Cloud Security and Privacy: SAAS, PAAS, and IAAS

Bokhari Nabil[1], José Javier Martínez Herráiz[2]

[1] Student at Faculty of Information and Knowledge Engineering, University of Alcala, Madrid, Spain
[2] Professor at Faculty of Information and Knowledge Engineering, University of Alcala, Madrid, Spain

Abstract
The multi-tenancy and high scalability of the cloud have inspired businesses and organizations across various sectors to adopt and deploy cloud computing. Cloud computing provides cost-effective, reliable, and convenient access to pooled resources, including storage, servers, and networking. Cloud service models, SaaS, PaaS, and IaaS, enable organizations, developers, and end users to access resources, develop and deploy applications, and provide access to pooled computing infrastructure. Despite the benefits, cloud service models are vulnerable to multiple security and privacy attacks and threats. The SaaS layer is on top of the PaaS, and the IaaS is the bottom layer of the model. The software is hosted by a platform offered as a service through an infrastructure provided by a cloud computing provider. The Hypertext Transfer Protocol (HTTP) delivers cloud-based apps through a web browser. The stateless nature of HTTP facilitates session hijacking and related attacks. The Open Web Applications Security Project identifies web apps' most critical security risks as SQL injections, cross-site scripting, sensitive data leakage, lack of functional access control, and broken authentication. The systematic literature review reveals that data security, application-level security, and authentication are the primary security threats in the SaaS model. The recommended solutions to enhance security in SaaS include Elliptic-curve cryptography and Identity-based encryption. Integration and security challenges in PaaS and IaaS can be effectively addressed using well-defined APIs, implementing Service Level Agreements (SLAs), and standard syntax for cloud provisioning.

Keywords:
Cloud, security, SaaS, PaaS, IaaS, privacy, web app, elliptic-curve cryptography, identity-based encryption, data security, SLA, HTTP, hypervisor

1. Introduction

The transition to cloud computing has gained considerable momentum globally across various industries and disciplines. The education, healthcare, military, public service, and other sectors are rapidly adopting and implementing cloud computing to achieve strategic goals and objectives, including gaining a competitive edge in the fast-changing market. Cloud computing enables private and public companies to leverage multiple benefits, including on-demand access to a pool of resources, cost-effective access to simplified and scalable IT infrastructure, and access to scalable storage and networking facilities. According to the National Institute of Standards and Technology (NIST), cloud computing is a model that enables convenient, on-demand access and resource pooling delivered by different cloud service providers.

Cloud service models such as software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) enable organizations to develop apps, host systems, and access pooled infrastructure leading to a competitive edge in the digitized business environment. However, despite the benefits, such as scalability and cost-effective access to pooled resources, cloud computing is vulnerable to diverse cybersecurity threats and attacks. This study explores cloud computing security and privacy challenges focusing on the attacks on SaaS, PaaS, and IaaS to recommend effective solutions, including elliptic-curve cryptography and identity-based encryption.

2. The Evolution of Computing Architecture

The starting point of cloud computing is mainframe computing in the 60s and 70s. Mainframe computing supported core memory, mass-storage devices, and computer graphic systems for plotting the aircraft. The SMP/open systems emerged in the '80s and '90s [16]. These systems supported a pool of homogeneous processors and independently administered software. Distributed computing emerged in the late '90s. Distributed computing supports web-based apps and multitier architecture [16]. Distributed computing paved the way for grid computing, providing virtualization of distributed computing resources. Cloud computing emerged in late 2000, supporting various service models, including IaaS, PaaS, and SaaS.

Manuscript received March 5, 2024
Manuscript revised March 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.3.3

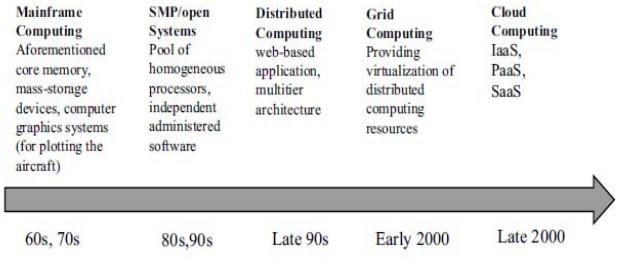


Fig.1.1 The Evolution of Computing Architecture [16]

Figure 1.1 presents a high-level summary of the key milestone in the evolution of computing architecture. Various factors drove the development, including the demand for distributed computing, elasticity, scalability, and access to on-demand computing resources.

3. Cloud Delivery Model

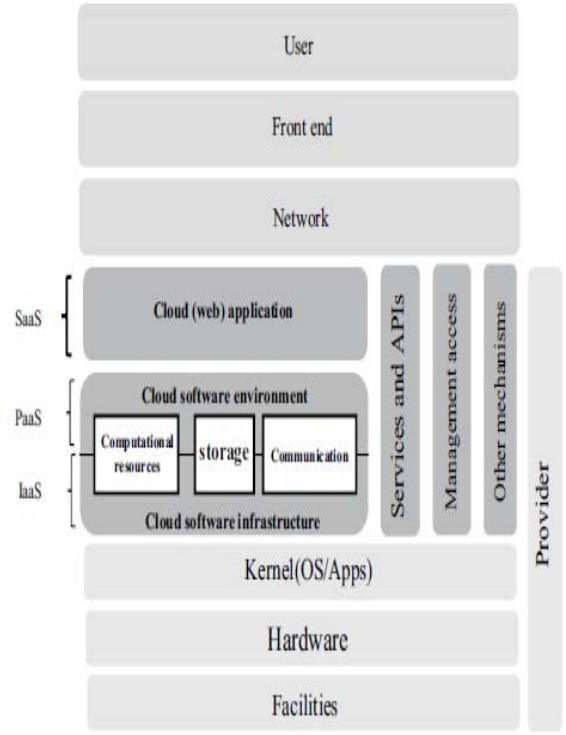


Fig. 1.2 Cloud Delivery Model [16]

Figure 1.2 presents the cloud delivery model. The model's key components include hardware, kernel (OS/apps), provider, user, and service models (SaaS, PaaS, and IaaS).

4. Actors in the Cloud

4.1 Cloud Provider

When assessing security and privacy challenges, it is imperative to understand the role of each actor in the cloud. The primary actors in the cloud include the cloud provider, consumer, broker, carrier, and auditor. A cloud provider is a company or individual responsible for providing cloud computing services to consumers [16]. The provider acquires and manages cloud software to organize and deliver unique services. In the SaaS service model, the provider's role is to deploy, configure, maintain, and update software.

Most of the software management and control responsibilities in SaaS and PaaS are coordinated by the provider [16],[15]. In IaaS service models, the primary roles of the provider include acquiring physical computing resources, including servers, storage, and networks for use by consumers, including organizations and individual users.

4.2 Consumer

A cloud consumer or customer is an organization or individual receiving cloud computing services offered by different providers. The consumer must sign service-level agreements (SLAs) with the provider of a specific cloud service [2],[4]). SLAs cover security, service quality, and cloud computing service performance. The consumer is responsible for ensuring that the SLAs meet their expectations.

4.3 Broker

Cloud brokers integrate the cloud services provided by the cloud provider to consumers. Consumers who have challenges integrating cloud computing services leverage the benefits of cloud brokers [16]. The broker manages cloud services' usage, delivery, and performance. Brokers offer service intermediation, aggregation, and service arbitrage in cloud computing.

4.4 Cloud Carrier

The role of the cloud carrier is to intermediate between the cloud consumer and the provider in delivering cloud services. The carrier dedicates secured connections to the provider and the consumer [16],[4]. The cloud auditor examines cloud services in an independent version.

4.5 Cloud Auditor

The auditor checks whether cloud services conform to standards and assesses security controls and performance issues. The auditor also considers the potential implications of failure to comply with cloud computing standards [16]. For instance, they assess the impacts of failure to implement adequate security and privacy controls in a cloud computing environment.

5. SaaS Security and Privacy Challenges

Software as a Service (SaaS) is the top layer in a cloud computing model. Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are the second and third layers. As a result, SaaS relies on PaaS to deliver its services to the cloud consumer [4]. Various techniques and approaches have been deployed to investigate security and privacy vulnerabilities in the three primary cloud service models. A survey by Modi [14] examined the security issues and solutions for the different layers of cloud computing. A similar study by Grozev and Buyya [5] investigated inter-cloud architecture and application brokering from the perspective of security challenges. A more relevant study by Kim [10] surveyed the security vulnerabilities and corresponding countermeasures in SaaS. Though these studies are appropriate, the challenge is that few studies have thoroughly exploited the specific security vulnerabilities affecting particular models. The research gap was also highlighted in Tabrizchi and Kuchaki Rafsanjani's study [16]. As a result, this study addresses this research gap by exploring the security and privacy vulnerabilities of SaaS, the most popular and commonly used cloud service model. The security vulnerabilities of SaaS are compared with PaaS and IaaS because of the interrelationship between these models.

Fig. 1.3 Cloud Service Models [7]

Figure 1.3 shows how the cloud service models are layered and the functions of each model. Refer to Appendix A for the cloud computing authentication components.

SaaS, the top layer, saves upfront establishment costs and supports a shared system environment. PaaS is used to develop and deploy applications and provide pre-build components [15],[7]. The bottom layer, IaaS, fully virtualizes the platform environment and provides on-demand access to computing infrastructure.

Customers access SaaS services using a web browser connected to the internet. As a result, security and privacy threats target users and SaaS providers. According to Iqbal [7], the primary security threats in SaaS include weak credentials, insecure passwords, and nefarious use of cloud computing, web-based applications, and malicious insiders. SaaS-based web applications are delivered through the Internet. In that connection, traditional web application security affects the SaaS environment [16]. The complexity is that most security threats targeting cloud-based web apps are unknown and uncontrollable.
According to the Open Web Applications Security Project, web apps' most critical security risks include injection, cross-site scripting, sensitive data exposure, and lack of functional access control. Web apps are also vulnerable to insecure direct object references, security misconfiguration, and broken authentication [7]. Comprehending the SaaS security and privacy challenges requires understanding the multitenant architecture of SaaS.

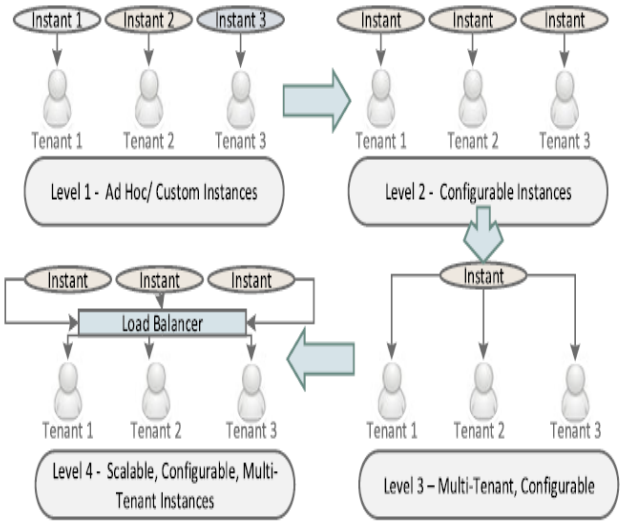


Fig 1.4 Multitenant Architecture of SaaS Model [7]

Figure 1.4 presents a high-level view of the multitenant architecture of SaaS. The key components include Ad hoc/ custom, configurable, scalable, and multitenant instances. Refer to Appendix B for the cloud virtual network architecture.

Application-level security is the main challenge in SaaS multitenant architecture. Cloud-based apps are primarily delivered through a web browser using Hypertext Transfer Protocol (HTTP). The stateless nature of this protocol can facilitate session hijacking because of the reliance on cloud apps for session handling. Previous studies have recommended various strategies for enhancing the security of SaaS applications. A study by Wen and Dong [17] suggests classifying SaaS layers as a strategy to improve the security of multitenant SaaS architectures. The study introduces a new quality model for determining the quality of services.

Despite these solutions, most studies fail to discuss the actual modeling variability among tenants in cloud computing [11],[2]. The challenges that have not been effectively addressed are the possibility of cloud service providers modifying data without the user's consent [8]. The modification, whether intentional or not, affects the behavior and security of cloud services. Consequently, application-level security and data security are crucial threats that must be addressed in SaaS.

6. PaaS and IaaS Security and Privacy Issues

The reliance on the SaaS layer on the PaaS layer increases security and privacy vulnerabilities. PaaS enables developers to develop and deploy software without purchasing or installing any software. The features of PaaS allow developers to deploy apps without the need for special system administration skills. Web apps can be deployed 5X faster on PaaS platforms than on traditional Dot NET and Java platforms [7]. However, the main security challenges in PaaS include application integration and vendor lock-in issues. The complexity is worsened by the twofold nature of security in PaaS, the platform's security, and the application's Security [9]. Therefore, the security issues for SaaS, directly and indirectly, affect the PaaS model.

On the contrary, the security vulnerabilities and challenges of IaaS are unique compared to those of PaaS and SaaS. The prevalent challenges for IaaS include hypervisor security, VM isolation, and virtual storage concerns. According to Iqbal [7], the attacks on virtualization layers include VM escape, denial of service, VM rootkits, and external modification of the hypervisor.

7. Recommended Solutions

Data and application security in SaaS can be enhanced by encryption to strengthen access control and authentication. Iqbal [7] assert that the primary access control models in a cloud computing environment include discretionary, role-based, and mandatory access controls. [12] propose an innovative technology for encrypting data using elliptic-curve cryptography to enhance data security and privacy in the cloud. Elliptic-curve cryptography leverages advanced systems and methodologies to ensure that only authorized users access data stored in the cloud [1]. Identity-based encryption was also leveraged in a study by Liu [13] to enhance data security in the cloud. Identity-based encryption leverages a unique identifier to generate the public key [3]. As a result, only authenticated users can access data leading to enhanced security in cloud computing.

Integration challenges in a cloud platform can be addressed using different strategies. One of the best strategies is to use well-defined APIs to simplify data integration across various cloud platforms. The implementation of SLAs helps define the rules governing data migration across diverse cloud platforms [7]. PaaS lock-in security issues and concerns can be addressed by leveraging open architecture and standard syntax for cloud provisioning. The security models should be analyzed continuously, and the security dependency associated with API be determined.

The security challenges associated with IaaS, specifically hypervisor threats, can be addressed by deploying software-based firewalls. Iqbal [7] recommend the integration and installation of hypervisor services correctly to help prevent security threats and attacks [6]. Besides, consumer interaction with virtual systems should be reduced. Combining these recommendations enhances the security and privacy of all the cloud service models, including SaaS, PaaS, and IaaS.

8. Conclusion

The study comprehensively analyzes the security and privacy vulnerabilities of the cloud service models, primarily SaaS. SaaS's security and privacy vulnerabilities include application-level security threats, data security, and authentication. The SaaS model is on top of the PaaS layer; therefore, the security threats and attacks are interrelated. The security and privacy threats for PaaS include integration, vendor lock-in, and the two-fold nature of security of the platform and the application deployed. Hypervisor security, VM isolation, and storage security issues are prevalent in the IaaS. SaaS's security and privacy issues can be effectively addressed using advanced encryption algorithms. The recommended algorithms include Elliptic-curve and entity-based encryption. Security and integration challenges in PaaS can be addressed using well-defined APIs, SLAs, and standard syntax for cloud provisioning. The security threats and challenges for IaaS can be addressed by correctly integrating hypervisor services and minimizing interaction with virtual assistance.

9. Recommendations for Future Research

Finally, this study has innovatively investigated the persistent security and privacy challenges targeting cloud service models, specifically SaaS. The SaaS security challenges are compared with the threats targeting PaaS and IaaS. Future studies should investigate each cloud service model's security and privacy threats. Future studies should leverage diverse methodologies and data collection methods, including qualitative and quantitative methods. A hybrid of qualitative and quantitative data will present a precise outlook of the current situation regarding the security of SaaS, PaaS, and IaaS. Besides, this study recommends elliptic-curve cryptography and identity-based authentication as the preferred encryption solutions to enhance the security and privacy of SaaS. Future studies should investigate how other algorithms can be leveraged to improve SaaS, PaaS, and IaaS security.

References

[1] ANAS, M., IMAM, R. and ANWER, F., 2022, January. Elliptic curve cryptography in cloud security: a survey. In 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 112-117). IEEE.

[2] AL NAFEA, R., and ALMAIAH, MA, (2021, July). Cyber security threats in the cloud: A literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779–786). IEEE.

[3] DENG, H., QIN, Z., WU, Q., GUAN, Z., DENG, R.H., WANG, Y. and ZHOU, Y., 2020. Identity-based encryption transformation for flexible sharing of encrypted data in the public cloud. IEEE Transactions on Information Forensics and Security, 15, pp.3168-3180.

[4] GIRS, S., SENTILLES, S., ASADOLLAH, SA, ASHJAEI, M. and MUBEEN, S. (2020). A systematic literature study on the definition and modeling of service-level agreements for cloud services in IoT. IEEE Access, 8, pp.134498–134513.

[5] GROZEV, N. and BUYYA, R., 2014. Inter-Cloud architectures and application brokering taxonomy and survey. Software: Practice and Experience, 44(3), pp.369-390.

[6] HASAN, M.M. and RAHMAN, M.A., 2020. A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment. Journal of Information Security and Applications, 50, p.102397.

[7] IQBAL, S., KIAH, M.L.M., ANUAR, N.B., DAGHIGHI, B., WAHAB, A.W.A. and KHAN, S., 2016. Service delivery models of cloud computing: security issues and open challenges. Security and Communication Networks, 9(17), pp.4726-4750.

[8] KHAN, S., GANI, A., WAHAB, A.W.A., BAGIWA, M.A., SHIRAZ, M., KHAN, S.U., BUYYA, R. and ZOMAYA, A.Y., 2016. Cloud log forensics: Foundations, state of the art, and future directions. ACM Computing Surveys (CSUR), 49(1), pp.1-42.

[9] KHAN, S. U., KHAN, H. U., ULLAH, N., and KHAN, R. A. (2021). Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach. Security and Communication Networks, 2021, 1-20.

[10] KIM, D. and VOUK, MA, (2014, December). A survey of common security vulnerabilities and corresponding countermeasures for SaaS. In 2014 IEEE Globecom Workshops (GC Wkshps) (pp. 59–63). IEEE.

[11] KONG, L., LI, Q. and ZHENG, X., 2010, November. A novel model supporting customization sharing in SaaS applications. In 2010 international conference on multimedia information networking and security (pp. 225-229). IEEE.

[12] KUMAR, A., LEE, BG, LEE, H. and KUMARI, A., 2012, October. Secure storage and access of data in cloud computing. In 2012 International Conference on ICT Convergence (ICTC) (pp. 336–339). IEEE.

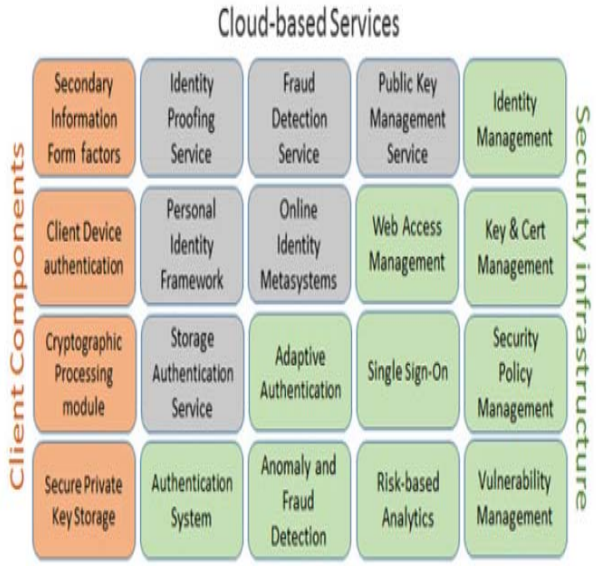
[13] LIU, Z., 2013, September. A secure, anonymous identity-based access control over cloud data. In 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies (pp. 292-295). IEEE.

[14] MODI, C., PATEL, D., BORISANIYA, B., PATEL, A. and RAJARAJAN, M., 2013. A survey on security issues and

solutions at different layers of Cloud computing. The Journal of Supercomputing, 63, pp.561-592.
[15] RAMACHANDRA, G., IFTIKHAR, M. and KHAN, F.A., 2017. A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, pp.465-472.
[16] TABRIZCHI, H. and KUCHAKI RAFSANJANI, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(12), pp.9493-9532.
[17] WEN, P.X. and DONG, L., 2013, September. Quality model for evaluating SaaS service. In 2013 Fourth international conference on emerging intelligent data and web technologies (pp. 83-87). IEEE.

Appendices

Appendix A: Cloud Computing Authentication Components [7]



Appendix B: Virtual Cloud Network Architecture [7]