

## A Quantitative Study on the Prevention and Detection of Financial Crimes Using Artificial Intelligence in Mauritius

**Zuleika Nooria Bibi Dinah**

Asia Pacific University of Technology and Innovation  
[nooriadinah@gmail.com](mailto:nooriadinah@gmail.com)

**Kannan Asokan**

Asia Pacific University of Technology and Innovation  
[kannan.asokan@apu.edu.my](mailto:kannan.asokan@apu.edu.my)

**Meera Eeswaran**

Asia Pacific University of Technology and Innovation  
[meera\\_ees@apu.edu.my](mailto:meera_ees@apu.edu.my)

### Abstract

Financial crime has emerged as a pressing concern across various industries, particularly within accounting firms, which handle vast amounts of data and transactions daily. Instances of theft, deceit, extortion, corruption, and money laundering abound, with the allure of illicit gains often outweighing perceived risks for so-called white-collar offenders. With the rapid evolution of digital technology, financial crime has taken on a new dimension, with criminal organizations operating internationally and illicit funds traversing physical and virtual boundaries to reach their destinations. In this landscape, Artificial Intelligence (AI) assumes a paramount role in the prevention and detection of financial crimes. The aim of this research is to assess the efficacy of Artificial Intelligence in mitigating financial crimes in Mauritius, focusing on three critical components: Machine Learning, Robotic Process Automation, and Neural Network. Utilizing a quantitative methodology grounded in primary data, an online questionnaire was administered to employees within accounting firms in Mauritius specializing in financial crime prevention and detection. This study employs the sophisticated analytical tools offered by the Statistical Package for the Social Sciences (SPSS) to investigate the dynamic relationships among three key variables: Machine Learning, Robotic Process Automation, and Neural Networks. Through rigorous analysis, this research aims to evaluate the effectiveness of these technologies in enhancing financial crime prevention and detection within the specific context of Mauritius. The analysis elucidates a noteworthy and positive correlation between these variables and the deterrence and identification of financial malfeasance, with Machine Learning demonstrating the most pronounced impact at 75.9%. Nevertheless, it is imperative to underscore the collective importance of all three variables in fortifying Mauritius's defenses against financial malpractice. These insights underscore the critical need for heightened awareness and adoption of Artificial Intelligence technologies to confront the burgeoning threat of financial crime effectively in Mauritius.

**Keywords:** *Artificial Intelligence, Machine Learning, Robotic Process Automation, Neural Network*

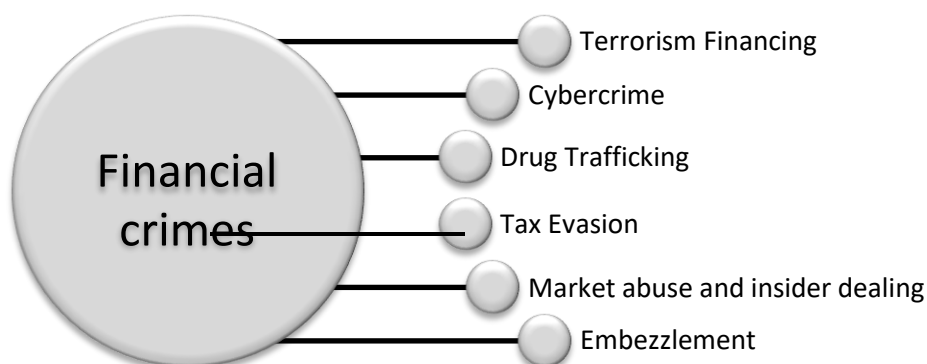
## 1.0 Introduction

Financial crime has emerged as a pressing concern for virtually all organizations in contemporary times. Despite its prevalence, there lacks a universally acknowledged definition for this concept. According to the International Monetary Fund (IMF), financial crime encompasses actions that result in financial harm or loss across a broad spectrum of non-violent activities. Primarily perpetrated through online channels, often intertwined with cybercrime, these illicit activities exert significant repercussions on financial institutions. Moreover, the proliferation of online transaction systems has contributed to a staggering increase in the volume of financial transactions. Consequently, both illicit and legitimate financial entities exploit the structured nature of transaction systems, leveraging the global ease of monetary transfers. Notably, financial crime cannot be viewed in isolation, given the intricate dynamics of its surrounding environment. Its evolution mirrors shifts in societal contexts and technological advancements. Against this backdrop, financial crime continues to proliferate and evolve into increasingly intricate and sophisticated forms. (J. Jung, J. Lee, 2017).

According to the International Monetary Fund (IMF), financial institutions may find themselves implicated in financial crimes through three distinct roles: as victims, perpetrators, or instrumentalities. In the first category, financial institutions can become targets of various criminal activities, including fraud, embezzlement, bank fraud, cyber financial crime, corporate fraud, breaches of information security, terrorist financing, and the manipulation or misrepresentation of financial information. These crimes pose significant risks to the integrity and stability of financial institutions, often resulting in substantial financial losses and reputational damage. In the second category, financial institutions may actively perpetrate harm onto others by engaging in activities such as the sale of fraudulent financial products or the misappropriation of customer funds. The third category involves financial institutions knowingly or unwittingly facilitating the retention or transfer of funds derived from criminal activities, regardless of whether the underlying crime is financial in nature. This includes activities such as money laundering, bribery, and corruption. By providing channels for the movement of illicit funds, these institutions enable the laundering of proceeds from various criminal enterprises, thereby perpetuating the cycle of illicit finance.

Addressing these multifaceted challenges requires the implementation of robust regulatory frameworks, the adoption of enhanced due diligence measures, and the fostering of greater cooperation between financial institutions, law enforcement agencies, and regulatory authorities. By strengthening regulatory oversight and compliance measures, financial institutions can mitigate the risks associated with financial crimes and uphold the integrity of the financial system. Through concerted efforts and proactive measures, the financial sector can work towards safeguarding against the diverse threats posed by financial crimes, thereby promoting stability, transparency, and trust in the global financial ecosystem.

**Figure 1: Types of Financial Crimes**



In the context of Mauritius, the European Commission (EC) has identified the country as a high-risk third country due to inherent vulnerabilities within its anti-money laundering and counter-terrorist financing mechanisms. Consequently, Mauritius has been placed on the grey list by the Financial Action Task Force (FATF), signifying deficiencies in its strategies for combating financial crimes (PWC Mauritius, 2020). Furthermore, the assessment conducted by Stephan Platt, a distinguished authority in regulatory investigations pertaining to financial crimes, has yielded a sobering evaluation of Mauritius. Platt's analysis has categorized Mauritius with a C+ rating concerning its capacity to address money laundering operations effectively (Fakun, 2018). This assessment underscores critical areas requiring attention within Mauritius' regulatory and enforcement frameworks to fortify its defenses against financial crimes comprehensively.

In light of the recent scandal involving the African Development Bank (AfDB) and the Burmeister and Wain Scandinavian contractor, Mauritius' ratings have experienced a downturn. This decline stems from revelations that an energy project conducted within Mauritius was compromised due to fraudulent and corrupt practices. Specifically, the AfDB has taken action by blacklisting the contractor for engaging in sanctionable activities, including financial payments to Mauritian officials and intermediaries to obtain sensitive information. These illicit payments facilitated the acquisition of insider knowledge advantageous during the pre-tender procurement phase. This instance not only highlights instances of corruption but also exemplifies a prevalent form of procurement fraud (Chelin, 2020).

Despite the longstanding concerns surrounding money laundering and terrorist financing in Mauritius, recent findings indicate a notable prevalence of other financial crimes within the island nation, including corruption, whistleblowing, Ponzi schemes, and fraud. Notably, the National Risk Assessment has identified fraud as a significant issue in Mauritius, rating it as "high" due to a surge in attempted business email invasion incidents. These incidents involve unauthorized attempts to access emails or breach other accounts with the intent of fraudulently transferring funds. The assessed gains linked to financial fraud during the evaluation period amounted to MUR 543 million (USD 16.1 million), with electronic fraud, swindling, and embezzlement accounting for the largest portion of profits (Cusack and Ramgoolam et al., 2020). These findings underscore the multifaceted nature of financial crimes in Mauritius and the imperative need for comprehensive strategies to address them effectively.

The ramifications of financial crimes extend beyond mere economic implications, profoundly impacting both governments and national economies, as well as the general population. These illicit activities not only impose substantial costs on human welfare but also pose significant threats to a country's financial and external stability. Financial crimes can erode public trust in government institutions and financial systems, potentially triggering widespread social and economic upheaval. Moreover, nations perceived to have inadequate structures for combating financial crimes are vulnerable to intensified scrutiny and condemnation from international stakeholders. This heightened scrutiny is particularly pronounced in international financial hubs such as Mauritius, which are characterized by extensive global economic activities. As such, these jurisdictions face heightened pressure to bolster their regulatory frameworks and enforcement mechanisms to effectively combat financial crimes and safeguard against reputational damage on the global stage (Abdullatif, 2020).

Henceforth, this study endeavors to examine the strategies for preventing and detecting financial crimes in Mauritius through the application of Artificial Intelligence (AI). It seeks to elucidate the efficacy of various sub-fields of AI, including Machine Learning (ML), Robotic Process Automation (RPA), and Neural Networks, in enhancing the detection and prevention mechanisms within the Mauritian context. By delving into the intricacies of AI technologies, this research aims to contribute significantly to the body of knowledge surrounding their utilization in combatting financial crimes. Specifically, it seeks to identify and analyze the specific applications of ML, RPA, and Neural Networks that hold promise for detecting and preventing various forms of financial crimes prevalent in Mauritius.

Moreover, this study aspires to provide insights into the practical implementation of AI-driven solutions within the Mauritian financial landscape, offering recommendations for policymakers, regulatory authorities, and financial institutions to enhance their capabilities in combating financial crimes effectively. Through a comprehensive exploration of AI's potential, this research endeavors to offer valuable insights and guidance for stakeholders seeking to strengthen their anti-financial crime strategies in Mauritius and beyond.

## **1.2 Problem Statement**

Addressing the pervasive issue of financial crime demands heightened attention globally, with Mauritius emerging as a focal point for concern. The staggering impact, amounting to trillions of dollars, underscores the imperative for financial institutions to fortify their defenses against such nefarious activities. As technological advancements increasingly facilitate the execution of intricate financial crimes, the imperative for law enforcement and legal entities within financial institutions to harness technological solutions intensifies (Rebovich, 2021). Oyuga (2018) underscores the global nature of the challenge, extending beyond Mauritius, wherein numerous firms engage with millions of consumers annually and maintain extensive networks of third-party vendors. However, the systematic examination of these connections for criminal ties remains disproportionately low, revealing critical vulnerabilities in current practices. Moreover, the prevalence of undisclosed financial crime incidents, attributed in part to internal corruption implications and apprehensions regarding reputational and financial repercussions, underscores the urgency for enhanced vigilance (Oyuga, 2018).

In response to the profound implications of financial crime, jurisdictions worldwide have instituted policies aimed at curtailing the flow of illicit funds to and from criminal organizations, thereby constricting their operational latitude (Ball et al., 2015). Consequently, the integration of cutting-edge technologies, notably artificial intelligence (AI), emerges as a linchpin in the arsenal against financial malfeasance. However, the adoption of AI is not without its challenges, characterized by substantial costs, unproven efficacy, and a conspicuous deficit in requisite expertise for deployment (Grint et al., 2017). Crosman (2019) accentuates the perils inherent in opaque algorithms underpinning AI, both from a risk management standpoint for institutions and a privacy perspective for individuals subject to scrutiny. Moreover, misapprehensions regarding AI's purported existential threats to financial institutions perpetuate hesitancy towards its widespread adoption (Bentley et al., 2018). These concerns extend beyond institutional boundaries, raising broader societal apprehensions regarding the perpetuation of financial crimes (Forwood and Bolton, 2018).

While machine learning (ML) holds promise as a potent tool in the fight against financial crimes, its integration remains characterized by a degree of experimentation rather than systematic implementation (Leo and Sharma et al., 2019). Notably, the opaqueness inherent in ML models, coupled with their susceptibility to outliers and overfitting, poses formidable challenges in operational contexts (Georgieva and Markova et al., 2019). This is particularly salient in scenarios marked by imbalanced datasets, wherein the proclivity for erroneous classification disproportionately impacts minority classes, as evidenced in credit fraud detection (Georgieva and Markova et al., 2019). Despite these complexities, the nexus between machine learning and the prevention and detection of financial crimes warrants meticulous examination.

Robotic process automation (RPA) emerges as a compelling avenue for financial institutions grappling with the multifaceted challenges posed by financial crimes (Griffiths and Pretorius, 2021). Nevertheless, lingering apprehensions persist regarding the potential exploitation of RPA to facilitate illicit activities, alongside attendant governance, control, and risk mitigation concerns (Griffiths and Pretorius, 2021). Additionally, the technological constraints inherent in RPA solutions, compounded by the indispensability of human judgment in handling unstructured data, underscore the imperative for circumspect evaluation (Gotthardt and Koivulaakso et al., 2020). Moreover, the vulnerability of RPA systems to cyber threats accentuates the exigency for robust security measures amidst escalating cybercrime incidents targeting financial institutions (Bhardwaj and Avasthi et al., 2019). Thus, the question endures: to what extent can robotic process automation be wielded as a potent weapon in the ongoing battle against financial crimes?

Although neural networks have emerged as indispensable tools in the realm of financial crime prevention and detection, persistent ambiguities underscore the need for nuanced evaluation (Georgieva and Markova et al., 2019). Notably, the inherent limitations of neural networks in grappling with imbalanced datasets, compounded by their suboptimal performance with structured data, engender substantial deliberation (Zhou, Zhang, and Wang et al., 2019). Furthermore, the resource-intensive nature of neural network training, juxtaposed against the exigencies of real-world financial crime scenarios, underscores the imperative for judicious resource allocation (Karimi and Akbari et al., 2020). Despite these challenges, the intricate interplay between neural networks and the prevention and detection of financial crimes merits sustained inquiry.

### **1.3 Theoretical Framework**

In recent years, more attention has been paid to financial crimes. To comprehend what, how, and why financial crime is needed and to encourage knowledge, skills, and know-how, there is a need to develop theory (Sujeewa and Yajid et al., 2018). Therefore, this can be illustrated through “The Fraud Triangle”.

### 1.3.1 The Fraud Triangle Theory

**Figure 2: The Fraud Triangle**



*Source: (Sujeewa and Yajid et al., 2018)*

The fraud triangle offers businesses a valuable framework for the analysis of their vulnerability to fraud and non-ethical behaviour and gives the means to prevent victims. All three aspects of the triangle must exist almost universally so that a person can act unethically. If a corporation can concentrate on preventing each element, fertile ground for undesirable conduct can be prevented. (Mansor, 2015). Therefore, to prevent financial crime, the Fraud triangle has 3 aspects that need to be considered and this is explained as follows:

**Pressure:** Companies have a strong influence solely on consumers' and workers' personal life. It may be beneficial to identify any potential challenges that the firm may have – such as money issues, drug usage, etc. Working to alleviate these problems can help avoid financial crime. (Schuchter and Levi, 2016).

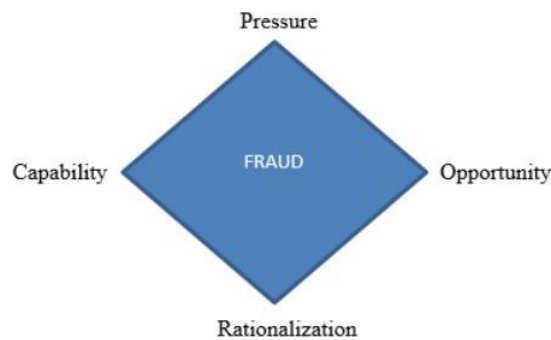
**Opportunity:** Financial institutions should always try to limit the possibility of fraud and unethical conduct. For every firm that wishes to remain safe against the risks of fraud, this is a worthy investment. (Schuchter and Levi, 2016).

**Rationalization:** One technique of avoiding fraud is to prevent people from ever having the opportunity to streamline behaviour. Companies may establish a policy of "zero tolerance" to fraudulent activities and recall this policy on a frequent basis to staff and consumers. Corporations can also ensure that individuals understand the cost of fraud to other consumers and workers. Making people aware of the serious repercussions makes it increasingly challenging to demonstrate unethical action. (Schuchter and Levi, 2016).

### 1.3.2 The Fraud Diamond

In their study, Wolfe and Hermonson (2004) stated that while perceived pressure or motivation may exist, as well as an opportunity and a rationale to commit financial crimes, fraud is unlikely to happen unless the fourth ingredient is there; capability.

**Figure 3: The Fraud Diamond**



*Source: (Sujeewa and Yajid et al., 2018)*

A person's position or job inside a corporation may provide him or her the capacity to generate or exploit a fraud opportunity that others do not have. According to Sujeewa and Yajid et al., (2018), a fraudster also possesses the requisite attributes and talents to be the proper person to pull it off, and this individual has identified this specific fraud opportunity and can bring it into reality. They discovered significant visible characteristics associated with people's ability to perpetrate fraud. These dangers include: (a) a position of authority or function inside the organization; (b) intelligence to abuse the accounting and internal control systems (c) pride and confidence (d) capacity to cope with stress effectively. In fact, with the emergence of new financial systems like Artificial intelligence, the fraud diamond is more pertinent today. It has created new opportunities for fraudsters who can take advantage of systemic weaknesses.

## **2.0 Literature Review**

The literature review will actually discuss the findings of previous researchers in relation to the dependent variable which is preventing and detecting financial crime and the independent variables such as Robotic process automation, Machine learning, and Neural networks. This chapter will also focus on a myriad of past reliable articles and journals to analyse each variable wisely followed by identifying the literature gaps. Lastly, the literature review will consist of the findings, objectives, and data collection of other researchers.

### **2.1 Prevention and Detection of Financial Crime**

Financial institutions have addressed the complexities of creating a creative solution to mitigate financial crime in order to reduce risks related to goodwill and sustainability over the years. With the latest developments in new technology, the complexities of the internet space have made combating financial crime difficult, with criminals adapting their tactical approaches in response to technological changes. The investigation of financial crimes can be hampered by internal conspiracies and sophisticated accounting report falsification. Furthermore, the rising incidence of financial crimes in multinational organisations can be attributed to internal perpetrators' belief that they can commit fraud with impunity. (Akinbowale, Klingelhofer and Zerihun, 2020).

In recent years, researchers have conducted detailed research on financial crime prevention. Financial crime is often connected with other offenses such as bank and non-bank theft, illegal transfer in another's possession for one's gain, deceit involving a violation of confidence and concealment, and incentive-driven. (Fauzi, Szulczyk, and Basyith, 2018). On the other hand, Lukito (2016) investigates the efficacy of Indonesian laws in preventing and eradicating money laundering activity, as well as the PPATK's ability to stop money laundering in Indonesia. The author's research draws on a review of the literature and a study of AML legislation. The author believes that a financial intelligence unit will help to prevent systemic crimes like money laundering and corruption. In addition, she examines anti-bribery laws and the critical role of the National Integrity System in strengthening anti-corruption enforcement in Indonesia. As a result, one of the most important aspects of preventing any financial crime is to raise awareness of the national ethics mechanism and anti-corruption enforcement with all public and private institutions in all business practices.

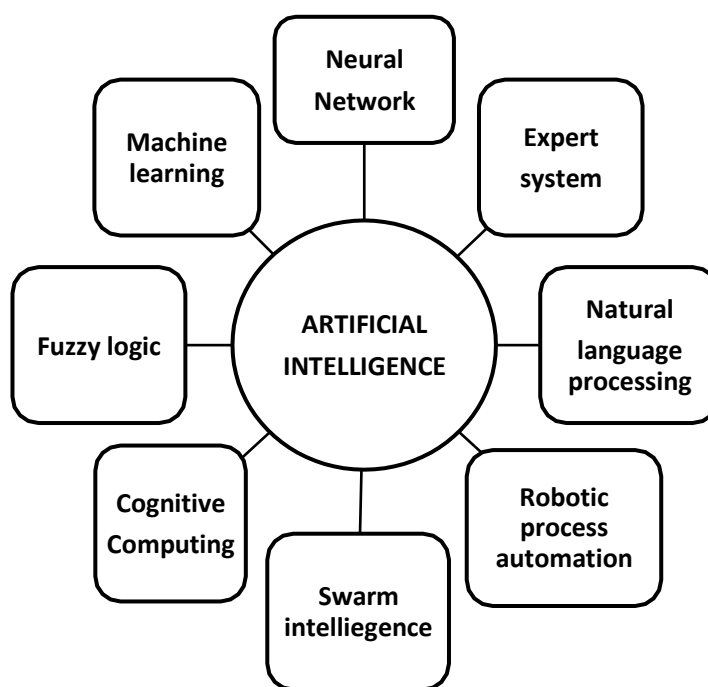
According to Akinbowale (2018), forensic accounting tool is a relatively recent trend in combatting financial crime especially in developing economies. As per the findings of his report, the use of forensic accounting tools has the potential to reduce the amount of time spent solving alleged criminal cases. This research also discovered that the level of forensic accounting awareness in government parastatals is comparatively poor, owing to the government's failure to release funds for proper instruction on the use of forensic accounting tools in terms of the acquisition of information and skills to aid forensic investigation gained in alleged fraudulent cases. Also, in this study, forensic accounting has been identified as more effective when computerized in a digital environment. It is therefore advisable for financial institutions, particularly the public sector should examine their forensic accounting plans and strategies in a digitalizing environment and forensic accounting software as a tool for rapid investigation and mitigation of financial crimes.

Halbouni, Obeid and Garbou (2016) stated that the key objective in conducting their research was to investigate the perception of fraud, the role of corporate governance, IT, and the conventional prevention and detection strategies of fraud among UAE firms by financial accountants and professional auditors (both internal and external auditor). It also aims to examine their views of fraud and prevention of the impact of demographic variables. The key contribution of this analysis is the finding that corporate governance plays a moderately important role in the prevention and detection of fraud in the UAE and provides evidence to senior management and boards of directors to raise knowledge of how important its supervisory role is to fulfil stakeholder duties and obligations. The relatively important position of the audit committee also implies that members of the audit committee must learn how to strengthen their confident monitoring through proper guidance and preparation in addition to being up-to-date with regulatory requirements and trends. The findings also reveal no substantial difference between the use of technical and conventional approaches between internal and external auditors in the audit.



## 2.2 Artificial Intelligence

AI is a broad phrase that refers to technological developments that enable robots to become "intelligent." In 1956, John McCarthy created the concept of artificial intelligence. Machine learning, Robotics, deep learning, natural process language, neural networks, expert systems, and augmented intelligence are just a few of the names given to describe AI. AI research aims to improve planning, knowledge representation, reasoning, learning, NLP, vision, and the capacity to move and manipulate objects. (Kunwar, 2019). AI functions on two levels: symbolic and data. For the database side, known as ML, users must give the computer a large amount of data before it can operate. The machine can learn in a much wider range of dimensions. A machine can analyse a large amount of high-dimensional data and identify patterns. Once these models are mastered, they can provide projections that humans cannot even attempt. (Takyar,2018). The main branches of AI can be illustrated below:



**Figure 4: Branches of AI (Ali and Rahman et al., 2016).**

Noor and Mansor (2019) conducted a quantitative study to examine one of the most prominent forms of financial crime which is whistleblowing among Malaysian public sector agencies. The use of artificial intelligence in the whistleblowing practice shall be tested for the objective of this analysis to determine the feasibility of this method. The results are likely to improve new efforts by the Malaysian government to combat fraud and corruption. Consequently, the findings of this paper show that the MACC can work effectively and immediately to resolve corruption charges by applying AI in whistleblowing activities. This will not only address an acute practical challenge but also lead to a better new, free corruption government. Consequently, it is suggested to integrate AI applications into all public sector institutions and necessary for the engagement of MACC with plaintiffs.

Yeoh (2019) on the other hand uses his own perception to discuss the intended positive and unintended negative consequences of AI implementation in financial crime. This paper focused largely on primary and secondary data as well as applicable laws and regulations, business cases and legal economic perspective. The author is focusing on cybercrime in his study, and he stated that AI could be an antidotes or an accelerator for financial crimes and in particular cybercrime. Research shows that 3 methods of curbing these cybercrimes is to apply criminal law. However, some felt that this is an inadequate way to keep AI officers responsible when existing AI programs have not been considered to be able to make ethical decisions. Rather, administrative penalties will be deemed more acceptable at this point. While AI malicious activities are held in vigilance, regulatory authorities in the USA and in the UK have chosen the state interventionist style to preserve their global competitiveness in this field in an innovative, market-oriented, permission-free strategy. To conclude the author added that AI systems will function both as the cure and accelerator to financial crimes, but political leaders and regulators are responsible for ensuring more of this former.

Hassan and Abdulrahman (2019) however use a descriptive research design to conduct a research based on qualitative and quantitative data from a sample of 200 employees of the UAE banks involved in the detection of fraud using basic random sampling and 10 data scientist were employed to carry out the qualitative study. This research highlights the main advantages and consequences of AI in the UAE banking sector and thus provides avoidance of the negative consequences and the risk factors. The author then concluded that the use of artificial intelligence was implemented in the financial sector, where it was seen that online financial transactions are booming and fraud detection and prevention has become easier through the online learning of the machine, where huge amounts of information can be analysed or fed by the machine learning tools.

Money laundering has always been a serious problem to mitigate. That is why Bedoya, Granados and Burgos (2020) carried out a research based on network science methodologies to apply to AI tools for AML framework. The purpose of this research is mainly to focus on the prevention of money laundering in a Columbian case using AI technology. They proposed a software architecture that is fundamental to reducing patterns of ML and terrorism. They found out that the AML schemes require a new paradigm that is a multidisciplinary framework that will provide a dynamic structure to understand the pattern of financial crime. For this reason, the combination of AI and network science is one of the new options to prevent financial crimes and complex problems.

### **2.3 Machine Learning**

Money laundering is considered as the third category of financial crime as stated by the IMF. Jullum and Loland et al., (2020) conducted research based on a supervised machine learning model which is applied to a comprehensive set of data from Norway's largest bank. The focus of this research is to create, explain and verify a machine-learning model for determining which financial transactions should be manually scrutinized for suspected money laundering. The model presented by researchers is trained by utilising three categories of historical data namely: "normal legal transactions", those identified as suspicious by the banks internal warning system, and probable money laundering instances submitted to authority. The algorithm is designed to forecast the likelihood of a new transaction being reported utilising information such as background details on the sender/receiver, previous behaviour, and transaction records. The findings of this research reveal that the prevalent

practice of not employing non-reported warnings in training the model might result in sub-optimal outcomes. The same is applied to the use of un-investigated transactions. However, they conclude that their newly devised model beats the banks' present methodology.

On the other hand, Minastireanu and Menista et al., (2019) conducted a systematic quantitative literature review based on machine learning algorithms. In this regard, this study evaluates existing studies in fraud detection with the objective of identifying and analysing each of these algorithms based on specific criteria, and a hierarchical typology is made. The main aim is to assess and categorize machine learning approaches best suited for detecting bank fraud in an online environment while keeping the following criteria: Low cost, High accuracy, and high coverage. A meta-analysis was then performed on a diverse set of publications of reviewed journals and conference papers from 2010 till the present. Out of these journals, 19 machine-learning approaches were mentioned and analyzed. The categorization of the algorithm that were most mentioned in the literature review includes support vector machines, artificial neural networks, and decision trees. These 3 algorithms are said to produce the best possible outcomes in terms of coverage and accuracy.

Financial statement fraud is another type of financial crime that is defined as the violation of auditing and accounting standards, laws, and regulations enforced by reporting bodies with the objective of misleading users of financial statements (Gabrielli and Mediolini, 2019). In relation to this, Lokanan et al., (2019) conducted research among Vietnamese companies due to the high prevalence of financial statement fraud. This research aims to apply machine learning detection algorithms to spot irregularities in the financial statements of Vietnamese publicly traded companies. The findings demonstrate that the model can rank quarterly financial statements in terms of creditworthiness and also indicated that the majority of Vietnamese financial statements are reliable but about a quarter of them are extremely anomalous suspicious.

Kumari(2019) has stated that due to the vast quantity of data created every second and kept in numerous format and platform, the threats of cyber-security has radically changed over the last few years. It necessitates the development of measures to prevent attacks and theft of crucial information. This allows machine learning and deep learning approaches to shine and demonstrate their ability to thwart cyber threats. In this study, the author discusses numerous attacks and solutions for preventing cybercrime, including machine learning and deep learning. According to her point of view, she concluded that machine learning and deep learning approaches have enabled businesses to assure the security of their data however, these strategies are subject to a variety of malicious assaults.

Financial crimes are considered to be dynamic and lack pattern hence making them difficult to detect. Criminals usually take advantage of current technology breakthroughs in order to bypass security checks resulting in financial disaster. In fact, Raghavan and Gayar (2019) conducted an empirical study by comparing Machine learning and deep learning models in fraud detection. The models are actually applied to 3 types of datasets namely the European, Australian and German datasets. The primary goal of their research is to discover which strategies are most suited for certain types of datasets as many businesses are engaged in innovative strategies to enhance their bottom line. In addition, this study aims to assist businesses to better comprehend how the various strategies perform on different datasets. According to their findings, the best approach for detecting fraud with large datasets would be the Support Vector Machine(SVM) paired with the Convolutional Neural Networks(CNN) for more accurate performance. However, for smaller datasets, ensemble techniques such as SVM, Random Forest and K-nearest neighbour (KNN) can yield significant improvements. Based on past research, the researcher was trying to find the relationship between the dependent

variable and the independent variable. Hence hypothesis  $H_{A1}$  is created in this study which indicates that:

$H_{A1}$ : There is a positive relationship between Machine learning and the prevention and detection of financial crime.

## 2.4 Robotic Process Automation

The costs of fraud continue to be a challenge for many institutions throughout the world. Griffiths and Pretorius (2019) investigate how RPA might help firms to decrease fraud and improve organisational audit effectiveness in spotting probable fraud areas and instances. The research was carried out by performing a literature review that included 22 publications from EBSCOhost, ProQuest, and ScienceDirect (selected by a procedure) on the pertinent research topic of RPA, fraud, and auditing. According to the findings, firms should investigate robotic process automation as a strategy of lowering fraud chances. RPA also helps firms improve the efficiency and efficacy of their audits.

Thekkethil, Shukla, and Beena et al., (2021) on the other hand carried out research that discusses how RPA may reduce fraud risks in the banking and finance sector by reassessing current procedures, minimising human mistakes, improving trade monitoring, automating threat identification and detection and lastly searching for anomalies. They mentioned that RPA actually switched time-consuming manual processes from humans to bots allowing banks to cut their headcount and prevent human participation. This will help to prevent human mistakes thereby improving customer experience. Also, they added that it is critical to invest in innovative technology that can aid in the detection and prevention of potential frauds, as fraudsters/hackers are always challenging the security system. They concluded that implementing RPA in financial organisations for loan processing and fraud detection has been quite effective. Its implementation has enhanced banking procedures to a highly sophisticated level.

Vehicle insurance fraud is regarded to be one of the most serious types of financial crimes. it involves the filing of fraudulent claims against vehicle insurance coverage. The seriousness of insurance violations ranges from modestly overstating claims to knowingly inciting accidents or losses. In relation to this, Patil, Kamanavalli et al., (2021) have conducted research on Vehicle fraud detection using RPA in the insurance sector. The paper focuses on the implementation of RPA tool called UiPath to automate tasks and integrate machine learning (ML) techniques such as Logistic regression(LR), Decision tree(DT), Random Forest(RF), Knearest neighbors(KNN) and Linear Discriminant Analysis(LDA). According to their findings, RPA is the most effective method for detecting vehicle insurance fraud. Thousands of claim forms may be categorized with high accuracy with a single click and it has been observed that in contrast to other ML approaches, LDA has an accuracy of 90%. Based on past research, the researcher was trying to find the relationship between the dependent variable and the independent variable. Hence hypothesis  $H_{A2}$  is created in this study which indicates that :

$H_{A2}$ : There is a positive relationship between Robotic Process Automation and the prevention and detection of financial crimes.

## 2.5 Neural Network

In the Asia Pacific region, prevalent types of fraud notably encompass corruption and asset misappropriation, with fraudulent financial reporting comprising a mere 10% of all occurrences, accompanied by an average loss of \$954,000, as elucidated by the ACFE survey delineated in the "Report to the Nations" in 2020. Consequently, Riany, Sukmadiliga, and

Yunita (2021) embarked on a research endeavour aimed at discerning the efficacy of the Artificial Neural Network (ANN) approach in detecting misleading financial reports and elucidating potential proclivities of businesses towards such fraudulent activities. The study's data analysis methodology entailed employing the ANN method, with the study population encompassing companies listed on the Indonesian Stock Exchange in 2019, alongside businesses substantiated to have engaged in deceptive financial reporting practices. A purposive sampling strategy was employed, yielding a dataset of 506 observations. The findings of the investigation underscore the capability of the ANN model in effectively identifying misleading financial reports, thereby offering valuable assistance to auditors in discerning substantial misstatements associated with fraudulent activities.

Utilizing wireless mobile devices to authenticate users' identities through fingerprints, passwords, photos, and sounds has become standard practice for internet transactions. However, in the event of compromised identification credentials, conventional information security protocols may prove insufficient in preventing online transaction fraud. Addressing this concern, Zhang, Zhou, Wang et al. (2019) propose a fraud detection model predicated on Convolutional Neural Network (CNN) architecture. This model incorporates an input sequencing layer responsible for organizing raw transaction characteristics into discernible convolutional patterns. Experimental results demonstrate the model's exceptional fraud detection efficacy, even in the absence of derived features, as evidenced by evaluation with online transaction data sourced from a commercial bank. In comparison to existing CNN-based fraud detection methodologies, the proposed model achieves a stabilized accuracy rate of approximately 91% and recall rate of around 94%, representing respective increases of 26% and 2%.

Georgieva, Markova, and Pavlov (2019) conducted research addressing the pervasive issue of payment fraud, which poses a significant challenge globally. Businesses and organizations suffer substantial financial losses annually due to fraudulent activities, with perpetrators constantly innovating their methods to perpetrate illegal acts. The study focused on developing a Neural Network model to detect fraudulent transactions, recognizing the considerable disparity between legitimate and fraudulent credit card transactions as a prominent feature of credit card traffic. Moreover, the scarcity of publicly available statistics due to confidentiality concerns necessitates innovative approaches to handle unbalanced datasets, prompting the utilization of resampling techniques in this study. The findings underscore the efficacy of the developed model, achieving a network accuracy of 94.2%. One of the primary advantages of employing a Neural Network for fraud detection lies in its capacity to analyse vast volumes of transactional data and customer behaviors, enabling the identification of anomalous credit card activity. Furthermore, akin to the human brain's ability to discern individuals based on behaviours and gestures, the Neural Network can assess a credit card's usage history to determine its legitimacy.

With the advancement of information and communication, cybercrime has become a worldwide issue. In general, crime detection algorithms identify crimes by training on related data over time, but certain samples in a dataset may have no label. As a result of which Karimi, and Abbasabadei et al., (2020) conducted research based on a semi-supervised neural network for the detection of cybercrime. The suggested technique divides the dataset into two sections namely "labelled and unlabelled" and uses the trained section to estimate the samples using pseudo-labels. According to the findings, the suggested strategy enhances accuracy, precision, and recall by up to 99.83% respectively.

On the other hand, Li and He (2020) conducted research based on a quantitative analysis method in order to detect and prevent cybercrime as well as they provide an innovative mathematical research tool for network activity analysis. Firstly, a new factor space research approach based on the "medium scale" is developed. On this premise, the notion of cybercrime behavioural factor discovery is introduced, and the associated cybercrime behaviour analysis model, the criminal factor neural network, is constructed. Second, utilizing the factor discovery concept, the learning method of a network behaviour neural network is explored. Simultaneously, a network behaviour learning algorithm based on diamond thinking is developed.

Finally, factor discovery ideas and factor neural network learning systems are used in the investigation of cybercrime model analysis and mitigation plans to give guiding decision support and issue solutions for public security sectors. The findings show that diamond-shaped neural network research offers the required experience and guidelines for learning and improving conventional network behaviour models. Daliri (2020) however conducted research based on the Neural Network technique and harmony search algorithm(HAS). The suggested system provides a solution based on HAS that is successful in predicting the optimum structure for the Neural Network and discovering the hidden algorithm in large amounts of data. Given that fraudulent activity may be recognized and halted before it occurs, the suggested system's findings demonstrate that it has an adequate capacity for fraud detection. The best accuracy obtained from the German dataset for the proposed method is 86, and lastly, the best result obtained for the identical recall criterion is 87. Based on past research, the researcher was trying to find the relationship between the dependent variable and the independent variable. Hence hypothesis  $H_{A3}$  is created in this study which indicates that :

$H_{A3}$ : There is a positive relationship between Neural Network and the prevention and detection of financial crimes.

## 2.6 Research Gaps

This study has meticulously examined the contributions of past researchers, endeavouring to contextualize their findings within the scope of this investigation. Notably, the research landscape has predominantly centered on diverse geographical regions, with Noor and Mansor (2019) delving into Malaysia, Granados and Burgos (2020) focusing on Columbia, Halbouni, Obeid, and Garbou (2016) conducting their study in the UAE, and Lukito (2016) directing their attention towards Indonesia.

However, a conspicuous lacuna emerges in the absence of research focused specifically on Mauritius, representing a significant gap warranting attention in this study. Despite assertions from prominent entities within the Mauritian business landscape, including the testimony of major corporations, startups, and Fortune companies, regarding the integration of cutting-edge technologies such as AI and blockchain to fortify their market positioning, the adoption of these innovations for combating financial crimes remains notably absent. Instead, reliance persists on conventional approaches such as regulation and regulatory fines, which have demonstrably waned in effectiveness (Matu, 2022). This discrepancy underscores a critical research gap concerning the utilization of innovative technologies for the prevention and detection of financial crimes in the Mauritian context.

Furthermore, the recent classification of Mauritius on the Financial Action Task Force's (FATF) grey list imparts added urgency to the imperative of addressing corruption concerns within the country. This development amplifies apprehensions among financial institutions regarding Mauritius' susceptibility to corrupt practices, accentuating the exigency for the adoption of contemporary strategies, notably artificial intelligence, in bolstering efforts to combat financial crimes. Thus, the imperative for research aimed at elucidating the efficacy of

AI-driven approaches in mitigating financial crime risks in Mauritius become increasingly apparent.

In conclusion, the identified research gaps underscore the pressing need for empirical investigations focused on Mauritius, particularly in the realm of leveraging innovative technologies like artificial intelligence for the prevention and detection of financial crimes. These gaps not only inform the trajectory of this study but also delineate avenues for future research endeavours aimed at enhancing the efficacy of anti-financial crime measures in the Mauritian context.

### **3.0 Methodology**

The aim of this quantitative study is rooted in a positivist and deductive approach, emphasizing factual exploration. Positivists typically favour quantitative research methodologies, leveraging surveys, statistics, and questionnaires for their reliability and representativeness. To glean insights into societal dynamics and uncover social patterns, the positivist tradition advocates for quantitative analyses, often through large-scale surveys. Accordingly, primary data will be procured via an explanatory survey, enabling researchers to delve deeply into the topic and elucidate hypotheses, facilitating replication studies for enhanced understanding. Additionally, the cross-sectional approach will be employed to examine the relationship between the dependent and independent variables. In cross-sectional studies, researchers analyse both results and exposures simultaneously within the population, without manipulating variables, to infer potential relationships and gather preliminary insights for further analysis.

This research will focus on collecting primary data from employees within registered accounting firms under the purview of the Mauritius Institute of Professional Accountants (MIPA), including accountants, auditors, forensic accountants, IT auditors, and compliance officers. Utilizing the Raosoft sample size calculator, with a margin of error of 10%, a confidence level of 90%, and a population size of 20,000, the study estimates a sample size of 96 respondents for the questionnaire. Various statistical methods, such as descriptive analysis, Cronbach's Alpha, Pearson's correlation coefficient, and multiple linear regression models, will be employed to comprehensively assess the numerical data.

The questionnaire comprises six sections totalling an estimated 37 questions. The initial section addresses demographic information such as name, age, gender, educational level, job title, and familiarity with Artificial Intelligence. Subsequent sections delve into the dependent variable—prevention and detection of financial crime—and the independent variables—Machine Learning, Robotic Process Automation, and Neural Networks. Data processing entails editing, coding, classification, tabulation, and diagrammatic representation. Moreover, to elucidate hypothetical relationships between dependent and independent variables, the study will employ SPSS software. In summation, this study adopts a rigorous and methodical approach to explore the intricacies of financial crime prevention and detection, leveraging quantitative methodologies to derive meaningful insights from the collected data.

### **4.0 Results, Findings and Discussions**

The objective of this chapter is to provide a comprehensive elucidation of the findings derived from hypothesis testing concerning the relationship between the dependent variable, namely the prevention and detection of financial crime, and the independent variables, namely Machine Learning, Robotic Process Automation, and Neural Network. This endeavour entails

a thorough analysis aimed at uncovering insights pivotal to the advancement of this research. The Pearson Correlation Coefficient will serve as a cornerstone in this chapter, enabling the quantification of the strength of relationships observed in the study. Additionally, the utilization of Multiple Linear Regression will complement these findings, bolstering the robustness and validity of the conclusions drawn herein. Undoubtedly, this section constitutes the crux of the chapter, as it encapsulates the primary findings germane to this research inquiry.

**Table 1: Reliability Test**

<b>Variables</b>	<b>Number of Items</b>	<b>Likert Scale</b>	<b>Cronbach's Alpha</b>
<b>Dependent Variable:</b>			
Financial Crime	9	1-5	0.874
<b>Independent Variable:</b>			
Machine Learning	8	1-5	0.908
Robotic Process Automation	8	1-5	0.917
Neural Network	7	1-5	0.921
<b>Overall Cronbach's Alpha</b>			<b>0.963</b>

*Source: Prepared by the Author (2022)*

The reliability test is the degree to which a scale generates consistent results when the same test is performed on the sample at multiple points. (Livingstone, 2018). The reliability test procedures also compute a variety of used measures of scale reliability as well as information on the relation between the variables. To test the reliability of the results, the Cronbach Alpha is used. Cronbach alpha is the most often used internal consistency metric ('reliability'). It is most typically used when many Likert questions create a scale in a survey/questionnaire to determine if the scale is reliable. Therefore, utilizing Cronbach's alpha will help to determine the reliability of the dependent variable which is the prevention and detection of financial crime, and the independent variable which is Machine learning, Robotic process automation, and Neural network. Theoretically, the Cronbach alpha reliability coefficient usually ranges from 0 to 1 and it can be negative as well. The general rule of thumb for a Cronbach alpha is that 0.70 and above is considered good, 0.80 is considered to be better and 0.90 and above is considered to be excellent. According to Table 1, the alpha values for financial crime, machine learning, robotic process automation, and neural network are respectively 0.874, 0.908, 0.917, and 0.921 with each variable above 0.70. Therefore, these values fulfill the range of Cronbach's Alpha. Likewise, the overall Cronbach's Alpha is 0.963 which is an acceptable value.

#### **4.1 Pearson Correlation Coefficient**

The Pearson Correlation Coefficient is also a statistical test that measures the statistical relationship or monotonic relationship between 2 continuous variables. Since this is based on the concept of covariance, it is regarded as the best approach to measure the relationship between the dependent variable and the independent variable. The monotonic relationship of a Pearson Correlation Coefficient means that as the value of one variable increases, the values of the other variable increase as well, or if the value of one variable increases, the other variable decreases. Therefore, in correlated data, if there is a change in one variable's magnitude then there will be a change in the magnitude of another variable either in the same direction or in the opposite.



The monotonic relationship between those 2 variables is actually a specific example of a linear relationship between the 2 variables that is in this case it is the dependent and independent variable (Schober, Boer and Schwarte, 2018). Hence, the range of correlation,  $r$  is between -1 to 1 as illustrated in Table 2 below. In addition, the two-tailed significance level is conducted in this chapter which is denoted by P- value. The p-value is a probability that compares the evidence to the null hypothesis ( $H_0$ ). A lower P-value gives more evidence against the null hypothesis. ( $H_0$ ). To determine the correlation, the P-value is compared to the significant level and it should be less than 0.05 ( $P < 0.05$ ) which proves that the relationship between the dependent and independent variables is significant. Therefore, the null hypothesis  $H_0$  is rejected, and the alternate hypothesis  $H_A$  is accepted. The P-value is mostly used to support the correlation as a very strong correlation does not necessarily mean that the relationship is significant.

**Table 2: Range of Correlation Coefficient,  $r$**

Pearson Correlation Coefficient, $r$	Relationship
$r=1$	Perfect relationship (Very strong correlation)
$r>0$	Positive relationship (strong correlation)
$r=0$	No relationship (No correlation)
$r=-1$	Negative relationship (No correlation)

*Source: Prepared by the Author (2022)*

**Table 3: Pearson's Correlation Coefficient**

Correlations					
		Financial crime	Machine learning	Robotic process automation	Neural Network
Financial crime	Pearson Correlation	1	.759**	.689**	.580**
	Sig. (2-tailed)		0	0	0
	N	125	125	125	125
Machine learning	Pearson Correlation	.759**	1	.844**	.716**
	Sig. (2-tailed)	0		0	0
	N	125	125	125	125
Robotic process automation	Pearson Correlation	.689**	.844**	1	.646**
	Sig. (2-tailed)	0	0		0
	N	125	125	125	125
Neural Network	Pearson Correlation	.580**	.716**	.646**	1
	Sig. (2-tailed)	0	0	0	
	N	125	125	125	125

*Source: Prepared by the Author (2022)*

According to Table 3 above, IV1 (Machine Learning) has demonstrated the strongest relationship with DV (financial crime) with a positive correlation of 0.759. It also implies that 75.9% of the variation in machine learning is expressed by the dependent variable. Lastly, as P-value is 0 which is less than 0.05 ( $P < 0.05$ ), it means that the correlation between the 2 variables is highly significant. With a correlation of 0.689, IV2 (Robotic process automation) has the strongest link with DV (financial crime). It can also be explained that the variation of 68.9% in Robotic Process Automation can be explained by the prevention and detection of financial crimes. The moderate strength of the link indicated that the variables were favourably or directly associated, as shown by the correlation coefficient's positive sign. Also, as P-value is 0 which is less than 0.05 ( $P < 0.05$ ), it means that the correlation between the 2 variables is highly significant. Finally, the last independent variable that is IV3 (Neural Network) shows the weakest relationship with the dependent variable which is a financial crime. There is a low positive correlation of 0.580 between financial crime and Neural Networks. However, it can be noted that P-value is less than 0.05 which means that there is enough evidence that the chance of odds is very limited as the correlation coefficient is highly significant.

#### 4.2 Multiple Linear Regression

To gain deeper insights into this research, multiple linear regression analysis is employed to elucidate the relationship between the dependent variable and the independent variables. This statistical technique involves fitting a linear equation to the data to ascertain the relationship between the two explanatory variables. As previously stated, each independent variable (X-value) is associated with a value of the dependent variable (Y-value). As depicted in Table 4, the correlation coefficient (R) signifies the strength of the relationship between the observed and predicted values. The range of R typically falls between -1 to 1, indicating whether the relationship between the variables is positive or negative. In this research, the R value is 0.766, indicating a high degree of positive correlation. Conversely, R squared ( $R^2$ ) is a statistical metric that measures the proportion of variation in the dependent variable (prevention and detection of financial crime) explained by the independent variables (Machine Learning, Robotic Process Automation, and Neural Network). Essentially,  $R^2$  indicates how well the data align with the regression model.

**Table 4: Model Summary<sup>B</sup> of Multiple Linear Regression**

Model	R	R square	Adjusted R <sup>2</sup>	Standard Error of the Estimate	Change statistics				
					R <sup>2</sup> Change	F Change	df1	df2	Sig. F Change
1	.766 <sup>a</sup>	.586	.576	.33980	0.586	57.100	3	121	0

a. Dependent Variable: Prevention and detection of financial crime

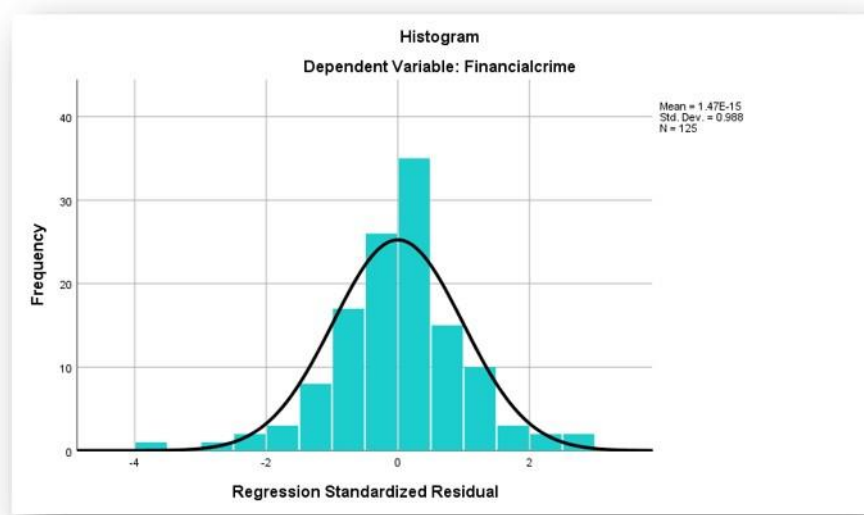
b. Predictors: (constant), Machine Learning, Robotic Process Automation, Neural Network

*Source: Prepared by the Author (2022)*

In this study, the  $R^2$  value stands at 0.586, signifying that the three independent variables collectively account for 58.6% of the variation in the dependent variable. Hence, it can be inferred that a significant relationship exists between the prevention and detection of financial crime and the independent variables. Nonetheless, the remaining 41.4% of variation in financial crime prevention and detection may be influenced by other factors.

Additionally, the bell-shaped curve depicted below illustrates the normal distribution of the dependent variable, i.e., financial crime. Notably, the curve exhibits symmetrical distribution on both sides. Researchers can utilize the empirical rule in statistics to ascertain the percentage of results falling within specific distances from the mean. The 68-95-99.7 rule, also known as the 3-sigma rule, delineates this distribution. Consequently, it can be inferred that the bell-shaped curve is perfectly symmetric, with 95% of values falling within 2 standard deviations from the mean. This translates to a 95% probability that a randomly selected score lies within -2 and +2 standard deviations from the mean (Mcleod, 2019).

**Figure 5: Histogram\_Dependent Variable**



*Source: Prepared by the Author (2022)*

### 4.3 Analysis of Variance Test (ANOVA)

According to Chanal and Steiner et al., (2022), Analysis of Variance (ANOVA) is a statistical method employed in hypothesis testing to ascertain the significance level of results and determine whether two or more means exhibit substantial differences. As illustrated in Table 5, the ANOVA table provides insights into how the regression equation captures the underlying data. The initial row of data is pivotal for assessing the predictive capacity of the regression model concerning the significance of the dependent variable. Of particular importance is the F-value, a key metric in regression analysis that evaluates the statistical significance of the independent variable's impact on the dependent variable. Furthermore, as elucidated by Thakur (2022), the F-value is derived by dividing the mean square by the mean square residual, facilitating the determination of overall result significance.

**Table 5: Analysis of Variance (Anova<sup>A</sup>)**

ANOVA <sup>a</sup>						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	19.779	3	6.593	57.100	.000 <sup>b</sup>
	Residual	13.971	121	.115		
	Total	33.750	124			
a. Dependent Variable: Prevention and detection of financial crime						
b. Predictors: (Constant), Neural Network, Robotic process automation, Machine learning						

*Source: Prepared by the Author (2022)*

In conjunction with the F-statistic, the P-value, denoted in the "Sig." column, serves as a critical indicator of significance. A P-value below the predetermined alpha level ( $P < 0.05$ ) indicates a lack of relationship between the independent and dependent variables, prompting rejection of the alternate hypothesis. The degrees of freedom (df) depicted in Table 5 reflect the extent of independence within the statistical data, signifying the number of variables that can vary independently. For this study, the df is calculated as 3, obtained by subtracting 1 from the total number of variables. Additionally, the residual degrees of freedom, computed based on the sample size of 125, amount to 124, underscoring the impact of sample size on df. The F-ratio, calculated as 57.100, attains significance at a P-value greater than or equal to 0.05. Consequently, with a significance level of 0.00, indicating rejection of the null hypothesis ( $H_0$ ) and acceptance of the alternate hypothesis ( $H_A$ ) at a 95% confidence level, it is inferred that a significant relationship exists between the dependent variable, prevention, and detection of financial crime in Mauritius, and the independent variables, Machine Learning, Robotic Process Automation, and Neural Network.

#### 4.4 Hypothesis Testing

##### **4.4.1 Relationship between Prevention and Detection of Financial Crime and Machine Learning**

- $H_{01}$ : There is no relationship between the prevention and detection of financial crimes and Machine learning in Mauritius.
- $H_{A1}$ : There is a relationship between the prevention and detection of financial crimes and Machine learning in Mauritius.

In this research, the null hypothesis  $H_{01}$  is rejected, and the alternate hypothesis  $H_{A1}$  is accepted, indicating a significant relationship between machine learning and the prevention and detection of financial crime in Mauritius. As elucidated by Priya and Saradha (2021), their study underscores a statistically significant correlation between the employment of machine learning techniques and the effectiveness of financial crime prevention and detection measures.

Their research findings illustrate that machine learning serves as an efficient model capable of identifying and mitigating financial crimes such as fraud by leveraging test data to yield more accurate, expedient, and efficient outcomes. Furthermore, the researchers assert that with the implementation of sophisticated machine learning algorithms, organizations can proactively combat fraudulent transactions and maintain a competitive edge against fraudulent actors. Notably, machine learning algorithms possess the capability to autonomously construct rules, thereby enhancing the detection of suspicious transactions, particularly in scenarios where transaction attributes are complex or certain transaction features remain obscured (Rakshit and Aslani et al., 2021). Moreover, Kaminski and Schonert (2018) highlight machine learning's pivotal role in bolstering the global effort to combat financial crimes. They emphasize that this advanced technology possesses the capacity to effectively manage vast volumes of both structured and unstructured data, allowing for the identification of patterns indicative of illicit financial behaviours. By leveraging machine learning algorithms, financial institutions and regulatory bodies can uncover nuanced insights into fraudulent activities, thereby enhancing their ability to detect and prevent financial crimes on a global scale.

#### **4.4.2 Relationship between prevention and detection of financial crime and Robotic process automation**

- $H_{02}$ : There is no relationship between the prevention and detection of financial crimes and Robotic process automation in Mauritius.
- $H_{A2}$ : There is a relationship between the prevention and detection of financial crimes and Robotic process automation in Mauritius.

In this study, the alternate hypothesis  $H_{A2}$  is accepted, while the null hypothesis  $H_{02}$  is rejected, indicating a significant relationship between the prevention and detection of financial crime in Mauritius and Robotic Process Automation (RPA). As affirmed by Aalst, Bichler et al. (2018), empirical evidence supports a positive correlation between the utilization of RPA and the effectiveness of financial crime prevention and detection measures. RPA aims to streamline organizational processes through automation, thereby reducing human interaction with computer systems. This approach is particularly pertinent given that common methods of concealing fraud involve the creation of fictitious physical documents, fraudulent transactions, and manipulation of accounting records among various firms. Thus, the findings of this research suggest that the automation capabilities inherent in RPA have the potential to mitigate the risk of financial crime.

Moreover, Hiregoudar et al. (2021) assert that RPA represents a cutting-edge technology for the detection of financial crime. With its ability to swiftly classify transactions with utmost accuracy and identify data manipulation with a single click, RPA emerges as a sophisticated tool for fraud detection. Additionally, Beena and Chopra et al. (2021) contribute further support to this hypothesis, highlighting RPA's ongoing evolution and its role in enhancing data quality, reducing manual errors, and providing expedited and secure services. Their findings underscore the potential of RPA to not only streamline operational processes but also to mitigate the risk of financial crime by leveraging its advanced automation capabilities. Overall, these insights underscore the significant potential of Robotic Process Automation as a valuable tool in the prevention and detection of financial crimes in Mauritius. By automating key processes and enhancing operational efficiency, RPA holds promise in bolstering the integrity of financial systems and mitigating fraudulent activities.

#### **4.4.3 Relationship between prevention and detection of financial crime and Neural Network**

- $H_{03}$ : There is no relationship between the prevention and detection of financial crimes and Neural Network in Mauritius.
- $H_{A3}$ : There is a relationship between the prevention and detection of financial crimes and Neural Network in Mauritius.

In this study, the null hypothesis  $H_{03}$  is rejected, while the alternate hypothesis  $H_{A3}$  is accepted, indicating a significant relationship between the prevention and detection of financial crime in Mauritius and Neural Networks. As previously elucidated in Chapter 2, Georgieva and Markova (2019) have affirmed a positive correlation between the utilization of Neural Networks and the efficacy of financial crime prevention and detection measures. Leveraging Neural Networks can offer substantial advantages in detecting fraudulent transactions by analysing transaction networks to identify abnormal patterns or behaviours. Moreover, Johnson and Khoshgoftaar (2019) have corroborated this finding, emphasizing a strong linear relationship between Neural Networks and the prevention and detection of financial crimes.

Their research demonstrates the effectiveness of Neural Networks in fraud detection, achieving a score of 0.8509 through the application of the random oversampling (ROS) technique to address class imbalance in training data. Furthermore, Gulati and Dubey et al. (2017) provide additional support to this hypothesis, reporting an impressive 80% accuracy rate in fraud detection utilizing Neural Networks with sample transaction data. Their findings underscore the potential of Neural Networks to effectively identify fraudulent activities within financial transactions. Additionally, Liu, Sun, and Zhang (2022) have contributed valuable insights by demonstrating the effectiveness of their model based on Neural Networks, known as the Hierarchical Attention-based Graph Neural Network (HA-GNN), in fraud detection. By aggregating neighbour information through various relations, HA-GNN exhibits significant potential in detecting fraudulent nodes with heightened accuracy and efficiency.

These collective findings highlight the pivotal role of Neural Networks as potent tools in the prevention and detection of financial crimes in Mauritius. Leveraging advanced technologies like Neural Networks can significantly enhance fraud detection capabilities and bolster the integrity of financial systems.

#### **5.0 Conclusion**

Being ranked as a high-risk third country by the European Commission (EC), the prevention and detection of financial crime is of paramount importance in Mauritius, particularly within the realm of accounting firms handling daily transactions. Artificial Intelligence (AI) has gained significant traction as a formidable tool in the ongoing battle against financial crime. Indeed, extensive research has delved into the relationship between AI and the prevention and detection of such illicit activities, with findings consistently indicating a positive correlation. In the present research paper, the researcher has proposed a comprehensive examination of three distinct branches of Artificial Intelligence: Machine Learning, Robotic Process Automation, and Neural Network. Through a quantitative study, it has been illuminated that all three independent variables exhibit a positive and statistically significant relationship with the prevention and detection of financial crime in Mauritius. This empirical evidence underscores the efficacy of leveraging AI technologies to bolster anti-financial crime measures.

Furthermore, the analysis reveals that Machine Learning emerges as the most influential variable, contributing a substantial 75.9% to the prevention and detection of financial crime. This highlights the pivotal role of Machine Learning algorithms in enhancing the efficacy of financial crime prevention and detection efforts. However, it is imperative to recognize the complementary significance of the other two variables—Robotic Process Automation and Neural Network. Despite their comparative contributions, both Robotic Process Automation and Neural Network play integral roles in fortifying the overall framework for combating financial crime in Mauritius.

In light of the foregoing insights, it is evident that the adoption of Artificial Intelligence technologies represents a promising avenue for augmenting financial crime prevention and detection strategies in Mauritius. By embracing AI-driven solutions comprehensively, stakeholders can better safeguard against the pernicious impacts of financial crime, thereby fostering a more resilient and secure financial landscape for all stakeholders.

### **5.1 Limitations**

The main limitation for this study is the absence of recent journals pertaining to Neural Network as for this study a set of journals as from 2015 to 2022 has been used in order to get a better insight on how Artificial Intelligence is helping to prevent and detect financial crimes. Moreover, there is a lack of published journals, articles and magazines when it comes to Mauritius, therefore, it was not easy to obtain facts and figures pertaining to financial crimes.

First and foremost, it is essential to acknowledge that this research on the prevention and detection of financial crimes is predicated on a limited scope, encompassing only three independent variables: Machine Learning, Robotic Process Automation, and Neural Networks. Such a restricted selection of independent variables may constrain the comprehensiveness of the study's findings and its ability to effectively evaluate the multifaceted landscape of financial crime prevention and detection. To enhance the robustness and relevance of future studies, it is imperative to incorporate more specific data and undertake comprehensive research endeavours.

Specifically, there is a pressing need to gather more nuanced information pertaining to the demographic landscape under scrutiny. By delving deeper into the demographic context, researchers can enrich the subject matter of their investigations, thereby offering more insightful and contextually relevant findings. Additionally, augmenting the literature review with a broader array of past studies will furnish researchers with a more comprehensive understanding of the existing body of knowledge, thus facilitating more informed analysis and interpretation.

Furthermore, the sample size of respondents utilized in this study, totaling 125 individuals, may be insufficient to yield statistically significant and reliable outcomes. Increasing the sample size is imperative to enhance the credibility and generalizability of the study's findings. Despite the challenges posed by the COVID-19 pandemic in gathering data, future researchers are urged to prioritize expanding the sample size to ensure greater accuracy and representativeness.

Moreover, it is noteworthy that this research predominantly focuses on approximately 162 accounting firms in Mauritius, a relatively narrow scope given the global prevalence of financial crime. To attain a more comprehensive understanding of this pervasive issue, future studies should aim to broaden the geographic reach or expand the organizational and national scope of inquiry. By diversifying the focus of research efforts, scholars can glean insights into a wider array of risk indicators and preventive measures pertinent to financial crime prevention and detection.

Lastly, while the utilization of the Statistical Package for Social Sciences (SPSS) for data analysis is common practice, it is essential to acknowledge potential inconsistencies that may arise. Future researchers are encouraged to explore alternative data processing tools to ensure the consistency and relevance of their results. By leveraging diverse methodologies and technologies, researchers can enhance the reliability and validity of their findings, thereby contributing to a more robust body of knowledge in the field of financial crime prevention and detection.

## **5.2 Recommendation**

As global digitalization continues its rapid advancement, the imperative to combat financial crime with cutting-edge technology becomes increasingly paramount. The proliferation of digital transactions, particularly in the realm of wire transfers, is witnessing a substantial surge, thereby exerting heightened pressure on accounting firms to effectively thwart and uncover financial crimes. This challenge is particularly pronounced for many accounting firms in Mauritius, where outdated tools and an underdeveloped services ecosystem still predominate, reliant on manual rule generation and lacking in self-learning capabilities. Compounding this challenge is the realization among criminals that technology can be exploited to their advantage, given the growing reliance on technology across firms.

Consequently, they have been able to orchestrate a wide array of fraudulent activities, leveraging the evolving landscape to their benefit. The ramifications of financial crime are profound, compelling many firms in Mauritius to allocate substantial financial resources, amounting to millions of Rupees, towards prevention efforts. However, amidst this complex landscape, Artificial Intelligence (AI) emerges as a proactive weapon in the fight against financial crimes. Recognized for its potential to revolutionize detection and prevention mechanisms, AI presents itself as an indispensable tool for accounting firms seeking to bolster their defences. Thus, it becomes imperative for firms to earnestly consider the integration of AI into their anti-financial crime strategies, recognizing its capacity to enhance efficacy and adaptability in combating evolving threats.

Furthermore, the early embrace of Artificial Intelligence is strongly advocated as a proactive measure to prevent and detect illicit activities. Currently, there exists a prevailing sentiment of apprehension rather than enthusiasm among employees regarding the adoption of technologies, with Artificial Intelligence often misconstrued as a potential replacement for roles such as accountants, auditors, and forensic accountants. Addressing this misconception is pivotal, and one effective approach involves instituting comprehensive training and awareness programs aimed at providing employees with a nuanced understanding of the capabilities of these advanced technologies. For instance, conducting awareness programs focused on the utilization of Artificial Intelligence can elucidate how its increasing integration enables firms to pivot towards delivering enhanced decision support, rather than being primarily engaged in data collection and manual analysis.



Moreover, the burgeoning utilization of AI necessitates a commensurate elevation in risk management practices within accounting firms, underpinned by robust governance frameworks and internal controls, thus fortifying defences against financial crimes. Additionally, firms should actively foster a culture that incentivizes and facilitates employee participation in AI-related training initiatives. Such endeavours encompass educating employees on how honing their proficiency in AI can augment their efficacy in day-to-day business operations. This concerted effort not only equips employees with the requisite skills but also fosters a mindset conducive to continuous learning and adaptation. By cultivating a "growth mindset" among employees, characterized by a readiness to embrace challenges and cultivate new competencies, firms can effectively navigate the evolving landscape shaped by technological advancements, thereby fortifying their resilience against financial crimes.

Incorporating this approach not only serves to educate employees about Artificial Intelligence but also enhances their skill sets, a critical component for investigators tasked with mitigating the risks associated with financial crimes and fulfilling their obligations in terms of detection and prevention. Financial crimes, while lacking a universal definition, are commonly understood as offenses with monetary ramifications. This broad categorization underscores the pervasive threat posed to firms engaged in daily transactions, as they remain susceptible to various forms of malfeasance, including corruption, money laundering, and fraud.

Compounding this challenge is the evolving sophistication of criminal tactics, which necessitates businesses to ensure that their workforce is adeptly equipped with the latest technological innovations to combat a diverse array of financial crimes. Artificial Intelligence emerges as a cornerstone in this endeavour, offering unparalleled capabilities in detecting patterns, anomalies, and trends indicative of illicit activities. By leveraging AI, businesses can fortify their defences against emerging and increasingly complex threats posed by criminals. Therefore, it becomes imperative for firms to invest in equipping their personnel with the requisite knowledge and skills to effectively utilize AI tools and technologies in their anti-financial crime efforts. This entails not only fostering a comprehensive understanding of AI's functionalities but also providing hands-on training to facilitate its practical application in investigative processes. Ultimately, by arming employees with cutting-edge technological tools such as Artificial Intelligence, businesses can bolster their resilience against financial crimes, safeguarding their assets, integrity, and reputation in an ever-evolving landscape fraught with risks and challenges.

Last but not least, the efficacy of such applications hinges significantly on the extent of support and the formulation of meaningful Artificial Intelligence-related policies by the government. Recognizing the transformative potential of Artificial Intelligence, the government of Mauritius has embarked on initiatives aimed at harnessing AI to foster sustainable development and enhance transparency in various accounting processes. Conscious of the imperative to remain abreast of global advancements, Mauritius is steadfast in its commitment to leveraging AI's profound impact. In the budget for 2018–19, the Prime Minister, the Honourable Pravind Jugnauth, underscored Mauritius' intent to establish the "Mauritius Artificial Intelligence Council" by 2025, signifying a proactive stance towards embracing AI-driven innovation. Complementing this initiative, the Mauritius Artificial Intelligence Strategy articulates a vision wherein AI serves as a linchpin of the nation's future development trajectory.

Recognizing AI's potential to drive growth, enhance productivity, and elevate living standards, the strategy delineates concrete measures aimed at achieving specific objectives, including the prevention and detection of financial crimes. Moreover, the consensus among stakeholders, as articulated by the working group (WG), underscores the transformative potential of AI and other cutting-edge technologies such as blockchain in addressing not only social and economic challenges but also in bolstering the resilience of financial institutions against the scourge of financial crimes plaguing the nation. Echoing this sentiment, the current Ministry of Technology and Innovation in Mauritius, led by Mr. Deepak Balgobin, espouses a fervent belief in AI's capacity to revolutionize the financial sector. Emphasizing its pivotal role in combating pervasive issues such as corruption and money laundering, Mr. Balgobin underscores AI's potential to reshape the financial landscape and usher in a new era of transparency and integrity. In sum, concerted governmental support and strategic policy frameworks are indispensable in harnessing the transformative potential of Artificial Intelligence to combat financial crimes and propel Mauritius towards a future characterized by innovation, inclusivity, and sustainable growth.

Conclusively, the mitigation of financial crime necessitates a concerted and collaborative effort among all pertinent stakeholders. Entities such as the Independent Commission, Statistic Mauritius, the Mauritius Revenue Authority (MRA), the Financial Intelligence Unit (FIU), the Competition Commission of Mauritius (CCM), and the Financial Service Commission (FSC) play pivotal roles in this endeavour. It is imperative that these entities engage in joint cooperation and coordination, leveraging their respective expertise and mandates to combat financial crime effectively. The imperative for collective action extends beyond these domestic agencies to encompass collaboration with international counterparts and regulatory bodies. By forging alliances with other institutions vested with law enforcement and regulatory authority, Mauritius can bolster its defences against financial crimes, thereby fostering a sustainable and resilient economy. In essence, the fight against financial crime demands a unified approach, wherein all relevant parties work in concert towards a shared goal of safeguarding the integrity of Mauritius' financial system and ensuring its long-term prosperity.

## 6.0 References

1. Aalst, W., Bichler, M., & Heinzl, A. (2022). Robotic Process Automation, 269-272. <https://doi.org/https://doi.org/10.1007/s12599-018-0542-4>
2. Acharuz, A., & Jhurry, D. (2018). Ncb.govmu.org. Retrieved from <https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf>.
3. Akinbowale, O., Klingelhöfer, H., & Zerihun, M. (2020). An Innovative Approach In Combating Economic Crime Using Forensic Accounting Techniques, 27(4), 1253-1271. <https://doi.org/10.1108/JFC-04-2020-0053>
4. Bedoya, O., Granados, O., & Burgos, J. (2020). AI Against Money Laundering Networks: The Colombian Case. <https://doi.org/10.1108/JMLC-04-2020-0033>
5. Beena, F., & Chopra, D. (2021). Robotic Process Automation in Banking and Finance Sector For Loan Processing And Fraud Detection. <https://doi.org/http://dx.doi.org/10.1109/ICRITO51393.2021.9596076>
6. Chanal, D., Steiner, N., Petrone, R., Chamagne, D., & Péra, M. (2022). Online Diagnosis Of PEM Fuel Cell By Fuzzy C-Means Clustering, 2, 359-393. <https://doi.org/https://doi.org/10.1016/B978-0-12-819723-3.00099-8>
7. Chelin, R. (2020). Bribe comes before a fall in Mauritius - ENACT Africa. ENACT Africa. Retrieved from <https://enactafrica.org/enact-observer/bribe-comes-before-a-fall-in-mauritius>.

9. Cusack, Ramgoolam, & M'crystal. (2020). Financial Crime Threat Assessment Mauritius, 2-33. <https://thefinancialcrimenews.com/wp-content/uploads/2020/06/Mauritius-Final-Long-Form-2020.pdf>.
10. Daliri, S. (2020). Using Harmony Search Algorithm In Neural Networks To Improve Fraud Detection In Banking System Sajjad, 2020, 2-5. <https://doi.org/10.1155/2020/6503459>. Fakun, N. (2018). Offshore and Money Laundering: a hanging sword over Mauritius. Le Defi Media Group. <https://defimedia.info/offshore-and-money-laundering-hanging-sword-over-mauritius>.
11. Fauzi, F., Szulczyk, K., & Basyith, A. (2018). Moving In the Right Direction To Fight Financial Crime: Prevention And Detection, 25(2), 362-368. <https://doi.org/10.1108/JFC-06-2017-0060>
12. Fakun, N. (2018). Offshore and Money Laundering: a hanging sword over Mauritius. Le Defi Media Group. <https://defimedia.info/offshore-and-money-laundering-hanging-sword-overmauritius>.
13. Gabrielli, G., & Medioli, A. (2019). An Overview of Instruments and Tools To Detect Fraudulent Financial Statements, 7(3), 76-82. <https://doi.org/10.13189/ujaf.2019.070302>
14. Georgieva, S., Markova, M., & Pavlov, V. (2019). Using Neural Network for Credit Card Fraud Detection, (2159), 1-11. <https://doi.org/10.1063/1.5127478>
15. Griffiths, L., & Pretorius, H. (2021). Implementing Robotic Process Automation for Auditing and Fraud Control, 1-11. <https://doi.org/10.1007/978-3-030-86761-4>
16. Gulati, A., Dubey, P., MdFuzail, C., Norman, J., & Mangayarkarasi, R. (2017). Credit Card FraudDetection Using Neural Network and Geolocation, 263(4), 1-6.
  - a. <https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042039>.
17. Halbouni, S., Obeid, N., & Garbou, A. (2016). Corporate Governance and Information Technologyin FraudPrevention And Detection Evidence From TheUAE, 32(6-7), 589-628.
  - a. <https://doi.org/10.1108/MAJ-02-2015-1163>
18. Hiregoudar, S., & Jadhav, S. (2021). Vehicle Insurance Fraud Detection System Using Robotic Process Automation and Machine Learning, 1-5. <https://doi.org/https://doi.org/10.1109/CONIT51480.2021.9498507>
19. Hassan, M., & Abdulrahman, A. (2019). The Impact Of Artificial Intelligence ( AI ) In Detecting Fraud In The UAE, 1-19. [https://www.eimj.org/uplode/images/photo/The impact of Artificial Intelligence AI in detecti ng fraud in the UAE..pdf](https://www.eimj.org/uplode/images/photo/The%20impact%20of%20Artificial%20Intelligence%20AI%20in%20detecti%20ng%20fraud%20in%20the%20UAE..pdf).
20. Johnson, J., & Khoshgoftaar, T. (2019). Medicare Fraud Detection Using Neural Networks, 1-35. <https://doi.org/https://doi.org/10.1186/s40537-019-0225-0>
21. Jullum, M., Loland, A., & Huseby, R. (2020). Detecting Money Laundering Transactions with Machine Learning, 23(1), 173-186. <https://doi.org/10.1108/JMLC-07-2019-0055>
22. Jung, J., & Lee, J. (2017). Contemporary financial crime”, Journal of Public Administration andGovernance, 7(2), 88-97. <https://doi.org/10.5296/jpag.v7i2.11219>
23. Kaminski, P., & Schonert, J. (2018). MONITORING MONEY-LAUNDERING RISK WITH MACHINE LEARNING, 1-2. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20analytics/our%20insights/ais%20growing%20impact/ais-growing-impact.pdf?shouldIndex=false>.
24. Karimi, A., Abbasabadei, S., Torkestani, J., & Zarafshan, F. (2020). Cybercrime Detection Using Semi-Supervised Neural Network, 29(2), 155-183. <https://doi.org/10.48550/arXiv.2202.00182>.

26. Kunwar, M. (2019). Artificial Intelligence In Finance: Understanding How Automation And Machine Learning Is Transforming The Financial Industry, 1-39.
  - a. <https://www.theseus.fi/handle/10024/>.
27. Kumar, A. (2022). Degree of Freedom in Statistics: Meaning & Examples. Data Analytics Data, Data Science, Machine Learning, AI. Retrieved from <https://vitalflux.com/degree-of-freedom-in-statistics-meaning-examples/>.
28. Kumari, M. (2019). Application Of Machine Learning and Deep Learning In Cybercrime Prevention – A Study, 1-4. <http://www.ijtrd.com/papers/IJTRD20407.pdf>.
29. Liu, Y., Sun, Z., & Zhang, W. (2022). Improving Fraud Detection Via Hierarchical Attention-Based Graph Neural Network, 1-11. <https://doi.org/https://doi.org/10.48550/arXiv.2202.06096>
30. Li, J., & He, P. (2020). Detection And Prevention of Cyber Crime Based on Diamond Factor Neural Network, 1437(1), 1-10. <https://doi.org/10.1088/1742-6596/1437/1/012011>
31. Livingston, S. (2018). Test Reliability—Basic Concepts, 1-46.
  - a. <https://www.ets.org/Media/Research/pdf/RM-18-01.pdf>.
32. Lokanan, M., & Tran, V. (2019). Detecting Anomalies In Financial Statements Using Machine Learning Algorithm The Case Of Vietnamese Listed Firms, 4(2), 181-201.
  - a. <https://doi.org/10.1108/ajar-09-2018-0032>
33. Lukito, A. (2016). Building Anti-Corruption Compliance Through National Integrity System In Indonesia: A Way To Fight Against Corruption, 23(4), 932-947. <https://doi.org/10.1108/JFC-09-2015-0054>
34. McLeod, D. (2019). Introduction to Normal Distribution (Bell Curve). Simplypsychology.org. Retrieved from <https://www.simplypsychology.org/normal-distribution.html#:~:text=The%20normal%20distribution%20is%20a,the%20curve%20sums%20to%20one>.
35. Minastireanu, E., & Mesnita, G. (2019). An Analysis of The Most Used Machine Learning Algorithms for Online Fraud Detection, 23(1/2019), 5-16.
  - a. <https://doi.org/10.12948/issn14531305/23.1.2019.01>
36. Noor, N., & Mansor, N. (2019). Exploring The Adaptation of Artificial Intelligence In Whistleblowing Practice Of The Internal Auditors In Malaysia, 163, 434-439.
  - a. <https://doi.org/10.1016/j.procs.2019.12.126>
37. Patil, N., Kamanavalli, S., Jadhav, S., Kanakraddi, S., & Hiremath, N. (2021). Vehicle Insurance Fraud Detection System Using Robotic Process Automation and Machine Learning, 1-5. <https://doi.org/10.1109/CONIT51480.2021.9498507>
38. Priya, G., & Saradha, S. (2021). Fraud Detection and Prevention Using Machine Learning Algorithms: A Review, 564-568. <https://doi.org/10.1109/ICEES51510.2021.9383631>.
39. PwC, (2020). PwC's Global Economic Crime and Fraud Survey 2020: Fighting fraud: A never-ending battle. <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>
40. Raghavan, P., & Gayar, N. (2019). Fraud Detection Using Machine Learning and Deep Learning, 334-339. <https://doi.org/10.1109/ICCIKE47802.2019.9004231>
41. Rakshit, S., Aslani, B., Rajah, E., & Vajjhala, N. (2021). Exploring The Role Of Artificial Intelligence And Machine Learning For Financial Intelligence In Nigeria, 1-5.
  - a. <https://doi.org/http://dx.doi.org/10.2139/ssrn.3833466>

43. Riany, M., Sukmadilaga, C., & Yunita, D. (2021). Detecting Fraudulent Financial Reporting Using Artificial Neural Network, 4(2), 60-69. <https://jurnal.unpad.ac.id/jaab/article/view/34914>.
44. Sujeewa, G., Yajid, M., Khatibi, A., Azam, S., & Dharmaratne, I. (2018). *THE NEW FRAUD TRIANGLE THEORY - INTEGRATING ETHICAL VALUES OF EMPLOYEES*, 16(5), 52-57. [http://ijbel.com/wp-content/uploads/2018/08/ijbel5\\_216.pdf](http://ijbel.com/wp-content/uploads/2018/08/ijbel5_216.pdf).
45. Takyar A. (2018). What is Artificial Intelligence? Understand artificial intelligence in 5 minutes.
  - a. <https://www.leewayhertz.com/what-is-artificial-intelligence-understand-ai-in-5-minutes/>.
46. Thakur, M. (2022). F-Test Formula | How to Calculate F-Test (Examples with Excel Template).EDUCBA. Retrieved from <https://www.educba.com/f-test-formula/>.
47. 44. Thekkethil, M., Shukla, V., (2021), 1-6. <https://doi.org/10.1109/icrito51393.2021.9596076>  
Wilson,
  - a. J. (2010) “Essentials of Business Research: A Guide to Doing Your Research Project” SAGE Publications, pp.7
48. Yeoh, P. (2019). Artificial Intelligence: Accelerator or Panacea for Financial Crime? 26(2), 634-646. <https://doi.org/10.1108/JFC-08-2018-0077>
49. Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2019). A Model Based on Siamese Neural Network for Online Transaction Fraud Detection, 2018, 1-9. <https://doi.org/10.1109/IJCNN.2019.8852295>

---

For instructions on how to order reprints of this article, please visit our website: <https://ejbm.apu.edu.my/> ©Asia Pacific University of Technology and Innovation