International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A SYMMETRIC ENCRYPTION SEARCH DATA

[1]D. Ganesh, [2]D. Prasanna, [3]D. Akshay Goud, [4] P. Sunil
[1,2,3]Student,[4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ABSTRACT :

Symmetric Accessible Encryption (SSE) is considered to handle the protection issue as well as the operability and classification in information reevaluating. Nonetheless, most SSE plans expect to be simply the cloud is straightforward yet inquisitive. This supposition that isn't appropriate 100% of the time. Furthermore, regardless of whether a few plans upheld confirmation, honesty or newness really taking a look at in a malevolent cloud, however the presentation also, security functionalities are not completely taken advantage of. In this paper, we propose a proficient SSE plot in view of which supports secure confirmation, dynamic refreshing, and multi-client questions.

Contrasting and the past condition of human expression, we plan the new information structure CBF. We likewise the to keep the noxious cloud from sending off a replay assault. The new planned CBF is like a front-motor to save clients cost for inquiry and check. Moreover, we plan the authenticator. We it is broadly utilized in data set motors and document frameworks. We likewise give a brief security confirmation of our plan. Then we give a point by point execution investigation.

I. INTRODUCTION :

Symmetric Accessible Encryption (SSE) is considered to handle the protection issue as well as the operability and classification in information reevaluating. Nonetheless, most SSE plans expect to be simply the cloud is straightforward yet inquisitive. This supposition that isn't appropriate 100% of the time. Furthermore, regardless of whether a few plans upheld confirmation, honesty or newness really taking a look at in a malevolent cloud, however the presentation also, security functionalities are not completely taken advantage of. In this paper, we propose a proficient SSE plot in view of which supports secure confirmation, dynamic refreshing, and multi-client questions.

Contrasting and the past condition of human expression, we plan the new information structure CBF. We likewise the

to keep the noxious cloud from sending off a replay assault. The new planned CBF is like a front-motor to save clients cost for inquiry and check. Moreover, we plan the authenticator. We it is broadly utilized in data set motors and document frameworks. We likewise give a brief security confirmation of our plan. Then we give a point by point execution investigation.

II. LITERATURE SURVEY :

Accessible symmetric encryption (SSE) permits a client to scramble his information in such a way that the information can be productively looked. SSE has down to earth application in distributed storage, where a client re-appropriates his scrambled information to a cloud server while keeping up with the accessible capacity over his information. The majority of the ongoing SSE plans accept that the cloud server tells the truth yet inquisitive. Be that as it may, the cloud may effectively undermine the inquiry interaction to keep its expense low. In this paper, we center around the pernicious cloud model and propose a new obvious accessible symmetric encryption plot. Our plan is based on the protected vagary confusion (iO) and can be considered as the initial step to apply iO in the SSE field. Also, our plan can be without any problem reached out to different functionalities, like conjunctive and Boolean inquiries. Besides, it can be reached out to understand an openly obvious SSE. Careful investigation shows that our plan is secure and accomplishes a superior exhibition.

III. PROPOSED SYSTEM :

In this paper, we propose an efficient SSE scheme based which supports secure verification, dynamic updating, and multi-user queries. Comparing with the previous state of the arts, we design the new data structure CBF to support. We also leverage the mechanism in the scheme to prevent the malicious cloud from launching an attack. The new designed CBF is like a front-engine to save user0s cost for query and verification. And it can achieve more efficient query and verification when there is no value matching the queried keyword.

METHODOLOGIES:

1.USER INTERFACE DESIGN :

In this module we plan the windows for the undertaking. These windows are utilized for secure login for all clients. To associate with server client should give their username and secret phrase then just they can ready to interface the server. On the off chance that the client as of now exits straightforwardly can login into the server else client
should enlist their subtleties, for example, username, secret word and Email id, into the server. Server will make the record for the whole client to keep up with transfer and download rate. Name will be set asclient id. Signing in is generally used to enter a particular page.

2.AUTHENTICATOR SERVER:

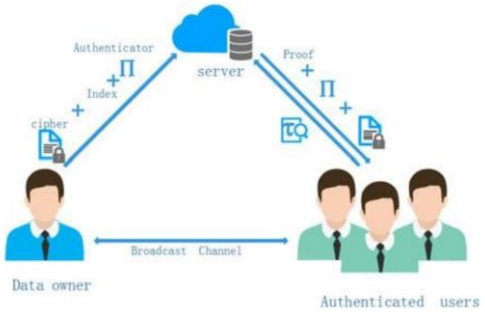
The first module is an authenticator server. First server has to login with a user id and password. Authenticator server has a data protector request. The user has a takes a permission from the server. Server has a accept then the user has a login. Same procedure of the data protector also takes a permission from the server. Authenticated server has a key request then have to approve and send. Authenticated server has a generate a trapdoor key.

3.DATA PROTECTOR :

The third module. Data protector has a register with all details. Then login takes the permissions from the server. Data protector has a data store. Data protector has a view file information.

4.AUTHENTICATED USER:

The fourth module is an authenticated user. Authenticated user has a file access search the documents the uploaded protector. Authenticated user has a download files. Authenticated user has a replay attacks.



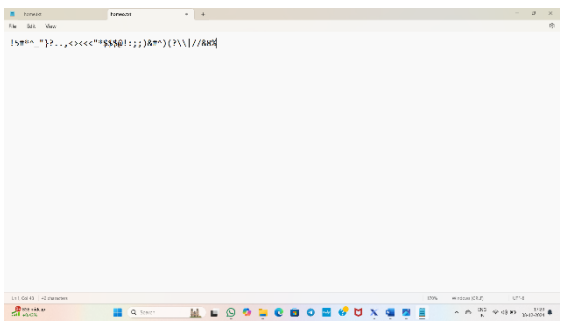
SYSTEM ARCHITECTURE

IV. FUTURE ENHANCEMENT:

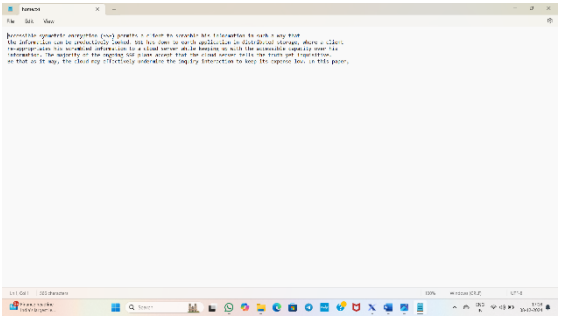
In future work, we can consider more complex searches, such as multiple keyword extraction and conjunction query search. In addition, the Bloom filter has the potential for errors, but the probability of errors is negligible. However, comparing with the improved computational overhead, the probability of this error is still acceptable.

V. RESULT AND IMPLEMENTATION :

OUTPUT:



Before Decryption



After Decryption

VI. CONCLUSION :

In this work, This paper introduces an efficient searchable symmetric encryption (SSE) scheme using B+-Tree and Counting Bloom Filter (CBF) to support secure verification, dynamic updates, and multi-user queries. The CBF enables quick verification of token existence in constant time ($O(1)$O(1)) for both the server and user and allows efficient updates. If a token exists, an authenticator is created by encrypting and signing the B+-Tree root and timestamp, enabling users to verify the integrity of server results. The scheme was implemented and tested, showing consistent performance, reasonable results, and low time costs, especially for queries that do not exist.

VI. REFERENCES :

[1] B. Waters. J. Bethencourt, and A. Sahai, "Ciphertext-policy attribute- based encryption," in Proc. IEEE Symp. Secure. Privacy, 2007, vol. 10, pp. 321–334.

[2] Tadjer, "What is cloud computing," ACM, vol. 51, pp. 9–11, 2011.

[3] A. K. Iyengar, "Enhanced clients for data stores and cloud services," IEEE Trans. Knowl. Data Eng., vol. 31, no. 10, pp. 1969–1983, Oct. 2019.

[4] X. Ge, Y. Wang, J. Fu, J. Wu, and L. Ping, "Cloud storage as the infrastructure of cloud computing," in Proc. IEEE Int. Conf. Intell. Computer. Cogn. Informat., 2010, pp. 380–383.

[5] L. Weng, L. Amsaleg, and T. Furon, "Privacy-preserving outsourced media search," IEEE Trans. Knowl. Data Eng., vol. 28, no. 10, pp. 2738–2751, Oct. 2016.

[6] S. Kamara, C. Papamanthou, and T. Roeder, "CS2: A searchable cryptographic cloud storage system," Microsoft Technical Report, pp. 380–383, 2011.

[7] K. Ren, B. Zhang, R. Xie, K. Yang, and X. Jia, "Effective data access control for multiauthority cloud storage systems," IEEE Trans. Inf. Forensics Secure., vol. 8, no. 11, pp. 1790–1799, Nov. 2013.

[8] L. M. Gupta, K. A. Nielsen, M. G. Borlick, and L. M. Gupta, "Method, system, and computed program product for distributed storage of data in a heterogeneous cloud," Int. Bus. Machines Corporation, vol. 10, 2019, Art. no. 171.

[9] H. Ancin, X. Chen, A. Jassal, D. H. Jung, G. B. Neustaetter, and S. H. Puttergill, "Systems and method for facilitating access to private files using a cloud storage system," U.S. Patent 9251114, Feb. 2016.

[10] K. Lauter and S. Kamara, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2010, pp. 136–149.

[11] K. Kurosawa and Y. Ohtaki, "UC-secure searchable symmetric encryption," in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2012, pp. 285–298.

[12] K. Kurosawa and Y. Ohtaki, "How to update documents verifiably in searchable symmetric encryption," in Proc. Int. Conf. Cryptology Netw. Secur., 2013, pp. 309–328.

[13] C. Papamanthou, E. Stefanov, and E. Shi, "Practical dynamic searchable encryption with small leakage," in Proc. Netw. Distrib. Syst. Secur. Symp., 2014, pp. 23–26.