DOI: https://doi.org/10.17762/ijritcc.v11i6.7379
***Article Received**: 25 March 2023 **Revised**: 10 May 2023 **Accepted**: 15 June 2023*

A Behaviour Study on Cloud Eco-System: Data Security Perspective

Niyati Gaur[1], Dr. Shashank Singh[2],
[1]Research Scholar, Department of Computer Science & Engineering, Integral University, Lucknow
[2]Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow

Abstract— Cloud eco-system is a revolution now, which modifies the way in which the IT-based services are being delivered to end customers. It is increasing or we can also say grown-up technology that delivers multiple benefits whether in terms of economics or in terms of cost-effective resource utilization. The ability to install and improve their services on that platform is made possible by the advent of cloud computing, which opens up new options for long-term solutions. Cloud computing's environmental and economic impacts must be considered while assessing its long-term viability. A growing number of organizations, businesses, and personal users are depending on services supplied by the cloud and keeping crucial information in the cloud because of its easy-to-use characteristics. The cloud, despite its widespread use, nevertheless has a number of drawbacks when it comes to data security. Customers are concerned about how their personal information is transported to and from the cloud. Research articles in this topic have been thoroughly analyzed and examined in this report.

Keywords- Communication technologies; Data Security, Cloud computing.

I. INTRODUCTION

When considering what IT in general needs: a method to expanding the capacities of a framework on-the-fly without contributing any new foundation, preparing another crew, or approving any new programming, the focus on data security in cloud computing becomes clear. Today, cloud services offer subscription or pay-as-you-go support; the services are delivered through the Internet in real time, which increases basic IT abilities into powerful regional capabilities (Rosado DG, 2012). Many security concerns arise when massive server farms are used to host applications and databases. Cloud computing security becomes more of a focus after considering how to maximise an airplane's power without building another base, preparing a new flight crew, or authorising any new system: (Akhter, 2016). In the second decade of this century, cloud computing appears to be one of the primary areas of development in information and communication technology. When new wireless data transmission technologies and internet coverage grow, new kinds of services can be made possible (S. Singh, 2016). Cloud-hosted services are becoming increasingly popular as a more flexible alternative to traditional local programmes that are bound to a single machine because of the proliferation of computing devices, especially mobile ones. There are huge economic and environmental incentives for research into ways to minimise energy consumption in rising data centres, and there are also major power consumption challenges on both ends of the system as mobile devices require good energy management to extend their battery life (Q. Shaheen, 2018). A decade ago, the topic of energy efficiency in data security in cloud computing systems arose as a relatively new field of scientific investigation. An growing number of papers are being published as a result of this increased study interest.

II. CLOUD DATA SECURITY

Adoption is hampered by concerns over security, compliance, privacy, and other legal considerations. Both the process by which programmes may be transferred to the Cloud Computing platform and the means by which Cloud Computing can be rendered safe at all levels (including the network, the host, the application, and the data) are the subjects of a significant amount of scepticism (S. Singh, 2016). Because of this unpredictability, the security of cloud computing has been regularly cited as the major fear by persons in charge of information technology. External data storage, dependence on the "public" internet, lack of control, varied tenancies, and integration with internal security measures are all potential danger areas (Li W, Ping, 2009). (Li W, Ping, 2009). (Li W, Ping, 2009). The cloud is separated from conventional technologies by a wide range of specific qualities, such as its large scale and the fact that the resources given by cloud providers are globally scattered, very diverse, and entirely virtualized. Traditional security methods, such as identity, authentication, and authorisation, are no longer essential for cloud computing since they are no longer needed. The security procedures applied in cloud computing are, for the most part, substantially identical to those used in any other type of information technology system. On the other side, cloud computing may provide businesses with risks that are distinct from those posed by conventional IT solutions. This is because there are many alternative cloud service models, operational models, and cloud service technologies that may be employed. The sad reality is that when security is built into the architecture of these systems, people regard them as being less adaptable. It is a significant source of concern for businesses that are moving essential applications and sensitive data to public cloud settings over which they have no control. It is the responsibility of cloud solution providers to ensure that the applications and services of their customers are protected by the same level of security and privacy controls that their customers currently have, to demonstrate to their customers that their organisation is secure and that they can meet the service-level agreements that they have made, and to demonstrate compliance to auditors (S. Puhan, 2020). When SaaS consumers are forced to rely on their suppliers for effective security, the issue of data protection becomes even more of a burden. Organizational data is routinely handled and retained on the cloud in unencrypted in SaaS. It is the role of the SaaS provider to assure that data is secure while being processed and stored. In addition, data backup is crucial for disaster recovery, but it also raises security concerns (Fernandes, 2014). (Fernandes, 2014). Concerns may develop around cloud service providers subcontracting additional services such as backups to third-party service providers. Most compliance rules, on the other hand, don't take cloud computing into account. Due to data being in the datacenters of the SaaS provider, regulatory compliance concerns including data privacy, segregation, and security may arise that must be maintained by the provider in order to remain compliant. Amazon and Ali Baba were early adopters of cloud computing, which was first introduced in the mid-1990s. Many security reviews, on the other hand, are attempting to develop more effective defences (see figure 1).

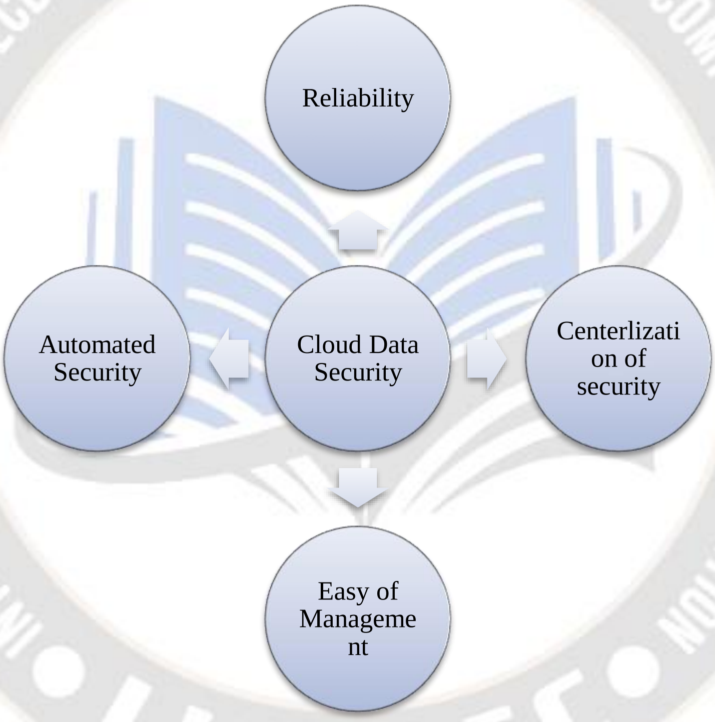

Figure 1: Data security domain in Cloud Environment

The discipline of computer science is seeing a rapid expansion at the moment. Cloud computing is being used to an extremely extensive degree by people these days. The Internet serves as the primary platform for cloud computing, which utilises the most advanced computational architecture available. The greatest concern that follows the deployment of an individual's cloud-based platform is that of the platform's safety. Because a cloud, as was said earlier, is web-based in its whole, obtaining data from a specific cloud is not something that is in any way difficult. The proliferation of cloud computing has led to an increase in the complexity of the associated security risks. Increasing numbers of individuals are becoming aware of the technology that simplifies the process by which they may break into various clouds and get the information that they want. Because so many companies have begun providing cloud-based solutions to their clients, ensuring the customers' data is secure is now one of the primary focuses of their efforts.

III. LITERATURE REVIEW

According to the findings of the research, we discovered that cloud computing is plagued with a number of problems, the most significant of which is related to security concerns. Approaches to energy-efficient resource management in cloud systems are now a hot issue that is being extensively researched by a lot of people.

M. Zakarya (2017) survey energy-aware data centre resource allocation. Virtualization, VM allocation, energy efficiency, power consumption, and cloud computing were studied. They've compared energy-aware cloud system designs to conventional and virtual data centres. This Study has further proposed taxonomy for energy-saving methods in cloud data centers, which were studied in three levels, such as power management, resource management, and thermal management. They have shown that the energy-saving approach became possible using renewable energy that plenty of recent research introduced this strategy. **Q. Shaheen (2018)** authors have presented a brief survey describing primary energy-conserving techniques in the cloud environment. To add, they have classified energy consumption approaches into five categories, including energy-efficient hardware, energy-aware scheduling, consolidation, energy conservation in a cluster of servers, as well as power-efficient networks. Finally, they have evaluated a few papers based on this classification. The researchers further have focused on consolidation techniques in three levels, containing task consolidation, server consolidation, and energy-aware task consolidation. **S. Puhan (2020)**have performed a comprehensive survey on energy-efficient computing, clusters, grids, and clouds. They have reported a number of approaches in the literature which contributed to improve energy efficiency. This chapter has proposed three taxonomies, covering such levels as scheduling, energy efficient computing, as well as energy-efficient technique at different levels to make data center greener. **M. Zakarya (2017)** studied the energy efficiency of a single system and large-scale cloud data centers, storage systems, and networking. Scientists in **Q. Shaheen (2018)** have reviewed energy-saving strategies in computational clouds. They explored state-of-the-art related to energy efficiency as well as performance administration, vitality for effective data centers, and resource distributions**(Jansen, W. A., 2011)**. What is more, they have studied the existing techniques in four stages, including tools, OS, virtualization, and data center. Their proposed taxonomy was divided into static and dynamic power management at the highest level. Businesses and attackers alike stand to gain greatly from the use of cloud computing, and both groups will be able to reap the benefits (Jamil, D, 2011). It is impossible to overlook the endless potential of cloud computing just because of the security concerns, and this may be the only channel of inspiration for cloud computing security models (Bhadauria, 2011). Multi-tenancy design can reduce the effect of security vulnerabilities in cloud computing. There are several security methods that are covered in practically each article, and they give some way to think about and mitigate such risks (Tianfield, 2012). The level of data security may be raised by including the server farm. Management providers may currently offer management solutions that give the highest level of security while also managing the expenses of a customer or organisation autonomously, thus security is superior to any standard framework (Chen, D, 2012). In any case, leveraging a variety of devices to gain management access while maintaining a high level of protection improves the overall security environment. However, the private cloud management approach provides the company with control over data or security information (Hamlen, 2010). In a cloud-based computing environment, the IT industry gains substantial advantages in terms of best practises and management frameworks (Fernandes, 2014). However, it has not been fully evaluated, and there are relatively limited options for information security challenges, such as different communication or management models. There are. Security concerns play a role in cloud killing. There are dedicated co-ops responsible for ensuring that frameworks and information are secure. A variety of ways and strategies are used to address these issues, such as multi-sensory, verification tools and cryptographic procedures; nevertheless these developments and techniques have few elements in the context of professional application (Hashizume, 2013). A variety of cloud-based monitoring and assessment methods will be used to properly examine and identify relevant security concerns. Cloud computing security relies heavily on identifying and addressing potential threats. It's no longer in the hands of specialised companies to control data, online applications, and management in the cloud; here, as well, a few free control issues surface to validate the specifics (Jensen, 2009). What else can I say? There is more. Data security, privacy, integrity, accessibility, encryption, and risk associated with web conferencing (IP) are all factors that must be considered when deciding how to manage the cloud. This includes ensuring that only authorised individuals have access to sensitive information, as well as addressing issues with data protection, personality management, assurance, robustness, privacy, integrity, and accessibility (S. Kaur, 2016). Security and separation are just two of many other concerns that must be addressed, such as the SLA (management contract between the professional organisation and the client), executions, dangers of perception, non-compliance, and strategic assessment.

Article Received*: 25 March 2023* ***Revised****: 10 May 2023* ***Accepted****: 15 June 2023*

Table 1 Effective instances For Data security in cloud environment accepted by Authors

Author ↓	Data Security in Cloud environment Instances →	Availability	Non-repudiation	Integrity	Confidentiality	Identification and authentication
Zhao G et. al. (2009)		√	√	√	√	√
MarinosAet. al. (2009)		√	√	√	√	√
Zhang Set. al. (2010)		√	√	√	√	√
M. M. Boroujerdi**et. al.**(2009)		√	√	√	√	√
F. Scott**et. al.**(2010)		√	√	√	√	√
N. Akhter**et. al.**(2016)		√	√	√	√	√
S. Ramgovind**et. al.**(2010)		√	√	*	*	√
A. Hammoud**et. al.**(2020)		*	√	*	√	√
C. Puliafito**et. al**. (2020)		√	√	√	√	*
Y. Mansouriet. al. (2021)		√	√	√	√	√
S. Ahamadet. al. (2021)		*	√	√	√	√
R. R. Patilet. al. (2018)		√	*	√	√	√
S. Puhanet. al. (2020)		√	√	√	√	√
Q. Shaheenet. al. (2018)		√	√	√	√	√
S. Singhet. al. (2016)		√	√	*	√	√

IV. NEED OF REVIEW

The cloud computing data security is a very important factor. This article deals with cloud computing and data security issues. The major key security problems in cloud computing is privacy and server availability. The traditional security method can’t solve the cloud security problem. The new hybrid method is to fulfill the cloud security needs. The characters ofcloud computing is scalability and reliability. They provide better service for the user and cloud computing provides transparent application service in remote resource access. The user can access data anywhere from the world. The cloud computing connected with more hardware resources its increase the capacity of server load. The cloud resources provide the service based on user needs. The cloud resource should be computing and storing in remote servers. The development of information technology field cloud computing is one of the major role. It provide higher storage platform with an affordable cost. The concept of virtualization technology provide reliable cloud data service. The cloud data is stored in virtual server user can’t protect their own data, they depends on the server provider. The service provider should give assurance of user data privacy and security. The industry store more data in cloud platform other people easily seen their personal data. The cloud service providing company give more importance of data security, then only customer trust their company and use their cloud platform. In traditional system hackers very rare to hack the individual data, but in the same situation cloud data storage hackers easily try to hack larger data. Avoiding this scenario higher level of data security is needed. The cloud computing administration deals with more problems in data security and privacy protection in cloud platform. The property of cloud computing sometimes traditional security problems may also occur like as virus, data hacking and security vulnerabilities.

V. CRITICAL OBSERVATION

Experts have given some specific statement in below order:

- Identification and Authentication Management refers to the functional checks for user identification and authentication that prevent malicious behaviours inside the cloud. These checks are carried out in order to ensure that users are who they say they are. **(E. Mathisen, 2011)**
- Controlling access to cloud resources may be a complicated process, especially when several people are accessing the same service at the same time. **(D. Zissis, 2010)**
- Security is compromised by the large number of cloud access points and users, which makes it vulnerable to impersonation by unauthorized parties and pirate persons. Clouds must take precautions to guarantee that only authorized users get access to their information **(D. Abraham, 2009)**
- Integrity is a cloud characteristic that is concerned with protecting cloud software against third-party undesirable acts like as fabrication, theft, deletion, and change. It is also known as data integrity. Atomicity, consistency, isolation and durability (ACID) are four characteristics of data integrity that are connected with a cryptographic key **(F. Scott, 2001).**
- Non-repudiation ensures that the sender and receiver of a communication are indistinguishable, making it impossible for either party to evade accountability for an action. **(S. Ramgovind, 2011).**
- Availability refers to the consistency of both hardware and software, both of which must be readily available to the user. There are no justifications for the CSP's inability to deliver these services, even in the case of system problems, fraudulent activity, or security breaches on their end. **(M. M. Boroujerdi, 2009).**

The security and risk assessment would include an examination of the effect that a range of threats and assaults would have on many areas of cloud computing, such as the adaptation of cloud computing, the preservation of secrecy and privacy of personal data, and the access and updating of data. As a result, it has become of the utmost importance for all company activities to be conducted in the cloud to locate the solution instructions that are most suitable and will increase security and privacy in the cloud environment.

VI. DISCUSSION

As a result of its cost-effectiveness and dynamic provisioning, cloud computing may be thought of as a flexible computing paradigm However, if the cloud's security issues aren't properly addressed, it might have a negative impact on cloud acceptance and growth. Organizations that deliver software, platforms, or infrastructures as a service via the cloud confront security challenges, as do the users of those services (companies or organizations who host applications or store data on the on the cloud). The cloud provider and the user both share the primary duty of ensuring that their cloud environment is safe and that their user's information and data are secure and transferred when the user accesses their data and cloud applications currently here. When a cloud administrator or agency decides to employ pre-existing cloud applications stored in a cloud data centre to store user data, the user can then upload that data to the cloud. Its output is highly sensitive, and confidential information is at danger from some attacks. Recently, the Cloud Computing In cloud computing, the security of some attack is a big concern. The cloud service provider now has to guarantee that all of the background information is in order. Perimeter complacency is a common problem with private clouds. Users assume that because the cloud is located on the company's internal network, it is safe from the Internet and viruses. Even if it is private, care and security requirements should not be reduced. You must also have complete control over all tiers of the stack in order to implement any typical network perimeter security measures. Users of the cloud rely on the cloud to store enormous amounts of data. To prevent unauthorised access to the stored data, the data owner should implement the appropriate security system, which assures confidentiality, integrity, and authentication. Attacks like eavesdropping and data leakage are possible in the cloud and can undermine confidentiality of data.

REFERENCES

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.

[2] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.

[3] Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011.

[4] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.

DOI: https://doi.org/10.17762/ijritcc.v11i6.7379
***Article Received**: 25 March 2023 **Revised**: 10 May 2023 **Accepted**: 15 June 2023*

[5] Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10) 2010, 278–281.

[6] Mr. Dharmesh Dhabliya. (2012). Intelligent Banal type INS based Wassily chair (INSW). International Journal of New Practices in Management and Engineering, 1(01), 01 - 08. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/2

[7] Jorvekar, G. N. ., Arjariya, T. ., & Gangwar, M. . (2023). Hybrid Feature Selection Techniques for Aspect based Sentiment Classification using Supervised Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 211 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2619

[8] Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.

[9] Joseph Miller, Peter Thomas, Maria Hernandez, Juan González,. Adaptive Decision Making using Reinforcement Learning in Decision Science. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/204

[10] Li W, Ping L: Trust model to enhance Security and interoperability of Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.

[11] N. Akhter and M. Othman, "Energy aware resource allocation of cloud data center: Review and open issues," Cluster Computing, vol. 19, no. 3, pp. 1163–1182, 2016.

[12] S. Singh, A. Swaroop, A. Kumar, et al., "A survey on techniques to achive energy efficiency in cloud computing," in 2016 International conference on computing, communication and automa- tion (ICCCA), IEEE, 2016, pp. 1281–1285.

[13] M. Zakarya and L. Gillam, "Energy efficient computing, clusters, grids and clouds: A taxonomy and survey," Sustainable Computing: Informatics and Systems, vol. 14, pp. 13–33, 2017.

[14] Q. Shaheen, M. Shiraz, S. Khan, R. Majeed, M. Guizani, N. Khan, and A. M. Aseere, "Towards energy saving in computational clouds: Taxonomy, review, and open challenges," IEEE Access, vol. 6, pp. 29 407–29 418, 2018.

[15] S. Puhan, D. Panda, and B. K. Mishra, "Energy efficiency for cloud computing applications: A survey on the recent trends and future scopes," in 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), IEEE, 2020, pp. 1–6.

[16] S. Kaur and S. Bawa, "A review on energy aware vm placement and consolidation techniques," in InternationalConferenceonInventiveComputationTechnologies(ICICT), IEEE, vol. 3, 2016, pp. 1–7.

[17] Jensen, M., Schwenk, J., Gruschka, N., &Iacono, L.L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.

[18] Sharma, M. K. (2021). An Automated Ensemble-Based Classification Model for The Early Diagnosis of The Cancer Using a Machine Learning Approach. Machine Learning Applications in Engineering Education and Management, 1(1), 01–06. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/1

[19] Hashizume, K., Rosado, D.G., Fernández-Medina, E., & Fernandez, E.B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), 5.