SYMMETRIC-KEY BASED VERIFICATION OF KEYWORD SEARCH OVER DYNAMIC ENCRYPTED CLOUD DATA

[1]Mugireddy Satya Narayanareddy,[2]Lekireddy Rajasekharreddy,[3]Isani Swetha,[4]P V Jagadeeswara Prasad

[1,2]Associate Professor, Department of CSE, Tadipatri Engineering College, Tadipatri, AP
[3,4]Assistant Professor, Department of CSE, Tadipatri Engineering College, Tadipatri, AP

ABSTRACT
Searchable and Verifiable As a crucial method of cloud security, symmetric encryption enables users to search for encrypted data in the cloud using keywords and validate the accuracy of the results. One of the most prevalent and important requirements for data owners in such schemes is dynamic update for cloud data. To our knowledge, all of the verifiable SSE systems that permit data dynamic update currently in use are based on asymmetric-key cryptography verification, which necessitates time-consuming processes. The sheer volume of cloud data could make the overhead of verification a major burden. Consequently, a crucial unsolved topic is how to implement keyword search over dynamic encrypted cloud data with effective verification. In this research, we investigate how to accomplish keyword search over dynamically encrypted cloud data with symmetric-key based verification and suggest a workable technique. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generate an authentication tag for each keyword. Benefiting from the accumulation property of our designed AAT, the authentication tag can be conveniently updated when dynamic operations on cloud data occur. In order to achieve efficient data update, we design a new secure index composed by a search table ST based on the orthogonal list and a verification list VL containing AATs. Owing to the connectivity and the flexibility of ST, the update efficiency can be significantly improved. The security analysis and the performance evaluation results show that the proposed scheme is secure and efficient.

KEYWORDS: Cloud Computing, Encryption

I. INTRODUCTION

Searchable and Verifiable As a crucial method of cloud security, symmetric encryption enables users to search for encrypted data in the cloud using keywords and validate the accuracy of the results. One of the most prevalent and important requirements for data owners in such schemes is dynamic update for cloud data. To our knowledge, all of the verifiable SSE systems that permit data dynamic update currently in use are based on asymmetric-key cryptography verification, which necessitates time-consuming processes. The overhead of verification may become a significant burden due to the sheer amount of cloud data. Therefore, how to achieve keyword search over dynamic encrypted cloud data with efficient verification is a critical unsolved problem. To address this problem, we achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification and propose a practical scheme in this paper. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generate an authentication tag for each keyword. Benefiting from the accumulation property of our designed AAT, the authentication tag can be conveniently updated when dynamic operations on cloud data occur. In order to achieve efficient data update, we design a new secure index composed by a search table ST based on the orthogonal list and a verification list VL containing AATs. Owing to the connectivity and the flexibility of ST, the update efficiency can be significantly improved. The security analysis and the performance evaluation results show that the proposed scheme is secure and efficient.

II. PROBLEM STATEMENT

- In the current work, the system leaks a lot of data for updates and can't be parallelized.
- Several forward-private DSSE systems that are both asymptotically complicated and performant in practise have been suggested..

III. EXISTING SYSTEM

Firstly, users may worry about whether their data is intactly stored in the cloud because the cloud data is out of their physical control. In order to solve this problem, some cloud storage auditing schemes are proposed to check the integrity of cloud data. In addition, users usually need to encrypt the data for keeping the privacy before outsource them to the cloud. It makes performing keyword search over encrypted cloud data become a new challenge. In order to address this issue, searchable encryption is proposed, which allows users to selectively retrieve cipher documents stored in the cloud by keyword-based search. Compared with searchable public key encryption, searchable symmetric encryption draws more attention owing to its high efficiency.
Static SSE. Song et al firstly proposed the searchable symmetric encryption scheme, in which a special two-layered encryption structure is constructed to encrypt each keyword. Goh et al proposed a keyword search scheme over encrypted cloud data based on the Bloom filter. Curtmola et al proposed two efficient keyword search schemes (SSE- 1

and SSE-2) over encrypted cloud data. These schemes can realize sub linear search, that is, the search cost is proportional to the number of the files matching the queried keyword. Cao et al. proposed a privacy-preserving multi-keyword ranked search scheme over encrypted cloud data by utilizing the similarity measure of "Coordinate matching" and "inner product similarity". In addition, some other static SSE schemes, such as semantic search scheme, similarity search scheme, ranked keyword search schemes, central keyword-based semantic extension search scheme, and keyword search scheme supporting deduplication, have also been proposed.

Dynamic SSE. In order to support data dynamic update, some dynamic SSE schemes have been proposed. Kamara et al. proposed a dynamic SSE scheme by extending the inverted index approach. This scheme can achieve sublinear search and CKA2-security. Subsequently, they proposed another dynamic SSE scheme based on keyword red-black tree index structure. This scheme supports parallel keyword search as well as parallel addition and deletion of files. Naveed et al. presented a dynamic SSE scheme via blind storage. Blind storage allows a data owner to store files on a cloud server in such a way that the cloud server does not learn the number of files. Xia et al. proposed a dynamic keyword search scheme over encrypted cloud data based on the tree-based index structure, which can support multi-keyword rank. Guo et al. proposed a dynamic SSE scheme based on the inverted index. It enables the data user to search several phrases in a query request. Also, their proposed scheme supports the sorting of the search results.

IV. PROPOSED SYSTEM

We develop a unique symmetric-key based Accumulative Authentication Tag (AAT) to produce an authentication tag for each keyword in order to allow the effective verification of dynamic data. The accumulation feature of our built AAT enables the authentication tag to be easily updated whenever dynamic operations on cloud data take place. The suggested AAT is computationally challenging for any attacker to discover various messages with the same tag since it is collision resistant. Additionally, it has the ability to withstand replay attacks, which stop the cloud server from delivering outdated data. We create a new secure index made up of a search table ST and a verification list VL to achieve effective data updating. ST is based on the orthogonal list and VL is a singly linked list. For each keyword, we construct a linked list with the same length aiming at hiding the frequency of each keyword. When performing modification operations, the cloud server can fleetly find the index nodes related to the modified files. When some files need to be added or deleted, the secure index can be conveniently enlarged or reduced. Owing to the connectivity and flexibility of ST, the update efficiency can be significantly improved. Based on the above technique and structure, we design the first keyword search scheme over dynamic encrypted cloud data with symmetric-key based verification. We give the security analysis of the proposed scheme and conduct the performance comparison with other work in terms of the search token generation efficiency, verification efficiency and update efficiency. The results show that the proposed scheme is secure and efficient.

V. MODULES

Data Owner

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Browse and enc and Uploads files, View all your uploaded files, Verify your secret key, Verify your file, View all search and pkey request.

- **Cloud Server**

The Cloud server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as View all cloud files ,Capture all attackers, View all attackers, View all key attackers, View all transactions, View all search requests, View File Rank Result, View Time Delay Results, View Throughput Results

- **END User**

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and can do the following operations like Register and Login, Request File Search and pkey and View Response, Search Files by Multi keyword, Download File.

VI. METHDOLOGY

In algorithm **IndexBuild**, the data owner builds the secure index I = (ST, VL). In ST, each row list Lwi ($1 \leq i \leq n$) is associated with one keyword wi . The head node of each row list stores the keyword permutation π(wi) as the address of this list. All head nodes are linked to the first column list Lf0 , which are used as look-up nodes for cloud server. The

index node of each row list stores the ciphertext Ewij = SKE.EncKwi (wij , vj) (1 ≤ j ≤ N) related to an index vector bit wij and the update times vj . All index nodes in the same column are linked to the column list Lfj , which corresponds to the file Fj . For each keyword wi , the authentication tag AATSi stored in the index node of VL is computed based on the accumulation property of AAT. When the data user would like to search files containing the interested keyword, he generates the trapdoor through algorithm GenToken. The cloud server can perform search operation through algorithm Search. In algorithm Verify, the data user computes the authentication tag for returned cipher texts, and checks whether these cipher texts are correct according to the authentication tag. In algorithm **UpToken**, the data owner generates update tokens for the updated files. Each token is composed by n + 2 elements. The first element denotes the identifier of the updated file and the last element denotes the cipher text of the updated file. Each middle element includes the values of updated index nodes in ST and the update value of AAT in VL. Owing to the connectivity and the flexibility of orthogonal list, the cloud server can update the secure index efficiently in algorithm Update. In modify operation, the cloud server replaces the value of each index node related to the updated file with the new one in ST and updates AAT value in VL according to the update value. In add operation, the cloud server adds a new column list in ST and updates AAT value in VL according to the update value. In delete operation, the column list related to this file in ST is deleted directly. The cloud server only needs to update AAT value in VL. Owing to the accumulation and the update property of AAT, the values of index nodes in VL can be conveniently updated.

VII. RESULTS SCREENSHOTS

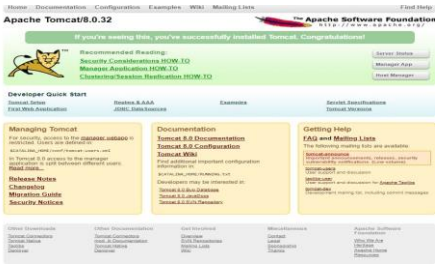

Fig 7.1: tomcat server

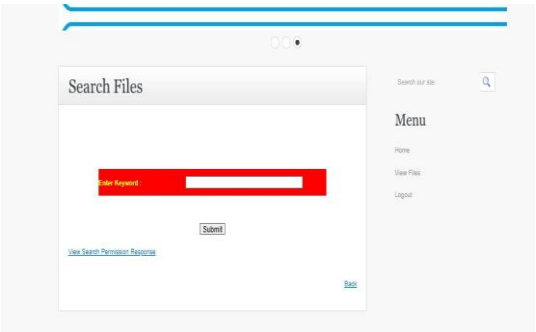

Fig7.2:filesearchbox

Fig 7.3: various users

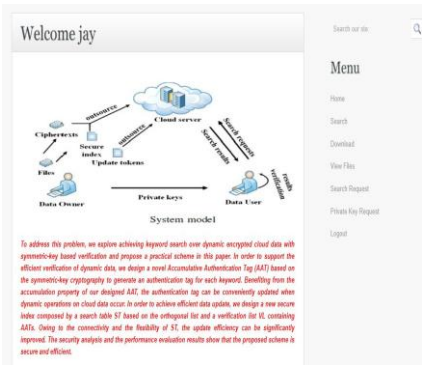

Fig7.4:userloginpage

Fig 7.5: cloud login

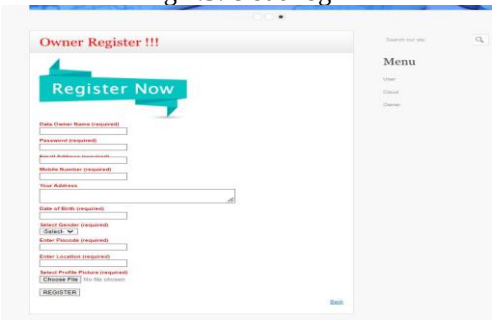

Fig 7.6: owner registration

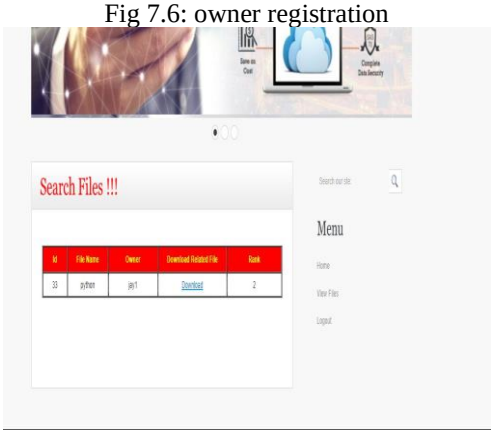

Fig 7.7: search files

Fig 7.8: login page

CONCLUSION

We investigate using symmetric-key based verification to implement keyword search over dynamically encrypted cloud data. We develop a unique Accumulative Authentication Tag (AAT) based on symmetric-key cryptography to produce an accumulative authentication tag for each keyword in order to allow the effective verification of dynamic data. The updated efficiency is further improved by a new secure index built on an orthogonal list and a single linked list. The proposed method is efficient and secure, according to the performance analysis and security analysis.

FUTURE SCOPE

As technology develops, so do the methods we employ to promote and improve our websites. Using the appropriate keywords in your content to assist search engines identify and rank your website was the main focus of keyword search in the past. This is beginning to change, though, as machine learning and artificial intelligence (AI) become more prevalent. AI can also be utilised to give users more individualised experiences. If you run a shopping website, for instance, AI can be used to suggest things based on what a customer has previously viewed. Sales and conversion rates can both rise with the help of this personalisation. Machine learning and AI will continue to play a bigger role in search engine optimisation as they develop. Based on our search history and preferences, we'll receive more customised results and recommendations. Additionally, a lot of data may be analysed using machine learning to find new trends and business prospects.

REFERENCES

[1] S. Kamara, C. Papamanthou and T. Roeder, “Dynamic searchable symmetric encryption,” presented at ACM Conference on Computer and Communications Security, pp. 965-976, 2012.
[2] C. Guo, X. Chen, Y. M. Jie, Z. J. Fu, M. C. Li and B. Feng, “Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption,” in IEEE Transations on Services Computing, vol. 99, No. 1939, pp. 1-1, 2017.
[3] Z. H. Xia, X. H.Wang, X. M. Sun and Q.Wang, “A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data,” in IEEE Transactions on Parallel and Distributed Systems, vol. 27, No. 2, pp. 340-352.
[4] S. Kamara and C. Papamanthou, “Parallel and Dynamic Searchable Symmetric Encryption,” presented at the International Conference on Financial Cryptography and Data Security, pp. 258-274, 2013.
[5] J. B. Yan, Y. Q. Zhang and X. F. Liu, “Secure multikeyword search supporting dynamic update and ranked retrieval,” in China Communication, vol. 13, No. 10, pp.
209-221, 2016.
[6] K. Kurosawa and Y. Ohtaki, “How to Update Documents Verifiably in Searchable Symmetric Encryption,” presented at International Conference on Cryptology and Network Security, pp. 309-328, 2013.
[7] Q. Liu, X. H. Nie, X. H. Liu, T. Peng and J. Wu, “Verifiable Ranked Search over dynamic encrypted data in cloud computing,” presented at the IEEE/ACM International Symposium on Quality of Service, pp. 1-6, 2017.
[8] X. H. Nie, Q. Liu, X. H. Liu, T. Peng and Y. P. Lin, “Dynamic Verifiable Search Over Encrypted Data in Untrusted Clouds,” presented at the International Conference Algorithm and Architectures for Parallel Processing, pp. 557-571, 2016.
[9] X. Y. Zhu, Q. Liu and G. J. Wang, “A Novel Verifiable and Dynamic Keyword Search Scheme over Encrypted Data in Cloud Computing,” presented at the IEEE
Trustcom/BigDataSE/ISPA, pp. 845-851, 2017.
[10] W. H. Sun, X. F. Liu, W. J. Lou. Y. T. Hou and H. Li, “Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud Communications(INFOCOM), pp. 2110-2118, 2015.
[11]. C. Wang, B. S. Zhang, K. Ren, J. M. Roveda, C. W. Chen and Z. Xu, “A privacy-aware cloud-assisted healthcare

monitoring system via compressive sensing," presented at INFOCOM, 2014 Proceedings IEEE, pp. 2130-2138, 2014.
[12]. X. L. Yuan, X. Y. Wang, J. Lin and C. Wang, "Privacypreserving deep inspection in outsourced middleboxes," presented at The 35th Annual IEEE International conference on computer communications, pp. 1-9, 2016.
[13]. J. Yu, K. Ren and C. Wang, "Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates," in IEEE Transactions on Information Forensics and Security, vol. 11, No. 6, pp. 1362-1375, 2016.
[14]. J. Yu, K. Ren and C. Wang, "Enabling Cloud Storage Auditing With Key-Exposure Resistance," in IEEE Transactions on Information Forensics and Security, vol. 10,
No. 6, pp. 1167-1179, 2015.
[15]. Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data," in IEEE Transaction on Dependable and Secure Computing, DOI Bookmark: 10.1109/TDSC.2018.2829880, 2018.
[16]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," presented at ASIACRYPT 2008: Advances in Cryptology, pp. 90-107, 2008.
[17]. Y. B. Miao, J. F. Ma, X. M. Liu, X. H. Li, Q. Jiang and J. W. Zhang, "Attribute-based keyword search over hierarchical data in cloud computing," in IEEE Transactions on Services Computing, doi:10.1109/TSC.2017.2757467, 2017.
[18]. Y. B. Miao, J. F. Ma, X. M. Liu, J. Weng, H. W. Li andH. Li, "Lightweight fine-grained search over encrypted data in fog computing," in IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2018.2823309, 2018.
[19]. D. X. Song, D. Wagner and A. Perrig, "Practical Techniques for Searches on Encrypted Data," presented at IEEE Symposium on Security and Privacy, pp. 44-55, 2000.
[20]. E. J. Goh, "Secure Indexes," presented at Technical Report 2003/216, IACR ePrint Cryptography Archive, ppt.
[21]P. Nagaraj, Dr A. V. Krishna Prasad, Dr. M. Venkat Dass, Kallepalli Rohit Kumar, "Swine Flu Hotspot Prediction In Regions Based on Dynamic Hotspot Detection Algorithm" Journal of Theoretical and Applied Information Technology(**JATIT),** 30th Nov-2022, ISSN:1992-8645, Vol-100, N0.22, Pages- 6535 to 6544.
[22]P.Nagaraj, Dr.A.V. Krishna Prasad, Dr.V.B.Narsimha, Dr.B.Sujatha " A swine flu Detection and Location using Machine Learning Techniques and GIS", International Journal of Advanced Computer Science and Application**(IJACSA),** Vol-13, No.9, 2022.Pages 1001 to 1009.
[23]P.Nagaraj , Rajesh Banala and A.V.Krishna Prasad, "Real Time Face Recognition using Effective Supervised Machine Learning Algorithms", **Journal of Physics**: Conference Series 1998 (2021) 012007 IOP Publishing doi:10.1088/1742-6596/1998/1/012007
[24]P.Nagaraj,Dr.M.Venkat Dass, E.Mahender "Breast Cancer Risk Detection Using XGB Classification Machine Learning Technique ",IEEE International Conference on Current Development in Engineering and Technology (CCET)-2022,Sage university, Bhopal, India, 23-24,Dec 2022.
[25]P. Nagaraj, Gunta Sherly Phebe, Anupam Singh, "A Novel Technique to Classify Face Mask for Human Safety", 2021 Sixth ICIIP Published in: 2021 Sixth International Conference on Image Information Processing (ICIIP),26-28 Nov. 2021, 10 February 2022 DOI: 10.1109/ICIIP53038.2021.9702607 Publisher: IEEE Conference Location: Shimla, India
[26]P. Nagaraj and Dr A. V. Krishna Prasad, "A Novel Technique to Detect the Hotspots Swine Flu Effected Regions", Published in: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO),15 November 2021 DOI:10.1109/ICRITO51393.20 21.9596422, Electronic ISBN:978-1-6654-1703-7 CD:978-1-6654-1702-0.