Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**

ATTRIBUTE BASED ACCESS CONTROL WITH DATA SECURITY OF CONJUNCTIVE QUERY OVER ENCRYPTED DATA

#1 Mr. G.Ramamohana Rao , #2 M.Tarakeswari, #3 V.Uday Kiran, #4 A.Lakshmi Anusha, #5 G.Chaitanya
#1Assistant professor in Department of IT, DVR & Dr.HS MIC College of Technology,Kanchikacherla
#2#3#4#5 B.Tech with Specialization of Information Technology , DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

Abstract_ This project addresses the fundamental issue of processing conjunctive queries on public clouds that include both keyword and range conditions in a privacy-preserving manner. No prior Searchable Symmetric Encryption (SSE)-based privacy-preserving conjunctive query processing technique can meet the three requirements of adaptive security, efficient query processing, and scalable index size. In this research, we present the first privacy-preserving conjunctive query processing system that meets all three of the above requirements. To achieve adaptive security, we propose an Indistinguishable Bloom Filter (IBF) data structure for indexing purposes. To accomplish quick query processing and structural indistinguishability, we propose the Indistinguishable Binary Tree (IBtree) data structure, which is extremely balanced.

To obtain scalable and small index sizes, we present an IBtree space reduction approach that removes redundant information from IBFs. To improve search performance, we introduce a traversal minimization approach. To keep our approach dynamic, we present updating techniques. We show that our system is adaptively secure using the IND-CKA secure model. This paper's main contribution is to provide conjunctive query processing with high privacy guarantees while being practical in terms of time and space. We implemented our scheme in C++, assessed it, and compared its performance to the previous KRB scheme for keyword searches and the prior PBtree strategy for range queries on two real-world datasets.

1.INTRODUCTION

The two ventures and end clients have been progressively re-appropriating their information and processing administrations to public mists for lower cost, higher unwavering quality, better execution, and quicker arrangement. Nonetheless, security has turned into the critical worry as information proprietor may not completely trust public mists. To start with, mists might have degenerate representatives. For instance, in 2010, a Google engineer broke into the Gmail and Google Voice records of a few youngsters. Second, mists might be hacked and clients may not be educated. Third, cloud offices might be worked in a few outside nations where security guidelines are challenging to uphold. This paper centers around the well known distributed computing worldview where an information proprietor stores information on a cloud and numerous information clients question the information. Figure 1 shows these three gatherings: an information proprietor, a cloud, and different information clients. Among the three gatherings, the information proprietor and information clients are trusted, yet the cloud isn't completely trusted. In this paper, we consider the basic issue of handling conjunctive questions that contain both catchphrase conditions and reach conditions on open mists in a protection safeguarding way. The question conditions in the where statements of SQLs are in many cases conjunctive states of watchwords and reaches.

A disjunctive inquiry can be effortlessly changed over into numerous conjunctive questions. For instance, in the SQL question select * from patient where NAME=John and age 30, the where statement contains a watchword condition NAME=John and a not as much as condition age < 30, which can be changed over into a reach condition age 2 [0, 30]. Specifically, we think about Accessible Symmetric Encryption (SSE) plans in light of the fact that symmetric encryption based security safeguarding plans are essentially more effective than hilter kilter ones. In SSE, the information proprietor fabricates a safe list I for an informational index D, and encodes every information thing di 2 D into (di)K utilizing a mystery key K that is divided among the information proprietor and information clients. Then, the information proprietor rethinks the solid list I alongside the arrangement of encoded information {(d1)K,(d2)K, ⋯ ,(dn)K} to the cloud. Given a conjunctive inquiry q, the information client creates a hidden entryway tq for q, and sends tq to the cloud. Base on tq and the safe list I, the cloud can figure out which encoded information things fulfill q without knowing the substance of the information and inquiry. However, in this cycle, the cloud ought not be ready to derive security data about the information things and questions, for example, information content, question content, and the measurable properties of property estimations. The file I ought to release no data about the information things in D. Note that an information thing di could be a record in a levelheaded data set table or a text report in an archive set

2.LITERATURE SURVEY

Non-SSE based Security Protecting Question Plans: Dan Boneh et al. proposed a predicate encryption named Secret Vector Encryption (HVE) to help conjunctive, subset, and reach question handling [26]. Elaine Shi et al. proposed a plan named MRQED utilizing character based encryption to deal with complex reach inquiries [27]. Bharath K. Samanthula et al. proposed a protection saving inquiry handling plan in light of homomorphic encryption and confused circuit methods that upholds complex questions over encoded information [29]. Be that as it may, these three plans have straight inquiry handling time concerning the absolute number of information records. Boyang Wang et al. proposed a multi-faceted reach question handling plan accomplishing sublinear inquiry handling time, in view of HVE and R-trees [28]; notwithstanding, it uncovers question conditions to the cloud. Besides, the plans proposed in [26]-[29] are lopsided cryptography based approaches, which have a high registering intricacy. For instance, the plan in [29] requires a few seconds to test whether an information thing fulfills a question condition. The plan in [30] takes on the ASPE approach [31] to scramble question ranges; in any case, the security of ASPE isn't secure against picked plain text assault [32]. Neglectful RAMs proposed by Goldreich and Ostrovsky can be utilized to help complex question handling with versatile security; in any case, this plan requires numerous rounds of association for each read and compose, which makes it very wasteful [33]. Arasu et al. depicted the plan of Cipherbase framework and introduced the plan of Cipherbase secure equipment and its execution utilizing FPGAs [34], which is not the same as our protected model as we don't consider to prepare unique equipment in cloud servers. SSE based Security Protecting Watchword Inquiry Plans: Other than the catchphrase question plans referenced in Segment 1.4, there are other SSE based protection safeguarding watchword inquiry plans, for example, the ones in [4], [5], [7] and the one in [8]. In [36], the creators proposed a plan for protection safeguarding string coordinating. Be that as it may, every one of them just accomplish nonadaptive security. Seny Kamara et al. proposed a plan to deal with SQL inquiries over encoded information for a social data set [37]. However, the plan in [37] doesn't upholds secure conjunctive questions that contain range conditions. SSE based Security Safeguarding Reach Inquiry Plans: All earlier SSE based protection saving reach question conspires, regardless of one-layered or multi-faceted, can't accomplish versatile security. Bucketing based range inquiry plans [38], [39] and request protecting encryption/hash capability based range question plans [2], [3], [40]-[42] can't

accomplish provably security, regardless of under the non-versatile or the versatile security model..

3.PROPOSED SYSTEM

We present the first SSE-based conjunctive query technique that allows both keyword and range conditions while meeting three requirements: adaptive security, efficient query processing, and scalable index sizes. To achieve adaptive security, we propose a data structure termed the Indistinguishable Bloom Filter (IBF) for index storage. Each element in an IBF has two cells: one for storing index information and the other for masking, which help us achieve node indistinguishability and allow the simulator of an IBF to simulate future unknown queries in a random Oracle model.

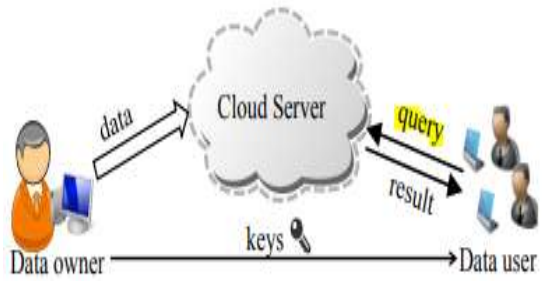


Fig 1:Proposed System Architecture

3.1 IMPLEMENTATION

1. **Data Owner:**

Using this module data owner will register with application and login with valid username and password. Owner will upload file encrypt data to secure data and generate tap door for respective query for not allowing cloud to know what type of data should be given to user request. Oner will view uploaded files and view tapdoor and related query.

data owner builds a secure index I for a data set D, and encrypts each data item di 2 D into (di)K using a secret key K that is shared between the data owner and data users. Then, the data owner outsources the secure index I I along with the set of encrypted data

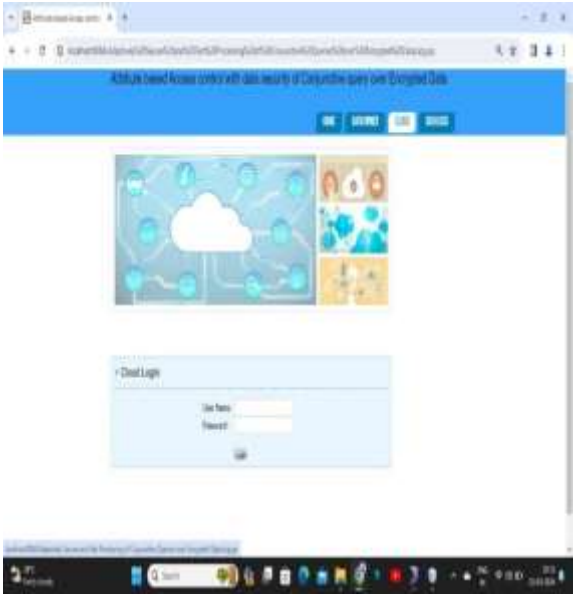
Cloud

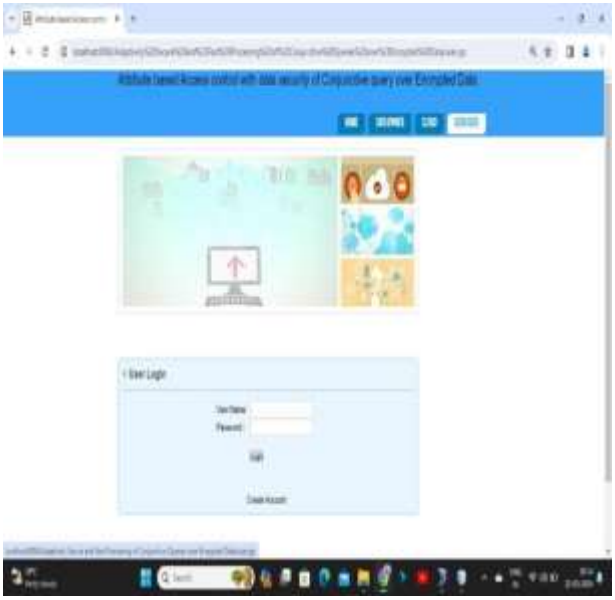
Using this module cloud will login to application view file uploaded by owner in encrypted format. Cloud can view requested files from user and using tapdoor key cloud can retrive requested data and give details to use with security key with out knowing what user has requested for. We assume that the cloud is semi-honest (also called honestbut-curious)

User:

Using this module user will register with application view files uploaded by various data users and view tap door kyes for query. User can request data to cloud based on tapdoor and get security key to decrypt file.

4.RESULTS AND DISCUSSION





5.CONCLUSION

We make four crucial contributions. First, we present the first privacy-preserving conjunctive query processing system that meets all three requirements: adaptive security, efficient query processing, and scalable index size. Our method incorporates several innovative ideas, including IBFs and IBtrees. Second, we offer the first probabilistic trapdoor computing algorithm, which generates many trapdoors for the same query. Third, we offer the IBtree space compression algorithm and the IBtree traversal minimization approach to improve space and query time efficiency. Fourth, we assessed our method using two real-world data sets. The experimental findings show that our technique is quick in terms of query processing time and scalable in terms of index size.

REFERENCES

R. Canetti, U. Feige, O. Goldreich, M. Naor. Adaptively secure multipartycomputation. STOC, pages 639–648. ACM, 1996.

J. Li and E. R. Omiecinski. Efficiency and security trade-off in supporting rangequeries on encrypted databases. In Proc. 19th IFIP Conf. on Data and App. Security & Privacy, pages 69–83, 2005.

A. Boldyreva, N. Chenette, and A. O'Neill. Order preserving encryption revisited:Improved security analysis and alternative solutions. In Proc. CRYPTO, pages 578–595, 2011.

D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypteddata. In Proc. IEEE Symposium on Security and Privacy (S&P), pages 44–
55. IEEE, 2000.

E. Goh. Secure indexes. Stanford University Tech. Report, 2004.

D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryptionwith keyword search. In Proc. EUROCRYPT, pages 506–522, 2004.

Y.-C. Chang and M. Mitzenmacher. Privacy preserving keyword searches on remoteencrypted data. In Third Inte. Conf. on Applied Cryptography and Network Security (ACNS), pages 442– 455, 2005.

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky. Searchable symmetricencryption: improved definitions and efficient constructions. In Proc. CCS, pages 79-88, 2006.

M. Bellare, A. Boldyreva, and A. O´ıNeill. Deterministic and efficiently searchableencryption. CRYPTO, pages 535–552, 2007.

S. Kamara, C. Papamanthou, and T. Roeder. Dynamic searchable symmetricencryption. In Proc. CCS, pages 965–976, 2012.

D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner. Highlyscalable searchable symmetric encryption with support for boolean queries. In CRYPTO, pages 353–373, 2013.

D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Stiner.Dynamic searchable encryption in very-large databases: Data structures and implementation. In NDSS. 2014.

R. Li, A. X.Liu, L. Wang, and B. Bezawada. Fast range query processing withstrong privacy protection for cloud computing. In Proc. VLDB, pages 1953–1964. IEEE, 2014.

Author's Profiles

#1:-Mr.G.Ramamohana Rao working as Assistant Professor in Department of IT in DVR & Dr, HS MIC College of Technology,Kanchikacherla-521180

#2:- M.Tarakeswari(20H71A1247) B. Tech with Specialization of
Information Technology in DVR & Dr. HS MIC College of Technology, Kanchikacherla-521180

#3:-V.Uday Kiran(20H71A1253) B.Tech with Specialization of Information
Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#4:-A.Lakshmi Anusha (20H71A1216) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology, Kanchikacherla-521180

#5:-G.Chaitanya(21H75A1202) B.Tech with Specialization of Information Technology in DVR & Dr. HS MIC College of Technology,Kanchikacherla-521180