

INVESTIGATING VULNERABILITIES IN PLUGGABLE DATA IN A UBIQUITOUS ENVIRONMENT USING AN ALGORITHMIC APPROACH

Suyog Sudhir Kulkarni¹, Shilpa Raghuvanshi²

¹PG Scholar, CSD, Dr. APJ Abdul Kalam University Indore, M.P. India.

²Assistant Professor, CSD, Dr. APJ Abdul Kalam University Indore, M.P., India.

ABSTRACT

In the IT sector, cloud computing is a hot study area that is used to distribute data and computing resources over the internet. The use of clouds is a new computer platform, in which the network is used to share the resources as a service. The primary function provided by cloud computing is cloud data storage, whereby The user has access to, and the data is handled, managed, and backed up during the connect. Because of the cloud, several sectors are embracing cloud computing with enthusiasm. capacities that a marginal asset can achieve. Nevertheless, the cloud keeps user data in somewhere that might lead to a data security breach. Consequently, safeguarding the cloud data is a significant problem that many sectors now face. But the data owner has amassed and saved the data on distant servers, and users can retrieve their data from the distant cloud servers that are not within the user's control. As a result, the collection of Data stored off-cloud presents a number of security challenges. Consequently, the One of the main areas of cloud computing study is cloud data protection. stage. Users benefit from enormous efficiency when data is outsourced to the cloud because They don't have to be concerned about maintaining hardware management. The. cloud computing pioneers, such as Amazon Elastic Compute Cloud (EC2) and Well-known examples are Amazon Simple Storage Service (S3) and others. Additionally, the internet Network-based services provide enormous storage.

1. INTRODUCTION

The cloud is often an insecure cloud environment where communication takes place on an untrusted network and where the resources and services are accessible to everyone. The public cloud, which includes Amazon AWS, Microsoft Azure, and Users do not fully trust the Google Cloud Platform. While the advantages of Although cloud computing is amazing, using untrusted cloud providers poses significant security risks. cloud-based settings. The data owners lose when they outsource their data to a public cloud. the stringent management of data kept on local storage devices. Within the open cloud, Unauthorized users and the cloud purposefully access the outsourced data. Sensitive data and administrators are acquired. One benefit of the Key Recovery approach is that the encryption key is fully known only to the user. This strategy protects the user's privacy while lowering the danger associated with the encryption key. The Key Recovery scheme's computational load and transformation speed are its drawbacks. The user's key renewal presents a significant difficulty for the Key Recovery program. The ciphertext could be retrieved with the help of the privacy-preserving cloud storage framework, which resolved issues with working with encrypted data and lessened the burden of managing it for the data owner. This technique combines symmetric and asymmetric encryption with the Key Derivation Algorithm, Bloom Filter, and Interaction Protocol. The credibility of cloud services is based on the availability of critical data with a third party. Data privacy is preserved through the encryption of the data prior to cloud storage. Notwithstanding encryption methods, conventional encryption methods have a number of drawbacks. The disadvantage of the conventional encryption method is that in order to look for a few details in the cloud storage, the owner of the secret key must download the complete encrypted file. The necessary file is then found by searching through the decrypted data. If the client uses a mobile device or there is a significant volume of encrypted data, the encryption methods will not be practical or effective. With the pluggable cloud, you may switch between public and private clouds without significantly altering the underlying application dependencies. Pluggable cloud addressed both functional and financial adjustments. First, it is necessary that the Pluggable clouds are only functional if the cloud service broker and cloud management platform (CSB) or alternative technologies that offer abstraction from native cloud services are employed. Should If not, managing the public cloud provider's native cloud services will be too difficult. native cloud services that are contract-free. Understanding the demand is the second prerequisite of the data storage that plugs in. Configuring a pluggable multicloud system is the third need. on top of the service charge. Traditional networks are used to access people in various services and save user profiles for cloud storage, backup data, and business descriptions. information for creating a backbone of the ubiquitous via the internet. A few of Data archiving, online data backup, catastrophe recovery, and cloud data storage are the problems. data compliances and compliance rules. The transferable nature of the Data storage in the cloud and information in cloud providers are created using The agreements and service level policy form the foundation for different technologies. The people who use it are authorized to transfer data between data providers as a portability option

2. OBJECTIVE OF THE WORK

The main objectives of the research are as follows:

1. To assess the research algorithmic performance for associated with ubiquitous cloud.
2. Identify necessary vulnerability to the contents of pluggable ubiquitous storage infrastructure.
3. Association of private pluggable storage infrastructure to the IaaS.
4. Pluggable data path synchronization with query.
5. Exploiting the availability of cloud resulting in the challenge of on-demand pluggable data association.

3. METHODOLOGY

The proposed The algorithm of the Attribute Based Encryption and Data Integrity is divided into two parts. The first part is the fragmentation and the second part is the encryption of the algorithm.

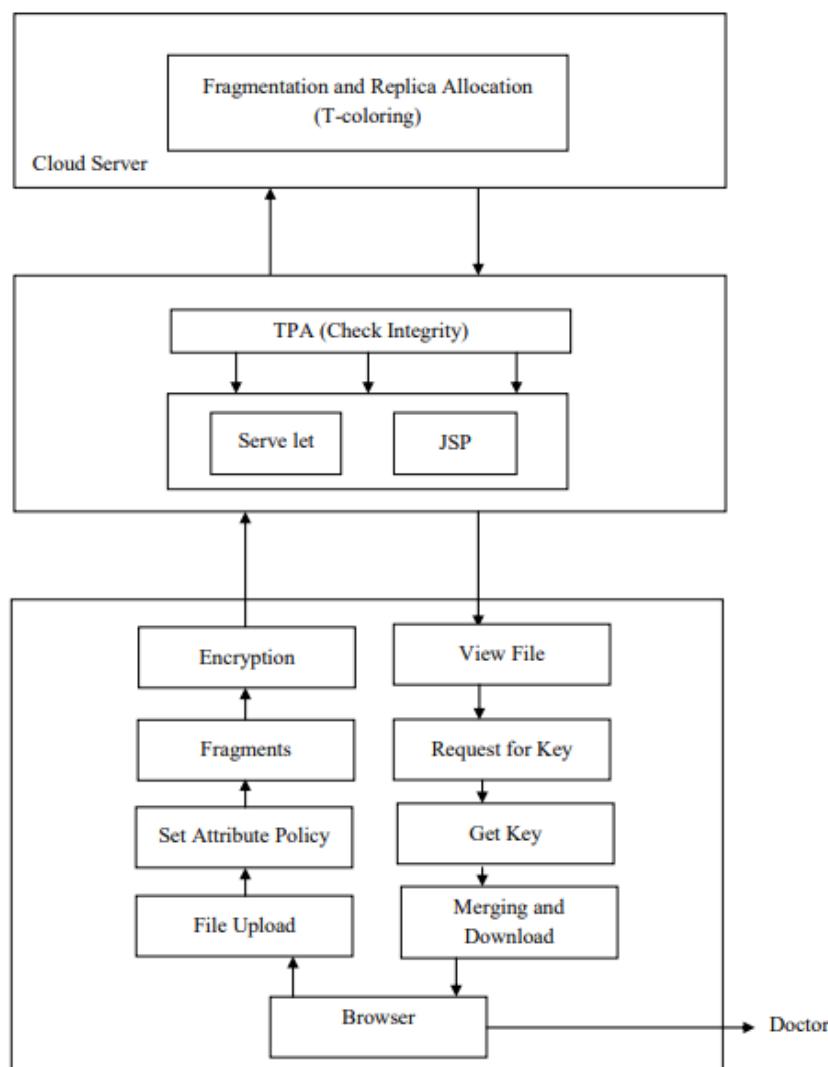


Figure 1: Block diagram of Attribute based Encryption and Data Integrity

4. RESULT

Accuracy and cloud data privacy were offered by the kernel interpolation-based technique made possible by optimization. Once the data has been encrypted, pluggable data is made available online. The third-party user is granted access to the data if they possess the relevant data key. The R-CSO algorithm uses the kernel interpolation coefficient to ensure the anonymity of data uploaded in the cloud. By altering the data size and training %, the kernel interpolation-based technique's performance is examined in terms of accuracy and DBDR. With a minimal DBDR of 10.66 when taking dataset 1 into consideration and a maximum accuracy of 84.99%, the kernel interpolation-based technique surpassed the previous approach. In accordance with the research goal, the pluggable data storage association has been discussed. The Eucalyptus cloud, which is open source, was used to design the experimental configuration. Using comparative techniques, the pluggable storage susceptibilities are effectively tested.

5. CONCLUSION

These days, cloud computing is a well-known model. Many businesses, including Google, Amazon, and Microsoft, are developing effective Cloud Computing systems more quickly by enhancing their offerings to cater to a wider range of consumers. However, users find it difficult to adjust to cloud service models due to privacy and security issues. Data outsourcing to the cloud entails a number of concerns related to protecting sensitive data, including protecting trade secrets, intellectual property, and private data that might fall into the wrong hands. Confidential material assembled online requires careful consideration of security controls and access to the contents. Storage may not be accessible to some sectors within the cloud infrastructure. Furthermore, information from several users could be combined into a single repository for cloud storage data access and deletion. The cloud is used to store sensitive data, which raises the possibility of security concerns that need to be addressed via authentication techniques. Three methods for data integrity verification are developed to provide privacy-protected data in order to address these problems. By refining the work with other concerns, the research can be expanded upon. Some of the future research directions for the enhancement of suggested approaches to provide greater privacy protection and data integrity checking utilizing cloud computing include the use of new techniques and algorithms. Furthermore, the cloud framework will be enhanced to manage the different features of cloudlets. Every solution has advantages and disadvantages, as the literature study shows, but the lack of data integrity techniques that can handle dynamic data operations and high computing costs is a prevalent problem. Furthermore, one of the key requirements in the future for creating a successful cloud computing paradigm may be computational viability.

6. REFERENCES

- [1] Wang, J., Zhao, Y., Jiang, S. and Le, J., "Providing privacy preserving in cloud computing", In 3rd International Conference on Human System Interaction, pp. 472-475, May 2010.
- [2] Nergiz, M.E., Atzori, M. and Clifton, C., "Hiding the presence of individuals from shared databases," In Proceedings of the 2007 ACM SIGMOD international conference on Management of data, pp. 665-676, ACM, June 2007.
- [3] Bhardwaj, S., Jain, L. and Jain, S., "Cloud computing: A study of infrastructure as a service (IAAS)", International Journal of engineering and information Technology, vol.2, no.1, pp.60-63, 2010.
- [4] Godse, M., & Mulik, S, "An Approach for Selecting Software-as-a-Service (SaaS) Product", IEEE International Conference on Cloud Computing, 2009.
- [5] Ma, D., "The Business Model of "Software-As-A-Service." IEEE International Conference on Services Computing, 2007.
- [6] Tsai, W., Bai, X., & Huang, Y, "Software-as-a-service (SaaS): perspectives and challenges", Science China Information Sciences, vol.57, no.5, pp.1–15, 2014.
- [7] C. Lv, Q. Li, Z. Lei, J. Peng, W. Zhang, and T. Wang, "PaaS: A revolution for information technology platforms", Educational and Network Technology (ICENT), 2010 International Conference on DOI: 10.1109/ICENT.2010.5532150 pp. 346- 349, 2010.
- [8] Yasrab, R., "Platform-as-a-Service (PaaS): The Next Hype of Cloud Computing," arXiv preprint arXiv:1804.10811, 2018.
- [9] J. Hurwitz, M. Kaufman, F. Halper, and D. Kirsch, "Hybrid Cloud for Dummies", vol. I: Dummies, 2012.
- [10] Lawton, G., "Developing Software Online With Platform-as-a-Service Technology", Computer, vol.41, no.6, pp.13–15, 2008.
- [11] Boniface, M., Nasser, B., Papay, J., Phillips, S. C., Servin, A., Yang, X., Kyriazis, D., "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds", 2010 Fifth International Conference on Internet and Web Applications and Services, 2010.
- [12] Tian, W., Su, S., & Lu, G., "A Framework for Implementing and Managing Algorithmic Study of Vulnerability Issues for Pluggable Data In Ubiquitous Environment 85 Platform as a Service in a Virtual Cloud Computing Lab", 2010 Second International Workshop on Education Technology and Computer Science, 2010.
- [13] Manvi, S. S., & Krishna Shyam, G., "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey", Journal of Network and Computer Applications, vol.41, pp.424–440, 2014.
- [14] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, "A view of cloud computing", Communications of the ACM, vol.53, no.4, pp.50–58, 2010.
- [15] Zhifeng Xiao and Yang Xiao., "Security and privacy in cloud computing", IEEE Communications Surveys & Tutorials vol.15, no.2, 843–859, 2013. Communications Surveys & Tutorials vol.15, no.2, 843–859, 2013.