International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website:https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February

DATA PRIVACY ISSUES IN CLOUD ENVIRONMENT

Pratiksha Kuldipsing Patil, pratiksharajput1105@gmail.com
Susmita Pradip Kunnar, susmitakunnar166@gmail.com
Affiliation: Department of Computer Science
Jijamata Mahavidyalaya Smt.G.G Khadse College,Muktainagar

Abstract

Cloud computing is widely used by organizations because it allows them to store and Process data easy, cut costs, scale when needed. However, using cloud services in real-world environments creates several security problems that concern both cloud providers and users. These problems include protecting data from unauthorized access, ensuring data accuracy and availability, managing virtual machines securely, controlling user access, and meeting legal and regulatory requirements. Practical deployment issues such as sharing resources among multiple users, lack of trust between cloud stakeholders, unclear service agreements, and limited ability to respond to security incidents also increase risks. This discussion shows that manysecurity solutions work well in theory but are difficult to apply effectively in real cloud systems. Therefore, strong security measures, clear management policies, and regular risk evaluation are necessary to make cloud computing safe and reliable.

Introduction

The rapid adoption of cloud computing has transformed how organizations store, process, and share data, offering scalability, flexibility, and cost efficiency. However, this shift has introduced significant data privacy challenges due to loss of direct control over information, multi-tenancy risks, cross-border data transfers, and evolving regulatory requirements.

Foundational studies such as Hassan Takabi et al.'s work on security and privacy challenges in cloud environments highlight concerns related to trust, data confidentiality, and access control in outsourced infrastructures.

Subsequent research explores privacy-preserving techniques including encryption, homomorphic encryption, differential privacy, secure auditing, and identity management frameworks to mitigate these risks. Despite these advancements, ensuring real-time privacy protection, regulatory compliance, and secure data analytics in distributed cloud architectures remains an open research problem. This underscores the need for robust, scalable, and adaptive privacy models tailored to modern cloud ecosystems.

Cloud computing, as defined by NIST, enables on-demand access to shared resources Like networks and storage with minimal management effort, characterized by on-Self-service, network, pooling, elasticity, measured. Measured services (Mell and Grance , 2011). Despite these benefits, security and privacy Challenges—such as data breaches, unauthorized access, insecure

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website:https://www.maulikavyanshufoundation.org/IJCTFS/index.ph
p Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February

APIs, multi-tenancy Risks, and denial-of-service attacks—persistently impede adoption (Agarwal et al., 2016;Shahzad, 2014).

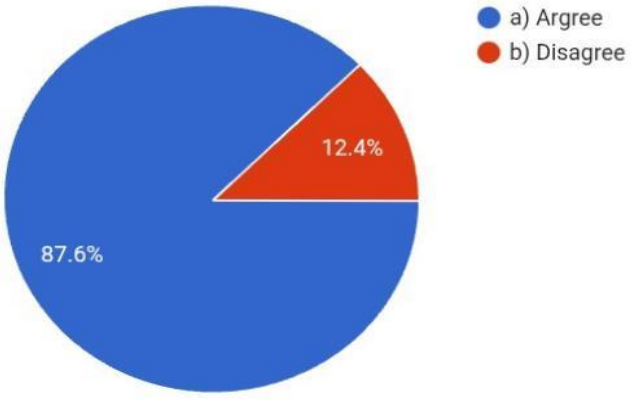
Foundational works like Ting-Ting Yu et al. (2010s), El Makkaoni et al.Controls , and redundancy for service-level protection in multi-tenant environments. Address Evolving threats like Dodos and deepfakes. Surveys such as IJERT (2013, 2017) and PaaS , and SaaS models. This paper reviews these contributions to identify gaps and Propose resilient cloud architectures.

Objective of the study

1. To study the level of awareness among regarding data privacy ricks in cloud computing
2. To analyse were trust in cloud service. Providers for protecting personal & organizational data.
3. To examine concerns related to data breaches in cloud environments
4. To identify user behaviour toward reading & understanding cloud privacy policies
5. To access overall user perception of data privacy challenges in cloud computing.

Data Analysis:

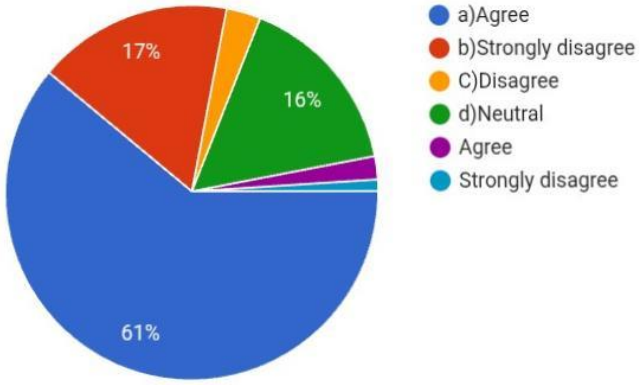
1.cloud data backup processes create privacy risk?



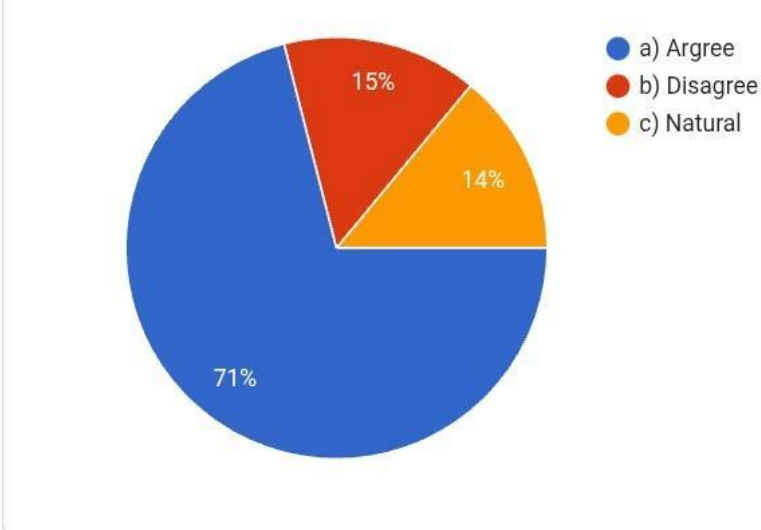
2.I am aware of data privacy risks in cloud computing

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website:https://www.maulikavyanshufoundation.org/IJCTFS/index.php Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February

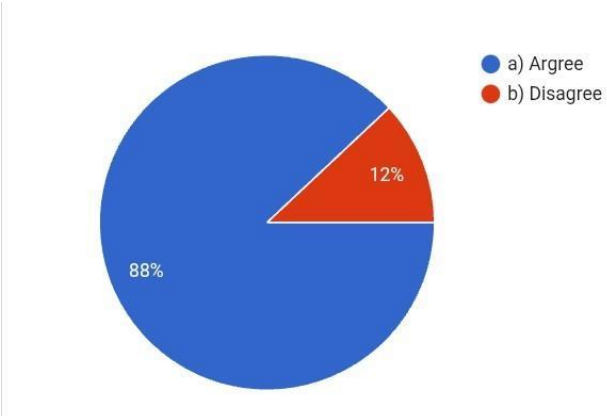
3.I am concerned about data breaches in cloud services.



4. Cloud computing requires an internet computing .



5. I trust cloud platform to keep my personal data secure.



International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website:https://www.maulikavyanshufoundation.org/IJCTFS/index.ph
p Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February

Hypothesis

H1: I am aware of data privacy risks in cloud computing ?

	Oi	Ei	Oi-Ei	(Oi-Ei) 2	(Oi-Ei) 2\E
Agree	69	20	49	2401	120.05
Disagree	10	20	-10	100	5
Strongly disagree	6	20	-14	196	9.8
Neutral	12	20	-8	64	3.05
Yes/No	3	20	-17	289	14.45
Total	100	-	-	-	152.35

Σ(Oi-Ei)2/E = 152.35

Degree of freedom = 6 – 1 = 5

Calculated x^2= 152.35

Tabulated X^2= 11.070

Since 152.35 > 11.070 hypothesis accepted.

H2: I am concerned about data breaches in cloud services ?

	Oi	Ei	Oi-Ei	(Oi-Ei) 2	(Oi-Ei) 2/E
Agree	61	20	41	1681	84.05
Strongly disagree	17	20	-3	9	0.45
Neutral	16	20	-4	16	0.8
Disagree	3	20	-17	289	14.45
Others	3	20	-17	289	14.45
Total	100	-	-	-	114.2

Σ(Oi-Ei)2/E= 114.2

Degree of freedom = 5-1=4

Calculated X^2= 114.2

Tabulated X^2 = 9.488

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website:https://www.maulikavyanshufoundation.org/IJCTFS/index.ph
p Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February

Since 114.2 > 9.488 hypothesis accepted.

Conclusion :

Cloud computing has become an important technology that makes work faster, easier, and cheaper. It gives users access to storage, computing power, and internet services whenever needed. Because of this, companies do not need to spend a lot of money on expensive hardware, and they can manage their resources more easily.

There are different types of cloud services like IaaS, PaaS, and SaaS. These help organizations improve their work and increase productivity. There are also different cloud models such as public, private, and hybrid clouds, which allow organizations to choose what best fits their security and performance needs.

Although cloud computing has many benefits, there are still some challenges like data security, privacy issues, and the need for a stable internet connection. However, with better security systems and new technologies, these problems are slowly being solved.

Although cloud computing has many benefits, there are still some challenges like data security, privacy issues, and the need for a stable internet connection. However, with better security systems and new technologies, these problems are slowly being solved.

Reference

1. Ting-Ting Yu et al. (2010s). Security Issues with Practical Deployment Concerns in Cloud Computing.
2. In their 2016 study, K. El Makkaoni, A. Ezzati, A. Beni-Hssane, and C. Mohamed collaborated to present their research findings. Cloud Security and Privacy Model for Secure Cloud Services.
3. Shaikh, A., & Gadge, J. (2016). Framework for Securing Shared Data in Multi-Tenant Cloud Environments.
4. Anitha, K. L., & Gopalakrishnan Nair, T. R. (2016). Smart Cloud Architecture for Security Issues and Vulnerabilities.
5. IJERT Authors. (2017). A Study and Survey of Security and Privacy Issues in Cloud Computing
6. IJERT Authors. (2013). Security & Privacy Issues in Cloud Computing.
7. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing.
8. garwal, et al. (2016). Evolution and Security Concerns in Cloud Computing.

9. Garg, et al. (2017). Security Techniques for Common Threats in Cloud Setups.
10. Sharma, et al. (2017). Data Security Challenges Across IaaS, PaaS, and SaaS Models.
11. Amara, et al. (2017). Cloud Threats, Architectural Principles, Attacks, and Mitigation Strategies.
12. Shahzad. (2014). State-of-the-Art Survey on Cloud Computing Challenges.
13. Rao & Selvamani. (2015). Data Protection and Privacy in Cloud Computing.
14. Deepali & Bhushan. (2017). Fog Layer for DDoS Protection in Cloud Computing.
15. Rewagad & Pawar. (2013). Digital Signatures and Encryption for Cloud Data Protection.
16. Chennam, et al. (2017). Multistage Encryption Algorithms for Cloud Storage.
17. Zaidi. (2023). Security and Privacy Vulnerabilities in Cloud Environments.
18. Al-Rimy, et al. (2022). Data Security Challenges and Solutions in Cloud Computing.
19. Subashini & Kavitha. (2014). Data Security Obstacles in Shared Cloud Environments.
20. Kumar & Misra. (2024). Privacy and Security in Cloud-Based Digital Transformation.
21. Lashkaripour. (2021). Core Security and Privacy Principles in Cloud Systems.
22. Mohammed Abdul Mateen, et al. (2024). IJCRT2406030: Biometric Authentication Techniques in Cybersecurity. IJCRT.