innovate, adapt to speed and scale, drive business agility, streamline operations, and reduce costs. As well as managing big data, cyber-security and quality control, emerging technologies such as Artificial Intelligence and many other capabilities are becoming available as services through cloud computing.

Cloud computing is a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources such as - servers, networks, storage, development tools, and even applications - that can be rapidly de- livered with a minimal management effort or service provider interaction [1]. It allows storing, accessing data and programs over the Internet instead of our computer's hard drive [2].

Cloud computing model is composed of four deployment models—public cloud, private cloud, hybrid cloud, and multi- cloud. Each one of these models has its own scope of services that presented to the users. The uses of Cloud Computing deployment based on different factors, such as customization capabilities, cloud services sharing, security requirements and location the services hosted [3]. Public cloud is a service run by an external vendor that may include servers in one or multiple data centers. Public clouds are shared by multiple organizations. Using

virtual machines, individual servers may be shared by different companies, a situation that is called "multitenancy" because multiple tenants are renting server space within the same server. Private cloud is a server, data center, or distributed network wholly dedicated to one organization [4]. A higher security and privacy are delegated by private clouds through the firewall and internal hosting [5]. Hybrid cloud deployments combine public and private clouds. An organization may use their private cloud for some services and their public cloud for others, or they may use the public cloud as backup for their private cloud [5]. Multi cloud using multiple public clouds. In other words, an organization with a multi-cloud deployment rents virtual servers and services from several external vendors [6]. Multi cloud deployments can also be hybrid cloud.

As well as three service models —Saas (Software as a Service), Paas (Platform as a Service) and Iaas (Infrastructure as a service) [7] as shown in [Figure 1: Cloud Service Models].

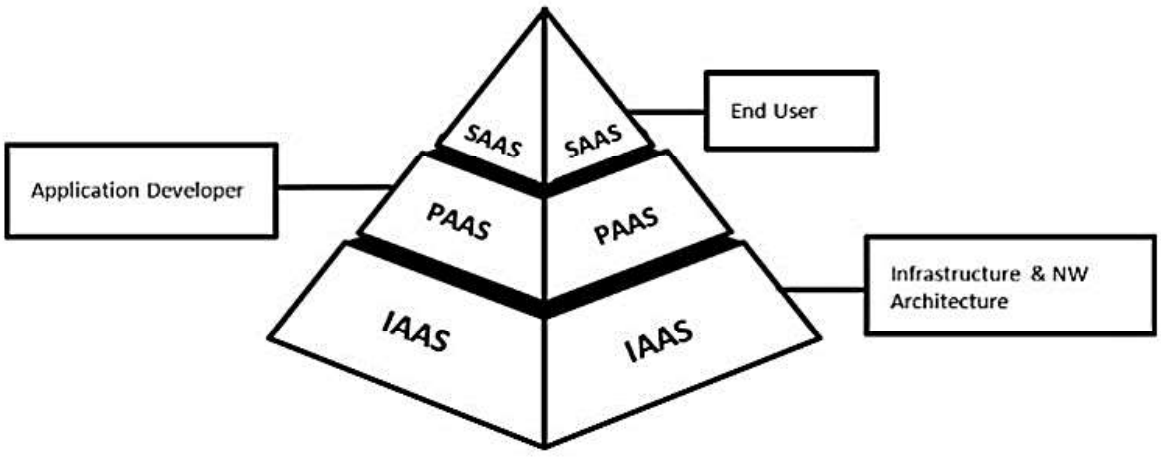

Figure 1: Cloud Service Models

Cloud service providers are responsible for running and maintaining application software, operating systems, and other resources. Infrastructure-as-a-Service (IaaS) model provides many resources like raw based storage, load balancers, virtual local area networks, IP addresses and software bundles [4]. a company rents the servers and storage they need from a cloud provider. They then use that cloud infrastructure to build their applications. IaaS examples: DigitalOcean, Google Compute Engine, and OpenStack.

In Platform-as-a-Service (PaaS) model, allows organizations to develop, build, and deploy their applications to support their own specific business needs [8]. Companies pay for the things they need to build their own applications. PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet. Such as Microsoft Azure, Salesforce.

Software-as-a-Service (SaaS) is a cloud-based distribution model for providing software to users. SaaS users can subscribe to an application instead of purchasing and installing it. Users can access SaaS through a web browser or application program interface (API) from any compatible device like smart phones and laptops etc. through the Internet [9].

An enormous number of organizations consider SaaS important because of its advantages that the customer does not need to buy licenses to get a service but can rent it, install, upgrade, maintain or run software [10]. As well as other advantages such as multi-tenancy that is considered one of the most significant concepts for any SaaS applications, reduce cost, configurability, and scalability [11]. Also, there are other benefits of SaaS such as Rapid Scalability, Accessibility from any location with Internet, Eliminates infrastructure concerns, Custom levels of service offerings and Bundled maintenance and Support [2].

Software as a Service (SaaS) is being increasingly adopted by firms for gaining business application software. This model differs from the traditional 'on-premises' model. In traditional model, software is traditionally owned, hosted and managed by the firm, while in SaaS it is owned, hosted, and managed by external providers and delivered to the firm through the Internet as a service [12].

The difference between traditional software applications and SaaS applications gives a rise to a different direction of requirements in the sense of operations and management, architecture, security and privacy, compliance, and quality. This implies that new requirements that have never been experienced before in software evolution have to be taken into consideration and focus on it [13]. The principal goal of requirements engineering process is to develop and as well as managing the requirements, gathering and defining service provided by the system to identify changes and irregularities between the project outcomes and the requirements. To make SaaS better in quality, we must focus on these key requirements to be considered and discussed at early stages, when requirements engineering team struggle to accomplish improved quality, shorter delivery deadlines and reduced requirements engineering cots. When referring to requirements related to an information system, we usually mean requirements originating from customer-side stakeholders. These requirements represent the views and needs of the people at the business or enterprise operations level, covering end-users, acquirers, customers, and a number of other stakeholders.

The requirements are recorded to solve the stakeholders' problems. These problems to be solved vary in their nature, and often the different stakeholders perceive the situation in very different ways. What makes the matter even more complicated is the set of requirements for fulfilling the stake- holders' needs. It typically has a strong connection not just to the domain that the stakeholders represent, but also to the history and to the environment, in which the system is to be operational. System

requirements are naturally closely related and connected to the customer-side requirements. But they ought to be written in a language that is clear, unambiguously and understood by system designers, developers, testers, as well as other people that work on the system provider's side. Perfectly, system requirements supplement the original end- user requirements and provide heavy understanding on what the system needs to be capable of doing. Making stakeholder and system requirements meet, appears to be the hardest and the most critical part of the development of any larger information system [14].

2- Related Work

Requirements Engineering (RE) is the process of finding, documenting, and administering the requirements for a computer-based system. The goal is to obtain a set of specifications, as the first stage in the system development process, to shape the foundation for more design and development of the desired system. Requirements engineering is a crucial phase at the beginning of every product development to define the scope of development together with customers [4].

Requirement Engineering is a set of different process that works at different levels, which are incorporated at individual and organizational level Projects [5]. Requirements engineering is the process of eliciting stakeholder needs and desires and developing them into an agreed-upon set of detailed requirements that can serve as a basis for all subsequent development activities [6]. Requirements engineering has become an important research topic in the field of software engineering. Particularly, with the efflorescence of the cloud computing paradigm, evolutions in social media and service computing, potential challenges of the requirement engineering process have grown in complexity and numbers. The new software systems which are anticipated to be scalable, able to be used on all variety of multiple platforms, containable, failure safe, and, in general, appropriate for distributed computing environments. Now, software is being diffused as Web services and as

software-as-a-service (SaaS) to be used by users on a wide variety of diversity smart devices, through the Internet protocols.

Some authors propose frameworks and methods, but there is no available empirical evidence on the elicitation methods utilized by cloud providers [15]. For instance, Chung, Lawrence, et al. proposed a goal-oriented simulation approach for cloud-based system design whereby starts with the eliciting and understanding of multiple stakeholders' goals, together with such domain characteristics as workflows, and utilized in generating a simulation model as a proxy for the cloud-based system architecture. They also use as the means of estimating the effect of design choices on the degree to which the different goals are satisfied. After a number of iterations, the result is approaching a design which may then be tested in a real cloud deployment [7].

Ramachandran and Muthu presented methods, techniques, and best practice requirements engineering and management as an emerging cloud service (SSREMaaES) and also, they introduced guidelines on software security as a service. They also debated an Integrated-Secure SDLC model (IS-SDLC), which will assist practitioners, researchers, learners, and educators. In addition, they are proposed software security requirements engineering and management as an emerging service (SSREMaaES). Which have potential to variation the method software has been developed traditionally and presents tools and techniques as a service which can be developed and shared with distributed stakeholders [8].

Abuhussein, Abdullah, et al. presented an approach to increase cloud qualities in existing requirement engineering processes and facilitate building SaaS with cloud qualities in mind. The proposed cloud requirements engineering approach depend on determine the number of cloud qualities to be used in SaaS and consequently handles any situated shortcomings. The proposed augmentation allows software engineers to collect and determine requirements with cloud qualities in mind, which makes

determining and remembering cloud-concerning features while grouping and articulating cloud application requirements less complicated. They are also presented sets of questions that software engineers can utilize when eliciting cloud-specific requirements [9].

Mouratidis, Haralambos, et al. presented a novel security modeling language and a group of original analysis techniques, for capturing and analyzing security requirements for cloud computing environments. The new in their proposed language lies in the combination of concepts from cloud computing, with concepts from security and goal-oriented requirements engineering to elicit, model and analyze security requirements for cloud infrastructures. Also, they are proposed three analysis techniques, which support an automated process where given a model of a cloud computing system, developed with the proposed language, will promote the model with new security knowledge, for example threats and vulnerabilities, alleviation strategies and assets and actor responsibilities [10].

3- Software as a Service

The SaaS model can be viewed as an evolution of the application services provision (ASP) model. SaaS goes one step further than ASP and is based on the use of multi-tenant architectures, enabling the sharing of infrastructures, and thus creating economies of scale. SaaS compromises the highest level of Cloud Computing (CC) services. SaaS ranges from simple office automation to more complex enterprise resource planning (ERP) and customer relationship management (CRM) applications[16].

With SaaS model, a single version of the application, with a single configuration is used for all customers (tenants). To support scalability, the application is installed on multiple machines which called horizontal scaling. In some cases, a beta version of the application is set up to offer accessing to pre-release versions of the applications

for testing purposes. Saas solutions represent many applications in the market of cloud, it can be divided into two main categories:

- Vertical SaaS: a software which targeted to the needs of a specific industry (e.g., software for the healthcare, agriculture, real estate, finance industries)
- Horizontal SaaS: the products which focus on a software category (marketing, sales, developer tools, HR). It can cover many industries and wide range of market [17].

The application architecture of SaaS (on-demand) cloud service is shown in [Figure 2 : Application Architecture of SaaS in Cloud Computing]. It consists of four layers [18]:

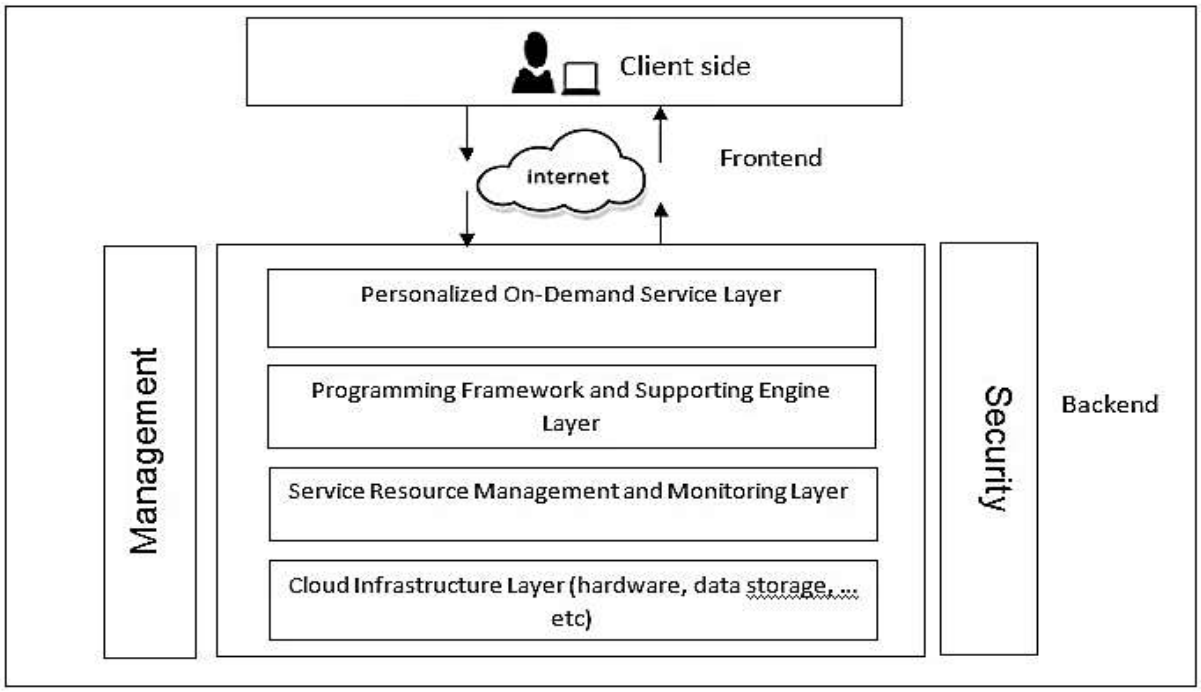

Figure 2 : Application Architecture of SaaS in Cloud Computing

1. Infrastructure Layer: It's responsible for providing multiple cloud centers involves controllable internal clouds. As well as supporting many resource types including hardware and software such as hard disk capacity, the size of RAM, CPU and so on. The cloud platform pools these resources to provide unified cloud services for upper-layer system modules and applications [19].
2. Service Resource Management and Monitoring Layer: The resources that provided by the infrastructure layer can be registered into the service resources management. In this layer, the client can ensure that he can get an appropriate platform for his application to do his purpose like deployment, development, hosting of web application, and testing [19]. Depending on different monitoring and management demands, specific resource models, management attributes, and monitoring policies can be defined to ensure scalability in resource management and monitoring [18].
3. Programming Framework and Supporting Engine Layer: This layer supports service programming according to the basic platform and service resources. It also provides engine support for service operation. In this layer, predefined service templates, visualized manual service composition, and automatic on-demand service composition for dynamic, large-scale environments is implemented. Efficient and reliable combining of applications for large-scale concurrency is also implemented.
4. Personalized On-Demand Service Layer: This layer determines how on-demand cloud services are provided to users. It determines how to support users in describing their demands and identifying resources. As well as defining the state of available resources and user scenarios to provide services that are adaptable to information changes. The applications in this layer can achieve the automatic scaling to do a maximum performance.

4- SaaS Stakeholders

In a traditional computing system, the major stakeholders are the providers and customers: the customers use, own, maintain, and upgrade the systems while the providers deal with the sale, installation, licensing, consulting, and maintenance of the technology concerned. Cloud computing variations the turns of the traditional stakeholders and adds new ones. These stakeholders include not only the providers and the customers of the service, but also, due to the singular nature of the delivery model for the service, the organizers who need to understand the effect of the location of the infrastructure of the service providers. We discuss these stakeholders in detailed in this section.

4-1 Cloud Consumers / End User

They are individual users and organizations that hoard their data in the cloud data center and dependence the service provider for data Computations. In the other word, the consumer in cloud computing is a human or an organization that has an official contract or settlement with a cloud provider to use information technology resources made available by the cloud provider. Specifically, the cloud consumer uses a cloud service consumer to access a cloud service [20]. In a cloud computing environment, the consumers are effectually subscribers, who now only purchasing the use of the system from the providers on an operational cost base. efficient use of cloud computing's possibilities will minimize the stress on the information technology departments as they become consumes less time in maintaining systems and more effective in improving and developing innovative applications for the organization [21].

4-2 Cloud Service Provider / Cloud user

A cloud service provider, this is the organization that own the fundamental resources and experience for managing the distributed cloud storage servers and offers some component of cloud computing usually infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals. A cloud computing service provider possesses and operate cloud computing systems to present service to third extremities. The providers will perform the maintenance and the improvements on the system which consumers were in responsible for it when they owned the systems. They will also be in charge of maintaining the software utilized on the cloud, in addition determining prices of the cloud services. Most cloud computing provider companies today have been large scale datacenters and software infrastructure[22].

4-3 Enablers / Cloud Provider

Cloud enabler refers to the technologies and manufacturers that do as the backbone for all cloud computing services and products. A wide term including technology sellers and solutions, a cloud enabler allows an organization to construct, deploy, combine, and deliver cloud computing solutions. The term ‘enablers’ describe those organizations that will provide products and services that simplify the delivery, adoption, and use of cloud computing. Cloud enablers are primarily information technology companies that evolve hardware, software, networking, storage, and other concerning product serving as a cloud environment component. For example, an organization that develops virtualization hypervisor cans the development of virtual machines, virtual private servers and other virtualization-based cloud solutions. A cloud enabler differs from a cloud service provider, as the cloud service uses technologies constructed by the cloud to deliver cloud services to end users and other organizations [23, 24].

As shown in figure [

Figure 3: SAAS Stakeholders] cloud providers optimize the usability of their own technology infrastructure offering storage solutions (hosting) and computer services (outsourcing), and cloud consumers pay for cloud services taking into account the type of service charge (i.e., pay per use, subscription, etc.) [15].

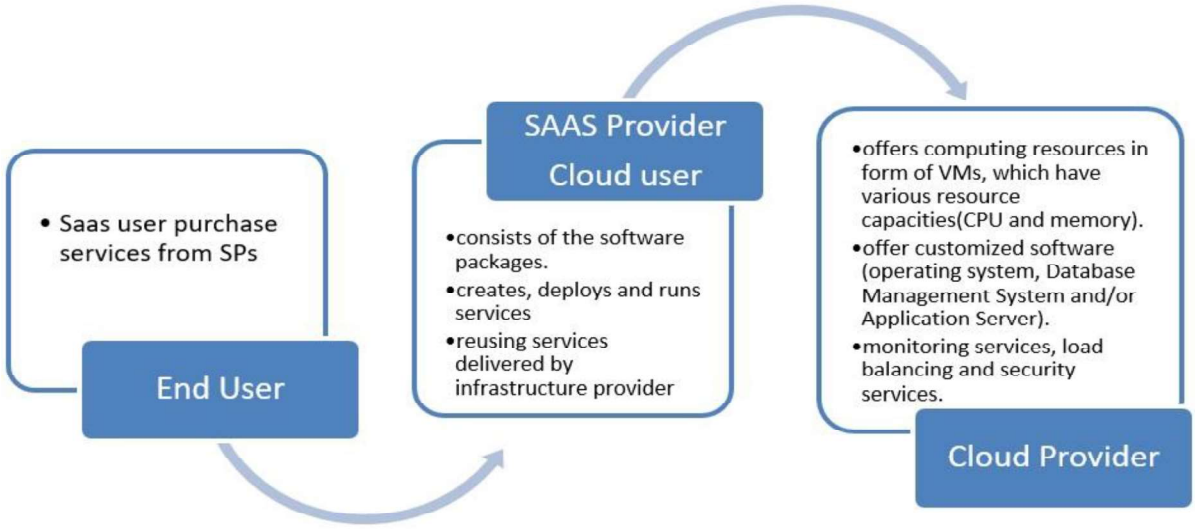

Figure 3: SAAS Stakeholders interactions

5- Requirements of SaaS Stakeholder's Perspective

The purpose of this contribution is to understand the components of a service and determine guidelines to requirements engineering for software as a service. Consequently, cloud services are seen by different aspects called dimensions. Six dimensions are proposed security and privacy, compliance, multitenancy, quality of service, architecture, management. Each dimension has its specific entities,

properties, and relationships. The proposed dimensions support the clarification of the requirements that determine specifications that clients need, and capabilities owned by providers into cloud computing. Requirement is what SaaS clients want from cloud service and the capability that is what SaaS cloud providers offer related to their efficiency in cloud services.

Requirements can be classified into functional and non-functional requirements. Functional requirements are capabilities that the product must do to satisfy specific user needs. Non-functional requirements are qualities that the product must have. Nonfunctional requirements are no less vital than functional requirements. Most of the requirements of SaaS are non-functional requirements. Non-functional requirements (NFRs) describe the general characteristics of a system. They are also defined as quality attributes (e.g., usability, reliability, security). They are not easy for stakeholders to articulate but they know that the software will not be usable without some of these non-functional characteristics [25].

5-1 Security and Privacy

Security refers to information security, which means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [2]. SaaS users have less control over security. Most of the Cloud providers know that the major problem banning the cloud computing adoption is security. So, the adoption of SaaS applications may raise some security concerns.

5-2 Cloud user (CU)

The CU is the most affected stakeholder if any kind of breach happens over cloud. The major challenges for CU are [26]:

- Secure access to the services: the main concern of CU is to access the services in a secure way and will share services only to the trusted entities.
- Data security: the user is always interested in the updating of its own data, but this concern is also subject to the unauthorized access also.
- Confidentiality: is defined as a set of rules that prevent unauthorized user from accessing sensitive information [27].because the data of CU are handled by third party and it has full control on data. If any type of attack happens, then the confidentiality will be breach.
- Data control: certain level of control on data in cloud.
- Service availability: the cloud-based services taken by the user should be available all the time and at all places.
- Interoperability: if the CU has any problem or dissatisfaction with vendor, then there should be a flexibility to migrate from one vendor to another. But generally, they face vendor lock-in problem.
- Trust between CU and CSP: the CU should have trust on CSP that he is giving secure services with all security measures. However, it is difficult to make this kind of trust between CU and CSP and for CSP to provide 100% secure services.
- Application security: flaws in Web applications may create vulnerabilities for the SaaS applications. Attackers have been using the Web to compromise user's computers and perform malicious activities such as steal sensitive data [28].

5-3 SaaS Provider / Cloud Service Provider

CSP is responsible for delivering cloud services to the CU [29]. The major threats and challenges for CSP are [26]:

- Eliminate internal threats—there can be a threat of hacking internal servers, leaking data either by intension, or un-intentional by internal employees.

- Secure administrator access rights—CSP is responsible for defining access of administrator rights to the trusted employees only.
- Sharing environment security—many users access same services. There should be proper maintenance of confidentiality, integrity, and authentication (CIA).
- Continuity in services— how a business will continue operating during an unplanned disruption in service. CSP needs to aware with the different type of attacks, which can disrupt services of the CSP to CU.
- Independence in software components—CSP has to make sure that if there is any security problem found in one software component, it should not affect to another.
- Accessibility: Getting to applications over the Web by means of Internet browser makes access from any system device, including open PC and cell phones [28].

5-4 Compliance

The expression of cloud compliance refers to the necessity that cloud-delivered systems must be in line with internal and external regulations. This compliance must be clear and auditable for regulators. Compliance can be defined in terms of a principle that enforces rules that implement the policies. These policies are nothing but the constituent of regulations. The compliance is the responsibility of the organizations and the service providers [30].

The consumer's requirements with respect to compliance are to ensure personal data protection and trust in those responsible for controlling and process their private data. Also, the Cloud providers must guarantee applied the following Data protection principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. More specifically, the personal data of the data subject must be processed according to the law requirements, in a fair and transparent manner.

Finally, integrity and confidentiality should be reassured to avoid unauthorized or unlawful processing or/and accidental loss, destruction or damage [31].

5-5 Quality of Service

Quality of Service plays an important role in distributed computing for multimedia and other essential applications. In Cloud Computing the term Quality of Service refers to the levels of availability, reliability and performance given by the infrastructure and by the platform and or an application that hosts it. It is major for cloud consumers, who wait from cloud providers to deliver the high level of the quality, and for cloud providers, who needs to find the right tradeoffs between operational costs and Quality of Service levels[32]. Quality should be linked to requirement, to denote that requirements should be there. There are many factors that will impact the quality of a system or application such as flexibility, maintainability, readability, performance, efficiency, scalability, availability and robustness, usability, and accessibility.

Quality of Service refers to the ability of networks to attain maximum bandwidth and handle other network elements like latency, error rate and uptime. Quality of Service include the management of other networks resource by allocating priorities to specific type of data (audio, video, and file).

Scheduling, admission control and dynamic resource purveyance are some techniques utilized to achieve more quality of service to the cloud SaaS applications[33].

5-6 Multi-tenancy

In cloud computing, multitenancy means that more than one heterogeneous tenant shares the single instance of the application. It increases the degree of resource sharing among tenants and brings down the operational cost [34]. Despite the reality

that they share resources, cloud consumers aren't knowing of each other, and their data is preserved totally disconnect. Multitenancy is a critical component of cloud computing; without it, cloud services would be quite less practical. Multitenant architecture is a feature in many types of public cloud computing, including IaaS, PaaS, SaaS. It's very important for evolving cloud computing application. Multi-Tenancy occurs when two or more virtual machines (VMs) belonging to different consumers share the same physical machine [35].

In Software as a Service (SaaS), applications are provided as a service by the Cloud Service Provider (CSP) where the consumer cannot observe or control the implicating infrastructure; here, Multi-Tenancy means that two or more consumers use the same service or application provided by the CSP regardless of the fundamental resources. This approach enables more efficient use of the resources. Because of data from multiple tenants are stored in the same database, there is a high risk of data infiltration between these tenants. So, security and privacy policies are needed to ensure that the data of the customers are stored independently from other customers [36]. The multitenancy concerns are as follows: privacy, dependability, reality, resource sharing, security, and profitability.

5-7 Architecture Requirements

SaaS customers concentrate on what services are provided rather than how these services will be provided. So, the cloud provider decision relies on the cost and performance according to the SLA. Make decision for using public, private or hybrid cloud. Most important issues while architecting for the cloud are networking and data management. As well as scalability, development complexity, not balanced workload and lack of availability [37]. Also include details about the reusable SaaS services, API requirements, and secure, disaster tolerant data centers. The architecture must have features like fault tolerant, comprehensive redundancy and uptime and fail over strategies [13] .SaaS architecture should permit restoring data

of one user without effecting other's data, minimum interruptions during upgrades as well as include Varying Levels of service agreements (SLA). SaaS architecture should be slowest cost, best reliability, and highest performance.

5-8 Scalability

Scalability is the ability of the cloud-based system to increase the capacity of the software service delivery by expanding the quantity of the software service that is provided when such increase is required by increased demand for the service over a period during which the service is exposed to a certain variation in demand for the service. Scalable cloud architecture is made possible through virtualization. Unlike physical machines whose resources and performance are relatively set, virtual machines (VMs) are highly flexible and can be easily scaled up or down. They can be moved to a different server or hosted on multiple servers at once. Third-party cloud providers also have all the vast hardware and software resources already in place to allow for rapid scaling that an individual business could not achieve cost-effectively on its own[38] .A scalable system provides several benefits, here are the most important ones:

- Highly customizable infrastructure according to specific customer's needs.
- Possibility of increasing or decreasing the system power according to the needs of the moment and the customer's availability.
- Scalability ensures a minimum service level even in case of failure [Xiao, Peng.].

5-9 Management Requirements

SaaS management is the business practice of pre-monitoring and managing the purchasing, licensing, and renewals of all the SaaS applications to a company's technology. The target of SaaS management is to reduce risk from unmanaged tools

or technologies, improve the value of purchased software, and increase the effectiveness of users who deploy SaaS applications.

Management requirements encompass many diverse processes. It may include administration- a central location to view and manage any data associated with SaaS products at an organization, license management, policy management, role-based access - The ability to restrict access rights to software based on user's needs and IT workflow automation. As well as centralized reporting- composed of records that contains necessary information to management, provisioning- It refers to the steps required to manage access to data and resources and make them available to users and systems. Also, monitoring and auditing SLA management, tenant management, plan SaaS renewals, capacity, data management and load balancing.

Efficient SaaS management means having a complete system of record of all SaaS apps, licenses, vendors, users, and compliance data, plus the workflows and automations to be sure that every is recorded for auditing.

Many organizations attempt to adopt to SAAS in various fields because of its low cost, high availability, and scalability features. But there are many problems such as infrastructure, accessibility, and monitoring potency. However, moving data to the cloud implies shifting control of the customer's data to the cloud service provider indefinitely. This paper attempts to identify and categorize a list of attributes shown in Table [**Error! Reference source not found.**] which depict the six aspects of r equirements for SAAS according to stakeholder's perspective. There are many requirements attributes that are critical for more than one stakeholder such as security, availability, reliability, scalability, efficiency, SLA compliance. These attributes consider the most critical requirements for any software as a service to be succeeded.

6- Conclusion

The cloud dimensions are explained in this paper and the attributes Characteristic of each one. Also, the SaaS model are viewed in detailed and two main categories of applications in the market of cloud that represent SaaS solutions they are Vertical SaaS and Horizontal SaaS. We also present the major stakeholders in SAAS cloud computing and clarified specific needs for each one of them as well as the requirements and priorities, and clarified the role played by each stakeholder in cloud computing architecture. our contribution in this paper is to understand the components of software as a service and determine guidelines to requirements engineering for SAAS. Consequently, cloud services are seen by different aspects called dimensions. Six dimensions proposed are security and privacy, compliance, multitenancy, quality of service, architecture, management. These attributes can be used to assess the end users and cloud service providers to build better SaaS cloud solutions according to the user's need and possibilities of the provider taking into consideration these requirements attributes.

References

[1] A. Samir and N. R. Darwish, "Reusability quality attributes and metrics of saas from perspective of business and provider," International Journal of Computer Science and Information Security (IJCSIS), vol. 14, 2016.

[2] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: a brief review," International Journal of Computer Sciences and Engineering, vol. 7, pp. 421-426, 2019.

[3] C. T. S. Xue and F. T. W. Xin, "Benefits and challenges of the adoption of cloud computing in business," International Journal on Cloud Computing: Services and Architecture, vol. 6, pp. 01-15, 2016.

[4] S. Namasudra, "Cloud computing: A new era," Journal of Fundamental and Applied Sciences, vol. 10, 2018.

[5] P. Srivastava and R. Khan, "A review paper on cloud computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 8, pp. 17-20, 2018.

[6] M. U. Bokhari, Q. Makki, and Y. K. Tamandani, "A survey on cloud computing," in Big Data Analytics, ed: Springer, 2018, pp. 149-164.

[7] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[8] S. B. Hiregoudar and V. Reshmi, "Cloud Computing: Overview of PaaS with Force. com Platform."

[9] M. A. Ikram and F. K. Hussain, "Software as a Service (SaaS) service selection based on measuring the shortest distance to the consumer's preferences," in International Conference on Emerging Internetworking, Data & Web Technologies, 2018, pp. 403-415.

[10] A. Joint and E. Baker, "Knowing the past to understand the present–issues in the contracting for cloud-based services," Computer Law & Security Review, vol. 27, pp. 407-415, 2011.

[11] V. Gonçalves and P. Ballon, "Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Platform-as-a-Service models," Telematics and Informatics, vol. 28, pp. 12-21, 2011.

[12] N. Wang, H. Liang, Y. Jia, S. Ge, Y. Xue, and Z. J. D. S. S. Wang, "Cloud computing research in the IS discipline: A citation/co-citation analysis," vol. 86, pp. 35-47, 2016.

[13] A. Tariq, S. A. Khan, and S. Iftikhar, "Requirements Engineering process for Software-as-a-Service (SaaS) cloud environment," in 2014 International Conference on Emerging Technologies (ICET), 2014, pp. 13-18.

[14] M. Ramachandran and Z. Mahmood, Requirements engineering for service and cloud computing: Springer, 2017.

[15] A. S. Zalazar, L. Ballejos, S. J. R. E. f. S. Rodriguez, and C. Computing, "Analyzing requirements engineering for cloud computing," pp. 45-64, 2017.

[16] E. Loukis, M. Janssen, and I. J. D. S. S. Mintchev, "Determinants of software-as-a-service benefits and impact on firm performance," vol. 117, pp. 38-47, 2019.

[17] S. Kurjakovic and K. Hinkelmann, "Enterprise Architecture Driven and User-Friendly SaaS Service Selection," in 2018 Sixth International Conference on Enterprise Systems (ES), 2018, pp. 196-203.

[18] H. S. Xiong Jinhua, Liu Hui, "On-Demand Service in Cloud Computing," vol. 8, pp. 15-20, 2010-12-25 2010.

[19] M. J. Kavis, R. A. Cohen, L. H. Sweet, P. W. M. Lusignan, M. Benayoun, T. Baker, et al., "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)," ed: Print, 2014.

[20] C. Fehling, F. Leymann, R. Retter, W. Schupeck, and P. Arbitter, Cloud computing patterns: fundamentals to design, build, and manage cloud applications: Springer, 2014.

[21] C. Bachleda and S. A. Ouaaziz, "Consumer acceptance of Cloud computing," Services Marketing Quarterly, vol. 38, pp. 31-45, 2017.

[22] A. Razaque and S. S. Rizvi, "Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment," Computers & Security, vol. 62, pp. 328-347, 2016.

[23] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing—The business perspective," Decision support systems, vol. 51, pp. 176-189, 2011.

[24] N. Porrawatpreyakorn, S. Nuchitprasitchai, K. Viriyapant, S. Tangprasert, and A. Chaipunyathat, "Understanding Key Enablers of Cloud Computing Adoption and Acceptance Over Time," in 2019 Research, Invention, and Innovation Congress (RI2C), 2019, pp. 1-6.

[25] B. R. Maxim and M. Kessentini, "An introduction to modern software quality assurance," in Software Quality Assurance, ed: Elsevier, 2016, pp. 19-46.

[26] G. Verma and S. J. S. C. S. Adhikari, "Cloud Computing Security Issues: a Stakeholder's Perspective," vol. 1, pp. 1-8, 2020.

[27] M. Rajesh, "A Systematic Review Of Cloud Security Challenges In Higher Education," The Online Journal of Distance Education and e-Learning, vol. 5, 2017.

[28] A. H. Shaikh and B. Meshram, "Security issues in cloud computing," in Intelligent Computing and Networking, ed: Springer, 2021, pp. 63-77.

[29] N. Subramanian, A. J. C. Jeyaraj, and E. Engineering, "Recent security challenges in cloud computing," vol. 71, pp. 28-42, 2018.

[30] A. Hashmi, A. Ranjan, and A. Anand, "Security and compliance management in cloud computing," International Journal of Advanced Studies in Computers, Science and Engineering, vol. 7, pp. 47-54, 2018.

[31] M. Kandira, J. Mtsweni, and K. Padayachee, "Cloud security and compliance concerns: Demystifying stakeholders' roles and responsibilities," in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), 2013, pp. 653-658.

[32] S. Prakash, "A Review on Quality of Service in Cloud Computing," in Big Data Analytics, ed: Springer, 2018, pp. 739-748.

[33] H. H. Ramadan and D. Kashyap, "Quality of service (QoS) in cloud computing," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 8, pp. 318-320, 2017.

[34] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," Peer-to-Peer Networking and applications, vol. 11, pp. 220-234, 2018.

[35] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," in 2014 IEEE 8th international symposium on service oriented system engineering, 2014, pp. 344-351.

[36] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of internet services and applications, vol. 4, pp. 1-13, 2013.

[37] W.-T. Tsai, G. Qi, and Y. Chen, "A cost-effective intelligent configuration model in cloud computing," in 2012 32nd International Conference on Distributed Computing Systems Workshops, 2012, pp. 400-408.

[38] A. A.-S. Ahmad and P. Andras, "Scalability analysis comparisons of cloud-based software services," Journal of Cloud Computing, vol. 8, pp. 1-17, 2019.