Abstract

Networked data contain interconnected entities for which inferences are to be made. For example, web pages are interconnected by hyperlinks, research papers are associated by references, phone accounts are linked by calls, and conceivable terrorists are linked by communications. Networks have turned out to be ubiquitous. Correspondence networks, financial transaction networks, networks portraying physical systems, and social networks are all ending up noticeably progressively important in our everyday life. Regularly, we are interested in models of how nodes in the system influence each other (for example, who taints whom in an epidemiological system), models for predicting an attribute of intrigue in light of observed attributes of objects in the system. The technique of SVM is applied which will classify the data into malicious and non-malicious. In the previous study authors proposed various model for privacy preserving which are group based records, K-anonymity etc. In the existing models there are various problems like it affect data utilities, harm the data identifiers. In the research work, the hybrid approach has been designed to ensure data privacy which is based on attribute and data identifiers.
References


Index Terms

Computer Science Security
Keywords

VoIP, SVM, KNN, Intrusions.