Abstract

Privacy preserving is utmost important in medical applications. Cryptography has numerous techniques to safeguard the privacy of the data. It is practice to use private key for encryption and public key for decryption in the area of cryptography. Conventionally, without decryption, data usability is difficult. However, the complications outweigh the private and public keys. This paper presents privacy preserving model based on Homomorphic encryption technique and model evaluation using classification technique. The homomorphic model highlights usability of the data without decryption. The objective of this paper is to show how the encrypted data is preserving underlying relations through classification tree. This paper presents two parts: Part-I describes the model building on medical data using PSO optimization and filter based co-efficient matrix (for encryption) to protect privacy of the data and part-II describes model evaluation using classification tree and clustering technique. The performance of the encryption is tested using predictive modelling technique (classification tree technique) and K-Means clustering technique, to assess whether the underlying relations are preserved in the encrypted data. The experimental results show that the underlying classification accuracy of encrypted
Privacy Preserving Model using Homomorphic Encryption

data and source data (non-encrypted) is just varying by +/- 5%.

References

2. Craig Stuntz (2010-03-18). "What is Homomorphic Encryption, and Why Should I Care?"


24. A Survey on Homomorphic Encryption Schemes: Theory and ImplementationABBAS ACAR, HIDAYET AKSU, and A. SELCUK ULUAGAC, Florida International University MAURO CONTI, University of Padua,


**Index Terms**

Computer Science Security

**Keywords**
Homomorphic Encryption, Predictive Modeling, Privacy Preserving Data Mining.