**ABSTRACT**

Intrusion finding faces the variety of challenges; intrusion detection system should faithfully detect malicious activities on a network and should perform expeditiously to address the big quantity of network traffic. During project, two problems of Accuracy and efficiency achieved through potency victimization Conditional Random Fields and superimposed Approach. Tend to demonstrate that top attack detection accuracy may be achieved by victimization Conditional Random Fields and high potency by implementing the superimposed Approach. The results on the KDD intrusion information set show that the projected system supported superimposed Conditional Random Fields outperforms different well-known strategies like the decision trees and therefore the naive mathematician. The development in attack detection accuracy is incredibly high, notably, for the U2R attacks and the R2L attacks applied mathematics Tests conjointly demonstrate higher confidence in detection accuracy for our technique. Finally, it is shown that proposed system is powerful and is in a position to handle clattering information while not compromising performance.