KNOWLEDGE GENERATION FOR STRATEGIC INVESTMENT IN STI WITH OPPORTUNITIES FOR MACHINE LEARNING AND CYBERSECURITY IN ZIMBABWE

Professor Gabriel Kabanda
Secretary General
Zimbabwe Academy of Sciences, TREP Building, University of Zimbabwe
Harare, ZIMBABWE
Email: gabrielkabanda@gmail.com/ profgkabanda@hotmail.com

Abstract

Research creates both knowledge and technology which are put into practical use through the process of innovation. The success in achieving applied scientific technologies can be measured in the form of technological solutions, patents, inventions, published research papers, etc. The purpose of the research was to formulate an economic framework and develop technological solutions for Zimbabwe with respect to knowledge generation, innovation and enterprise development. This was compounded by an exploration for opportunities in cybersecurity and machine learning for use in the knowledge generation and dissemination business. Cybersecurity is an amalgamation of technologies, processes and operations purposed to preserve and protect computer information systems from cyber attacks or unauthorized access. Machine Learning (ML) entails the automatic data analysis of large data sets and production of models for the general relationships found among data. The Pragmatism paradigm was used as the research philosophy in this research as it epitomizes the congruity between knowledge and action. The qualitative aspect was primarily used in the knowledge generation component which was based on an integral research architecture which combines descriptive, narrative, theoretical, and experimental survey methods, through focused group discussions as the major research design. The quantitative dimension used an experiment as a research design to explore prototype models for cybersecurity and machine learning. Priority projects for strategic investment were identified for commercialization and these were on post harvest technologies; small scale mining/mineral value addition/bio mining; clean water alternatives; tiles technologies from mining waste; ICT innovations in Machine Learning and Cybersecurity; and defence technologies. A Bayesian Network model for Cybersecurity was developed to guide implementation of future cybersecurity systems in Africa. The research used the KDDCup 1999 intrusion detection benchmark dataset in order to build an efficient network intrusion detection system. The sample comprised primary data with 42 variables in a set of 494,020 instances that was analysed using mainly the SNORT open source software and other Bayesian Network supportive platforms. A Bayesian Network model was developed which took into consideration the most efficient ML algorithms.

Key Words: Knowledge generation, innovation, sustainable development, economic framework, Cybersecurity, Artificial Intelligence, Machine Learning.

THOMAS, E. M., Temko, A., Marnane, W. P., Boylan, G. B., & Lightbody, G. (2013). Discriminative and generative classification techniques applied to automated neonatal seizure detection. *IEEE Journal of Biomedical and Health Informatics*. https://doi.org/10.1109/JBHI.2012.2237035

TRUONG, T.C; Diep, Q.B.; & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. Symmetry 2020, 12, 410.

UMAMAHESWARI, K., and Sujatha, S., (2017). Impregnable Defence Architecture using Dynamic Correlation-based Graded Intrusion Detection System for Cloud, Defence Science Journal, Vol. 67, No. 6, November 2017, pp. 645-653, DOI : 10.14429/dsj.67.11118.

WILSON, B. M. R., Khazaei, B., & Hirsch, L. (2015, November). Enablers and barriers of cloud adoption among Small and Medium Enterprises in Tamil Nadu. In: 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 140-145). IEEE.