An Approach for implemented Secure Proxy Server for Multi-user Searchable Encryption without Query Transformation

CJ Karthik[1], K Narayana[2], B Srinivasulu[3]

[1]*Student, Department of Computer Science and Engineering, Sechachala Institute of Technology, Puttur, Andhra Pradesh, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, Sechachala Institute of Technology, Puttur, Andhra Pradesh, India.*
[3]*Assistant Professor, Department of Computer Science and Engineering, Sechachala Institute of Technology, Puttur, Andhra Pradesh, India.*

---***---

Abstract - *Cipher-policy attribute-based encryption (CP-ABE) focus on the problem of access control, and keyword-based searchable encryption scheme focus on the problem of finding the files that the user interested in the cloud storage quickly. To plan an accessible and characteristic based encryption plot is another test, we propose a productively multi-client accessible quality based encryption plot with trait repudiation and give for distributed storage. In the new plan the trait repudiation and give procedures of clients are designated to intermediary server. Our plan underpins multi trait are disavowed and allowed at the same time. Besides, the watchword accessible capacity is accomplished in our proposed plan. The security of our proposed plan is lessened to the bilinear Diffie-Hellman (BDH) supposition. Moreover, the plan is turned out to be secure under the security model of vagary against specific ciphertext-arrangement and picked plaintext assault (IND-sCP-CPA).This paper proposes a secure proxy server approach that performs the search operation without transforming the user queries. This approach also returns the top-k relevant documents to the user queries by using Euclidean distance similarity approach. Based on the experimental study, this approach is efficient with respect to search time and accuracy.*

Key Words: Cloud computing, multi-user, searchable symmetric encryption.

1. INTRODUCTION

Cloud computing is witnessing rapid innovations in the recent years. It has two principle undertakings putting away and getting to information and projects by methods for Internet instead of utilization of a PC's hard drive. The substance cloud exhibits a broad scope of administrations. It diminishes the intricacy of the systems, makes arrangement for customization, versatility, effectiveness and so forth. Plus, the data put away on cloud is by and large not effortlessly lost. On account of its on-request nature, you could commonly purchase distributed computing a similar way you would purchase power, telephone utilities, or Internet access from a service organization.

As cloud technology is becoming more and more wide-spread, the challenges ((like leaking of sensitive data [1], hacking [2], un-encrypted data at risk [3–5] involved in maintaining the technology is also increasing. Cloud security, the arrangements, innovations, controls and so forth that are utilized to ensure the information, the different applications on the cloud and the related framework, is turning into a basic field of research in the field of Network Security, and all the more extensively in Computer Security.

In the setting of seeking on open key-encoded information, clients who scramble the information can be not quite the same as the proprietor of the decoding key. This makes the model for multi-essayist/single-peruser SE. A more summed up model further enables each client to compose a scrambled record to the database and also to look inside the encoded space, including those ciphertexts created by different clients.

The information proprietor to create and send back the essential trapdoor data to enable her do to the hunt, as appeared in the agent work [15]. In this manner, the information proprietor is required to be online constantly. Nonetheless, the underlying objective of the information proprietor is to re-appropriate his stockpiling and administrations to the cloud server, so evacuating the per-inquiry collaboration between the information proprietor and the customer is a coveted component.

The data owner to first use a special encryption algorithm which produces an encrypted version of the database, including encrypted metadata, that is then stored on an external server. Later, data owner can interact with the server to carry out a search on the database and obtain the results (this is also called the symmetric setting as there is only one writer to the database, the owner, who uses symmetric encryption.)

Straightforward encryption innovation can secure information classification effortlessly. Be that as it may, it isn't conceivable to look inside the scrambled space. With the end goal to look for a specific catchphrase, client needs to decode the information first, before beginning the seeking procedure. It isn't down to earth especailly when the volumne of 2 Authors Suppressed Due to Excessive Length information is substantial. Accessible encryption (SE) [31,4,10,7,6] is a cryptographic crude tending to scrambled pursuit.

2. RELATED WORK

In the multi-writer/multi-reader setting, a number of schemes [3,11,32,1] were presented with a high level of security, but the search time is linear in the number of keywords per document. The plan in [26] enhanced the inquiry multifaceted nature by expelling the need of TTP in past plans. What's more, a more grounded model for access design security was proposed in [29].

Notwithstanding, every one of these plans just help single watchword looks.

The plan utilizes deterministic encryption and straightforwardly releases the pursuit design notwithstanding the entrance design. . Starting late, Jarecki et al. [15] extend the arrangement with Cash et al. [6] to a lone writer/multireader setting, which secures each and every lovely component given by the primary arrangement yet requires a for every request coordinated effort between the data proprietor and the customer. It ought to be focused on that one of the principle contrasts between mystery key accessible encryption and its publickey partner is that the last can never again hold inquiry protection once an inquiry is known, in light of the fact that one can specify and scramble every conceivable catchphrase utilizing general society key, and afterward coordinate the question being referred to. After some time, accessible encryption has developed into predicate encryption (e.g., [16], [17], [18]), which speaks to a summed up idea covering different cryptographic natives, for example, character based encryption, property based encryption, and past. Predicate encryption focuses at taking care of more mind boggling inquiries upon scrambled information, e.g., run questions, disjunctions, et cetera. While being all the more intense, predicate encryption works at the cost of higher calculation cost. Considering the normal extensive volume of 265 client gets to over the cloud, the genuine possibility of utilizing the crude, e.g. [19], is misty.

As a final note, the scheme proposed in this work can be viewed as an adaptation of our earlier work [20] to the setting of enterprise-outsourcing-database-to-cloud. The plan in [20] applies to the situation that various clients are qualified for hunt as well as keep in touch with the database, though the ebb and flow work thinks about that a solitary information proprietor (i.e., the undertaking) keeps in touch with the database, while numerous clients are approved to look. The two in truth supplement one another. What's more, contrasted with [20], the all-encompassing plans contained in Section V, e.g., executing partition of obligation, fluffy catchphrase look, are new outcomes.

3. PROPOSED METHODOLOGY

In this section we define our proposed scheme that is more secure, accepts automatic updates and is simpler to implement. Here we first define the notions and preliminaries required to define the scheme and then we outline the structure of our proposed scheme.

A. Notations and Preliminaries
F = Set of m information documents (f1, f2, … , fm) in the record gathering to be redistributed to the cloud server. m = Represents add up to number of documents to be redistributed.

T = Set of n identifiers or tokens (t1, t2, … , tn) removed from each document in the record gathering F in the wake of sifting through stop words.

n = Total number of tokens extricated in the wake of expelling stop words.

I = accessible Index worked from the tokens removed from document gathering F. This list contains n records.

REQ = multi-catchphrase ask for created by the information client.

Enc(ti) = encoded result for each scrambled watchword dependent on condition (2).

α = ASCII estimation of letter sets in the tokens extricated.

ID (fi) = identifier created for a document fi ∊ F

SK = symmetric mystery key created and circulated to approved clients.

B. REQ' = Scrambled multi-watchword request created by data customer and sent as a trapdoor to cloud server for glancing through the information.Framework for plan We here characterize our proposed plan that depicts a multi-catchphrase positioned pursuit and utilizations an updatable list of the request O(n x 3). We utilize the accompanying phrasing to depict our plan: we have an information proprietor that has a gathering of m documents F= {f1, f2, f3, … .., fm) to be re-appropriated to the cloud server. Before redistributing, every one of the tokens are removed from the records. The documents are then scrambled utilizing a symmetric encryption plot. The tokens are then sifted to expel the stop words and rest n tokens are gathered into a list table. The file table contains n lines and 3 sections that contain the tokens, document identifiers, pertinence score of each record as for the token. The tokens are spoken to as an arrangement of n esteems T= (t1, t2, t3, … , tn). When a record is included its identifier is produced and it is mapped to the file table. In the event that an officially existing document is altered it additionally produces another identifier for the document and prior record for that records are erased from list table. The tokens gathered subsequent to separating the stop words are then encoded with symmetric encryption calculation. A second level of encryption is also provided by encrypting the encrypted keywords with the following scheme [1]

$$Enc\ (ti) = + + \ldots\ldots\ldots + \quad (3)$$

$$Enc\ (ti) = \sum \quad (4)$$

Where x is a randomly generated large real number, which needs to be same for both indexed token and queried token. k Represents the length of the token, and l represents the position of the alphabet in the token. After encryption, the encoded documents and doubly scrambled record is re-appropriated to the cloud server. On the client's side when questioned catchphrases are scrambled utilizing indistinguishable encryption strategies from for ordered watchwords there is a plausibility of recurrence investigation assault. To beat this assault when a hunt is started from a client the estimation of x is naturally changed after each pursuit. Subsequently every time a pursuit is handled a similar token will have diverse incentive for ciphertext and henceforth recurrence investigation assault could be controlled. Thus the whole methodology happens in three stages: one on the information proprietor's end, second on the information client's end and third on the cloud server's end. The proposed scheme works on the following algorithms:

GenKey (r) - It Generates the symmetric encryption key SK using the security parameter r. This symmetric key is shared between the data owner and the authorized users.

Preprocessing (F, SK, x) – This calculation separates the tokens from the record accumulation F, at that point channels the stop words, figures the significance scores for documents for each extricated token dependent on tf-idf rule. The tokens are then scrambled utilizing condition (2). The list, I, is the reencrypted utilizing symmetric key, SK. The x is arbitrarily created and imparted to the approved client. The record gathering F is additionally scrambled utilizing symmetric encryption An Efficient Multi-catchphrase Symmetric Searchable Encryption Scheme for Secure Data Outsourcing 69 Copyright © 2016 MECS I.J. PC Network and Information Security, 2016, 11, 65-71 cryptographic plan. This accessible encoded file I' and scrambled record accumulation F' are re-appropriated to the cloud server. CreateReq (REQ, SK, x) – the approved client when produces a multi-watchword inquiry, REQ, the calculation forms the question, sift through stop words, encodes the rest of the tokens utilizing SK and afterward re-scrambles them utilizing condition (2), to REQ'. This encoded hunt ask for is then sent to the cloud server to make an inquiry over the scrambled file.

As soon as this search request is generated and sent to the cloud server the randomly generated x value for encryption in equation (2) is automatically regenerated and updated. Score calculate (I’,REQ’)- On receiving the search request cloud server computes the score of each file in I’ with respect to REQ’ based on equation (1). Search (REQ’,I’) – cloud server calls Score calculate(I’,REQ’) and sorts the files based on their relevance scores and sends back encrypted files to the user.

Decrypt(SK, F’) - the data user receives the encrypted files. The user then decrypts the files. Hence files are securely ranked searched over encrypted data.
Hence, the entire scenario is considered to be divided into three phases or modules:

Data Owner Module (Initialisation phase)

1) Data owner calls GenKey(r) algorithm to Generate the symmetric encryption key SK using the security parameter r. This symmetric key SK is shared between the data owner and the authorized users to access the outsourced files fi ∊ F (1≤ i ≤ m).
2)The information proprietor calls Preprocessing(F,SK,x) calculation to remove tokens T from each fi ∊ F, and afterward sift through the stop words to make an arrangement of n tokens T={ti│1≤i≤n}. The information proprietor at that point computes the significance scores dependent on tf-idf rule for every ti ∊ T. It at that point makes a (n * 3) accessible altered file I containing (ti │FID │Rel. Score) and a document record table containing (FID│ Fname │update status).
3) Each token ti is then encoded utilizing condition (2). Whole document gathering F is encoded utilizing a symmetric cryptographic plan with SK and afterward the doubly scrambled record, and encoded document accumulation are re-appropriated to the cloud server.

Data User Module (Retrieval Phase)

An approved information client can call CreateReq (REQ, SK, x) calculation to produce a multi-watchword look ask for REQ = (t1, t2, … .. , ts). REQ is scrambled twice to produce REQ', and afterward client sends REQ' to the cloud server.

When the client starts the pursuit by creating a scrambled inquiry REQ', our calculation consequently refreshes the estimation of parameter x in condition

Cloud server Module (processing and Ranking Phase)

1) Cloud server gets REQ', which contains encoded tokens and calls Scorecalculate(I',REQ') calculation to process the importance scores for the records.
2) After figuring the importance scores the documents are arranged in diving request as indicated by the scores.
3) Top k positioned documents are grabbed from the arranged rundown and sent to the client who started the hunt ask.

4. CONCLUSION

We have proposed a very simple and efficient multi-keyword symmetric searchable encryption scheme that could be used to create a searchable index and is able to make an efficient search over encrypted cloud data. The proposed scheme is more efficient than TRSE scheme [4]. It utilized a doubly encryption strategy which makes it similarly more secure and effective yet straightforward and simple to execute. Our strategy additionally considers programmed refreshes as and when another record is included, erased or adjusted in the given document set. At last we embedded the plan on a genuine informational index that indicates decrease in time required to create, refresh and seek in an encoded record.

5. FUTURE SCOPE

Currently By using proxy server approach, Hash Value computation for large File Size will be performance hit. So further in future work we can use Attribute-Based Encryption for encrypting the File Data. To figure the File Tag, rather than utilizing entire record information we will utilize File Attributes to seek. In Future Scope, It can be finding Video Spam content & Image Spam Content.

REFERENCES

[1] R. Chow, et. al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proc. IEEE International Conf. on Cloud Computing, pp. 85-90, 2010.

[2] S. Kamara and K. Lauter, Cryptographic Cloud Storage. Proc. Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010.

[3] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, 2009.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovskey, Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. Proc. ACM Conf. on Computer and Communications Security, CCS'06, pp. 79-88, 2006.

[5] Y. Chang and M. Mitzenmacher, Privacy Preserving Keyword Searches on Remote Encrypted Data. Proc. Applied Cryptography and Network Security, ACNS'05, LNCS 3531, pp. 442- 455, 2005.

[6] E. Goh. Secure Indexes, http://crypto.stanford.edu/eujin/papers/secureindex/secureindex.pdf, 2003.

[7] D. Song, D. Wagner, and A. Perrig, Practical Techniques for Searches on Encrypted Data. Proc. IEEE Symp. on Security and Privacy, S&P'00, pp. 44-55, 2000.

[8] D. Naor, M. Naor, and J. Lotspiech, Revocation and Tracing Schemes for Stateless Receivers. Proc. Advances in Cryptology, Crypto'01, LNCS 2139, pp. 41-62, 2001.

[9] L. Ballard, S. Kamara, and F. Monrose, Achieving Efficient Conjunctive Keyword Searches over Encrypted Data. Proc. International Conf. on Information and Communications Security, ICICS'05, pp. 414-426, 2005.

[10] P. Golle, J. Staddon, and B. Waters, Secure Conjunctive Keyword Search over Encrypted Data. Proc. Applied Cryptography and Network Security, ACNS'04, pp. 31-45, 2004.

[11] Z. Yang, S. Zhong, and R. N. Wright, Privacy-Preserving Queries on Encrypted Data. Proc. Computer Security, ESORICS, LNCS 4189, pp. 479-495, 2006.

[12] C. Wang, et. al., Secure Ranked Keyword Search over Encrypted Cloud Data . Proc. IEEE International Conf. on Distributed Computing Systems, ICDCS'10, pp. 253-262, 2010.

[13] D. Boneh, G. di Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search. Proc. Eurocrypt'04, pp. 506-522, 2004.

[14] M. Abdalla, et. al., Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Proc. Crypto'05, LNCS 3621, pp. 205-222, 2005.

[15] Y.H. Hwang, and P.J. Lee, Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System. Proc. International Conf. on Pairing-Based Cryptography, Pairing'07, 2007.

[16] J. Katz, A. Sahai, and B. Waters, Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Proc. Advances in Cryptology, EUROCRYPT'08, LNCS 4965, pp. 146-162, 2008.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-Gained Access Control of Encrypted Data. Proc. ACM Conf. on Computer and Communications Security, CCS'06, pp. 89-98. 2006.

[18] E. Shen, E. Shi, and B. Waters, Predicate Privacy in Encryption Systems. Proc. Theory of Cryptography, TCC'09, LNCS 5444, pp. 457-473, 2009.

[19] M. Li, S Yu, N. Cao, and W. Lou, Authorized Private Keyword Search over Encrypted Data in Cloud Computing, Proc. International Conf. on Distributed Computing Systems, ICDCS'11, pp. 383 - 392, 2011.

[20] Y. Yang, F. Bao, X. Ding, and R. H. Deng, Multiuser private queries over encrypted databases. Journal of Applied Cryptography, Vol. 1(4), pp. 309-319, 2009, INDERSCIENCE PUBLISHERS.

[21] D. Boneh, B. Lynn, and H. Shacham, Short Signatures from the Weil Pairing. Proc. Asiacrypt'01, LNCS 2248, pp. 514-532, 2001.

[22] J. Li, et. al., Fuzzy Keyword Search over Encrypted Data in Cloud Computing. Proc. INFOCOM Mini-Conference, 2010.