ADVANCED STRATEGIES FOR PRIVACY PRESERVING OF ASSOCIATION RULE MINING: OPTIMIZATION IN SECURED WIRELESS COMMUNICATION

ABSTRACT

Today, privacy-protected data mining is a crucial study area that extracts essential information from databases while concealing sensitive data.Data transformation is used in the Association Rule Hiding (ARH) process to secure sensitive information. There are several algorithms offered for hiding sensitive data. In order to promote data privacy during wireless communication in cloud, privacy-preserving association rules mining techniques have recently been developed.

In Stage 1 we offer a correlation rule mining-approach that preserves user confidentiality while mining encrypted data for wireless data transmission in cloud-based settings. We suggest using the Coupled Animal Fish Migration Optimization (CAFMO) and Enhanced Genetic Algorithm (EGA) to provide both query privacy and data privacy while hiding data frequency. With regard to the usefulness and privacy of the assessment metrics, the performance of the suggested approach is compared to that of the existing methods. When compared to the current technique, the experimental results demonstrate that the proposed method mines the privacy protected association rules from the database with the highest privacy of 0.99 and the least utility of 0.0994. We demonstrate that the recommended approach outperforms the existing one by approximately 3– 5 periods in terms of association rule mining efficiency.

In Stage 2, we provide an association rule mining technique that preserves user privacy while mining encrypted data via Advanced Encryption Standard (AES) in the cloud. We suggest using intelligent craving honey bee optimization (ICHBO), which assures no data or information challenges and no unintentional effects on the information's usefulness. ICHBO offers confidentiality throughout data collection and interaction. Data owners that encrypt their data and distribute it to clouds using a Data Share Allocator (DAS) technique are included in the suggested framework model. We assign our procedures to the test in large-scale tests to get approval for their display.The evaluation results revealed the mined data obtained using our systems are trustworthy compared to other existing techniques. According to the results of our performance evaluation, our approach is very effective and has a responsibly higher security level and convergence speed.

In Stage 3, we suggest Genetic Algorithm-Tuned Remora Optimization (GAT-RO) for privacy preservation in wireless communication. The proposed methodology contains two distinct phases: the production of a secret key and the process of rule mining. The initial step in the mining process is the application of the Horse Herd Optimization (HHO) approach to extract the association rule mining from the input data. The algorithm GAT-RO is developed by incorporating the Genetic Algorithm (GA) with the Remora Optimization (RO) technique, which generates a secret key for enhancing privacy. The algorithm then uses six

factors privacy, Rate accuracy preservation, level of change, and failure rate of concealment, and rate of false rules generation, utility in its objective function to select a secret key that the sanitized database can use to hide sensitive information. The testing was carried out using MATLAB. The findings demonstrate that the GAT-RO approach achieves privacy of (0.2), a degree of alteration of 1.4, a rate of concealment failure of 0.028, and a rate of information preservation of 0.099, a utility of (0.98), and a rate of false rules generation (0.92) for T10I4D100k dataset. Our suggested GAT-RO technique provides exciting outcomes for privacy in wireless communication.