iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55416

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Cloud Security and Privacy

Aayushi Bhansali
Department Of Computer Science and Engineering, Cloud Technology And Mobile ApplicationSchool of Engineering and Technology JAIN Global Campus, Jakkasandra Post Kanakapura Taluk, Ramanagara District Bengaluru, Karnataka, India - 562112

Abstract: Over the last decade, cloud computing has grown and evolved significantly. It provides cost-effective solutions as well as a wide range of adaptable services. Many businesses are using cloud services. Users mostly use cloud services to save data in a virtual environment.
Users have no knowledge of or influence over what happens in the cloud, and nothing in the cloud is visible to them, which raises security and privacy problems. Malicious administrators can mess with the integrity, privacy, virtual machines, and volatile confidentiality of cloud services. Clouds are vulnerable to hacking, and their integrity, availability, and data security are all in jeopardy.

I. INTRODUCTION

Cloud computing is an evolving paradigm and has generated significant interest in academics and industry.[1] The cloud has totally changed the topography of communication infrastructures, storage, computing and services. It enables on-demand availability of computational and storage resources.
While cloud computing can help companies break the physical bonds between their users and IT infrastructure, it comes with many security threats that require to be overcome in order to fully benefit from its advantages. Despite the advantages of cloud computing, many companies still face security threats that can severely affect their operations. This is why implementing it requires the proper security measures to avoid these risks.
Without the proper security and privacy solutions, this revolutionary computing paradigm could become a failure. Unfortunately, many of the concerns that cloud users have are still not addressed. Without the right security and privacy solutions, the cloud could become a huge failure.

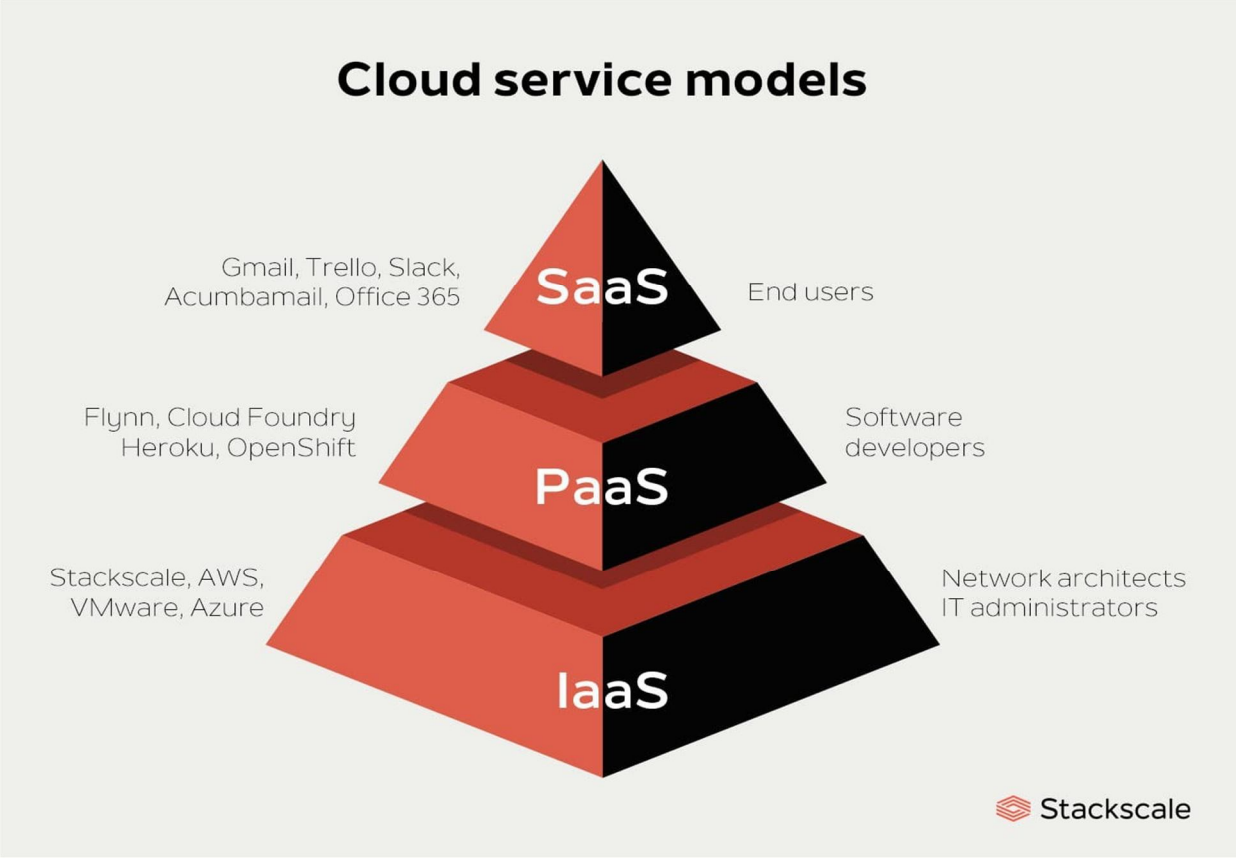
II. CLOUD COMPUTING DEFINITION

Although many researchers have tried to define the cloud computing concept, no single standard has been established. The most appropriate definition is given by NIST:
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models.[2]

III. CLOUD SERVICE MODELS

As a service delivery model, it is possible to identify three basic types of cloud services offered by providers.[2]

1) *Software as a Service (SaaS):* Software as a Service (SaaS) is a type of software that provides a service instead of buying and installing software.[2]
2) *Platform as a Service (PaaS):* Platform as a Service (PaaS) is a type of software that provides a platform in the cloud, upon which applications can be developed and executed. [2]
3) *Infrastructure as a Service (IaaS):* Infrastructure as a Service (IaaS) is a type of service in which providers offer computing power and storage space on demand.[2]

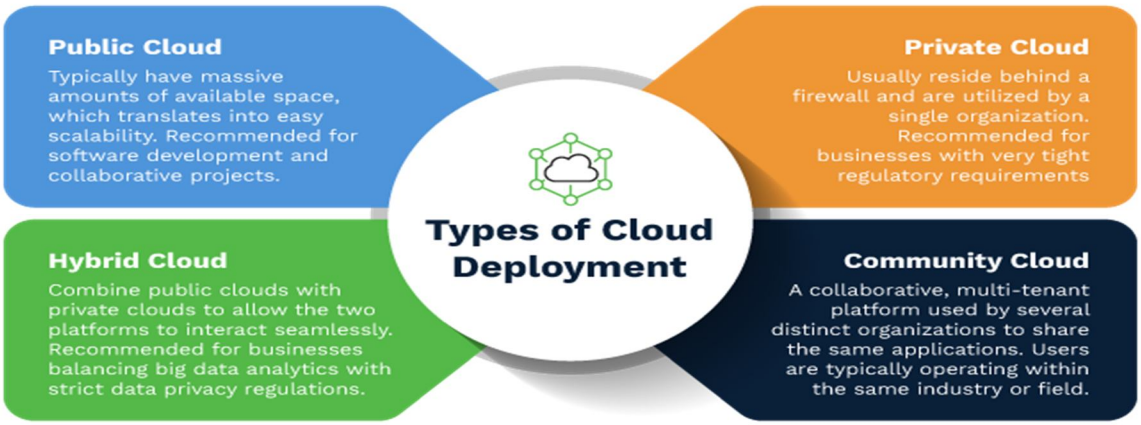


https://www.stackscale.com/blog/cloud–service–models/

IV. CLOUD DELIVERY MODELS

The four basic cloud delivery models are provided by the National Institute of Standards and Technology (NIST). These models are used by agencies to deliver various applications and business services e ciently.[2]

1) *Private Cloud:* Private cloud is a type of cloud service that is provided to an organization, usually on-site.
2) *Public Cloud:* Public cloud is a type of cloud that is available to the public or owned by an organization.
3) *Community Cloud:* A community cloud is a shared pool of cloud services that support a specific community. It can be managed by an organization or a third party.
4) *Hybrid Cloud:* A hybrid cloud is composed of different types of cloud infrastructure.



https://www.vxchnge.com/blog/different–types–of–cloud–computi ng

V. CLOUD SECURITY RISKS

Businesses and organizations are increasingly using cloud computing to store and process their data. However, this entails a number of security issues. The potential for a data breach is one of the key concerns connected to cloud computing. Unauthorized access to sensitive data kept in the cloud can have a negative impact on a company's finances and reputation. Cyberattacks like DDoS attacks and malware infections pose a concern as well since they might jeopardize the security and dependability of cloud services. Additionally, attackers may be able to take advantage of vulnerabilities caused by the shared infrastructure of cloud computing. To reduce these threats, cloud service providers must employ robust authentication and encryption techniques, conduct frequent security audits, and give their clients access to information about their security procedures. By creating and putting into practise robust security policies, keeping an eye on who has access to their cloud resources, and routinely evaluating their cloud architecture, businesses that employ cloud computing must also take proactive measures to control and minimize these risks.

VI. CLOUD SECURITY CONTROLS

The many safeguards that cloud service providers implement to guard against unauthorized access, data breaches, and other security risks are referred to as cloud security controls. Encryption, which includes converting data into an unreadable format that can only be decoded with a unique key, is one of the main security mechanisms used in cloud computing. Access controls are another essential element of cloud security since they guarantee that only authorized users have access to the data and resources of the cloud. To guard against hacker assaults and illegal access, cloud providers also deploy network security controls including firewalls, intrusion detection systems, and virtual private networks (VPNs). Identity and access management, threat detection and response, and data encryption are further security measures that cloud services employ. The strength of the security programme of the cloud provider, the security measures put in place by the client, and the degree of openness and visibility offered by the cloud provider are all factors that affect how successful these security controls are. Therefore, in order to secure the security of their data in the cloud, enterprises must carefully assess the security controls of possible cloud service providers and establish their own security procedures.

VII. CLOUD PRIVACY ISSUES

When businesses choose to store and handle their data on the cloud, they must take a number of privacy issues into account. Data ownership is one of the key privacy problems with cloud computing. Customers should be informed that the cloud provider owns the data they keep there rather than them, as this could cause problems with compliance and the law. Additionally, since data may be governed by various laws and regulations depending on the nation in which it is housed, the physical location of cloud servers can also have an impact on data privacy. Another issue is the potential for privacy violations caused by third-party service providers having access to data as part of the cloud service delivery chain. To avoid unauthorized access to their data, organizations must also confirm that the access controls, encryption, and other security measures used by their cloud providers are adequate. The fact that keeping personal data in the cloud may increase the danger of data breaches, which can result in data loss, identity theft, and other privacy violations, must also be known by enterprises. Organizations must carefully assess the privacy rules and practices of their cloud service providers to reduce these risks, and they must put in place their own privacy measures to safeguard their data.

VIII. TRUST AND TRANSPARENCY

To give clients the assurance that their data is being managed securely and responsibly, trust and transparency are essential components of cloud security and privacy.

Organizations need to be aware of how their data is handled, kept, and safeguarded in order for them to trust their cloud service providers. Giving consumers access to security logs and reports, regular security audits, industry standard compliance, and other security procedures of their cloud providers are all examples of transparency in cloud computing. The location of their data centers, the kinds of security controls they have in place, and the precise security measures they employ to secure customer data should all be disclosed by cloud service providers. This openness enables businesses to assess the dangers of hosting their data in the cloud and make educated decisions about their cloud service providers. Over time, trust is developed through a history of dependable service, a shown dedication to security, and e cient customer-cloud provider communication. Therefore, in order to forge enduring bonds with their clients and preserve their standing as dependable and trustworthy service providers, cloud providers must place a premium on openness and trust.

IX. CASE STUDY

Under Armour, a well-known sportswear company, experienced a data breach in 2018 that exposed the personal information of over 150 million people. Their cloud-based health software, MyFitnessPal, which kept user usernames, email addresses, and hashed passwords, was the source of the incident. The business took precautions to encrypt the passwords, but they neglected to safeguard its encryption keys, leaving the hashed passwords open to brute-force attacks.

Under Armour suffered serious reputational and financial losses as a result of the breach because it was required to alert customers and provide credit monitoring services. The hack served as another reminder of how crucial effective security measures and risk management procedures are in cloud computing. Under Armour added further security measures in reaction to the hack, including multi-factor authentication, stronger encryption, and frequent security assessments. The business also made an effort to be more open and communicative with its users about its security procedures.

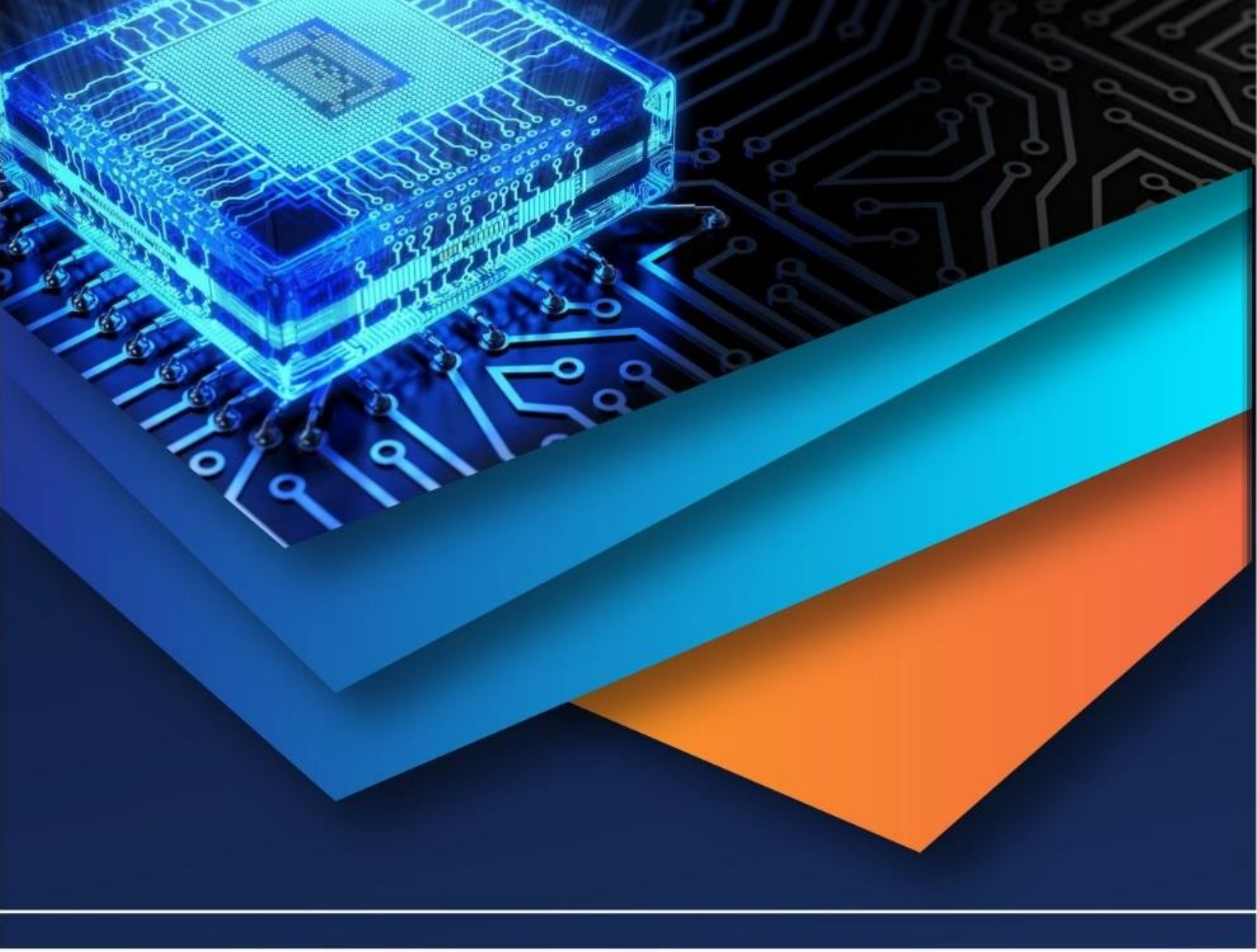
This case study shows the significance of good security measures and risk management procedures in cloud computing while illuminating the potential repercussions of a cloud security breach. It also underlines the necessity of openness and communication regarding security measures between cloud service providers and their clients in order to develop and uphold confidence.

X. CONCLUSION

The flexibility, scalability, and cost reductions offered by cloud computing have revolutionised the way businesses store and handle their data. The adoption of cloud computing does, however, also bring with it a number of security and privacy threats that must be taken into account and minimised. To secure the data of their clients, cloud service providers must prioritise security measures and risk management procedures, and businesses employing cloud services must take proactive measures to manage their own security risks. Building and sustaining secure and dependable cloud environments requires transparency and trust, and good communication between cloud service providers and their clients is key to guaranteeing that security and privacy concerns are handled. Businesses can profit from cloud computing by being aware of the risks and putting robust security and privacy measures in place.

REFERENCES

[1] Hassan Takabi , James B. D. Joshi,(University of Pittsburgh) & Gail- Joon AHN (Arizona State University). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy
[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.
[3] Borkar, A., & Gupta, P. (2019). Cloud Security: A Systematic Review. Journal of Network and Computer Applications, 130, 32-52.
[4] AlZu'bi, Z., & Al-Saraireh, Y. (2020). Cloud computing security and privacy issues: A survey. Journal of Information Privacy and Security, 16(1), 1-21.
[5] Huang, J., & Cai, Z. (2019). Cloud security and privacy: taxonomy and challenges. Journal of Cloud Computing, 8(1), 1-19.
[6] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM conference on Computer and communications security, 199-212.
[7] Yang, K., Lu, Y., & Huang, C. (2014). Privacy and security for cloud computing. IEEE Communications Surveys & Tutorials, 16(2), 843-8



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY