# ABSTRACT

Currently the implementation of Good Corporate Governance (GCG) in organizational commitment is the key to success in achieving effective, efficient and sustainable business performance. One implementation of GCG is a fraud management through a fraud detection.

In previous research, fraud detection performed on voice services with data sources Call Detail Record. Discussion of this research focuses on fraud in the data and Internet services that have not been done in previous studies. Fraud on data services and internet is done through the misuse of network configuration / IT by employees. The data used is based on the activity log of the administrator who is responsible for running the configuration. Fraud can not be solved with the usual query, so that the necessary process to form a pattern of data which is then processed through data mining. Research requires the development of data models that suit the needs of fraud detection.

This study includes several data preparation stages: data collection, data selection, data integration, data cleansing, data transformation, identifying significant components, handling imbalance data, and classification process. Identification of significant components using Principal Component Analysis. The data used has imbalance proportions. Imbalance data are handled with Synthetic Minority Over-sampling Technique. The classification method used is the supervised classification which is Naive Bayes classifier that assumes that there are no dependencies between attributes. The process of Principal Component Analysis showed that the significant attributes, namely: indication, sid, access_device, username, services, and timestamp. Naïve Bayes classifier perform simulations with 48.361 data and get good results with an accuracy of more than 91%.

**Keywords:** data mining, fraud detection, principal component analysis, classification algorithm, Naive Bayes classifier.