**Advancements in Query Optimization Using Privacy-Preserving Machine Learning Models**

**Abstract**

The increasing reliance on data-driven decision-making across various industries highlights the need for efficient query optimization in database systems, particularly in privacy-sensitive domains such as healthcare. Integrating machine learning (ML) with privacy-preserving cryptographic technologies offers a transformative approach to secure and optimize query execution. This study explores the design of an advanced query optimization ML model leveraging technologies like homomorphic encryption (HE), proxy re-encryption (PRE), and differential privacy. These innovations enable secure query optimization while maintaining the confidentiality of sensitive data. Future research directions include scalable HE algorithms, lightweight cryptographic solutions, and the integration of decentralized frameworks such as blockchain for enhanced security and trust.

**Index Terms**

Query Optimization [1], Privacy-Preserving Machine Learning [2], Homomorphic Encryption (HE) [3], Proxy Re-Encryption (PRE) [4], Differential Privacy [5], Encrypted Data Processing [6], Blockchain in Databases [7], Federated Learning [8], Secure Query Execution [9], Cryptographic Algorithms [10], AI-Driven Optimization [11], Privacy-Sensitive Environments [12].

**Introduction**

With the rapid growth of data-intensive applications, query optimization has become a critical area in database management. In privacy-sensitive domains, such as healthcare, optimizing queries on encrypted data while preserving security is particularly challenging. Traditional approaches often require data decryption for processing, which risks exposing sensitive information. Privacy-preserving cryptographic technologies combined with ML offer the potential to address these challenges by enabling secure, efficient, and intelligent query optimization. This paper proposes an innovative ML model that incorporates cryptographic methods to optimize queries without compromising data privacy.

**Overview of Cryptographic Technologies in Query Optimization**

Cryptographic methods such as symmetric and asymmetric encryption, HE, and PRE have demonstrated their ability to secure data during storage and transmission. These technologies can be adapted to ML-based query optimization models in the following ways:

1. Homomorphic Encryption (HE): Allows computations to be performed directly on encrypted data, ensuring that sensitive information remains secure throughout the optimization process.
2. Proxy Re-Encryption (PRE): Facilitates secure sharing of query results between parties by re-encrypting data without exposing original encryption keys.
3. Blockchain: Provides a decentralized and tamper-proof framework for query logs, ensuring transparency and trust.

**Problem Statement**

Current query optimization models face significant limitations in privacy-sensitive contexts. Traditional systems often rely on plaintext data for optimization, which creates security vulnerabilities. Key challenges include:

1. Data Confidentiality: Ensuring sensitive data remains secure during query optimization.
2. Interoperability: Enabling seamless optimization across disparate systems without compromising privacy.
3. Computational Overhead: Managing the complexity of cryptographic methods within ML models.

**Research Gap**

While cryptographic technologies address data security, there is a lack of ML models that effectively integrate these methods for query optimization. Existing systems struggle to balance computational efficiency with privacy preservation. This research aims to bridge this gap by developing an ML-driven query optimization model that operates securely on encrypted data.

**Proposed Model**

The proposed ML model leverages advanced cryptographic methods and AI techniques to optimize queries in a secure manner. Key components include:

1. Encrypted Query Representation: Queries are represented as encrypted vectors using, HE, allowing the ML model to analyze and optimize them without decryption.
2. Secure Feature Extraction: Differential privacy techniques are used to extract query features while ensuring data confidentiality.
3. Decentralized Optimization Framework: Blockchain technology ensures that query optimization processes are transparent and tamper-proof.

**Results and Analysis**