Abstract

Differential Privacy is proposed to provide a solution to the problem of data security that can ensure that data utility and data privacy can be maintained and controlled properly. Differential Privacy is growing rapidly and is considered a promising method and has been used by various parties such as Apple and Google in their security systems. In this study, an experimental test was conducted on the aggregate query 'count' to study the performance of one of the differential privacy mechanisms, namely Exponential Mechanism on the Student's Alcohol Consumptions dataset. The Student's Alcohol Consumptions dataset is relevant to previous research. Where this dataset contains sensitive information related to high school students' alcohol consumption so that their privacy must be maintained. Furthermore, the optimal value of ε (epsilon) is determined by testing the relative error value on the use of the value of ε (epsilon) and analyzing its effect on the privacy tradeoff. The experimental study conducted shows that the value of $\varepsilon = 10$ in the Student's Alcohol Consumptions dataset maintains the privacy tradeoff well (with an average error in each category = 22%) so that the dataset meets ε -differential privacy.

Keywords: Differential Privacy, Exponential Mechanism, Privacy Tradeoff