Optimizing Cryptographic Technique using Meta-Heuristic based Class Topper Optimization Algorithm

Rambilas Ganguly; Debasis Acharya; Aliva Mandal; Arya Sundar Das; Yubraj Shaw; Brainware University, Barasat, Kolkata-125, West Bengal, India

Abstract

This paper proposes a novel approach for optimizing cryptographic techniques using a metaheuristic algorithm to enhance data privacy, security, and integrity. Given the sensitivity of data, advanced encryption methods like encrypted communication, hashing, and secure access control are essential. While hashing and access control ensure integrity, homomorphic encryption allows computations on ciphertext, improving confidentiality without decryption. To address limitations in existing methods, this work integrates the Class Topper Optimizer (CTO) with cryptography to develop an intelligent, privacy-preserving system. A cryptographic problem is model using student data (e.g., grades, behaviour) to support evidence-based academic interventions. The goal is to enable data-driven decision-making while preserving trust and privacy, and the approach is applicable to other data-driven domains.

To address the shortcomings of existing methods, an intelligent cryptographic technique optimized with a metaheuristic algorithm is proposed. The Class Topper Optimizer is integrated into cryptography to develop a privacy-preserving system. For analysis, a cryptographic problem is modeled using student data (e.g., grades, behavior) to guide evidence-based academic interventions. The goal is to support data-driven decisions while safeguarding student trust. This method is adaptable to other data-driven systems as well.

Keywords

Optimization algorithm, Time dial setting (TDS), Plug setting 27 (PS), Coordination Time Interval (CTI), Fitness, Genetic algorithm

1. Introduction

In the modern digital era, securing data against unauthorized access and cyber threats is of paramount importance. Cryptographic techniques form the backbone of secure communication systems, ensuring data confidentiality, integrity, and authentication. However, traditional cryptographic algorithms often face challenges such as computational overhead and susceptibility to advanced attacks. This necessitates the