MULTI-POINT DATA SECURITY MECHANISM TO FACILITATE SECURE CLOUD DATA STORAGE SOLUTIONS

[1]Vineesh R, [2]Dr. M K Jeyakumar

[1]Research Scholar, [2]Professor, Dept. Computer Application
[1]Noorul Islam Center for Higher Education
[2]Cloud Computing, Cloud Data Storage, Cloud Service Providers, Cloud Data Storage Security

***Abstract*- This literature review's objective is to present information on the application of Multi-Agent System (MAS) strategies that can help cloud computing platforms ensure the security of their cloud data storage (CDS). The proactive and reactive capabilities of MAS, which are frequently deployed, are highly helpful for cloud data storage security (CDSS). A collection of agent communities make up the system's architecture. In this study, we construct a multi-cloud environment for secure data storage that functions as a public cloud, offers affordable pricing, and employs two layers of encryption for the data kept in the cloud. Additionally, cloud computing introduces a new paradigm and makes it easier for users to use information storage so they may build dynamic apps that can be accessible from anywhere via the internet. The cloud makes use of various storage systems where data is remotely managed, supervised, and backed up. The end customers can keep their data online thanks to this service. so that consumers can utilise the internet to access the data from any place and at any time. Usability, bandwidth, accessibility, disaster recovery, and cost savings are advantages of adopting cloud storage. We employ a powerful AES algorithm that offers greater anonymity and privacy for a number of users in the cloud and keeps the data in many clouds so that users can later retrieve it with the keys while granting access to it via cloud-based access control. The two main concerns in this area are security and pricing, and they vary substantially depending on the provider one chooses.**

Keywords: **Cloud Computing, Cloud Data Storage, Cloud Service Providers, Cloud Data Storage Security.**

1. INTRODUCTION

The National Institute for Standards and Technology (NIST) defined cloud computing as "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 little management effort or service provider interaction" (Badger et al., 2011). Both public and private enterprises can profit from modern cloud computing's evolving methodology's cost-saving calculations and adaptable services provided by Cloud Service Providers (CSP). Using a suitable access policy, CSP must guarantee the confidentiality, security, and integrity of outsourced data storage.

A cutting-edge advancement in technology, cloud computing offers remunerated access to hardware and software resources. The crucial method for managing several tenants in the usage of resources to conceal data movement from customers is virtualization. The capacity to supply services using internet resources to external consumers is made possible by the immense flexibility of cloud computing. A typical cloud computing model that provides sharing services through the internet. (Jaber and Zolkipli [17]).

The term "cloud computing" describes both the hardware and system software in the datacenters that provide the applications as services via the Internet. Based on who offers the cloud services, NIST (Badger et al., 2011) identified four fundamental cloud delivery models. For effective and optimum delivery of applications and business services, the agencies may use one model or a combination of other models. the following four delivery models:

(i) *Private cloud* in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.
(ii) *Public cloud* in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service.
(iii) *Community cloud* in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). These services may be managed by the organizations or a third party and may exist offsite.

Figure 1. Cloud Computing Model

2. REVIEW OF LITERATURE

A new security system is presented by Dinesh Devkota et al. (2015)[1] that will protect cloud computing services from hacks and invasions. It has also been studied how to secure servers used for data storage and cloud computing. In addition to these methods, a recently created method for security in cloud-based servers (MIST) has been provided.

Neha Kajal et al. (2015)[2] conducted an analysis of the many security issues that need to be fixed in order to make cloud computing more secure. This will help to improve the cloud computing's potential advantages, making it impossible for consumers to reconsider adopting it.

Cloud computing was discussed by Tejinder Sharma et al. in [2013][3]. A new paradigm for large-scale distributed computing called cloud computing is beginning to emerge. Large data centres now house computing and data that was formerly stored on desktop and portable PCs. It has the capacity to make use of remote resources by leveraging the power of the Internet and wide area network. Cloud computing has a lot of security problems.

Peng Yong et al. (2012)[4] analyzed the researcher's contributions to adapt cryptographic techniques for cloud storage security. The relationship between cloud storage and cryptographic techniques was reviewed for identifying the application likelihood of cryptographic techniques in cloud storage. The research analysis shows that implementing cryptographic techniques in cloud storage ensures the security of the data stored in the cloud and provides a research direction for developing efficient cryptographic solutions to bring out security enhancements in cloud storage.

Luca Ferretti et al. (2014)[5] have proposed adaptive encryption withnovel architecture for public cloud databases. The encryption techniques proposed to increase the confidentiality level and novel architecture recommended reducing the cost of access in cloud databases. The proposed architecture's performance and feasibility were investigated with a large set of experiments to ensure confidentiality and decrease data access cost. The proposed scheme left multi-user data access, storage, and key management as an open issue.

Ricardo Padilha & Fernando Pedone (2015)[6] insist that cloud computing need to incorporate data confidentiality for secure data storage and access. For byzantine fault-tolerant systems, the study focused on implementing a firewall, cryptography, and secret sharing based systems to achieve data confidentiality in the cloud. The confidentiality cost has become a fair trade-off in the cloud
environment.

- ***Mobile cloud computing***

Mobile cloud computing is an architectural pattern where data storage and CPU-intensive processes are performed on the cloud and mobile devices are largely used as thin clients to connect with the application and render results handled from the cloud environment. The various strategies were discussed as follows: Lazaros and his colleagues [5] argued that new cloud model and migration techniques are necessary to successfully bring cloud compute closer to mobile users. It consists of a local cloud attached to the remote access infrastructure and a back-end cloud. This can be broken down into a number of task migration policy classes, ranging from absolutely awkward ones. Up until the general migration procedure of a cloud provider, each client or server independently decides on its relocation options [6].

Liang and his coworkers [7] put up a sound strategy that carried out the novel concept. Deterministic Finite Automata Based functional PRE is a broad notion for Proxy Re-Encryption (PRE) (DFA-based FPRE). The original and most reliable DFA-based FPRE framework that adapts to the novel concept. In this scheme, a message is encoded in a figure content associated with a record string of self-assertive length, and a descriptor is only true if a DFA associated with his/her mystery key recognises the string. A semi-trusted intermediary who has been handed a re-encryption key is allowed to modify this encryption to another figure content associated to another string.

Chu and his coworkers' [8] demonstration of how to effectively, safely, and adaptably share information in distributed storage, as well as the specified limit of the number of most severe ciphertext classes, is also included. Typically, the amount of ciphertexts in the distributed storage increases quickly. They describe novel open key cryptosystems that produce ciphertexts of constant size, making it possible to perform clever decoding operations on any collection of ciphertexts. This is more flexible than different levels key assignment, which can only maintain spaces if all key-holders have a similar course of benefits.

➢ ***Integrity and Forward security***

Integrity, regarding data and framework security, is the affirmation that information must be accessed or adjusted by those endorsed to do all things considered. Actions were taken to ensure integrity incorporate controlling the physical state of networked terminals and servers, restricting access to data and keeping up exhaustive authentication ones.

Author	Cloud Security Yes/ No	Data Sharing Yes/ No	Algorithm	Threats Yes/ No
Indalecio *and his colleagues* 2016,[9]	Yes	Yes	Apache CloudStacks interface	NO
Mauro *and his colleagues* 2016,[10]	Yes	Yes	Optimal control and Predictive control, Energy-aware consolidati-on and Monte Carlo optimization	No
Dai *and his colleagues* 2016, [11]	Yes	Yes	MinES and MinCS yield scheduling	No
Li *and his colleagues* 2016, [12]	Yes	Yes	SecCloud	No
Heng *and his colleagues* 2016, [13]	Yes	Yes	Ciphertext-Policy Attribute-Based Encryption	No

Table 1: *Comparison of Related Works*

➢ ***Data confidentiality***

Information security is basically that territory of the law that administers what may and what may not with individual data stored on the cloud.

Wen et al [14] concentrated on managing data and the convergent key when users frequently updated it and they planned to improve schemes to support data owner privacy preservation by a session-key based concurrent key administration method, called SKC, to protect the dynamic overhaul in the information De-duplication. Convergent key management systems SKC and Convergent Key Sharing (CKS) for cross-user data deduplication in the Cyber-Physical Social System are proposed (CPSS). Every owner of information can verify the correctness of the convergent key in SKC, and CKS

can dynamically renew the convergent key and support multiple Local Communication Networks (inter-LCNs) data deduplication without the aid of a gateway (GW).

Zhang et al[15] .'s discussion of the adoption of public cloud computing administrations covers administrative consistency, data security and protection, management acceptable requirements, and more. Clients may view the author's hybrid cloud computing approach as a realistic and cost-effective way to maximise the benefits of both their private (old) server farms and the public cloud. These demonstrate the construction of a hybrid cloud computing model, allowing users to construct a distinct architecture in which a dedicated asset stage continues to operate to provide base administration workload and a different and shared resource platform handles peak flash crowd load.

➢ ***Social cloud computing***

It is a shared social distributed computing. In cloud computing to incorporate the sharing, bargaining, and leasing of computing resources across over associates whose proprietors and administrators are checked through a social network or reputation system.

To use online connections in social networks to infer a level of trust between customers, Chard et al [16] analysed associations that are generally seen as genuine connections. The idea was to create a dynamic "Social Cloud" using these connections, giving users the ability to exchange a variety of resources within a social community. Additionally, the inherent socially restorative mechanisms (motivations) can be used to empower a cloud-based system for long-term offering to reduce security concerns and overheads are present in traditional cloud settings. A social commercial space serves as a mechanism for controlled sharing due to the unusual way the Social Cloud works. The social market is unique in that it uses societal and monetary practises to promote exchange.

3. Results

There has been a lots of research in the field of cloud computing in recent years. Out of the numerous publications published since 2001, 69 papers that are pertinent to the research's objectives have been extracted by SLR. Results and analysis of the papers that were extracted during the SLR process are covered in this part. In the appendix section, we have provided a full overview of the list of identified difficulties and mitigation strategies. In recent years, research has mostly concentrated on services like grid computing and has followed distributed computing. The research on the new paradigm of cloud computing, which is the next generation of computing, has accelerated over the past ten years. In the past ten years, we have mostly concentrated on security-related elements of cloud computing. During the literature review, a total of 69 papers were located. The majority of the studies that were chosen were published between 2010 and 2011, which yielded 52 papers and 25 papers, respectively. among the others are three papers released in 2009. The graph below displays empirical data from studies on cloud computing security conducted during the previous ten years.

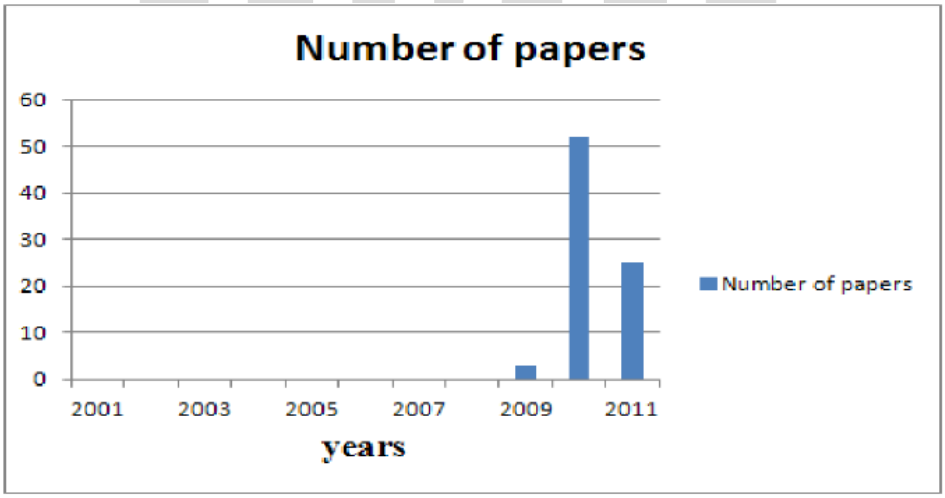

Figure 2: Number of papers published in year wise

4. CONCLUSION

In this research, we describe a novel technique for data storage privacy protection in a multi-cloud setting. Because of its technical capabilities, it also offers a number of breakthroughs in cloud computing. For optimum storage and accuracy for different users, load-balancing in a multi-cloud environment may also be a part of the feature work. As a technology that makes it possible to provide elastic, on-demand storage and computing capabilities without the

requirement for hardware ownership, cloud computing is becoming more and more popular. However, a number of privacy and security laws mandate that cloud users be given sufficient protection, which makes it more difficult to create cloud services that preserve users' private. Delegated access control in multi-cloud, which protects privacy, provides the essential features needed for a strong, affordable, and secure cloud security deployment.

REFERENCES:

1. D. Devkota, P. Ghimire, D. J. Burris and D. I. Alkadi, "Comparison of Security Algorithms in Cloud Computing," IEEE, pp. 1-7, 2015.
2. Neha Tirthani: "Hellman and elliptical curve cryptography, Proceedings of TCC", volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)
3. Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013
4. Peng Y ong, Zhao Wei, X ie Feng, Dai Zhong-hua, Gao Y ang & Chen Dong-qing 2012, 'Secure cloud storage based on cryptographic techniques', The J ournal of China Universities of Posts and Telecommunications, Elsevier, vol. 19, no. 2, pp. 182-189.
5. L uca Ferretti, Fabio Pierazzi, Michele Colajanni & Mirco Marchetti 2014, 'Performance and cost evaluation of an adaptive encryption architecture for cloud databases', IEEE Transactions on Cloud Computing, vol. 2, no. 2, pp. 143-155.
6. Ricardo Padilha & Fernando Pedone 2015, 'Confidentiality in the cloud', IEEE Security & Privacy, vol. 13, no. 1, pp. 57-60.
7. Lazaros Gkatzikis and Iordanis Koutsopoulos, "Migrate or Not Exploiting Dynamic Task Migration in Mobile Cloud Computing Systems", IEEE Wireless Communications, vol. 20, no. 3, pp. 24-32, 2013.
8. S H Manjula, Bindu Reddy E, Shaila K, L Nalini, Venugopal K R and L M Patnaik, "Base-Station Controlled Clustering Scheme in Wireless Sensor Networks", IFIP Wireless Days Conference, Dubai, e-ISBN: 978-1-4244-2829-8, p-ISBN: 978-1-4244-2828-1, pp. 1-5, November 24-27, 2008.
9. Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong and Qi Xi, "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing", IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, October 2014.
10. Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 468-477, February 2014.
11. Guillermo Indalecio, Fernando Gomez-Folgar, and Antonio J. GarciaLoureiro, "GWMEP: Task Manager-as-a-Service in Apache Cloud Stack", IEEE Internet Computing, vol. 20, no. 2, pp. 42-49, March/April 2016.
12. Mauro Gaggero and Luca Caviglione, "Predictive Control for EnergyAware Consolidation in Cloud Datacenters", IEEE Transactions on Control Systems Technology, vol. 24, no. 2, pp. 461-474, 2016.
13. Xiangming Dai, Jason Min Wang and Brahim Bensaou, "EnergyEfficient Virtual Machines Scheduling in Multi-Tenant Data Centers", IEEE Transactions on Cloud Computing, vol. 4, no. 2, pp. 210-221, 2016.
14. Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai, "Secure Auditing and Deduplicating Data in Cloud", IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386-2396, August 2016.
15. Heng He, Ruixuan Li, Xinhua Dong and Zhao Zhang, "Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud", IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, October-December 2014.
16. Mi Wen, Kaoru Ota, He Li, Jingsheng Lei, Chunhua Gu and Zhou Su, "Secure Data Deduplication with Reliable Key Management for Dynamic Updates in CPSS", IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 137-147, December 2015.
17. Hui Zhang, Guofei Jiang, Kenji Yoshihira and Haifeng Chen, "Proactive Workload Management in Hybrid Cloud Computing", IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 90-100, 2014.
18. Kyle Chard, Kris Bubendorfer, Simon Caton and Omer F. Rana, "Social Cloud Computing: A Vision for Socially Motivated Resource Sharing", IEEE Transactions on Services Computing, vol. 5, no. 4, pp. 551-563, October-December 2012.
19. S. Tabassam, Security and Privacy Issues in Cloud Computing Environment, *Journal of Information Technology and Software Engineering*, **7**(5), (2017), 216.