Form 2 : Literature Documents

1. Team No: 12

2. Project Title: A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public Cloud

3. Problem Statement:

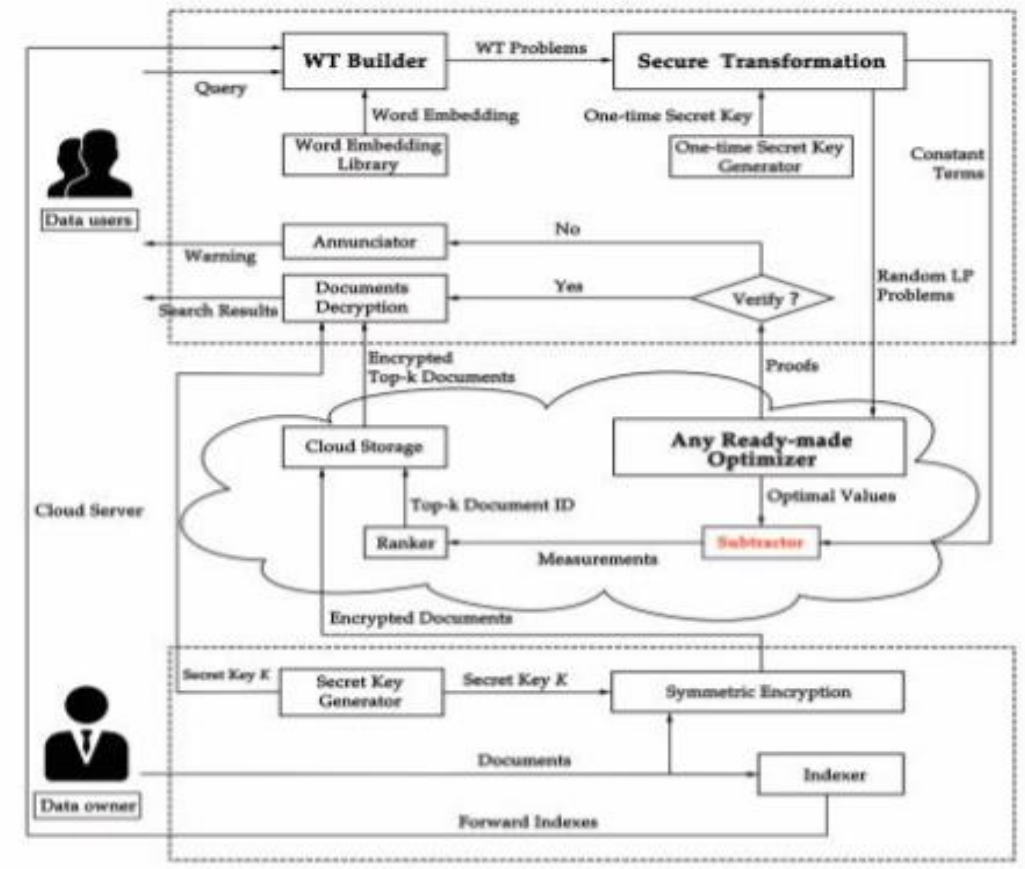
Existing semantic searching schemes lack verifiable searching as they rely on predefined keywords for forecasted results. Queries are expanded on plaintext, limiting accuracy. To address this, we propose a secure verifiable semantic searching scheme. By formulating a word transportation problem, we calculate the minimum word transportation cost (MWTC) for optimal matching on ciphertext. We transform these problems into random linear programming (LP) problems for encryption. Using the LP duality theorem, we design a verification mechanism ensuring correctness. Security analysis confirms confidentiality and verifiability. Experimental results demonstrate improved accuracy compared to existing schemes.

4. Problem illustration:

In traditional semantic searching schemes, reliance on predetermined keywords often leads to inaccuracies in search results. These methods expand queries based on plain text, which can limit precision. To overcome these challenges, we propose a novel secure and verifiable semantic searching scheme. Our approach involves formulating the search problem as a word transportation problem, aiming to minimize the word transportation cost (MWTC) for optimal matching within ciphertext. We then convert these problems into random linear programming (LP) instances for encryption purposes. Leveraging the LP duality theorem, we develop a verification mechanism to ensure the correctness of search results. Our scheme is designed to uphold confidentiality and verifiability. Through rigorous security analysis, we validate the robustness of our approach. Experimental evaluations further demonstrate the enhanced accuracy of our scheme compared to existing methods, showcasing its potential to revolutionize semantic searching by addressing issues of accuracy, security, and verifiability simultaneously.

5. Concept Tree:

At the root of the concept tree lies the main or overarching concept. This concept is then branched out into more specific sub-concepts or sub-categories. Each sub-concept can further branch out into more detailed and specialized concepts, creating a hierarchy that allows for a clear and structured representation of knowledge. Concept trees are commonly used in various fields such as education, knowledge management, information retrieval, and data organization. In education, concept trees are often used to outline the curriculum or learning objectives, with each branch representing a different topic or subtopic that students need to learn. In knowledge management and information retrieval, concept trees are used to categorize and organize information in databases or knowledge bases, making it easier to navigate and retrieve relevant information. One of the key benefits of concept trees is their ability to visually represent complex ideas or knowledge domains in a way that is easy to understand and navigate. They provide a framework for organizing information and exploring relationships between different concepts, facilitating learning, information retrieval, and knowledge discovery.



6. Comparison of Existing Strategies for Problem Solve

Sl.No	Strategies	Advantages	Disadvantages
1.	Keyword-Based Encryption	Simple Easy to Implement, Fast retrieval of encrypted data based on Keyword matching.	Limited Security, Lack of semantic understanding.
2.	Semantic Hashing	Improved Accuracy, Robust encryption scheme compared to simple keyword-based approaches	Higher computational overhead, Challenges in maintaining semantic relevance over time
3.	Homomorphic Encryption	Allows for computations to be performed on encrypted data without decryption, Supports complex operations	Resource intensive computations, Limited support for computations
4.	Secure Multiparty Computation	Enables collaborative computation on encrypted data, Offers strong privacy guarantees and verifiability.	Complex implementation and coordination among multiple parties.

7.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.

Signature Team Members

1. K JASHWANTH ROY(20EG105624)

2. M VAMSHI KRISHNA (20EG105629)

3. M SUSHMITHA(20EG105723)

Signature Supervisor

Dr. C. DASTAGIRIAH