**Abstract**

Passwords are a vital component of system security. Though there are many alternatives to passwords for access control, password is the more compellingly authenticating the identity in many applications. They provide a simple, direct means of protecting a system and they represent the identity of an individual for a system. The big vulnerability of passwords lies in their nature. Users are consistently told that a strong password is essential these days to protect private data as there are so many ways for an unauthorized person with little technical knowledge or skill to learn the passwords of legitimate users. Thus it is important for organizations to recognize the vulnerabilities to which passwords are subjected, and develop strong policies governing the creation and use of passwords to ensure that those vulnerabilities are not exploited. In this work password strength prediction is modeled as classification task and supervised machine learning techniques were employed. Widely used supervised machine learning techniques namely C 4.5 decision tree classifier, multilayer perceptron, naive Bayes classifier and support vector machine were used for learning the model. The results of the models were compared and observed that SVM performs well. The results of the models were also compared with the existing password strength checking tools. The findings show that machine learning approach has substantial capability to classify the extreme cases - Strong and weak passwords.