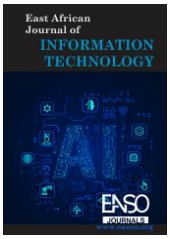


East African Journal of Information Technology
eajit.eanso.org
Volume 5, Issue 1, 2022
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm

Sharifa R. Mambo[1*] *& Christopher A. Moturi*[1]

[1] University of Nairobi P. O. Box 30197, GPO, Nairobi, Kenya
* Correspondence ORCID ID: https://orcid.org/0000-0003-4913-8767; email: sherigga@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Date Published: *23 December 2022*

Keywords: *Healthcare, Health Insurance Claim, Fraud, Naïve Bayes Classification, Data Mining*

ABSTRACT

The extent, possibility, and complexity of the healthcare industry have attracted widespread fraud that has contributed to rising healthcare costs hence affecting patients' health and negatively impacting the economy of many countries. Despite putting up various technologies and strategies to fight fraud such as planned, targeted audits, random audits, whistle-blowing, and biometric systems, fraud in claims has continued to be a challenge in most of the health insurance providers in Kenya. This paper explored the application of data mining in detecting fraud in health insurance claims in Kenya. Classification algorithms (Naïve Bayes, Decision Tree and K-Nearest Neighbour) were used to build predictive models for the knowledge discovery process. After conducting several experiments, the resulting models showed that the Naïve Bayes works well in detecting fraud in claims with 91.790% classification accuracy and 74.12% testing hit rate. A prototype was developed based on the rules extracted from the Naïve Bayes model, which, if adopted, will save costs by detecting fraud as it is committed. Fraud detection in health insurance claims is much needed in many countries so as to help reduce loss of money and in return improve service delivery to patients.

APA CITATION

Mambo, S. R. & Moturi, C. A. (2022). Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm. *East African Journal of Information Technology*, *5*(1), 244-255. https://doi.org/10.37284/eajit.5.1.1023

CHICAGO CITATION

Mambo, Sharifa R. and Christopher A. Moturi. 2022. "Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm". *East African Journal of Information Technology* 5 (1), 244-255. https://doi.org/10.37284/eajit.5.1.1023.

HARVARD CITATION

Mambo, S. R. & Moturi, C. A. (2022) "Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm", *East African Journal of Information Technology*, 5(1), pp. 244-255. doi: 10.37284/eajit.5.1.1023.

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

IEEE CITATION

S. R. Mambo & C. A. Moturi "Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm", *EAJIT*, vol. 5, no. 1, pp. 244-255, Dec. 2022.

MLA CITATION

Mambo, Sharifa R. & Christopher A. Moturi. "Towards Better Detection of Fraud in Health Insurance Claims in Kenya: Use of Naïve Bayes Classification Algorithm". *East African Journal of Education Studies*, Vol. 5, no. 1, Dec. 2022, pp. 244-255, doi:10.37284/eajit.5.1.1023.

INTRODUCTION

Healthcare insurance fraud is a serious problem globally. Frauds in health care systems have not only led to additional expenses but also degradation of the quality and care provided to patients (Verma, Taneja & Arora, 2017). A high number of claims are often submitted on a daily basis hence making a review of individual claims a very difficult task (van Capelleveen et al., 2016). The Health Insurance Fraud Survey Report for 2013 by the Association of Kenya Insurers (AKI, 2013) estimates that 143 cases of medical insurance fraudulent claims were reported and out of the US$ 2.53 million lost, only 2% of the amount was recovered. Similarly, the American National Health Care Anti-Fraud Association reports that in 2017, 91.6 million health claims were processed some of these health insurance claims are fraudulent with a very high price tag running into tens of billions of dollars each year (NHCAA, 2019).

To make the health insurance industry free from fraud, it is necessary to focus on the elimination or minimisation of fraudulent claims. Rashidian, Joudaki, and Vian (2012) found that there is a lack of evidence of the effect of the interventions to combat healthcare fraud; however, this paper investigated the potential of data mining to alleviate the problem. Data mining is the process of extracting hidden information from a massive dataset and categorising valid and unique patterns in data. Data mining has been applied to detect fraudulent claims in the health insurance system (Kirlidog & Asuk, 2012; Joudaki et al., 2015; Phua et al., 2010; Koh & Tan (2011). There is a need to leverage data mining to detect fraud, abuse, waste, and errors in health insurance claims in order to reduce recurrent losses and enhance patient care. This paper sought to use a supervised data mining technique to help in detecting fraud in health insurance claims in Kenya.

HEALTH INSURANCE FRAUDS

Fraud in health insurance is done by intentional deception or misrepresentation by malicious insurers and individuals to gain the financial benefit at the expense of the deserved patient or family as well as the government. The most common types of fraud include billing for services not rendered, aberrant billing, improper coding, performing medically unnecessary procedures, misrepresenting non-covered services as covered, and false claims. Fraud affects the insurers, policyholders, insurance customers, and beneficiaries in terms of the increased cost of accessing insurance and quality of services offered. Barasa et al. (2018) found that, although well-intentioned reforms have been undertaken by the National Hospital Insurance Fund (NHIF), Kenya's national and largest insurance provider, weak accountability mechanisms have led to an increase in cases of fraud by the NHIF and health care providers.

To detect and combat healthcare fraud, a broad range of fraud detection tools have been used. They include but are not limited to fraud reporting hotline, email, written leads, information on sharing, internet and media searches, in-house as well as field investigations, and data mining and other software applications (NHCAA, 2019). Employment of fraud awareness, education, and training is crucial as preventive measures.

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Use of Data Mining in Health Insurance Fraud Detection

Data mining tools and techniques can be used to detect fraud and abuse in large sets of insurance claim data. The anomaly detection technique calculates the likelihood or probability of each record being fraudulent by analysing past insurance claims (Kirlidog & Asuk, 2012). The cases that are marked by data mining tools as fraudulent can be subjected to further investigation. Koh & Tan (2011) explored the application of data mining in key areas of healthcare that include the evaluation of treatment effectiveness, management of healthcare, customer relationship management, and the detection of fraud and abuse. Joudaki et al. (2015) found that most studies have focused on algorithmic data mining without emphasis on or application to fraud detection efforts in the context of health service provision or health insurance policy. They recommend seven general steps to data mining of health care claims.

Van Capelleveen et al. (2016) showed that outlier detection could be utilised in automatic detection systems as it may identify new patterns of potential healthcare fraud. Bauder and Khoshgoftaar (2018a) proposed a machine-learning approach for Medicare fraud detection using publicly available data and labels of claims for known fraudulent medical providers. They successfully demonstrated the efficiency of employing machine learning with random under-sampling to detect Medicare fraud. The results showed that the C4.5 decision tree and logistic regression learners have the best fraud detection performance, particularly for the 80:20 class distribution with average AUC scores of 0.883 and 0.882, respectively, and low false negative rates.

Verma, Taneja and Arora (2017) applied Statistical Decision rules, k-means clustering on period-based claim anomalies outliers detection, and rule-based association mining with Gaussian distribution on disease-based anomalies outlier detection. Hasheminejad and Salimi (2018) proposed a novel sliding time and scores window-based method called FDiBC (Fraud Detection in Bank Club), which, when given the scores of a customer, can detect fraud in a bank club. The results obtained show that FDiBC has the ability to detect fraud with 78% accuracy, which is good enough for use.

With the proliferation of data mining techniques and the continued availability of public healthcare data, the application of these techniques towards fraud detection has the potential to reduce healthcare costs greatly (Bauder & Khoshgoftaar, 2018b). Data mining applications can therefore, greatly benefit all stakeholders in the healthcare industry.

Classification of Data Mining Techniques

The most common and well-accepted classifications of data mining used by machine learning experts divide data mining methods into ‘supervised’ and ‘unsupervised’ methods (Phua et al., 2010). Supervised data mining methods are usually used for classification and prediction objectives including traditional statistical methods such as regression analysis, discriminant analysis, neural networks, Bayesian networks and Support Vector Machine (SVM). Supervised methods require confidence in the correct categorisation of the records (Rashidian, Joudaki &Vian, 2012). Examples of the supervised methods that have been applied to healthcare fraud and abuse detection include decision trees (Shin et al., 2012), neural networks, genetic algorithms and Support Vector Machines (Kirlidog & Asuk, 2012).

RESEARCH METHODOLOGY

Research Design

This study used quantitative experimental research. A prototype system was developed to quantify the results. The data used for this research was obtained from the Centers for Medicare & Medicaid Services, a website that publicly releases physician Medicare claims data and outlines the costs and

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

services provided to Medicare patients. The dataset covered claims for the period 2008 to 2010. The data was obtained in Excel file format and converted to WEKA readable format, the format that is acceptable prior to present any classification model. The WEKA workbench (Holmes, Donkin & Witten, 1994) contains a collection of visualisation tools and algorithms for data analysis and predictive modelling together with graphical user interfaces for easy access. Different algorithms are supported by WEKA: classification, regression, decision trees and clustering. This tool allows users to quickly try out and compare different machine learning methods on new data sets. The CRISP-DM (Cross-Industry Standard Process for Data Mining) methodology was used to analyse the data.

Data Selection and Filtering

The original claims dataset was classified into different groups, i.e., approved, denied, cancelled, and in litigation. The 'approved' and 'denied' claims were selected on the assumption that the approved claims were thought to be non-fraudulent and the denied claims were thought to be fraudulent. The data was then filtered for selecting claims with only complete and useful data. WEKA and Excel were applied to remove repeating claims, claims with zero amount and claims with missing columns.

Model Classification Training and Testing

The training of the models for the experimentation was done by employing the 10-fold cross-validation and the percentage split (66%) classification models. The classification was analysed to measure the accuracy of the classifiers in categorising the claims into specified classes. A confusion matrix was used to test the correctness of the model's classification.

RESULTS AND DISCUSSION

Analysis of data was done through 6 experiments whose results are shown in the tables below.

Experiment I: J48 10 Folds Using Default Values

Table 1: Confusion matrix for J48 10 folds using default values

	True No	True Yes	Class Precision
Pred No	13987	1941	59.3%
Pred Yes	2254	2812	80.1%
Class recall	87.8%	53.5%	
Accuracy	76.5547%		
Classification error	1.325%		

From the confusion matrix of experiment 1, the J48 Decision tree algorithm recorded an accuracy of 76.554%. The classifier classified 15987 normal claims correctly, while 2254 claims were misclassified as claims with the anomaly. Out of 4753 claims found with anomaly 1941 claims were misclassified as normal customers, thus giving a class recall of 53.5%. The probability of misclassification is approximately 1.325% as given by classification error. The class precision is 59.3% for the prediction 'No' and 80.1% for the prediction 'Yes'.

Experiment II: J48 with 66% Percentage Splits

Table 2: Confusion matrix for J48 10 with 66% percentage split

	True No	True Yes	Class Precision
Pred No	5702	761	60.4%
Pred Yes	1007	894	79.4%
Class recall	78.8%	53.5%	
Accuracy	76.4921%		
Classification error	1.302%		

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

From the confusion matrix of experiment 2, the J48 Decision tree recorded an accuracy of 76.4921%. The classifier classified 5702 normal claims correctly, while 1007 claims were misclassified as claims with the anomaly. Out of 1655 claims found with an anomaly, 761 claims were misclassified as normal customers, thus giving a class recall of 53.5%. The probability of misclassification is approximately 1.320% as given by classification error. The class precision is 60.4% for the prediction 'No' and 79.4% for the prediction 'Yes'.

Experiment III: Naïve Bayes 10 folds

Table 3: Confusion matrix for Naïve Bayes 10 folds

	True No	True Yes	Class Precision
Pred No	16159	1756	75.8%
Pred Yes	180	5488	98.9%
Class recall	90.2%	96.8%	
Accuracy	91.7907%		
Classification error	1.089%		

From the confusion matrix of the above experiment, Naïve Bayes simple algorithm recorded an accuracy of 91.790%. The classifier classified 16159 normal claims correctly, while 180 claims were misclassified as claims with an anomaly. Out of 8018 claims found with anomaly 1756 claims were misclassified as normal customers, thus giving a class recall of 96.8%. The probability of misclassification is approximately 1.089% as given by classification error. The class precision is 75.8% for the prediction 'No' and 98.9% for the prediction 'Yes'.

Experiment IV: Naïve Bayes with 66% Percentage Split

Table 4: Confusion matrix for Naïve Bayes with 66% percentage split

	True No	True Yes	Class Precision
Pred No	5549	579	75.9%
Pred Yes	70	1820	98.8%
Class recall	90.6%	96.3%	
Accuracy	91.9057%		
Classification error	1.107%		

From the confusion matrix of the experiment above, the Naïve Bayes classifier recorded an accuracy of 91.9057%. The classifier classified 5549 approved claims correctly, while 70 claims were misclassified as claims with the anomaly. Out of 2399 claims found with an anomaly, 579 claims were misclassified as normal claims, thus giving a class recall of 96.3%. The the probability of misclassification is approximately 1.107% as given by classification error. The class precision is 75.9% for the prediction 'No' and 98.8% for the prediction 'Yes.'

Experiment V: K-Nearest 10 Folds

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Table 5: Confusion matrix for K-Nearest 10 folds

	True No	True Yes	Class Precision
Pred No	16037	1878	54.0%
Pred Yes	2605	3063	86.0%
Class recall	89.5%	54.0%	
Accuracy	80.9905%		
Classification error	2.25%		

From the confusion matrix of experiment 5, the K-Nearest Neighbor classifier scored an accuracy of 80.9905%. The classifier classified 16037 approved claims correctly, while 2605 claims were misclassified as claims with an anomaly. Out of 2399 claims found with anomaly 1878 claims were misclassified as normal claims, thus giving a class recall of 54.0%. The the probability of misclassification is approximately 2.254% as given by classification error. The class precision is 54.0% for the prediction 'No' and 86.0% for the prediction 'Yes.'

Experiment VI: K-Nearest with 66% percentage split

Table 6: Confusion matrix for K-Nearest with 66% percentage split

	True No	True Yes	Class Precision
Pred No	5524	604	61.7%
Pred Yes	915	975	85.8%
Class recall	90.1%	51.6%	
Accuracy	81.651%		
Classification error	2.254%		

The results above denote that the K-Nearest Neighbor classifier got81.651%best accuracy score. The classifier classified 5524 approved claims correctly, while 915 claims were misclassified as claims with an anomaly. Out of 1579 claims found with anomaly995 claims were misclassified as normal claims, thus giving a class recall of 51.6%. The the probability of misclassification is approximately 2.254% as given by classification error. The class precision is 61.7% for the prediction 'No' and 85.8% for the prediction 'Yes'.

Comparison of the Classification Models

Table 7: Comparison of classification models

Classification Model		Correctly classified	Misclassified	Better classifier
K-Nearest	10 Folds	19100	4483	Naïve Bayes
	66% split	6499	1519	
Decision Tree	10 Folds	15978	7605	
	66% split	12946	5771	
Naïve Bayes	10 Folds	21,647	1936	
	66% split	649	3294	

The comparison based on classification accuracy and performance of the three classification models shows the Naïve Bayes classifier as the best classifier in terms of accuracy percentage and accurately placing instances.

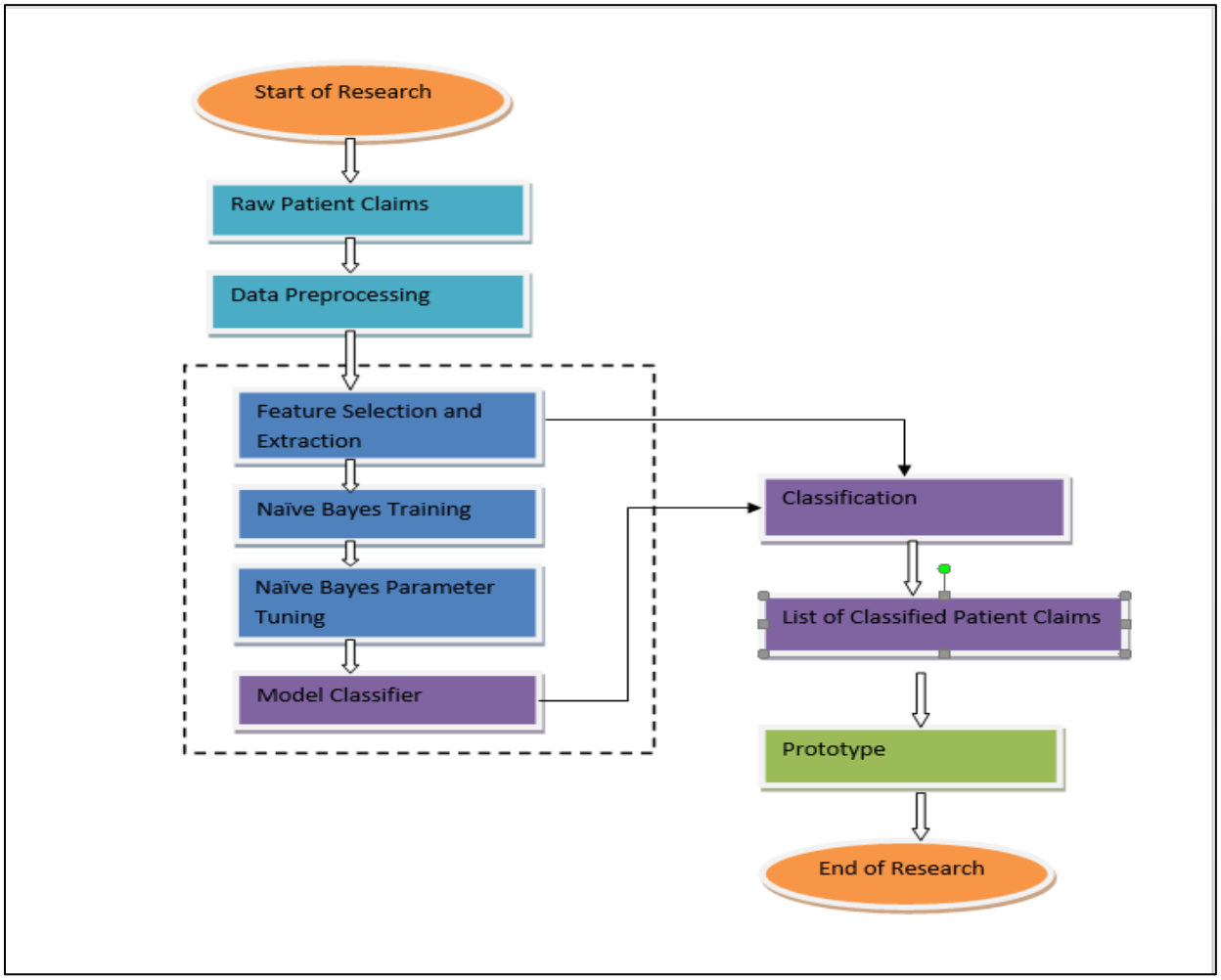
Naïve Bayes Model Training and Testing

The methodology shown in *Figure 1* was adopted to design and develop the model for detecting and predicting fraud in the claims. The data was trained using the Naïve Bayes classification classifier. The

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

unlabeled data was tested and the output file generated classifying claims as either normal or fraudulent

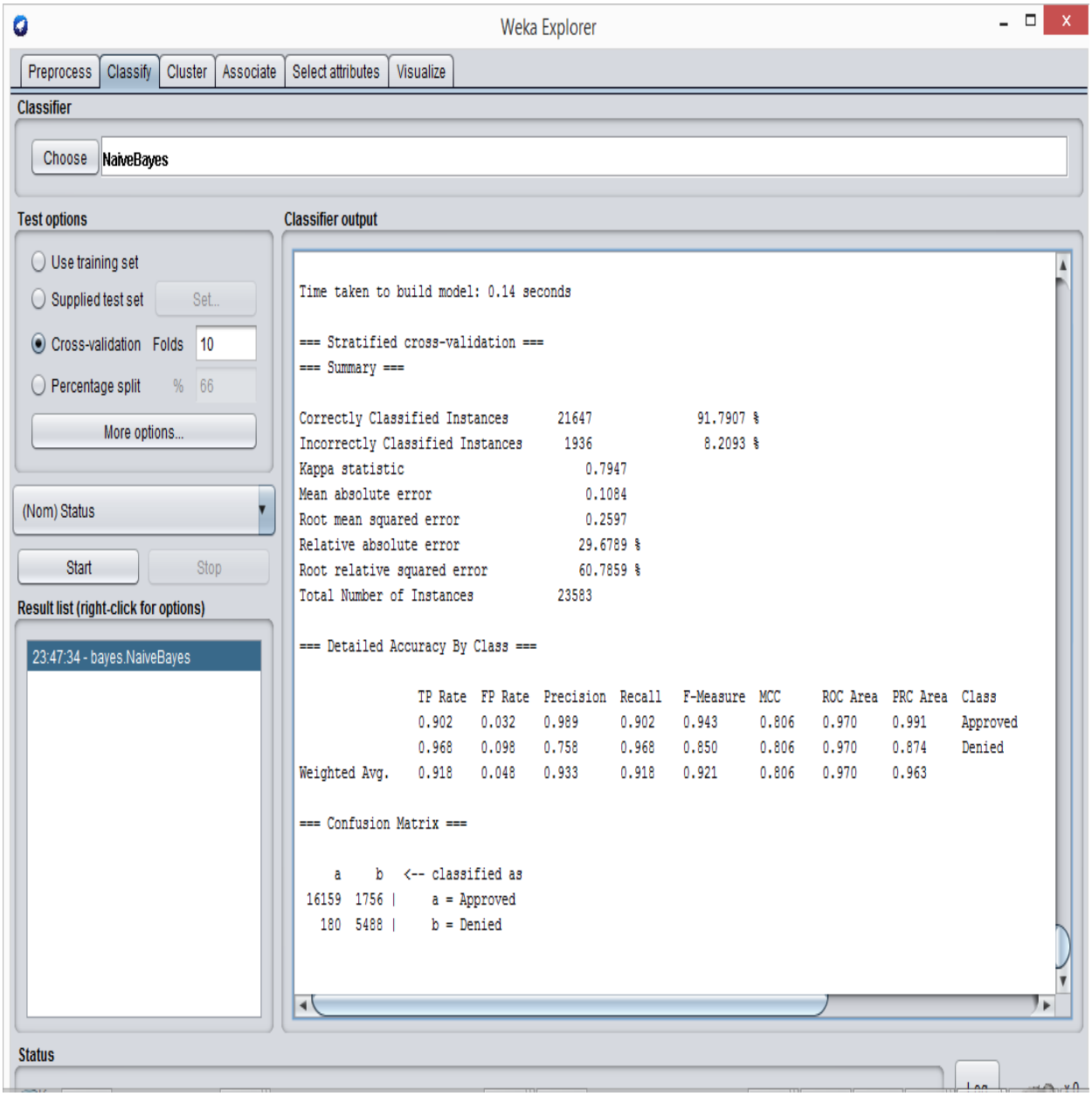
Figure 1: Proposed framework for detection of fraud in claims flowchart



In order to classify the claims as abnormal or normal, ten-fold cross-validation was used to test and evaluate the classifier. 91.7907% accuracy was achieved by the model during training and during testing, and a 72.12% hit rate was achieved with the supplied test dataset, as shown in the WEKA *Figures 2 & 3*.

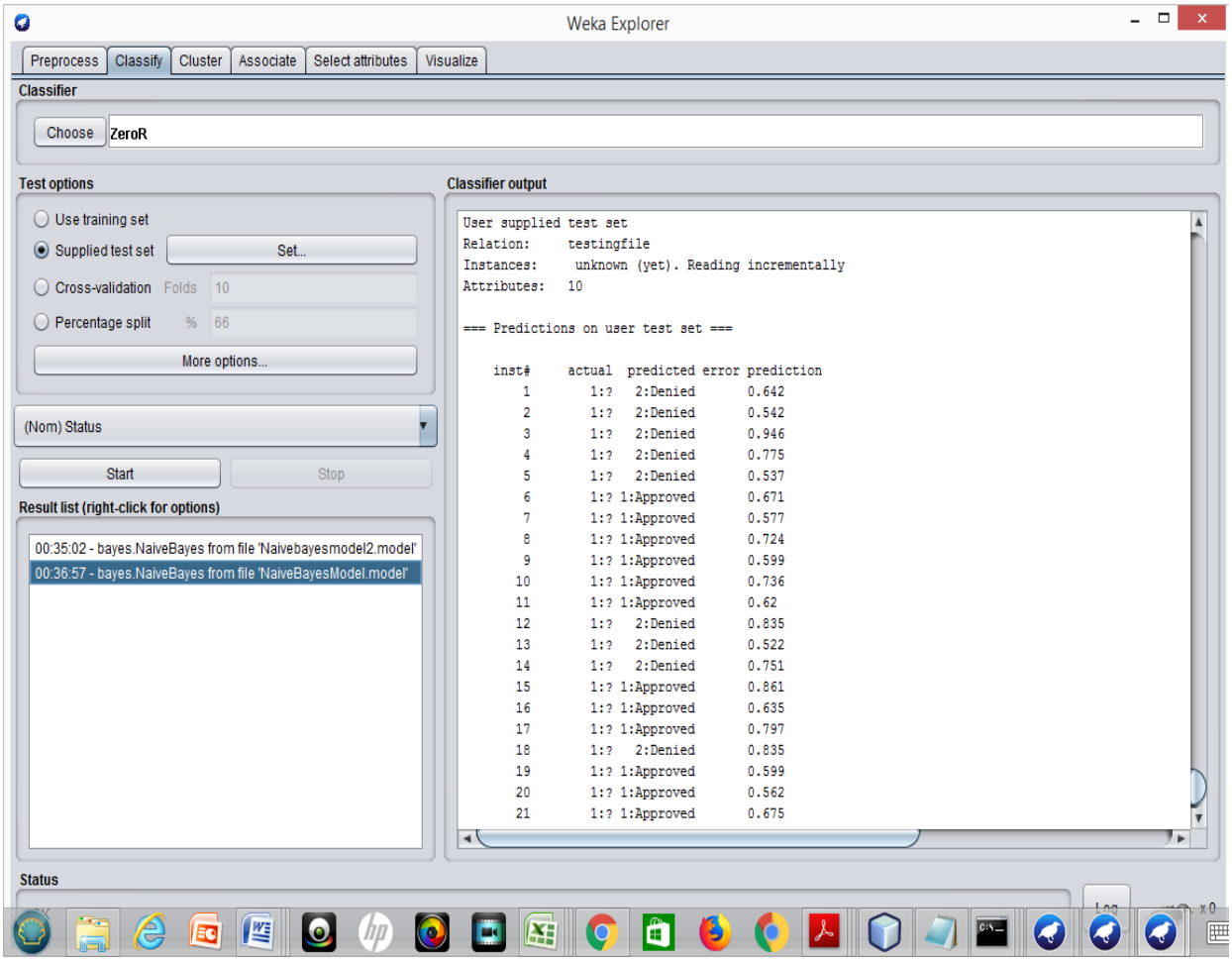
Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Figure 2: Naïve Bayes model training results



Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Figure 3: Naïve Bayes model testing results



The Prototype

A simple Java application was developed, as shown in *Figures 4 to 6* below, to deploy the model. The system loads by asking the user to provide a training dataset for the claims to check. A model is then built using the dataset provided. On clicking the predict button, the user should provide the claims to check for fraud. An output is then presented on whether the claims are fraudulent or not.

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Figure 4: Prototype home page

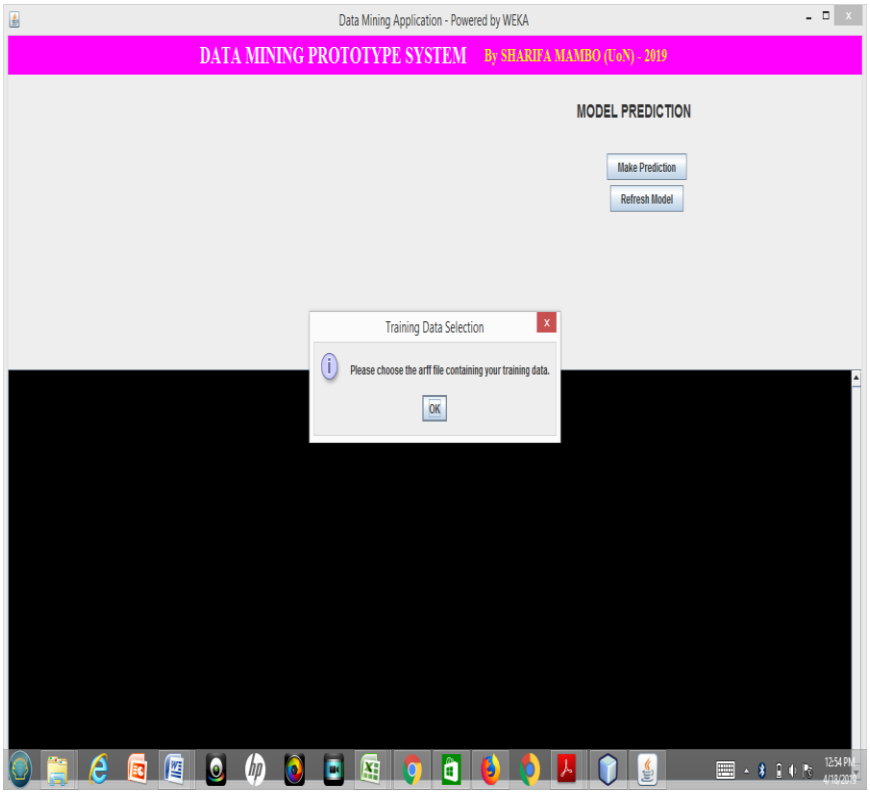
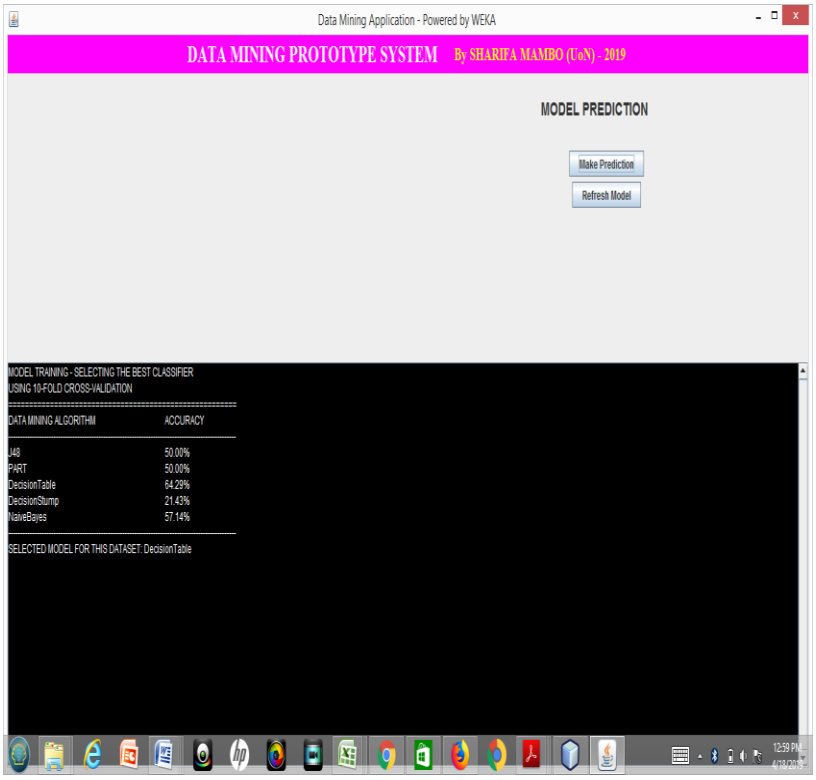
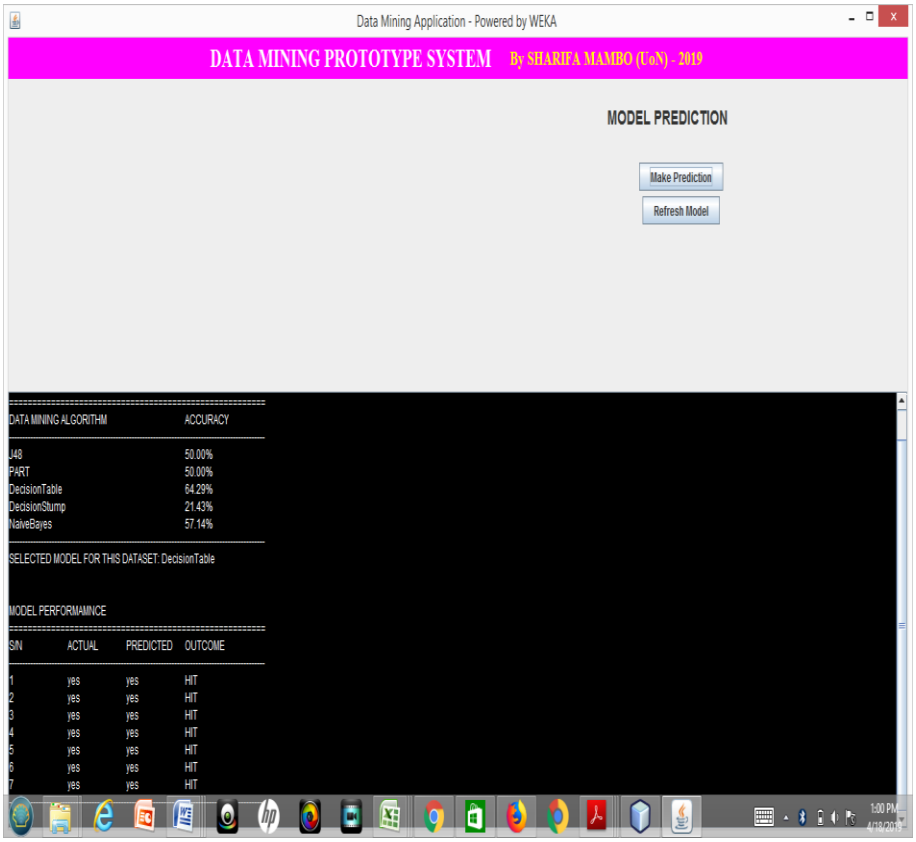


Figure 5: Model Building



Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Figure 6: Predicting results



CONCLUSION

Kenya needs to develop mechanisms to predict the widespread and very costly fraud in her healthcare system. The results of this study demonstrated how Naïve Bayes could be applied to groups of data under investigation to detect any abnormal behaviour in the data. The prototype proposed is built on the best two classification models that will guarantee any health insurance company a detection hit rate of 60 - 70%. This fraud detection system, when fully developed, will benefit the health insurance companies not only in improving its handling of fraud in claims but also in registering tremendous savings**.**

REFERENCES

AKI. (2013). *Health Insurance Fraud Survey Report*. Nairobi, KE: Association of Kenya Insurers. Retrieved from https://www.akinsure.com/images/pdf/Medical InsuranceFraudSurvey.pdf

Barasa, E., Rogo, K., Mwaura, N., & Chuma, J. (2018). Kenya National Hospital Insurance Fund Reforms: Implications and Lessons for Universal Health Coverage. *Health Systems & Reform*, 4(4), 346-361.

Bauder, R. A., & Khoshgoftaar, T. M. (2018a). The detection of Medicare fraud using machine-learning methods with excluded provider labels. In *The Thirty-First International Flairs Conference.*

Bauder, R., & Khoshgoftaar, T. (2018b). A survey of medicare data processing and integration for fraud detection. In *2018 IEEE international conference on information reuse and integration (IRI)* (pp. 9-14). IEEE.

Article DOI: https://doi.org/10.37284/eajit.5.1.1023

Hasheminejad, M.H. & Salimi, Z. (2018). FDiBC: A Novel Fraud Detection Method in Bank Club based on Sliding Time and Scores Window. *Journal of AI and Data Mining*, 6(1), 219-231

Holmes, G., Donkin, A., & Witten, I. H. (1994). *Weka: A machine-learning workbench*. Hamilton, New Zealand: The University of Waikato.

Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2015). Using data mining to detect health care fraud and abuse: a review of literature. *Global journal of health science*, 7(1), 194.

Kirlidog, M., & Asuk, C. (2012). A fraud detection approach with data mining in health insurance. *Procedia-Social and Behavioral Sciences*, 62, 989-994.

Koh, H. C., & Tan, G. (2011). Data mining applications in healthcare. *Journal of healthcare information management*, 19(2), 65.

NHCAA. (2019). *The Challenge of Health Care Fraud*. Washington, DC: National Health Care Anti-Fraud Association. Retrieved from https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

Phua, C., Lee, V., Smith, K., &Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.

Rashidian, A., Joudaki, H., &Vian, T. (2012). No evidence of the effect of the interventions to combat health care fraud and abuse: a systematic review of literature. *PloS one*, 7(8), e41988.

Shin, H., Park, H., Lee, J., & Jhee, W. C. (2012). A scoring model to detect abusive billing patterns in health insurance claims. *Expert Systems with Applications*, 39(8), 7441-7450.

Van Capelleveen, G., Poel, M., Mueller, R. M., Thornton, D., & van Hillegersberg, J. (2016). Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. *International journal of accounting information systems*, 21, 18-31.

Verma, A., Taneja, A., & Arora, A. (2017). Fraud detection and frequent pattern matching in insurance claims using data mining techniques. In *2017 Tenth International Conference on Contemporary Computing (IC3)* (pp. 1-7). IEEE.

