Practical Multi-Keyword Ranked Search with Encrypted Cloud Data Access Control

Mrs. Vijaya Ramineni [1], Mr. Gajula Dhanush Kumar [2]

#1 Associate Professor In The Department Of AI & IT at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District,A.P.

#2 MCA Student In The Department Of Computer Applications at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District, A.P

ABSTRACT_ Data owners are increasingly inclined to store their data in the cloud due to the rapid growth of data volume in the cloud computing environment. Despite the fact that information reevaluating decreases calculation and capacity costs for them, it definitely brings new security and protection worries, as the information proprietors lose direct control of delicate information. Meanwhile, the majority of current ranked keyword search schemes concentrate primarily on improving search efficiency or functionality, but they do not simultaneously provide effective access control or formal security analysis. To address these restrictions, in this paper we propose an effective and security saving Multi-watchword Positioned Search plot with Fine-grained admittance control (MRSF). By combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and improving the secure kNN method, MRSF can perform ciphertext retrieval with high accuracy. In addition, the polynomial-based access strategy enables it to effectively refine users' search privileges. Formal security examination shows that MRSF is secure regarding secrecy of rethought information and the protection of record and tokens. Broad examinations further show that, contrasted and existing plans, MRSF accomplishes higher pursuit exactness and more functionalities productively.

1.INTRODUCTION

AS another figuring worldview [1], distributed computing offers pervasive and on-request admittance to adaptable calculation and capacity assets. As a result, both businesses and individuals now routinely outsource local data to cloud servers. Data owners actually lose direct control over their data despite the fact that this measure significantly reduces hardware and maintenance costs. Owners of highly sensitive data, such as electronic medical records and financial documents, have undoubtedly experienced some security concerns as a result. People and businesses may be reluctant to outsource their sensitive data to an unreliable third-party cloud service provider because of this level of suspicion. As a result, concerns regarding security will emerge as one of the primary impediments to the widespread use of cloud computing [2].

Before outsourcing their data to the commercial public cloud, data owners typically encrypt their data to prevent possible leakage. However, plaintext-based information retrieval technologies cannot be applied to outsourced data because conventional data encryption schemes prevent the cloud from running authorized calculations on its storage (such as retrieving the relevant file for a specific customer). A minor arrangement is to download every one of the information and decode them locally, yet this might prompt a tremendous misuse of transfer speed and calculation assets [3]. Subsequently, how to accomplish productive information recovery while guaranteeing information security turns into a difficult issue.

The Searchable Symmetric Encryption (SSE) [4, 5, 6, 7, 8, and 9] is generally regarded as a promising approach to resolving the conflict between data use and confidentiality.

2.LITERATURE SURVEY

2.1) S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.

Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA adaptability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions

2. 2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Although some cloud servers store data, which raises a number of privacy concerns, cloud computing is a revolutionary computing paradigm that enables flexible, on-demand, and low-cost resource utilization. To protect cloud storage, a number of approaches based on attribute-based encryption have been proposed. However, identity privacy and privilege control receive less attention than data content privacy and access control in most projects. AnonyControl, a semianonymous privilege control method, is presented in this paper to address the data privacy and user identity privacy concerns of existing access control methods. To prevent identity leaks, AnonyControl decentralizes authority, resulting in semi-anonymity. In addition, it extends file access control to privilege control, making it possible to fine-tune privilege management for all cloud data operations. Then, we present the AnonyControlF, which achieves complete anonymity and completely prevents identity leakage. Our performance evaluation demonstrates the viability of our schemes, and our security analysis demonstrates that, under the DBDH assumption, both AnonyControl and AnonyControl-F are secure.

3.PROPOSED SYSTEM

The proposed framework planned a few broad trials to investigate the connection among irregularity and search precision. As a natural relaxation of the standard IND-CPA security definition, we propose an optimal security concept for MRSF as indistinguishability under same-closeness-pattern chosen-plaintext attacks (IND-CLS-CPA), inspired by [27]. According to the definition of IND-CPA, an attacker will easily take advantage of MRSF's inevitable leakage of closeness and equality (such as the access pattern). To demonstrate that MRSF is IND-CLS-CPA secure, we present a comprehensive and in-depth security analysis in this paper. Besides, the security of MRSF under work of art and novel assaults in the realized foundation model.

In particular, the following is a summary of the contributions made in this paper:

Improved search precision In correlation with the past positioned multi-watchword search plans, MRSF accomplishes higher hunt precision by developing report records with TF-IDF rule. Using a real-world dataset, experiments show that MRSF outperforms the other options in search accuracy without adding a lot of extra work to the computer.

Lightweight access control with fine-grained controls By extending the polynomial-based access strategy to document indexes and search queries, MRSF provides lightweight access control rather than the time-consuming encryption and decryption operations found in attributed-based schemes. The improved secure kNN algorithm incorporates the access control mechanism in MRSF, preserving the benefits of user-granular access privileges.

_ A formal security guarantee and a higher level of privacy protection. The ideal security thought of MRSF is characterized and hypothetically demonstrated as IND-CLS-CPA, i.e., the classification of files and search questions are both checked as IND-CLS-CPA secure. Further examination of security issues in the Known Background Model demonstrates that MRSF resists the proposed attacks. This demonstrates that MRSF is ultimately more secure than the previous secure kNN-based schemes.

3.1 IMPLEMENTATION

Data Users

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Search Documents, View Files, Request Secret Key, Download.

Data Owner

In this module, there are n numbers of users are present. Dataowner should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Upload, View Files, View Secret Key Request and send response.

Cloud

In this module, the Cloud has to login by using valid user name and password. After login successful he can do some operations such as View Data ,activate user and owner ,view Users View Owner data in encrypted format .

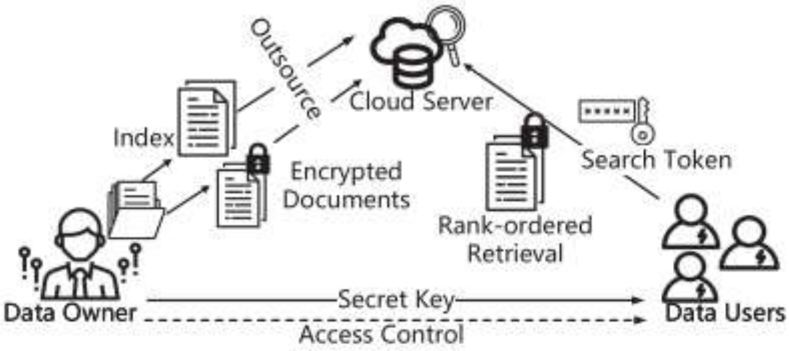
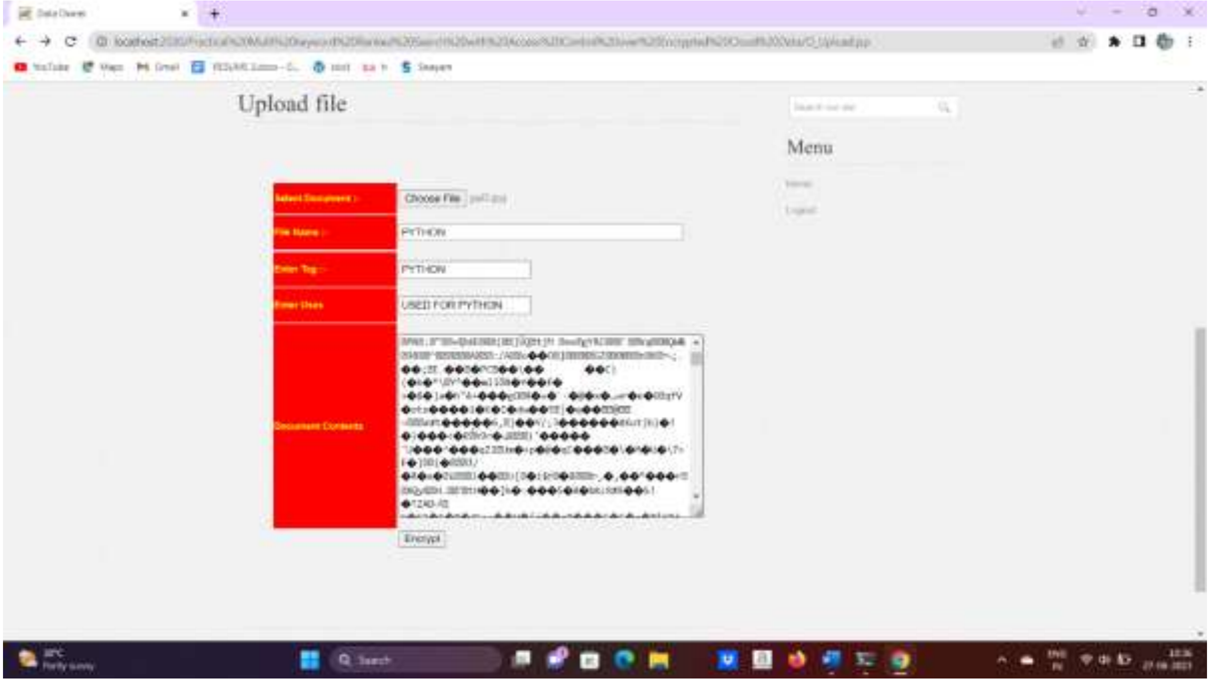


Fig 1: Architecture

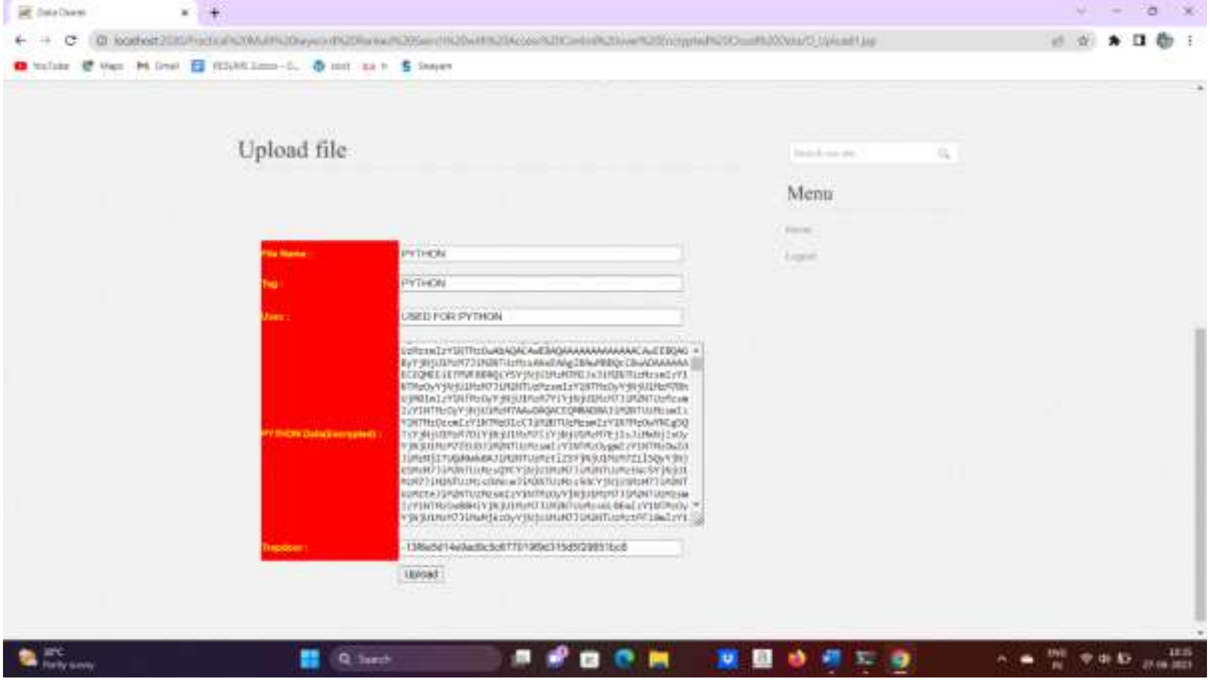
4.RESULTS AND DISCUSSION



Upload file

Select Document :	Choose File
File Name :	PYTHON
Enter Tag :	PYTHON
Enter Uses	USED FOR PYTHON
Document Contents	[illegible]

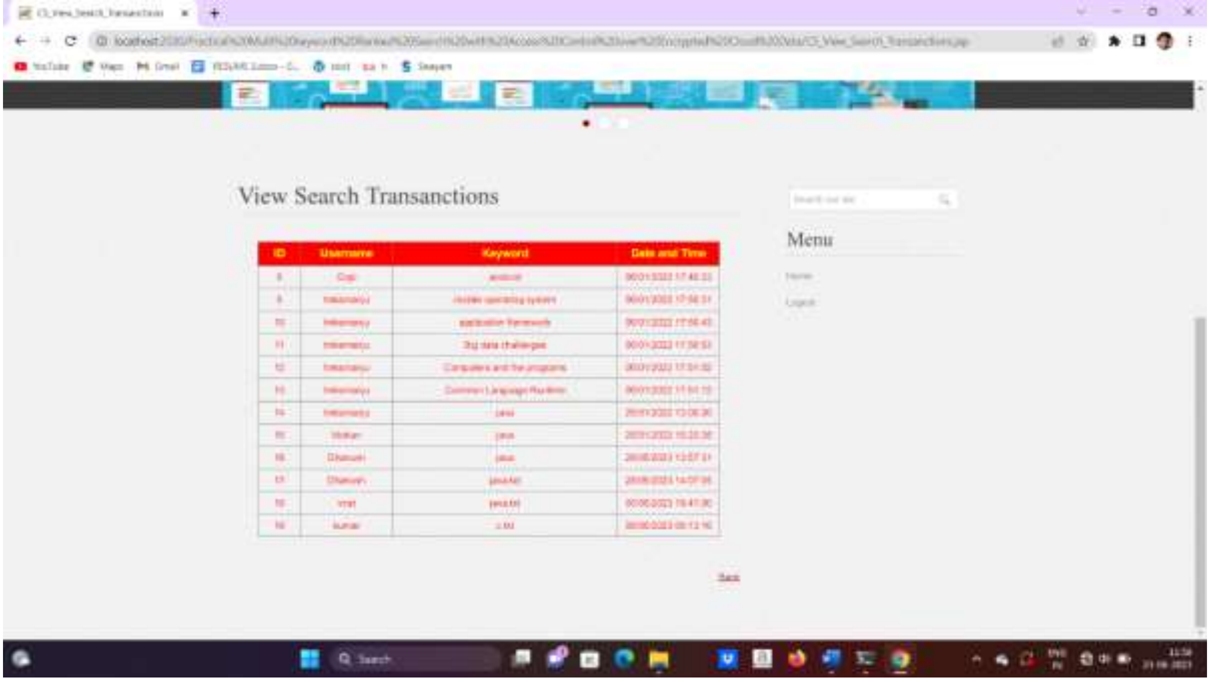
Fig 2:ENCRYPTION



Upload file

File Name :	PYTHON
Tag :	PYTHON
Uses :	USED FOR PYTHON
PYTHON Data(Encrypted) :	[illegible]
Trapdoor :	[illegible]

Fig 3: DECRYPTION



View Search Transanctions

ID	Username	Keyword	Date and Time
8	[illegible]	android	[illegible]
9	[illegible]	mobile operating system	[illegible]
10	[illegible]	application framework	[illegible]
11	[illegible]	big data challenges	[illegible]
12	[illegible]	Computers and the programs	[illegible]
13	[illegible]	Common Language Runtime	[illegible]
14	[illegible]	java	[illegible]
15	[illegible]	java	[illegible]
16	Dhanush	java	[illegible]
17	Dhanush	java.txt	[illegible]
18	[illegible]	java.txt	[illegible]
19	kumar	c.txt	[illegible]

Fig 4:Data search based on ranking

5.CONCLUSION

We present a privacy-preserving multi-keyword search strategy with lightweight fine-grained access control (MRSF) in this study. In addition to realising access control, MRSF achieves a better search performance and a higher security level when compared to earlier schemes. We combine the TF-IDF rule with the standard coordinate matching approach and integrate the access control strategy with the improved secure KNN scheme to increase the practicability and security of MRSF. Formal security definitions and analysis reveal that MRSF is IND-CLS-CPA secure; we also demonstrate that MRSF is resistant to the representative KPAs. Finally, detailed analyses show the aspects that influence MRSF search accuracy and efficiency.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2010, pp. 253–262.

[2] L. Zhang, Y. Zhang, and H. Ma, “Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data,” IEEE Access, vol. 6, pp. 34 214–34 225, 2018.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[4] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Secur. Privacy, 2000, pp. 44–55.

[5] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Proc. Int. Conf. Appl. Cryptography Netw. Secur., 2005, pp. 442–455.

[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” J. Comput. Secur., vol. 19, no. 5, pp. 895–934, 2011.

[7] M. Abdalla et al., “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,” in Proc. Annu. Int. Cryptol. Conf., 2005, pp. 205–222.

[8] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptogr. Techn., 2004, pp. 506–522.

[9] M. Bellare, A. Boldyreva, and A. O’Neill, “Deterministic and efficiently searchable encryption,” in Proc. Annu. Int. Cryptol. Conf., 2007, pp. 535–552.

[10] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 383–392.

[11] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn., 2010, pp. 62–91.

[12] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. Int. Conf. Pairing-Based Cryptogr., 2007, pp. 2–22.

[13] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., 2004, pp. 31–45.

[14] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Int. Conf. Inf. Commun. Secur., 2005, pp. 414–426.

AUTHOR PROFILES

Mrs Vijaya Ramineni completed her Master of Computer Applications (MCA), M.Tech in (CSE) from Acharya Nagarjuna University. She has published more than10 papers in indexing Journals, currently working as an Associate Professor in the department of AI & IT at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District. Her areas of interest are Data Mining, Cloud Computing and MachineLearning.

Mr. Gajula Dhanush Kumar, as MCA student in the department of DCA at DVR & DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District. He has completed BSC in MARUTHI DEGREE COLLEGE From KRISHNA UNIVERSITY. His areas of interests are Networks, Machine Learning and Cloud Computing.