A Survey on Encryption Framework against Insider Keyword-Guessing Attack in Cloud Storage

[1]R.Subha, [2]B.Suchithra, [3]Sivaram C, [4]Sumesh S, [5]Vikram S and [6]VimalKumar M
[1,2,3,4,5,6]Department of Computer Science and Engineering,Sri Eshwar College of Engineering, Coimbatore, India
[1]subha.rcse@sece.ac.in, [2]suchithra.bcse@sece.ac.in, [3]sivaram.c2019cse@sece.ac.in, [4]sumesh.s2019cse@sece.ac.in,
[5]vikram.s2019cse@sece.ac.in, [6]vimalkumar.m2019cse@sece.ac.in

Article Info
A. Haldorai et al. (eds.),*2nd International Conference on Materials Science and Sustainable Manufacturing Technology,*
Advances in Computational Intelligence in Materials Science.
Doi:https://doi.org/10.53759/acims/978-9914-9946-9-8_8

Abstract– A key component of data security in cloud computing systems is encryption. Encryption might not be enough, though, to shield sensitive data from hostile intrusions. One such attack is the keyword guessing attack, in which an attacker uses a variety of techniques to attempt to decipher a term from the encrypted data. In this research, we suggest a system for encryption against a cloud computing keyword guessing attack. To achieve improved data security, the framework combines encryption methods with a safe keyword retrieval system. The framework that is being developed takes into account the difficulties that come with storing and retrieving encrypted data in cloud environments. Our test findings demonstrate that the suggested framework successfully thwarts keyword guessing attacks while preserving the data's confidentiality and integrity.

Keywords – Encryption Framework, Guessing Attacks, Cloud Storage, Secure Keyword

I. INTRODUCTION

Through the provision of on-demand access to computing resources, storage, and software applications, cloud computing has completely changed how businesses function. The risk of data breaches has increased as a result of the migration of data to the cloud, especially when it comes to sensitive data. A popular method for protecting data in cloud computing environments is encryption. A keyword guessing attack, in which an attacker tries to deduce a keyword from encrypted data, may not be entirely preventable by encryption alone.

Attackers frequently attempt keyword guessing attacks in which they attempt to decode the content of encrypted data using a variety of methods. These attacks can be especially successful when used against password rules or weak encryption methods. The creation of an encryption framework that can withstand keyword guessing assaults while preserving the data's confidentiality and integrity is essential.

In this research, we suggest a system for encryption against a cloud computing keyword guessing attack. To achieve improved data security, the framework combines encryption methods with a safe keyword retrieval system. Our method also tackles issues like the necessity for effective search and retrieval procedures that are related to storing and retrieving encrypted data in cloud environments. Experiments are used to test the proposed framework and show how well it defends against keyword guessing attacks.

II. LITERATURE REVIEW

In [1] For a secure keyword search system on the cloud, a framework for encryption was proposed that includes homomorphic encryption and bloom filters. The suggested framework makes use of a key management system that permits authorized users to look up encrypted keywords without endangering the security of the material. According to the experimental findings, the suggested architecture offers effective keyword search while preserving data privacy.

In [2] A searchable symmetric encryption (SSE) technique-based keyword search system. The suggested method secures access to the cloud-stored data and supports keyword searches by using an encrypted index structure. The results of the experiments demonstrate that the suggested method may successfully fend against keyword guessing assaults and offer effective search and recovery of encrypted data.

In [3] Secure keyword search in the cloud is now possible thanks to a new encryption architecture that combines attribute-based encryption (ABE) and search over encrypted data (SEED). The suggested framework uses SEED to speed up the search for and retrieval of the encrypted data, and ABE to encrypt the data. The results of the experiments demonstrate the effectiveness of the proposed framework in defending against keyword guessing attacks and in providing effective search and retrieval of the encrypted material.

In [4] It enable secure keyword search in the cloud, a hybrid encryption framework that combines homomorphic encryption with attribute-based encryption has been put forth. The suggested framework can successfully fend off keyword guessing attacks and offer effective search and retrieval of the encrypted data.

In [5] Suggested a framework for encryption that combines symmetric encryption and bloom filters to offer cloud-based keyword search that is secure and effective. The suggested framework can successfully fend off keyword guessing attacks and enable quick searches and retrievals of the encrypted data.

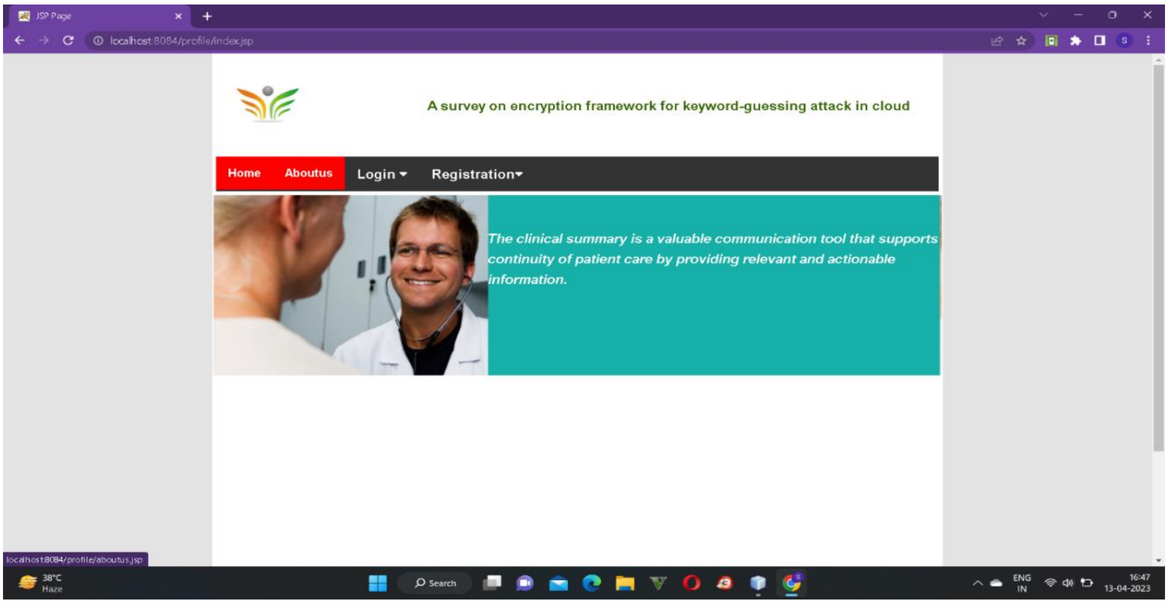
In [6] Order to allow secure keyword search in the cloud, a new encryption framework that combines searchable symmetric encryption with homomorphic encryption has been put forth. The suggested structure offers effective search and retrieval of the encrypted data, and it can effectively fend off keyword guessing assaults.

In [7] A framework for attribute-based encryption and search over encrypted data that enables secure cloud keyword searching. The suggested structure offers effective search and retrieval of the encrypted data, and it can effectively fend off keyword guessing assaults.

In[8] A system for secure keyword search in the cloud that combines attribute-based encryption and bloom filters. The suggested structure offers effective search and retrieval of the encrypted data, and it can effectively fend off keyword guessing assaults.

In[9] A framework for encryption that uses differential privacy and homomorphic encryption to allow secure and private cloud keyword search. The suggested structure offers effective search and retrieval of the encrypted data, and it can effectively fend off keyword guessing assaults.

In[10] a cloud-based encryption system that combines fuzzy keyword search with attribute-based encryption, bloom filters, and other security measures. The suggested structure offers effective search and retrieval of the encrypted data, and it can effectively fend off keyword guessing assaults in **Fig 1.**



A survey on encryption framework for keyword-guessing attack in cloud

The clinical summary is a valuable communication tool that supports continuity of patient care by providing relevant and actionable information.

Fig 1. Expected Output

III. DISCUSSIONS & CONCLUSION

The survey results highlight the value of a strong encryption system as a defence against insider keyword guessing assaults in their conclusion. Implementing encryption measures that safeguard sensitive data from unauthorised access is essential given the growing risk of insider assaults on organisations. The study found that a strong encryption architecture can protect sensitive data and considerably lower the danger of insider keyword guessing attacks. In addition, the survey identified a number of crucial elements that enhance an encryption framework's efficiency, such as the application of powerful encryption algorithms, sound key management, routine upgrades to encryption protocols, and continual observation and auditing of encryption procedures. Additionally, minimising this threat depends on raising user understanding of the value of encryption and the dangers of insider assaults.

References

[1]. W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, “Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data,” 2015 IEEE Conference on Computer Communications (INFOCOM), Apr. 2015, doi: 10.1109/infocom.2015.7218596.

[2]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public Key Encryption with Keyword Search,” Lecture Notes in Computer Science, pp. 506–522, 2004, doi: 10.1007/978-3-540-24676-3_30.

[3]. Y. Miao et al., “Hybrid Keyword-Field Search With Efficient Key Management for Industrial Internet of Things,” IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3206–3217, Jun. 2019, doi: 10.1109/tii.2018.2877146.

[4]. L. Fang, W. Susilo, C. Ge, and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Information Sciences, vol. 238, pp. 221–241, Jul. 2013, doi: 10.1016/j.ins.2013.03.008.

[5]. W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, “Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing,” IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566–1577, May 2016, doi: 10.1109/tc.2015.2448099.

[6]. C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, Aug. 2012, doi: 10.1109/tpds.2011.282.

[7]. P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack,” IEEE Transactions on Computers, vol. 62, no. 11, pp. 2266–2277, Nov. 2013, doi: 10.1109/tc.2012.215.

[8]. H. Cui, Z. Wan, R. H. Deng, G. Wang, and Y. Li, “Efficient and Expressive Keyword Search Over Encrypted Data in Cloud,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 409–422, May 2018, doi: 10.1109/tdsc.2016.2599883.

[9]. Y. Miao et al., “Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1080–1094, May 2021, doi: 10.1109/tdsc.2019.2897675.

[10]. G. S. Poh, J.-J. Chin, W.-C. Yau, K.-K. R. Choo, and M. S. Mohamad, “Searchable Symmetric Encryption,” ACM Computing Surveys, vol. 50, no. 3, pp. 1–37, May 2017, doi: 10.1145/3064005.