**Abstract**

Passwords are ubiquitous authentication methods and they represent the identity of an individual for a system. Users are consistently told that a strong password is essential these days to protect private data. Despite the existence of more secure methods of authenticating users, including smart cards and biometrics, password authentication continues to be the most common means in use. 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. This work employs machine Learning technique to analyze the strength of the password to facilitate organizations launch a multi-faceted defense against password breach and provide a highly secure environment. A supervised learning algorithm namely Support Vector Machine is used for classification of password. The linear and nonlinear SVM classification models are trained using the features extracted from the password dataset. The trained model shows the prediction accuracy of about 98% for 10-fold cross validation