**International Journal of Advanced Science and Research**
**www.allsciencejournal.com**
**ISSN: 2455-4227**
**Received: 07-12-2022, Accepted: 24-12-2022, Published: 10-01-2023**
**Volume 8, Issue 1, 2023, Page No. 1-6**

# Analytical approach to attacks and vulnerabilities on cloud application service: Proposed study

**Olukiran Oyenike Adunni[1], Aiyeniko Olukayode[2], Ayepeku Olukayode Felix[3]**
[1] Department of Computer Engineering, Faculty of Technology and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[2] Department of Computer Science, Lagos State University, Lagos, Nigeria
[3] Department of Mathematical Computing Sciences, Thomas Adewumi University, Oko, Kwara State Nigeria

**Abstract**
Cloud computing creates an interesting environment that enables people and establishments to accomplish numerous functions such as reachable storage space, use of business software, specialised or customised software and development of a convincing network platform. The information and Communications Technology (ICT) world witnessed and still witnessing the growth of a technology model named cloud computing with applications such as software as a service (SaaS), which emerged as a revolutionary paradigm through which organizations can optimize their ICT investment. SaaS is an innovation in which services and data are stored in massively accessible data centres in the cloud and can be retrieved through procedures online, appropriate for the obsolete traditional method where organisations develop commercial data centres, set up the software and are accountable for managing their IT infrastructure. This paper conducted a review on the vulnerabilities of Cloud Application Services (SaaS), critical challenges posed by the adoption and usage of cloud computing (SaaS) ascribed to possible attacks exploiting these vulnerabilities and proposes required security components to prevent the attacks and mitigate the risk of such exploitation, especially but not limited to the geographical location, Nigeria and developing countries in Africa.

**Keywords:** clouds, cloud application services, information and communication technology, vulnerabilities

## Introduction

Cloud computing is a highly demanded computer system resource, most importantly the storage of data and power of computation having no strong administration by the user [1]. The outsized clouds frequently possess functions scattered across many environments, each environment is recognised as a data center [2]. Cloud computing advantages virtually touch everyone's life. It applies uses and storage platforms as services over the online environment with little or no cost being fully involved. An individual utilises cloud computing services regularly, For instance, the web-based email platforms (Google and Yahoo) to interchange information; social networking sites (Facebook, LinkedIn, MySpace and Twitter) to share information and remain
in contact with associates or colleagues [3]; on-demand subscription services (Netflix and Hulu) to watch programs or movies on the TV and; cloud storages (Zumo Drive and Dropbox) for music, videos, photos and documents online storage, collaboration tools (google docs) to work with an individual on the same document in real-time [4]; and online backup tools (Jungle Disk, Carbonite, and Mozy) to routinely store data into servers within the cloud. Businesses and companies give services from providers of cloud computing services to make moderate the working costs and ease cash flow. The advancement in Information Technology (IT) domain has been significant through this technology [5, 6, 7].

In information technology, there have been numerous improvements that transformed how services are considered and conveyed to consumers [8, 9]. One of these significant improvements is Cloud computing, which affects every field and organisation. With cloud computing, start-up organisations need not bother about the investment of a huge amount of money in setting up huge data centers. Programmers can commence the building of software applications on top of platforms that can enable fast web application expansion, that can be installed instantaneously [10].

Organizations need not purchase costly software that may be out-of-date within a particular period and also huge operating costs of maintenance are limited. Furthermore, the innovative types of internet hardware clients (IoT devices and mobile) will perform more efficiently than conventional internet clients with over a billion devices [11].

Various developments, prospects and needs include applications of mobile interactive, parallel systems, increase in the size of data, upsurge of analytics, requirement of bringing the data close to the applications, Internet of Things and decisions taken in real-time [12,13]. This paper considers the analytical approach to attacks and vulnerabilities in cloud application services of cloud computing.

## Literature review

### 1. Overview of Cloud Computing

The technology is noticeable in computer technology which uses the online platform and central remote servers for the maintenance of information or data application. Cloud is a network or internet that is located in a secluded place. Cloud computing renders collective services to local servers or storage resources. It enables the services via the network or internet as shown in Figure 1.

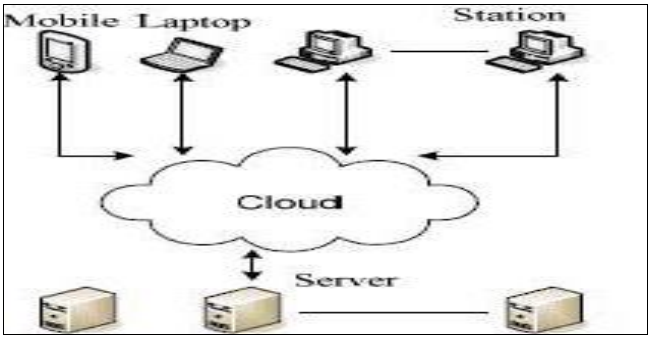


**Fig 1:** Cloud Computing [14]

Nowadays, the latest technology remains cloud computing which is employed for storage and accessibility of information through the internet instead of storage devices such as hard drives, flash drives, disk drives and so on. Cloud computing involves the manipulation, configuration and accessibility of software and hardware resources remotely. It renders online storage of data, applications and infrastructure as shown in Figure 2.

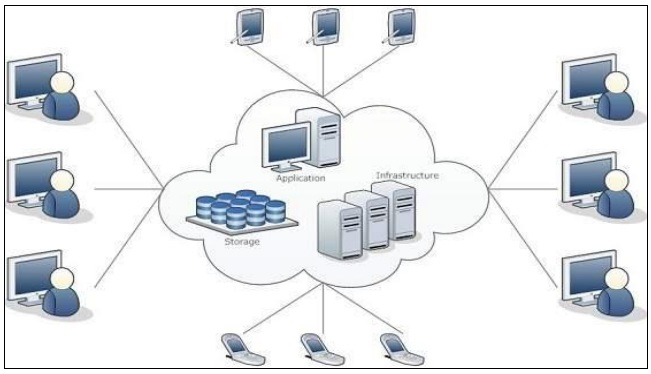


**Fig 2:** Structure of Cloud Computing [15]

All system applications and services are kept in the cloud. It offers a distinct, stress-free and simple interface to the users and the architecture is unseen. The technology consists of three major segments: Infrastructure, Application and Platforms. Each segment performs different tasks with products in diverse locations for business use.

## 2. Overview of Software as a service (SaaS)

SaaS is a method of conveying software and applications across the internet as a service [16]. As an alternative to the installation and maintenance of software, it is simply accessing via the internet, freeing yourself from complex software and hardware management [17]. SaaS applications are occasionally referred to as on-demand software or hosted software. Whatever the name, the applications of SaaS are achieved on a SaaS provider's servers [18]. The provider accomplishes the accessibility to the application, including ease of use, effectiveness and security [19].

Applications of SaaS can be set up in a cloud environment and retrieved via the online platform through users or web browsers. This extremely decreases the upfront commitment of resources [20]. The installation applications of SaaS can be done with little strength and be available in a very short period to a large group of users and therefore, it makes the SaaS model quite attractive to enterprises [21]. SaaS has attracted wide attention by being identified as a software application pattern. SaaS distributes software as a service, thus differentiating software users from software owners. Through SaaS, the users of software rent web-based software from providers of service as a substitute for buying software licenses.

The SaaS model decreases the usage cost of software and improves the tractability of business growth [22]. Software users can use the newest version of software and enjoy the most advanced technology with no need for updating. Top-most and the easiest layer of cloud computing, applications like word processors, video editors and databases are put on by the service provider of the cloud and they are made freely accessible to the customers on-demand or pay-as-you-go through the internet [23]. The National Institute of Standards and Technology (NIST) defines Cloud Software as a Service (SaaS) as follows Software as a Service (SaaS).

The ability delivered to the consumer is to apply the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface such as a web brows (web-based email) or a program interface [24]. The consumer needs not to manage or regulate the fundamental cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [21].

Consumers can employ the provider's applications running on cloud infrastructure through SaaS. The accessibility of these applications is provided by client devices through a thin client interface such as a web browser (web-based email) [25]. The management or control of fundamental cloud infrastructure including network, servers, operating systems, storage or individual application capabilities cannot be achieved by a consumer, with the likely exception of inadequate user-specific application settings for configuration.

## 3. Cloud Computing Models

The accessibility of cloud computing is categorised into three diverse service models which each fulfill a single set of demands for commercial activities. These three models are SaaS, Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [26].

### (i) Software-as-a-Service (SaaS)

Cloud-based applications over the internet are being made available through SaaS [16]. Generally available ones are email, calendaring, and office toos (Microsoft Office 365), Google Apps, Facebook, YouTube and Salesforce [27]. SaaS produces comprehensive programs that can be purchased on a pay-as-you-go from a cloud service provider.

### (ii) Platform-as-a-Service (PaaS)

It represents the complete advancement and placement platform in the cloud with properties that allow it to supply all things from simple cloud-based applications to refined, cloud-enabled enterprise programs [28]. Users develop or install their applications on the platform (languages, libraries, and tools) produced by the cloud provider. Users do not have control over the essential infrastructure (servers, storage, network) and operating systems [29]. Users have incomplete power to alter the environment settings. Examples of PaaS providers include Microsoft Azure, AWS Elastic Beanstalk Google App Engine, Apache Stratos, OpenShift Heroku and Force.com.

**(iii) Infrastructure-as-a-Service (IaaS)**
This is a service of cloud computing where enterprises hire or rent servers for storage and computation in the cloud [30]. Users can run any Operating system or application can be run on the rented servers without maintaining and operating costs of those servers. Examples are Rackspace, Amazon Web Services (AWS), Microsoft Azure, Digital Ocean, Linode, Google Compute Engine (GCE) and Cisco Metapod,

## 4. Architecture of SaaS
SAAS architecture is grouped into two types [16].

### 1. Single Tenant saas architecture
Single-tenant systems choose to store data for a single organisation. Single-tenant systems provide a user's database and instance of the software application, positioned on a server or detached via broad security regulations to create its virtual server, users of single-tenant systems like the benefits of software configurability, robust functionality and security improvement. An on-demand model, single-tenant SaaS is the best solution that several organisations should apply due to their industry, geography or security requirement which gives them the necessity for configurability and customization.

### 2. multi-Tenant saas architecture
These systems store information for many organisations on a single server. Multi-tenant systems placement of data from many organisations on the same server, usually splitting them from each other through a simple partition that averts information from transferring from one organisation to another. As the information is contained on the same server, each of the organisations applying the software is running a similar basic application with the same basic functionality and with the same limited configuration abilities.

## 5. Cloud SaaS Security vulnerabilities and attacks
Several measures have been taken to curb cloud (SaaS) security vulnerabilities and attacks. However, there are still some vulnerabilities that exist in cloud SaaS which are highlighted as follows;

**Data Breaches:** Threat of a breach in data is not particular to cloud computing, but it constantly rates as a serious issue for cloud customers. According to Jay Heiser, research vice president at Gartner, "Through 2020, 95% of cloud security failures will be the customer's fault."

**Data loss with no backup:** A mishap or disaster can result in the loss of customer data permanently except for measures in place for data backup.

**Insider Threats:** A present study reported that 53% of establishments surveyed confirmed insider attacks against their establishments.

**DDoS Attacks:** Distributed denial-of-service attacks are major threats to customers of cloud and providers including outages of lengthy service, reputational damage and access to customer data.

**Insecure APIs:** As the public "front door" to your application, an API is likely to be the initial entry point for attackers. Use pen testing to uncover security weaknesses in the APIs you use.

**Exploits:** The many tenancy environments of the cloud where customers share computing resources mean shared memory and resources may produce new attack surfaces for malicious actors.

**Account Hijacking.** By applying credentials that have been stolen, attackers may have entrance to critical services of cloud computing, negotiating the privacy, reliability and availability of those services.

**Advanced Persistent Threats:** Various advanced persistent threat groups not only focus on cloud environments but employ public cloud services to perform their attacks.

**Spectre & Meltdown:** Meltdown is used by attackers to sight data on virtual servers situated on the same hardware, potentially disastrous for cloud computing hosts. Spectre is worse to exploit, but harder to fix too. The security issues are shown in Figure 3.

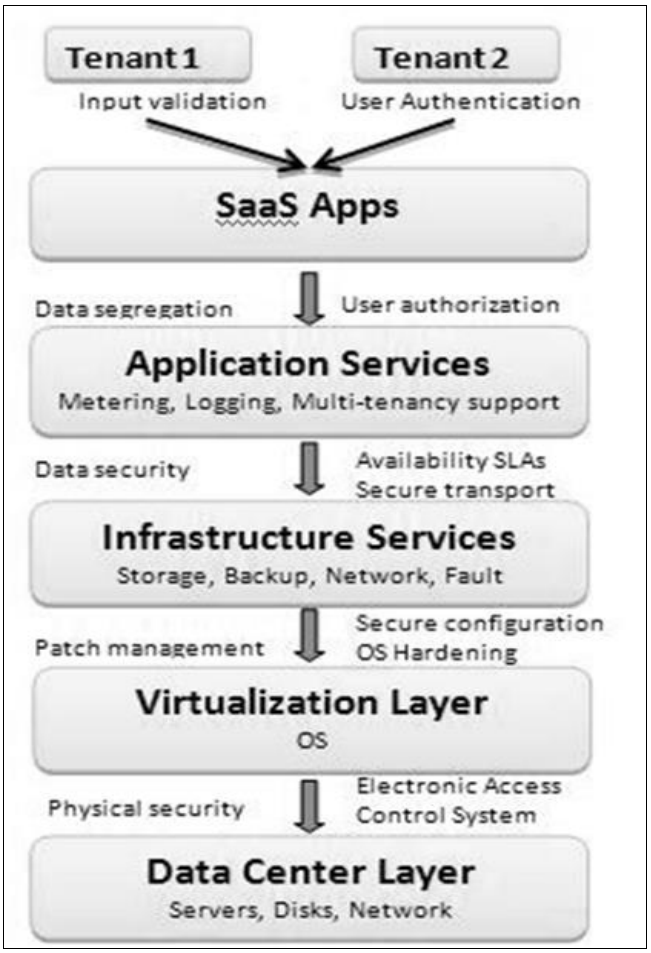


**Fig 3:** Security Issues in SaaS [35]

## 6. Security Challenges of saas
two main security challenges of saas are; traditional security challenges and cloud specific security challenges [35].

### 6.1 Conventional security challenges
The security problems in conventional communication systems are also traceable to the cloud, the cloud computing presents new attack vectors that will make attacks either

possible or simply easier to carry out [36]. Some of the traditional security issues which also affect the SaaS model have been described as follows:

1. Authentication and Authorization
2. Availability
3. Data Confidentiality
4. Virtual Machine security

### 6.2 Cloud-specific security challenges

The security and privacy of data remain the major concerns in cloud computing [37]. Cloud service providers must ensure the protection of contents from various malware, and there are different policies and mechanisms for Cloud service providers [38]. The following key Cloud Specific Security Challenges should be carefully considered as an integral part of the SaaS application development and deployment process:

1. Information security
2. Network security
3. Cloud standards
4. Data segregation
5. Data Access
6. Data Breaches
7. Backup
8. Identity management and sign-on process.

## 7. SAAS Vulnerability Solution

There are several studies on cloud security [31]. Many groups and organizations have so much interest in developing security products and standards for the cloud as shown in Table 1.

**Table1:** Security Areas and Possible Solutions

| S/N | Security Areas | Current/Possible Solutions |
|---|---|---|
| 1 | Authentication and authorization | Open Authorization<br>Two Factor Authentication<br>OAuth |
| 2 | Availability | Data Dispersion |
| 3 | Data Confidentiality | Attribute-based Proxy Re-Encryption |
| 4 | Virtual Machine Security | Reconfigurable distributed virtual machine<br>Survey on Virtual machine Security |
| 5 | Network Security | Network Security for virtual machines<br>Network Security Sandbox |
| 6 | Cloud standards | IEEE Cloud Computing Standard Study Group<br>ITU Cloud Computing Focus Group<br>Cloud Security Alliance |
| 7 | Data Access | Multi-user access policies<br>Data Access Management |
| 8 | Web application security | Web Application Scanners |
| 9 | Data breaches | |
| 10 | Backup | Agentless Method for Data Backup and Recovery |
| 11 | Identity management and sign-on process | CSA's Identity and Access Management Guidance |
| 12 | Information security | Information Security Risk Management Framework |

Based on the vulnerabilities in Table 1, the solution is to be integrated into the present deployment of the SaaS in cloud computing architecture to secure cloud SaaS deployment and adoption. For secure product engineering, software vendors should treat security as part of the product engineering lifecycle. At each phase of development (architecture, design, coding), a security review should be performed. This will help with faster identification of any security issues and lower rework costs for any security fixes that need to be implemented. This architecture design would be the focal point for the proposed solution and experiment test.

### 7.1 A model-based framework for security deployment and testing

Mouelhi *et al*. proposed an approach based on architectural, functional, and fault models and focus on security policies. The study proposes a model-based approach for the specification, deployment, and testing of security policies in Java applications. The approach started with a generic security meta-model of the application. It captures the high-level access control policy implemented by the application and was expressed in a dedicated domain-specific language. Before such a model is further used, the model needs to be verified to check the soundness and adequacy of the model concerning the requirements. Afterward, the model is automatically transformed into policy decision points (PDP). Since such PDPs are usually not generated from scratch but are based on existing frameworks, the output of the transformation is, for instance, an XACML (Extended Access Control Markup Language) file that captures the security policy. This transformation step is essential in MBT since an identified security issue at a model level does not automatically imply the same issue at the implementation level, nor does a model without security issues automatically imply the same on the implementation. Mouelhi *et al*. used mutations at the model level to ensure that the implementation conforms to the initial security model. Finally, the test objective is to check that the implementation (security policy) is synchronized with the security model this was down in the development and architectural stage.

Let us assume that we want to plan the security testing activities for businesses application that are separated into three tiers:

1. First-tier: A front-end that is implemented as a rich client using modern web development techniques, i.e., HTML5 and JavaScript, e.g., using frameworks such as AngularJS or JQuery.
2. Second-tier: A typical middle-tier implemented in Java (e.g., using Java Servlets hosted in an application server such as Apache Tomcat).
3. Third-tier: A third-party database that provides persistence for the business data that is processed in the second tier. Figure 7 illustrates this example architecture where the dotted vertical lines mark the trust boundaries of the application. #no figure 7

### Related work

[31]presented problems that confronted cloud computing users over the securities challenge and it also revealed the highly threatening factors which are a real matter of concern. The problems have been identified as having great impacts on confidentiality and users' trust. Risks in Security, as well as privacy risks with efficiency and impactful solutions, are challenging tasks to comprehend. Accessibility, dependability, integrity and privacy are

widely the factors that are brought in applications for security-related subjects. As the improvement in cloud computing is rising, the future will be full of risks and threats to its security. The providers and users must know the potential risks to security and be ready with solutions to handle these problems for the protection of information from any form of attack. Appreciated ideas and challenges of key open research were given in the work to recognize the problems of the cloud. The study gave a novel approach to this field and assist the researcher in discovering likely answers for these risks and threats.

Data security risks and attacks in cloud are known susceptibilities for many variables affecting cloud computing carried out by [32]. The investigation was to study the diverse modules of cloud computing as well as present major security issues. Also, the work produced different sorts of security threats with some new security concepts and alleviation techniques and recommended yet to come directions.

A survey on the risks and vulnerabilities of cloud computing was presented [26]. The study further discussed threats such as breaches of data, loss of data, malicious insiders, service denial, vulnerable systems and APIs, hijacking of accounts, vulnerabilities of shared technology, abuse of cloud services, insufficient security tools, human error, ransomware, Spectre and Meltdown, unsecured IoT devices and the related susceptibilities for each of these threats.

A literature review of the service delivery model for cloud computing, SaaS utilizing the security problems including the traditional and cloud-specific security problems related to the model was conducted [33]. Several problems that are linked to the new cloud paradigm were considered. Data storage security in a cloud platform remains a major concern that thwarts people from using the cloud. A practical solution to security and user data privacy, when it is positioned in a public cloud was mentioned. Further study on several security tools was examined to give clear services that users trust.

[34] tried to handle attacks that target SaaS, gave solutions that can assure the security of data, like SSL identified to be one of solutions to protect the data circulation, CTB that permits the identification of incoming packets to defend against DoS attacks or encrypted data and classification model, which aids in securing the stored data.

## Conclusion

With the various advantages of a cloud-based system, there are still many practical issues that have to be provided solutions. Cloud computing is a disruptive technology with several pending issues that exist particularly related to security. As described in the study, currently security has a lot of loose ends which scares away several potential users. Until a proper security module is not in place, potential users will not be able to leverage the true benefits of this technology. This security module should handle all the issues arising from all directions of the cloud. The security models should also be integrated into the present deployment of the SaaS in cloud computing architecture to secure cloud SaaS deployment and adoption. This will therefore help with faster identification of any security issues and lower rework costs for any security fixes that need to be implemented.

## References


1. Deshpande P, Sharma SC, Kumar PS. “Security threats in cloud computing,” in International Conference on Computing, Communication and Automation, ICCCA,2015:5(3):632-636.
2. M. Mehrtak *et al.* “Security challenges and solutions using healthcare cloud computing,” *J. Med. Life*,2021:14(4):448-461.
3. Almudawi NA. “Cloud Computing Privacy Concerns in Social Networks,” *Int. J. Comput*,2016:22(1):29-36.
4. Jain AK, Sahoo SR, Kaubiyal J. “Online social networks security and privacy: comprehensive review and analysis,” *Complex Intell. Syst*,2021:7(5):2157-2177.
5. Chimakurthi VNSS. “The Future Of Cloud Computing Amidst A Desperate Security Maze: The Impact Of COVID And The Future Challenges,” Asian J. Humanit. Art Lit,2021:8(2):75-84.
6. Molo MJ *et al.* “A Review of Evolutionary Trends in Cloud Computing and Applications to the Healthcare Ecosystem,” Appl. Comput. Intell. Soft Comput, 2021, 1-16.
7. Razaque A, Shaldanbayeva N, Alotaibi M, Alotaibi A, Murat, Alotaibi X. “Big data handling approach for unauthorized cloud computing access,” Electron,2022:11(1):1-20.
8. Kiswani JH, Dascalu SM, Harris FC. “Cloud computing and its applications: A comprehensive survey,” *Int. J. Comput. their Appl*,2021:28(1):3-24.
9. Alajmi Q, Sadiq AS, Kamaludin A, Al-Sharafi MA. “Cloud Computing Delivery and Delivery Models: Opportunity and Challenges,” Adv. Sci. Lett,2018:24(6):1-10.
10. Al-Rousan T. “Cloud computing for global software development: Opportunities and challenges,” *Transp. Syst. Eng. Concepts, Methodol. Tools, Appl.*,2015:2(3):897–908.
11. M. N. Rajeswari, “Overview of Cloud Computing,” J. 0f Emerg. Technol. Inov. Res.2019:6(3):18-35.
12. Kaur C. “The Cloud Computing and Internet of Things (IoT),” Int. J. Sci. Res. Sci. Eng. Technol,2020:7(10):19-22.
13. Odun-Ayo I, Okereke C, Orovwode H. “Cloud computing and internet of things: Issues and developments,” in Proceeding of the World Congress on Engineering,2018:(1):1-7.
14. Okonoboh MA, Tekkali S. “Real-Time Software Vulnerabilities in Cloud Computing: Challenges and Mitigation Techniques, 2011.
15. Govindasamy K, Velmurugan. “A Study on Classification and Clustering Data Mining Algorithms based on Students Academic Performance Prediction,” Int. J. Control theory Appl,2017:10(23):147-0160.
16. Ikram MA, Hussain FK. “Software as a service (saas) service selection based on measuring the shortest distance to the consumer’s preferences,” *Lect. Notes* Data Eng. Commun. Technol,2018:17:403-415.
17. Kaur B. “Software as a service,” Int. Res. J. Eng. Technol,2015:2(3)789-792.
18. SG, MS. “Securing Software as a Service Model of Cloud Computing: Issues and Solutions,” Int. J. Cloud Comput. Serv. Archit,2013:3(4):1-11.
19. Hosniara Pervin. “Software as a service and security,” World J. Adv. Res. Rev,2021:11(3):327-331.

20. Ouf S *et al*. "Business intelligence software as a service (SAAS)," in 2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN, 2011, 641-649.
21. Pushpa RB, Swapna KG. "Issues & Solution of SAAS Model in Cloud Computing," *IOSR J. Comput. Eng*, 2018, 40-44.
22. Desale R, Kolhatkar P, More A, Katira P, Jaybhaye KPSM. "Software as a Service (SaaS) for Management information system using multiple tenants," *Int. J. Eng. Res. Appl*,2013:3(3):42-46.
23. Patrick ZPG, Satyanarayana KVV. "Optimization of service level agreements (SLAs) within SaaS cloud IT infrastructure," *J. Crit. Rev*,2020:7(1):414-420.
24. Wang Y, LeBlanc D. "Integrating SaaS and SaaP with dew computing," in Proceedings - 2016 IEEE International Conferences on Big Data and Cloud Computing, BD Cloud 2016, Social Computing and Networking, Social Com 2016 and Sustainable Computing and Communications, Sustain Com, 2016, 590-594.
25. Jagli D, Purohit S, Chandra NS. "Saasqual: A quality model for evaluating SAAS on the cloud computing environment," Adv. Intell. Syst. Comput,2018:654:42-437.
26. Suryateja PS. "Threats and Vulnerabilities of Cloud Computing A Review," *Int. J. Comput. Sci. Eng*,2018:6(3):297-302.
27. Taufiq-hail GA, Alanzi ARA, Affendi S, Yusof M, Alruwaili M. "Software as a Service (SAAS) Cloud Computing : An Empirical Investigation on University Students ',' *Interdiscip. J. Information, Knowledge, Manag*,2021:16:213-253.
28. Pastore S. "The Platform as a Service (PaaS) Cloud Model: Opportunity or Complexity for a Web Developer?," Int. J. Comput. Appl,2013:81(18):29-37.
29. DT, GR. "Platform-as-a-Service (PaaS): Model and Security Issues," *TELKOMNIKA Indones. J. Electr. Eng*,2015:15(1):151-161.
30. Shahzadi S, qbal M, Qayyum ZU, Dagiuklas T. "Infrastructure as a service (IaaS): A comparative performance analysis of open-source cloud platforms," in *IEEE International Workshop on Computer-Aided Modeling and Design of Communication Links and Networks, CAMAD*, 2017, 1-6.
31. Sasubilli MK, Venkateswarlu R. "Cloud Computing Security Challenges, Threats and Vulnerabilities," in Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT, 2021, 476-480.
32. Thabit F, Sharaf P, Al-ahdal AHA, Sudhir P. "Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques," J. Inf. Comput. Sci,2020:10(12):35-57.
33. Devi KCL, Venkataramana. "Security Issues in SaaS Delivery Model of Cloud Computing," Int. J. Sci. Eng. Res,2017:8(5):34-40.
34. Soufiane S, Halima B, "SaaS Cloud Security : Attacks and Proposed Solutions," *Trans. Mach. Learn. Artif. Intell*,2017:5(4):1-12.
35. Subashini S, Kavitha V. "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *J. Netw. Comput. Appl*,2011:34(1):1-11.
36. Rupra SS. "Investigate the Security Challenges in SaaS Private Cloud using OwnCloud Investigate the Security Challenges in SaaS Private Cloud using OwnCloud," Mara Res. Journals,2020:3(1):12-22.
37. Kanwal I, Shafi H, Memon S, Shah MH. "Cloud Computing Security Challenges: A Review," Int. J. Innov. Eng. Res. Technol,2020:7(6):459-469.
38. Shahzad F. "State-of-the-art survey on cloud computing security challenges, approaches and solutions," Procedia Comput. Sci,2014:(37):357-362.