Grenze International Journal of Engineering and Technology, June Issue

Analyzing and Monitoring Data Security and Privacy Protection Issues in Modern Cloud Computing Systems

Anil Barnwal[1], Satyakam Pugla[2] and Rajesh Jangade[3]
[1-3]Amity University, Noida, UP
Email: barnwal02anil@gmail.com

***Abstract*— Cloud computing is one of the very popular techniques that provide scalable solutions for storing, processing and managing data. To provide complete overview of the topic, the organizational approach analyzes secondary data resources and performs thorough assessment of existing literature. Systematic literature review synthesized research on effects of cloud computing on data management. The review highlights the transformative potential of cloud computing, enabling scalable and adaptable data storage and processing. This empowers businesses to manage large datasets efficiently. Nevertheless, the inherent accessibility of cloud environments presents significant data with confidentiality with more focus on security concerns. Addressing these concerns requires implementing strong security measures, including encryption and access control, alongside adherence to data protection laws like RGDP. Ultimately cloud computing enhances data management techniques that necessitates a strong focus on data security and compliance.**

***Keywords*— Data Storage, Data Privacy, Cloud Computing, Data Management, Encryption, RGDP, Data Integrity, Security Threats.**

I. INTRODUCTION

In modern era, the usage of cloud computing has fundamentally changed the way of managing data, providing numerous ways of processing and storing data [1-2]. Privacy of data is the most important factor as it includes protecting sensitive data stored in the cloud against unauthorized access, cyber-attacks and security breaches.

According to National Institute of Standards and Technology (NIST), cloud computing permits users to access shared computer resources whenever they require [3] through a network. This helps with effective analysis and management of data. However, various difficulties related to securities and privacy of data can be improved using accessibility of cloud.

Privacy of data includes various protection standards like access control, encryption of data and data protection rules like Regulation of General Data Protection (RGDP) that maintains accuracy and secrecy of data by reducing security risks. It is the most important way to generate and maintain faith in cloud computing systems [4].

As the dependencies on cloud services for requirement of data is increasing, it is important to understand and implement secure data protection systems. Various studies examine these important elements to negotiate the complex territory of data privacy and data security in cloud computing environment.

Most important factor of the cloud computing is the protection of private information so that it can maintain the trust and follows the rules of HIPPA (U.S.)

Grenze ID: 01.GIJET.12.2.243_20

Department of health and Human Services) and RGDP. Safety against intellectual property is important here. Some of the key aspects comprise privacy rules, data protection and employment of compliance procedures [5]. This research provides an in-depth analysis of the vital elements to efficiently bargain the complex landscape of security and personal information of cloud computing systems.

II. Review of Literature

The important aim of this review of literature is to inspect the various issues of privacy and data security in cloud computing by going through various journals, books and academic publications. Some of the important aspects include access control, encryptions that follow RGDP regulations and problems faced due to vendor lock-in. The main aim is to integrate various research works by understanding interaction between policy to maintain privacy of data, ethics and technology in cloud computing. The goal of this research is to create the best industrial practices and provide information for future research. Some of the key aspects are:

A. Protection of Data

In cloud computing system, protection of data depends on various encryptions techniques that are used for storing and sending data over cloud. Modern advanced encryptions techniques [6] are used against unauthorized access and protection of data. Accessing the data depends on who is using the data and what permission [7] is given to him. Data security is improved by applying tough access control techniques against unauthorized access and security breach. These combined measures are important for maintaining authenticity and confidentiality of data in cloud computing environments.

B. Privacy of Data

In Cloud computing environment, privacy of data is administered by tough legislative framework like the Regulation of General Data Protection (RGDP) which was applied by European Union in the year 2016. These frameworks implement challenging necessities for data safety [8-9]. Effective agreeable administration is important for compliance as it ensures that users will give well defined consent for data processing tasks [10]. Management is bound to follow transparent regulations that instruct users how to use their private data. Privacy of data is improved by providing specific control on data sharing by using advanced management techniques. Suitable regulations and permissions are required to protect user's personal data so that people develop more faith in cloud computing systems. Some of the important elements of data privacy are shown in table 1. It includes regulatory compliance and permission to develop faith and protection of personal information.

TABLE I: PRIVACY OF DATA PROTECTION

Feature	Details
Agreeable Administration	Effective agreeable administration is needed for ensuring data processing from informed users.
Maintaining Transparency	To fulfill the regulations of transparency, users should explain about the usage of data for organization.
Regulatory Framework	Regulations of general Data Protection (RGDP) impose tough regulations on data protection.

C. Availability of Data

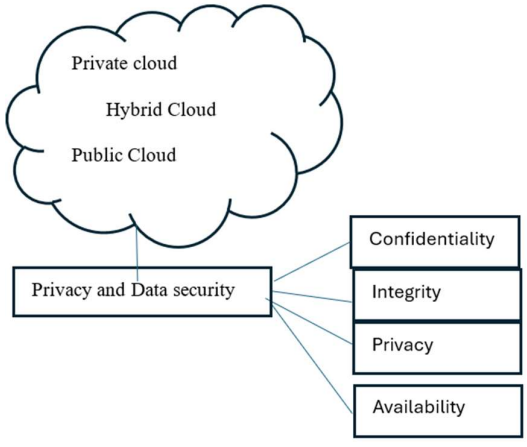

Fig-1: Privacy and data security in cloud computing environment [12-13]

Availability of data is very important in case of theft, hard disc failures and disturbance due to bad network. It tells how a consumer can recover or access data in those situations and autonomously authenticates it when the cloud service provider fails to deliver data.
The main concern of users is how their data is stored on servers worldwide. Cloud providers must obey the rules of countries where their servers are located otherwise it might affect consumers [11]. Users must have knowledge of various legalities. To build confidence, cloud service providers should deal with the various issues of the consumers like integrity, data security and confidentiality. Cloud service provider ensures the data safety and regulations of data storage.

D. Integrity of Data

To avoid unauthorized access and destruction of data, the information system requires data integrity. In standalone systems these issues are solved using ACID (atomicity, consistency, isolation and durability) properties of DBMS. Some new issues are created in cloud computing due to multiple access points and huge size. Tough permission, monitoring issues, digital signatures and RAID methods are required for maintaining integrity of cloud systems. Some of the complex policies related to cloud integrity verification are offered by the HAIL system and Proof of Retrievability concept is provided by Bowers et Al.

E. Confidentiality of Data

To protect data on the clouds often it needs to carry out complex verification processes and access controls. Due to internal risk and data provider's uncertainty, reliability and responsibility of cloud should be enhanced [14]. Directly storing crucial data is risky.
Even after providing complex safety norms and encryption, it sometimes fails to report complex demands such as querying, well-tuned permissions [15] and current updates. To overcome these challenges, it is necessary to upgrade today's security of cloud computing systems.

F. Uncertainties

Cyberattacks and data breaches are the main security threats [16] that arise in today's cloud computing systems. Following the Regulation of General Data Protection (RGDP), a standard of European Union, produces new intricacy by following tough data protection rules. Standards of data control authority tells where data is originated and allowable positions for storage of data. Vendor lock-in puts an important problem by limiting its effectiveness to interchange service providers [17]. It is essential for businesses to handle these problems by ensuring data security, maintaining regulatory supplies and preserving adaptability in cloud computing environments. Below table 2 gives a quicker reference that pinpoints the major problems that an enterprise may face within cloud computing environment and highlights its position and cause.

TABLE II: MEASURE OF UNCERTAINTIES

Uncertainties	Details
Security Problems	Cyber-attacks and data breaches provides important security concerns
Data position	Data dominance rules state where data is located and what are various threats
Regulatory Compliance	Intricacies come from tough data protection rules such as RGDP

E. Reducing Impact

To ensure the safety of data, while it is being sent or stored over the internet, cloud computing uses complex encryption techniques. Restricting unauthorized access [18] and position-based control systems are some of the access control systems. Supervisory agreement includes ongoing investigation and sticking to data protection guidelines like RGDP [19]. Suitable permissible management concepts allow the customers to control their data sharing choices by enhancing privacy [20]. These methods together increase the security of cloud computing by ensuring integrity and privacy of data to follow legal rules. Apart from that, consumers have full control over their personal data. Below table 3 shows a summary to decrease the risks related to cloud security along with concise explanations and importance of each part.

TABLE III: REDUCING IMPACT

Reducing Impact	Details
Encryption	Guarantees protection of data while it is being stored or sent
Access Control	Apply security methods like RBAC to avoid unauthorized access
Regulatory Compliance	Needs investigation and compliance with rules of data protection like RGDP
Agreeable Administration	Allows users to put control on their data sharing thus enhancing more privacy

F. Best Methods

To strengthen the privacy of data in cloud computing, complex encryption technologies are used for safety of data while it is being stored or sent over the cloud. Applying strict access restrictions ensures only authorized users can access the confidential data [21]. Continuous audits boost the strong belief in data protection standards. Transparency over the use of data and steps for managing consent gives consumers a free hand in controlling their data [22]. Applying checks on security, it is possible to apply quicker action plans in case of security breach [23]. These protocols ensure the safety and privacy of data in cloud computing atmosphere.

III. PROCESS

In the paper "Analyzing and maintaining data security and Privacy in current Cloud Computing Systems" researchers have done the review of literature on cloud computing systems, focusing more on security and privacy of data [24-27]. They studied various resources using keywords like cloud computing and RGDP, to find modern tendency [28-32]. Analyzing various case studies and surveys, policies of proper decision making are developed in the environment of data privacy [33-35].

IV. RESULT AND DISCUSSION

The surveys reveal the importance of privacy and security of data in cloud computing environment. To support this survey some important efforts are RGDP compliance, robust encryption techniques, agreeable administration, access control etc. Threats like security exposure and vendor lock-in have been continuously analyzed [36]. To avoid these threats [37] there is the requirement of a comprehensive method and effective procedure which priorities security and privacy of data. To guard sensitive data and preserve digital ecosystem in the growing cloud computing systems [38] it is necessary to prioritize their features. To maintain the use of technology and ethics this trust in the security of data is necessary.

REFERENCES

[1] K.Liu, L.Dong, Research on Cloud Data Storage Technology and Its Architecture Implementation, Procedia Engineering, Vol-29, pp-133-137, 2012

[2] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," Alexandria Engineering Journal, vol. 84, pp 275-284, 2023

[3] S.Hina, M.S.Azhar, G.A Shah, S.Zahid, S.G abbas, Z.Hannif, "Threat Modelling in smart firefighting Systems: Aligning MITRE Attack Matrix & NIST security Control", Internet of Things, Vol -22, pp-1070-1076, 2023

[4] A. Barnwal, V.S.Dixit : Energy efficiency in Cloud computing, International Journal of Scientific Research and Review, vol 4, Issue 2, pp 45-54, 2015

[5] N. A. Rakha, "Cyber Law: Safeguarding Digital Spaces in Uzbekistan," International Journal of Cyber Law, vol. 1, no. 5, 2023.

[6] O. van Daalen, "The right to encryption: Privacy as preventing unlawful access," Computer Law &Security Review, vol. 49, p. 105804, 2023.

[7] D.Draheim, M. Khalid, A. Qadir, S. A. Shah, and S. Hameed, "Towards SDN-based smart contract solution for IoT access control," Computer Communications, vol. 198, pp. 1-31, 2023.

[8] D. J. Solove and P. M. Schwartz, EU Data Protection and the GDPR. Aspen Publishing, 2023.

[9] A. Barnwal, S. Pugla, R. Jangade ; "Various Security Threats and their Solutions in Cloud Computing; International Conference on Computing, Communication and Automation (ICCCA2017)"; pp 773-780, 2017

[10] A. K. Akinwunmi, "Consent As a Mechanism for Control Over Personal Data," 2023.

[11] S. Davis et al., "Cloud security in a bioanalytical world: considerations for use of third-party cloud services for bioanalysis," Bioanalysis, no. 1, 2023.

[12] S. P.Praveen, R. Balamanigandan, and S. S. Vellela, "Strategic Survey on Security and Privacy Methods of Cloud Computing Environment," Journal of Next Generation Technology, vol. 2, no.1, 2022.

[13] A. Barnwal, A. Dwivedi, R. Jangade, S. Pugla , "Effective Management of Security of Risk in Cloud Computing Environment, International Conference on Sustainable Computing Techniques in Engineering, Science and Management"; vol 9; issue 23; pp 211-218, 2016

[14] U. R. Saxena and T. Alam, "Provisioning trustoriented role-based access control for maintaining data integrity in cloud," International Journal of System Assurance Engineering and Management, vol. 14, no. 6, pp. 2559-2578, 2023.

[15] X. Jia, Y. Ming, Y. Guo, M. Wang and C. Zhang,"Encrypted and Compressed Key-Value Store with Pattern-Analysis Security in Cloud Systems," IEEE Transactions on Information Forensics and Security, 2023.

[16] M. S. Malik, M. Zubair, and H. Akbar , "The Security Issues and challenges in Cloud Computing," International Journal for Electronic Crime Investigation, vol. 7, no. 1, pp. 13-32, 2023.

[17] T. Weldemicheal, "Vendor lock-in and its impact on cloud computing migration," ed, 2023.
[18] O. Zorlu, A. Ozsoy, and S. A. Sert, "A Role-Based Access Control Management Model on Blockchain for Restricted Facilities: An Airport Example," in 10th International Conference on Recent Advances in Air and Space Technologies (RAST), pp. 1-6: 2023.
[19] Bertolaccini et al., "The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database," European Journal of Cardio-Thoracic Surgery, vol. 64, no. 3, 2023.
[20] S. T. D. G. Erdogan, "Check for A Need for Privacy Assistive Technology in Notice and Consent Paradigm in IoT," in Digital Sovereignty in Cyber Security: New Challenges in Future Vision: First International Workshop, CyberSec4Europe 2022, Venice, Italy, April 17–21, 2022, Revised Selected Papers, 2023, p. 35: Springer Nature.
[21] T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O.Olaniyi, and O. J. Okunleye, "Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach," Available at SSRN 4612909, 2023.
[22] H. Asgarinia, A. Chomczyk Penedo, B. Esteves, and D. Lewis, ""Who Should I Trust with My Data?"Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies,"Information, vol. 14, no. 7, p. 351, 2023.
[23] O. M. Agbede, "Incident Handling and Response Process in Security Operations," 2023.
[24] D.H. Parekh, R.Sridharan, "An Analysis of Security Challenges in Cloud Computing" , IJACSA, Vol 4, No 1, 2013
[25] J.J.Angudi, "Security challenges in cloud computing: A comprehensive analysis", World Journal of Advanced Engineering Technology and Sciences, 2023
[26] R.Soni, N.Uikey, "Cloud Computing Security and Challenges: An In-Depth Analysis", International Journal on Science and Technology (IJSAT), Vol 16(2), 2025.
[27] M.Alenezi, "Safeguarding Cloud Computing Infrastructure: A Security Analysis" , Computer Systems Science and Engineering, Vol 37(2), 2021
[28] R. K. Sharma, "Multi-Tenant Architectures in Modern Cloud Computing: A Technical Deep Dive", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol 11, No 1, 2025.
[29] B. Varghese, R. Buyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, vol 79, pp 849-861, 2018.
[30] P. K. Paul, P. S. Aithal, "Cloud Security: An Overview and Current Trend", International Journal of Applied Engineering and Management Letters (IJAEML), Vol 3(2), pp 53-58, 2019.
[31] C.Yang, Q. Huang, Z. Li, "Big Data and cloud computing: innovation opportunities and challenges", INTERNATIONAL JOURNAL OF DIGITAL EARTH, Vol 10, No 1, pp 13-53,2017.
[32] G.N. Phu, T.H.Thi, H.T.N.Bich, "The impact of cloud computing technology on cloud accounting adoption and financial management of businesses", Humanities and Social Sciences Communications, 2025
[33] A. Ateeq, "The Mediating Role Of Engagement In The Relationship Between," Management, vol. 21, no. 3, pp. 435-447, 2023.
[34] F. S. M. Al Balushi, A. A. A. Ali, and M. Alzoraiki,"The Impact of Forecasting Strategy and Training and Development Strategy on Preparing Leadership Competencies Administrative Support in the Sultanate of Oman," International Journal of Intellectual Human Resource Management (IJIHRM), vol. 3, no. 01, pp. 34-41, 2022.
[35] M. H. Allaymoun, M. Khaled, F. Saleh, and F.Merza, "Data Visualization and Statistical Graphics in big data analysis by Google Data Studio–Sales Case Study," in 2022 IEEE Technology and Engineering Management Conference (TEMSCON EUROPE), pp. 228-234, 2022.
[36] R. S. S. Dittakavi, "Evaluating the Efficiency and Limitations of Configuration Strategies in Hybrid Cloud Environments," International Journal of Intelligent Automation and Computing, vol. 5, no. 2, pp. 29-45, 2022.
[37] N. Hussain, P. Rani, H. Chouhan, and U. S. Gaur, "Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues," Federated learning for IoT applications, pp. 169-183, 2022.
[38] B. Krishna, S. Krishnan, and M. Sebastian, "Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective," Information Technology & People, 2023.