Form 1: Project Information Form

1. Team No: 12

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

3. Team Details:

S. No	Hall Ticket No	Name
1	20EG105624	KARNATI JASHWANTH ROY
2	20EG105629	M VAMSHI KRISHNA
3	20EG105723	MADHIRAJU SUSHMITHA

4. 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.

5. Source of Project:

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.

6. Final Outcome:

Proposed a secure verifiable semantic searching scheme employing word transportation (WT) problem to calculate similarity on ciphertext. Transformed WT into random linear programming (LP) for encrypted MWTC. Utilized LP duality theorem for verifiability. Demonstrated scheme's higher accuracy and security through analysis and experimentation on two datasets.

7. What are the parameters considered for project evaluation?

In evaluating the proposed secure verifiable semantic searching scheme, key parameters include accuracy, efficiency, security, and scalability. Accuracy assesses the precision of search results compared to existing schemes. Efficiency measures the computational overhead introduced by encryption and verification mechanisms. Security analysis evaluates the scheme's resilience against various attacks and data breaches. Scalability examines the scheme's ability to handle increasing data volumes and user demands without compromising performance. Experimental results on real-world datasets provide empirical evidence of the scheme's effectiveness in meeting these parameters.

8. Development Environment:

Database Server	: MySQL
Server	: Apache Tomcat
Platform	: Java
Cloud	: DriveHQ

Signature Team Members **Signature Supervisor**