Due to the rapid growth in the Information and Communication Technology (ICT) infrastructures, application and services, both corporate and individuals including government now depend on cyber space for almost every day- to day activity. This development has brought about the disappearance of network boundary between computers on the internet, thereby making the security of Confidentiality, Integrity and Availability (CIA) of individual's information a great concern. Intrusion Detection System (IDS) has emerged as an important component of secure network as it filters and monitors the network traffic for any anomaly or misused connection. Machine learning technique has been useful in the area of intrusion detection due to their model free properties, which makes them to learn the network pattern and identifies them as either normal or malicious (attack). However, IDS suffers some performance challenges such as low detection and high false alarm rates. The focus of this research work is to develop a novel ensemble based model by integrating Multilayer Perceptron Neural Network (MPNN) and Sequential Minimal Optimization (SMO) classifiers to enhance the performance of IDS. Kyoto 2006+ intrusion detection dataset is used to evaluate the performance of the model. The results show that the ensemble of MPNN+SMO classifier outperformed ensemble of Random Forest (RF) and Average One Dependency Estimator (AODE) in terms accuracy, detection rate, false alarm rate, and Hubert index measurement. It is concluded that combination of multiple classifiers requires serious consideration so that the weak algorithm will not weigh down the performance of the model.