IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96103

Optimal Matching over Encrypted Data on Public Cloud: A Verifiable Semantic Searching Scheme

Darshan T R[1], Usha M[2]

Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India[1]

Professor, Department of MCA, Bangalore Institute of Technology, Bangalore, India[2]

Abstract -Secure data recovery in the open cloud requires extensive semantic analysis of encoded data. Inconsistent word recovery administration is what it aims to provide, making inquiries and query elements flexible. Because they rely on predetermined watchwords to validate query items from the cloud and because the exact matching is carried out by enlarged semantically terms with specified catchphrases, existing semantic searching plans do not allow verified searching. In this study, we suggest a protected verified semantic searching through conspire. In order to calculate the base word transportation cost (MWTC) as the similarity between queries and archives for semantic ideal matching on ciphertext, we generate word transportation (WT) issues and provide a secure change to transform WT issues into arbitrary direct programming (LP) concerns. In order to design a verification component that uses the transitional information provided in the matching cycle to assess the precision of query items, we research the duality hypothesis of LP. The security analysis demonstrates how our plan may assure Verifiability and discretion. Our plan has a higher precision than other plans, according to the results from two datasets.

I. INTRODUCTION

Distributed computing's inherent adaptability and what makes cloud benefits so well-known is flexibility and tempt cloud users to reevaluate their capacity and calculations in the public cloud. Despite the fact that distributed computing is getting more and more prevalent in business and academia, cloud safety is now one of the key obstacles to its development. The public is becoming more aware of distributed information-breaking computing events like the Apple Fappening and the Uber information breakouts. On a fundamental level, cloud administrations should provide information confidentiality and trustworthiness in accordance with predefined conventions. Regrettably, when cloud server providers assume complete control over information and execute norms, they may lead unethical behaviour in actuality, such as sniffing sensitive data or making incorrect estimates. As a result, before re-appropriating capacity and calculation to the cloud, cloud clients should encrypt their data and set up an outcome verification instrument. Because Song et al. [1] suggested this idea,

The researchers are from Shenzhen Graduate School of Electronics Engineering and Computer Science of Peking University, Shenzhen 518055, Communication and Information Security Laboratory, China. Yuesheng Zhu is the contributing author. About the plot of accessible encryption, accessible encryption has gotten a lot of attention. In any way, standard accessible encryption plans assume certain search terms should a predetermined watchwords within the updated archives, posing a clear hindrance to these plans' similitude estimation based solely on particular matching between inquiry and report catch phrases. As a result, a few works presented semantic looking at plans to give inconsistent words recovery administration, making the query items and inquiry terms flexible and doubtful. In any case, verifiable searching strategies rely on establishing the fixed outcomes of predetermined catchphrases to guarantee the accuracy of the cloud-supplied query item. Along these lines, the difference in semantic and verifiable looking over encoded information is widened by the linguistic adaptability plans also the consistency of verified plans. Contrary to how Fu et al. [2] suggested a verifiable semantic investigation layout that uses long query words to obtain the predetermined watchwords connected with inquiry words, they then used the lengthy catchphrases to search on an image-based file. In any case, their strategy only checks if all of the records containing the lengthy catch are returned to clients and requires customers to rank all of the reports in order to obtain top-k relevant archives. It aims to create a secure semantic looking through idea to support verified looking in this method. The vast majority of today's secure systems for semantic searching use the semantic relationships between words to do plaintext question generation, then carry out precise coordination with specifics using the inquiry words and words that are stretched out to build semantic links. keyword searches in repurposed archives. Secure semantic looking through based equivalent [3], [4], reliable semantic looking through based common data model [5], [6], secure semantic looking by way of thought order [2], [7], [8]. As we can see, these strategies only make use of the most fundamental information about the words' semantics. Equivalent word charts, For instance, just use equivalent word ascribes, while shared data models only employ co-events data. Despite Liu et al[9] .'s findings associate using Word2vec with utilising semantic data from word embeddings, their methodology hurts the semantic data by condensing all the word vectors in a single step. We believe

DOI: 10.17148/IARJSET.2022.96103

that for high hunt precision, secure semantic searching methods should also leverage a a lot of semantic information and do ideal matching on the ciphertext between words. We offer a safe verifiable semantic looking through plot in this research that treats question and report matching as an ideal matching task. The archive words are referred to as "providers," the query words are referred to as "customers," and the semantic data is referred to as "item," with the The base word transportation cost (MWTC) is used to measure how well queries and records match. In order to build the word transportation (WT) problems, we first familiarise word embeddings with record and address words Euclidean distance is used to measure how similar two words are in this way. Nonetheless, Sensitive information may be uncovered by the cloud server in WT scenarios, such as word comparison. We also suggest a protected WT issues are modified to become arbitrary direct programming (LP) problems for ciphertext semantic ideal matching. As a result, Cloud computing can use any ready-made enhancer without needing to discover private information, to address RLP issues and receive encoded MWTC as estimates. We study the dualistic theory of straight programming (LP) and establish a list of fundamental criteria that the middle data displayed in the matching system must meet, given that the cloud server could be utilised to go back incorrect/out-of-date query items. As a result, we can confirm whether the cloud handles RLP concerns correctly, as well as the accuracy of search outcomes. The following summarises our new concepts:

1. By approaching the matching between queries and reports as a perfect complement task, We look into the main direct programming suppositions (LP) to provide a strong verifiable semantic ideal matching on the ciphertext is done using a semantic looking through plot.

2. The "transportation" word (WT) problem is formed present a reliable strategy for converting WT problems into irregular direct programming (LP) issues to obtain estimates of the least expensive word transit between enquiries and data for safe ciphertext semantic ideal matching.

3.We study the LP duality theory, and then give a novel understanding that exploits the midway information produced by the matching system as proof that the query items are accurate to support verifiable looking.

II. RELATED WORK

In the 20 years Accessible encryption has improved because Song et al.[1] .'s peeking over encrypted cloud data proposal gained a lot of attention for its viability. As a result, various efforts have attempted to improve the security and utility of accessible encryption. Many works in the security exploration line figure out definitions of safety along with novel ways to attack current schemes The Gohetal [10] proposed the semantic protection from versatile picked watchword attack (IND-CKA) security model for report files, which demands record lists not to expose objects in archives.Nonethelessnonetheless, the IND-CKA definition not saying that the questions need to be careful. Security definitions for symmetric accessible encryption are improved by Curtmola et al. [11], then offer your chosen watchword attacks and adaptive selected keyword attacks. Furthermore, Islametal. [12] first revealed the entry design leakage, which was exploited to learn sensitive data about the scrambled records, and after that, in view of the, Liu et al. [13] presented a fresh attack hunt design spillage. For the powerful accessible encryption designs that help information expansion and erasure, The forward security and reverse security principles were proposed by Stefanov et al. Along another line of inquiry into utility, numerous works have identified common sense capacities future needs, such as positioned search and semantic search to increase the accuracy of search queries. A few works also proposed verified looking through plans to ensure query item accuracy. Compared to Positioned Encrypted Data Search Positioned searching entails the ability of the cloud server determine the importance scores that range each record and the query, then store the archives without revealing private data. [15] presented the concept of single keyword positioned search, which encoded importance ratings and ranked scrambled archives using a modified one-to-many request safeguarding encryption (OPE). Cao and co, introduced the multikeyword positioned search conspire (MRSE), which deals with paired the solid kNN calculation (SeckNN) [17] and vectors encode using the internal outcome of the scrambled vectors as the similarity metric after the vectors. Additionally, Yu et al. [18] encoded significance ratings and data using homomorphic encryption and comprehend a vector space model search plot with several keywords. Kermanshahi and others. [19] recently proposed a nonexclusive solution for assisting multi-catch positioned and scanning strategies that can defend opposed against a few assaults offered by OPE-based strategies by utilising various homomorphic encryption procedures. Semantic Searching with Confidence. Traditional accessible encryption methods have a general drawback in that they cannot evaluate the value of searches and archives without using semantic information between words. Under the vector space paradigm, The first equivalent accessible encryption scheme was presented by Fu et al to overcome any barrier between words with similar meanings and the specified catchphrases. They used the similar word watchword thesaurus based on Thesaurus, New American Roget's College (NARCT) to first expand the catchword set, and then they used the expanded watchword set to produce secure files with SeckNN. In [5] and [6], reliable semantic looking through based on the shared data model plans using the request safeguarding encryption computation. In light of the common data used in [20], A plan created by Xia et al. [6] calls for the cloud to build a semantic relationship library. Regardless, any plans according to the changed file can compute the shared data model. [2], [7], [8] offered a safe semantic search through plans according to the idea order using the SeckNN computation. Fu et al., for instance, A focal catch semantic augmentation search was created by [8] via plot that identifies a large based on the amount of query terms syntactic relationships, then uses the WordNet idea order tree to expand the main term. Word2vec was developed by Liu et al. [9] to handle both searches and archives as minimal vectors, inspired on word installing used in plaintext data recovery. However, because they directly aggregate all of the word vectors, their practise destroys the semantic content of word embedding.

III. CONCEPT OF THE PROBLEM

The security model, the framework engineering, and the fundamental documentations used in this paper are all defined in this part.

Framework Architecture

The information proprietor, information clients, and the cloud server are the three components of our framework, as evident in Fig. 1. The data's creator is large number of value records, however with few materials available on adjacent devices. As a result, the proprietor is quite eager to use Initialize() to set up the suggested conspiracy. The owner encrypts reports F with secret key K to obtain ciphertext archives C, which he subsequently re- suitable for the cloud server. Files I are worked on by the information owner, who then delivers files I and K to information clients. Information clients are the looking through applicants who submit the hidden entrance asking the cloud server an inquiry for gaining top k reports connected to. Clients input irregular question words q, then use BuildRLP() to construct irregular straight programming issues, irregular word transportation concerns, and the related regular terms as a hidden entry. A short time later, clients get top-k scrambled reports and confirmations I returned from the cloud, A. When passes our verification component, clients call VerDec() to unscramble archives. A transient, specialised cooperative, the cloud server stores and completes the recovery cycle for the scrambled record dataset C. Once getting the hidden entrance, The cloud server runs SeaPro() to address the using any immediate analyzer, after that at that point, acquires the scrambled least values for the term "transportation cost". The top-k scrambled reports are returned to clients after the cloud arranges the characteristics in ascending order. Simultaneously, Likewise, the cloud server gives evidences to prove that the query items are correct.

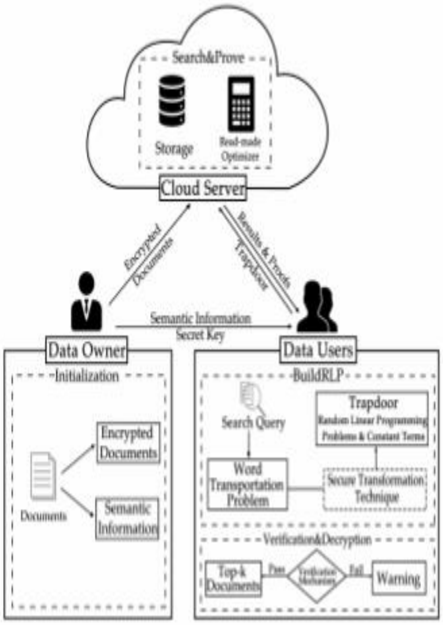


Figure 1. The design of our safe, dependable semantic investigation searching technology.

Assurance Model

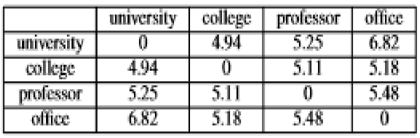
We believe the data owner and users may be trusted have been given authorization from the data owner The channels of communication between the proprietor and users are protected by current security standards like SSL and TLS. In terms of the cloud server, our system can withstand a more difficult security model than the "a mediocre server" utilised in currently available safe semantic search methods [4], [3], [6], [5], [8], [9], [7]. In our concept, the dishonest cloud server tries to produce counterfeit or fraudulent search results and gather private data, but it does not alter or destroy the sourced materials. As a result, under such a security paradigm, our safe A semantic scheme should offer confidentiality and verifiability.

The following list of key notations is used in this paper:

- q: The inquiry that a data user entered.
- d: the dataset's total number of documents.
- m: how many keywords are used in a document.
- n: how many words make up the query.
- F: F represents the plaintext documents dataset, where fi stands for a particular document within F.
- C: Secure documents C = (c1,c2), where ci stands for a record in the C database.
- Ψ: WT issues with the questions and materials,and $\Psi = \{\psi 1,\psi 2 ...\psi i ...\psi d\}$, where ψi indicates a WT issue with the q with fi.
- Ω: RLP issues with the questions and documentation,and $\Omega = \{\omega 1,\omega 2 ... \omega i ...\omega d\}$, where ωi an RLP issue for the q with fi is shown by.
- θ: The RLP problem's two issues ω.
- Δ: Every RLP problem's constant terms, and $\Delta = \{\delta 1,\delta 2 ...\delta i ...\delta d\}$, where δi denotes the RLP problem's constant term ωi.
- Λ: Proofs for each RLP issueand $\Lambda = \{\lambda 1,\lambda 2 ...\lambda i ...\lambda d\}$, where λi serves as evidence for ωi.
- β: The word transportation problem's least expensive solution.
- Π: RLP problem optimal values, and $\Pi = \{\pi 1,\pi 2 ...\pi i ...\pi d\}$, where πi indicates the RLP problem's ideal value ωi.

Table 1

VALUES OF THE EUCLIDEAN DISTANCE BETWEEN WORDS



	university	college	professor	office
university	0	4.94	5.25	6.82
college	4.94	0	5.11	5.18
professor	5.25	5.11	0	5.48
office	6.82	5.18	5.48	0

- Ξ: The measured between q and documents using encrypted minimum word transportation costs, and $\Xi = \{\xi 1,\xi 2,\xi 3 ... \xi i ...\xi d\}$, where ξi represents the distance between q and fi.

IV. PRELIMINARIES

Embedding words

A vector-space word delegate technique is called word installation that protects the major features of words as well as their semantic relationships. to become familiar with word vector representations, brain language models are prepared to restrict the expectation mistake. As a result, we can use word embeddings to examine semantic data between words through mathematical operations. The Euclidean distance values for "college, school, teacher, and office," for example, are simply in accordance with our judgement that the more meaningful the terms are, the more modest the Euclidean distance is, as seen in Table I. Plaintext data recovery projects such as question development, cross-modularity, and zero-shot recovery recovery have focused on word inserting. In this study, word embeddings are used to collect without divulging it to the cloud server, semantic information between words.

Earth Mover

The Earth Mover's Distance (EMD) is presented as a measurement in PC vision to catch the marks transporting disparities across pictures. The name EMD is derived from its intuitive meaning: We see one distribution as the earth's surface expanded out correctly positioned, one as a collection of, and the other apertures in the same location. The outcome is EMD, what is the price to fill the gaps? with earth as a base measure of labour. EMD has been used in a variety of applications, including motion acknowledgment, plaintext recovery, archive categorization, music kind classification, and quality identification, due to its advantages in resolving challenges such as multifeatured markings.

DOI: 10.17148/IARJSET.2022.96103

We can see that EMD is an example of direct programming problems. As a result, we study the key hypotheses of straight programming and security calculations in this work in order to create a strategy for recognising securely matching semantic ideals on the ciphertext.

V. SUGGESTIVE APPROACHES

The proposed main methodologies depicted in Fig. 1, such as the secure transformation method, the word transit issue, and the verification mechanism, are presented in this section. Transportation optimal matching is an example of the term.

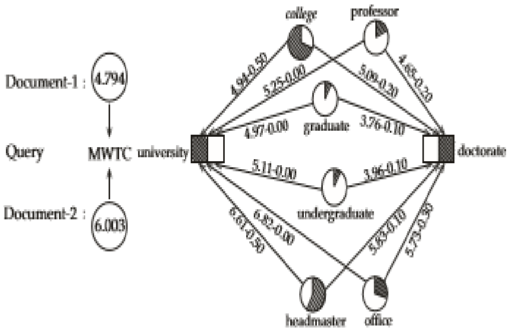


Figure 2. The weight of a word is represented by the relative area of the shadow; The line segment's length displays the the approximate Euclidean separation between two words that are connected; and The line segment's number M-N denotes the amount of transportation involving two words that are linked. In this instance, the MWTC between the document and the query 1 is 4.794, and the MWTC between the query and document 2 is 6.003, indicating that Compared to document 2, document 1, the question is more pertinent.

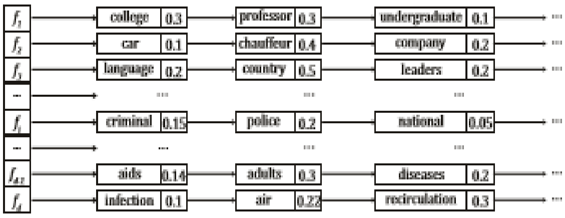


Figure 3. An illustration of a document forward index. Future indices are the datastructure storing the mapping from each document to its keywords. Each keyword in our system is given a normalised weight that represents the relevant score between the term and a particular page.

Problem of Transporting Words for the Best Matching

The way we say "transportation" (WT) problem as a linear programming optimal transportation problem, treating query and document matching as an ideal matching assignment. As shown in Fig 2, To find the lowest possible word transportation cost, we use WT problems (MWTC) in order to compare queries and documents for similarity. We introduce forward indexes as document semantic data. to represent documents in WT issues. Figure 3 illustrates a case study for forward indexing. The keywords distributions for a document are defined as The forward index's weight for each keyword. As a result, we must choose keywords for each page and determine the importance of each keyword in each document. We search for keywords in our system using the TF-IDF (term frequency inverse document frequency) criterion without losing generality. Furthermore, we establish weights utilising (1):

weight(w,f) =1 |fi|·(1 + lnfi,w)·ln1 + d fw, (1)

where w stands for a particular keyword, f expresses a particular document, |fi| represents the document's length, fi,w is The number of documents that contain the phrase w is indicated by the term frequency TF of the keyword w in the f, and d is

DOI: 10.17148/IARJSET.2022.96103

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Figure 4. When m=3, n=2, consider the matrix V as an example. In our word transportation problem, the constraint Vx = W is constructed using the matrix V.

The total the dataset's document count. We define the weights of the query terms to be equal and apply the same method to represent the inquiry.We standardise the each document's or query's weight to 1 in this study. Words used in documents are viewed as "suppliers," words used in queries as "consumers," and semantic data as "product" provided forward documents and query indexes. Therefore, Given the forward index of a document f and the query q, we may state the WT problem as follows.:
WT(f,q) =min
m X i=1
n X j=1
fi,jdi,j
depending on
n X j=1
fi,j = efi , i = 1,2,3 ...,m
m X i=1
fi,j = eqj,j = 1,2,...,n fi,j ≥ 0 m X i=1 n X j=1 fi,j = 1,

Secure Transformation Technique

Because the basic WT problem potentially reveal sensitive information, word transportation concerns cannot be immediately adapted to the secure semantic searching strategy. As a result, we present a method of safe transformation for realising semantically ideal ciphertext matching, ensuring information Transparency and honesty in word transportation situations. Users in our system use our safe a method for transforming WT issues are transformed into random linear programming (RLP) challenges, which the cloud may solve using any ready-made optimizer, and obtain without learning important information the minimum word transmission cost in encrypted form (EMWTC). Every WT problem is encrypted specifically via our secure transformation method. ψ = (c,V,W,I) using a unique secret key KT = (A,Q,γ,R,r), in which A is an mn×mn invertible random matrix, Q is an invertible, (m+n)(m+n) random matrix., γ is a genuine benefit, An mn×1 random vector is r. and R is a generalised permutation matrix of size mn×mn. The original goal function cTx is first converted to the encrypted version cTAy- cTr with x = Ay r. One of the possible solutions to the RLP problem is represented by the symbol y, which stands for a mn×1 decision vector. Keep in mind that we demand that each ri be at least 0, where i=1, 2,..., mn. With x in place of Ay −r, We modify the initial WT issue. ψ to (4). In (4), The constraint condition is defined IAy ≥ Ir is similar to that the i-th a component of the vector T1 = IAy does not fall below the i-th a component of the vector T2 = Ir, where i=1,2,...,mn. min cTAy−cTr depending on VAy = W + VrIAy ≥ Ir.

$$\underset{\mathbf{r}}{\begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \end{pmatrix}} \text{———} \underset{\mathbf{R}}{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{r_5} \\ 0 & 0 & \frac{1}{r_6} & 0 & 0 & 0 \\ 0 & \frac{1}{r_4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{r_2} & 0 \\ \frac{1}{r_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{r_3} & 0 & 0 \end{pmatrix}}$$

Figure 5. An illustration of how the matrix R is generated, if m=3 and n=2,

A crucial component of the secret key KT is the matrix R, It has a non-negativity requirement and is used to conceal sensitive information Ix ≥ 0 in the sense of a transportation issue. The reciprocal of the components in the random vector r are the nonzero elements in R.due to identity matrix I IA = A is confirmed. Consequently, we modify the original WT problem. ψ to (5). In (5), The constraint condition is defined Ay ≥ r tantamount to saying the i-th a component of the vector T3 = Ay does not fall below the i-th portion of the vector r, where i=1,2,...,mn.min γcTAy−γcTr depending on QVAy = Q(W + Vr) Ay ≥ r.

Result Verification Mechanism

We create a result verification system that uses the intermediate data created while doing the matching to verify the truthfulness of search outcomes. Because the best ciphertext matching is a problem with linear programming (LP), To create our verification method, we apply the strong LP problem theorem and expand the duality theory of LP. The dual programming problem for each RLP problem is initially created ω. In light of (7) of ω, To create its dual problem, we use Lagrange multipliers θ, Following is: max g(s,t) depending on V0Ts + I0Tt = c0 t ≥ 0 g(s,t) = W0Ts + LTt

VI. CONCLUSION

We provide a safe, verifiable semantic search approach that views the query-document matching problem as a word transportation optimal matching problem. In order to create the word transportation (WT) issue and a method for outcome verification, We go into the fundamental theorems in linear programming (LP). We provide a safe transformation method for WT problems into LP problems at random by formulating the minimal word transportation cost (MWTC) problem to determine the degree of similarity between searches and documents. The result is, our approach is straightforward to because Without having to become familiar with secret information in the WT problems, any ready-made optimizer can solve the RLP problems and obtain the encrypted MWTC, put this into practise. In the Meanwhile, we think that further privacy-preserving linear programming applications can be implemented using the suggested secure translation technique. By detecting an understanding that uses interim data generated during the best matching procedure to assess the precision of search results, We fill the need for semantic verification in the search. We examine the LP duality theorem and formulate a set of necessary and sufficient requirements for the intermediate data. Our technique has higher accuracy than previous systems, according on testing results on two TREC collections. In the future, we intend to investigate how to develop secure cross-language searching methods using the ideas of secure semantic searching.

VII. REFERENCES

[1] 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.

[2] Z. Fu, J. Shu, X. Sun, and N. Linge, “Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data,” IEEE Trans. Consum. Electron., vol. 60, no. 4, pp. 762–770, 2014.

[3] Z. J. Fu, X. M. Sun, N. Linge, and L. Zhou, “Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query,” IEEE Trans. Consum. Electron., vol. 60, no. 1, pp. 164–172, 2014.

[4] T. S. Moh and K. H. Ho, “Efficient semantic search over encrypted data in cloud computing,” in Proc. IEEE. Int. Conf. High Perform. Comput. Simul., 2014, pp. 382–390.

[5] N. Jadhav, J. Nikam, and S. Bahekar, “Semantic search supporting similarity ranking over encrypted private cloud data,” Int. J. Emerging Eng. Res. Technol., vol. 2, no. 7, pp. 215–219, 2014.

[6] Z. H. Xia, Y. L. Zhu, X. M. Sun, and L. H. Chen, “Secure semantic expansion based search over encrypted cloud data supporting similarity ranking,” J. Cloud Comput., vol. 3, no. 1, pp. 1–11, 2014.

[7] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, “Semantic-aware searching over encrypted data for cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2359–2371, Sep. 2018.

[8] Z. J. Fu, X. L. Wu, Q. Wang, and K. Ren, “Enabling central keywordbased semantic extension search over encrypted outsourced data,” IEEE Trans. Inf. Forensics Security., vol. 12, no. 12, pp. 2986–2997, 2017.

[9] Y. G. Liu and Z. J. Fu, “Secure search service based on word2vec in the public cloud,” Int. J. Comput. Sci. Eng., vol. 18, no. 3, pp. 305–313, 2019.

[10] E. J. Goh, “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, pp. 216–234, 2003.

[11] 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.

[12] M. S. Islam, M. Kuzu, and M. Kantarcioglu, “Access pattern disclosure on searchable encryption: Ramification, attack and mitigation.” in Proc. ISOC Network Distrib. Syst. Secur. Symp., vol. 20, 2012, pp. 12–26

[13] C. Liu, L. H. Zhu, M. Z. Wang, and Y. A. Tan, “Search pattern leakage in searchable encryption: Attacks and new construction,” Inf. Sci., vol. 265, pp. 176–188, 2014.

[14] E. Stefanov, C. Papamanthou, and E. Shi, “Practical dynamic searchable encryption with small leakage.” in Proc. ISOC Network Distrib. Syst. Secur. Symp., vol. 71, 2014, pp. 72–75.

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

DOI: 10.17148/IARJSET.2022.96103

[16] N. Cao, C. Wang, M. Li, K. Ren, and W. J. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, 2013.

[17] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proc. ACM Symp. Int. Conf. Manage. Data, 2009, pp. 139–152.

[18] J. D. Yu, P. Lu, Y. M. Zhu, G. T. Xue, and M. L. Li, "Toward secure multikeyword top-k retrieval over encrypted cloud data," IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 239–250, 2013.

[19] S. K. Kermanshahi, J. K. Liu, R. Steinfeld, and S. Nepal, "Generic multikeyword ranked search on encrypted cloud data," in Proc. Springer Eur. Symp. Res. Comput. Secur., 2019, pp. 322–343.

[20] L. F. Lai, C. C. Wu, P. Y. Lin, and L. T. Huang, "Developing a fuzzy search engine based on fuzzy ontology and semantic search," in Proc. IEEE Int. Conf. Fuzzy Syst., 2011, pp. 2684–2689.