You are invited to a virtual seminar hosted by ICCSSA
on 15 August 2022 at 16:30

GUEST SPEAKER: Dr Wilbert Chagwiza

Wilbert Chagwiza is a data science manager at Standard Bank (SBSA) in the Fraud Risk Management department, specialising in machine learning models development to predict suspicious and fraudulent transactions both in South Africa and the African region. Prior to joining SBSA, Wilbert worked as a senior data scientist at EOH Holdings, heavily involved in machine learning models development for product marketing, insurance sales and credit score cards development. He is also involved in academia, which is supervising masters and doctoral students in the fields of statistics, data science & machine learning and financial mathematics at University of the Witwatersrand, University of Venda, National University of Science & Technology (Zimbabwe) and University of Lusaka (Zambia). He is also an external examiner at the University of South Africa, assisting MANCOSA and IMM in dissertation supervision. Wilbert holds: PhD in Financial Mathematics from University of Venda; MSc in Financial Engineering from National University of Science & Technology (Zimbabwe); MSc in Operations Research from National University of Science & Technology (Zimbabwe); MComm in Finance from Great Zimbabwe University (Zimbabwe); BComm (Hons) in Financial Modelling from University of South Africa; and BSc (Hons) in Mathematics from Bindura University of Science Education (Zimbabwe).

TITLE: Fraud Detection using Multi-level Machine Learning Models

Individuals and companies are losing a lot of money through fraud. Fraudsters are very skilful and know who to target and when to target. The rise of online transactions due to Covid19 restrictions and lockdowns has led to more individuals and companies being exposed to internet/ online fraud transactions. Fraudsters are heavily involved in the banking industry, insurance industry and telecommunications industry. There are various forms of methods which fraudsters use to trick the unsuspecting victims that include vishing, smishing and phishing. Unsuspecting victims are: responding to unknown calls; click unknown website links sent to them via SMS; or clicking unknown websites sent through emails. Individuals and companies are finding it very difficult to cope with the high rate of fraud transactions and are not able to distinguish between genuine and non-genuine calls, SMSs and emails. Fraudsters are using different cash-out mechanisms that include: buying crypto-currency locally or internationally; sending instant money to themselves or other people; buying vouchers for themselves or other people; buying prepaid services; and buying internet data bundles for resell at cheaper prices. Fraudsters can either imitate or not imitate victims' transaction behaviour, and therefore general pattern matching/ analysis is not adequate to detect fraud transactions. Due to randomness in fraudsters' behaviour, appropriate multi-level machine learning models can be used to detect hidden fraud behaviours which include support vector machines, Tabnet, Bayesian Networks, LARS and gradient boosted machines.

CLICK HERE TO JOIN:

ICCSSA
INSTITUTE FOR PRACTICING STATISTICIANS