Development of a multi-objectives integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation

Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer and Mulatu Fekadu Zerihun

Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa

Abstract

Purpose – This study aims to investigate the feasibility of employing a multi-objectives integer-programming model for effective allocation of resources for cyberfraud mitigation. The formulated objectives are the minimisation of the total allocation cost of the anti-fraud capacities and the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots.

Design/methodology/approach – From the literature survey conducted and primary qualitative data gathered from the 17 licenced banks in South Africa on fraud investigators, the suggested fraud investigators are the organisation's finance department, the internal audit committee, the external risk manager, accountants and forensic accountants. These five human resource capacities were considered for the formulation of the multi-objectives integer programming (MOIP) model. The MOIP model is employed for the optimisation of the employed capacities for cyberfraud mitigation to ensure the effective allocation and utilisation of human resources. Thus, the MOIP model is validated by a genetic algorithm (GA) solver to obtain the Pareto-optimum solution without the violation of the identified constraints.

Findings – The formulated objective functions are optimised simultaneously. The Pareto front for the two objectives of the MOIP model comprises the set of optimal solutions, which are not dominated by any other feasible solution. These are the feasible choices, which indicate the suitability of the MOIP to achieve the set objectives.

Practical implications – The results obtained indicate the feasibility of simultaneously achieving the minimisation of the total allocation cost of the anti-fraud capacities, or the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots – or the trade-off between them, if they cannot be reached simultaneously. This study recommends the use of an iterative MOIP framework for decision-makers which may aid decision-making with respect to the allocation and utilisation of human resources.

Originality/value – The originality of this work lies in the development of multi-objectives integer-programming model for effective allocation of resources for cyberfraud mitigation.

Keywords Cyberfraud, GA solver, MOIP model, Pareto front, Optimum solution

Paper type Research paper

Journal of Financial Crime
Vol. 30 No. 6, 2023
pp. 1720-1735
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-10-2022-0245

1. Introduction

Financial and economic crimes have reportedly had an adverse effect on the world's economy and the socio-economic environment (Saddiq and Bakar, 2019, p. 911). The increasing rate of economic crime because of lack of a suitable framework to tackle the challenge has contributed to the loss of reputation, and goodwill, customer dissatisfaction and financial loss in many financial organisations (Goel and Shawky, 2009, p. 404; Martin and Rice, 2011, p. 803; Saini *et al.*, 2012, p. 202; Kraemer-Mbula *et al.*, 2013, p. 544; Lagazio *et al.*, 2014, p. 60). Dlamini and Modise (2012, p. 1) explain that to reduce cyberfraud incidences, the first line of defence is cybersecurity. One type of fraud that is prevalent in banking institutions is cyberfraud. It is one of the ultimate challenges faced by many financial institutions and other corporate organisations. The crime is usually perpetrated using the internet or cyberspace and it involves unauthorised intrusion into personal or an organisation's information to swindle resources for personal benefit. It usually occurs whenever perpetrators explore internet connection to cyberspace or other ICT enabled outfits to commit fraud (Hunton, 2009, p. 532; Walden, 2007; Dalla and Geeta, 2013, p. 997; Akinbowale *et al.*, 2022).

Cyberfraud can be summarised as a criminal act that involves the use of information technology infrastructure to have unauthorised access to confidential information, illegal data interference and interception, computer or system interference, forgery and some electronic fraud (Tiwari *et al.*, 2016, p. 46). It comprises computer-enabled actions complemented with global networks either by definite entities or otherwise and has become a major challenge to law enforcement agencies globally (Okeshola and Adeta, 2013, p. 98; Monni and Sultana, 2016, p. 13; Meephlam, 2017, p. 17). Hence, the crime is digital in nature. The cyberspace is characterised by unethical practices, with cyberfraud on the increase over the years (Uma and Padmavathi, 2013, p. 39). This has led to the rapidly increasing number of cases of cyberattacks on both the advanced and emerging economies (Uma and Padmavathi, 2013, p. 392; Kshetri, 2019, p. 77). The exploitation of the cyberspace for cyberfraud such as securing information without authorisation, malware attacks, IP theft, fiscal fraud, extortion, online fraud, spying, disabling of networks, fake links, impersonation, data and cash theft are consequential to the customer, financial institution and the economy at large (Detica Limited, 2011, p. 1).

Several online fraud-related cases have been witnessed in the banking sector such as credit card fraud, ATM fraud, cyber money laundering, phishing, malware and hacking (Saleh *et al.*, 2017, p. 86; Rao, 2019; 148, p. 150; Okutan and Çebi, 2019; Ch *et al.*, 2020, p. 4). In general, the main aim of any type of fraud is to siphon money by intruding into an account of individual or bank or through other means. This is in agreement with Dzomira (2014, p. 17), who stated that online fraud can be classified into two types, namely: direct fraud (e.g. money laundering and embezzlement) and indirect fraud (e.g. identity theft, malware and phishing).

The South African Banking Risk Information Centre (SABRIC) (2020, p. 18) reported that in 2020, online fraud accounts for the smallest fraction of the reported digital banking crime incidences (1.1%), but has the highest percentage of gross loss (45.1%). On the other hand, mobile banking fraud accounts for 59.7% of the reported digital banking crime incidences with 14.8% of gross loss. This suggests that higher value of the fraudulent transactions were committed through online fraud compared to mobile banking fraud in 2020. In 2019, a total of 3,304 online fraud cases were reported which cost R 117,705,112 in gross sum, while in 2020, the number of reported online fraud incidences increased by 19% but with a 19% decrease in the gross sum losses (SABRIC, 2020, p. 18). For mobile banking fraud, a total of 12,575 cases were reported in 2020 which cost R 28,245,948 in gross loss, while in 2020, the

number of reported mobile banking fraud incidences by 67.66% with an increase in gross loss by 61.10% (SABRIC, 2020). According to SABRIC (2020, p. 18), the most common forms of digital banking crime are social engineering, phishing and vishing.

In combating cyberfraud, many activities may have to be executed simultaneously within a certain period by a limited number of human resources having different skills. This study proposes an approach for the allocation of multi-skilled human resources to combat cyberfraud, taking into consideration the fact the anti-fraud capacities have diverse ability, experience and knowledge. The multi-objectives integer programming (MOIP) model focuses on five categories of human resources: the organisation's finance department, the internal audit committee, the external risk manager, accountants and forensic accountants. It consists of two steps: firstly, the formulation of the objectives and the use of the Pareto front to obtain a set of non-dominated solutions. The purpose is to provide the decision makers with an iterative MOIP framework to aid decision-making with respect to the development of a work plan for the allocation and utilisation of human resources on a daily basis. This is to ensure a more effective response to cyberfraud incidences in all cyberfraud incident prone spots.

The aim of this study is to investigate the feasibility of employing a multi-objectives integer-programming model for effective allocation of resources for cyberfraud mitigation. Its motivation stems from the fact that a MOIP model is suitable for making decision about resource allocation and cost minimisation. The use of a MOIP model can address these two different objectives simultaneously. The findings from this study highlights the feasibility of the MOIP model to achieve the sated objectives or a trade-off between them.

The rest of the paper is organised as follows: the succeeding section (Section 2) presents an overview of some existing literature, while Section 3 presents the methodology employed for achieving the objective of the study. Section 4 presents the results obtained and discussion while the Section 5 presents the conclusion, recommendation, policy implications and direction for future study.

2. Literature review

This section presents the overview of the existing literature on the peculiarities of the South African context and of cyberfraud mitigation in financial institutions.

2.1 South African context

A report from the Barclays Africa Group Ltd. (2017a, p. 14) indicates that the emerging digital technologies have increased the scarcity of human resources in the areas of data analysis, IT and risk management in the banking sector. To tackle this challenge, in South Africa, for instance, the Amalgamated Bank of South Africa has made substantial investments in the development of human capacity and recruitment in the area of IT, data analytics and cyber security over the years (Barclays Africa Group Ltd., 2017b, p. 39). The banks also stresses the need for the integration of data, state-of-the-art infrastructure and human collaborations across all the networks to ensure effective relationships with the shareholder of the bank (Barclays Africa Group Ltd., 2017b, p. 35). Also, the First Rand Group indicates that their expenditure on human capacity development increased by 240% in 2017 (FirstRand Group Ltd., 2017, p. 9).

The Standard Bank in South Africa considers the acquisition of the relevant skills and expertise as a major concern in a bid to cope with the trend of digitisation. To cope with this challenge, they continuously develop training and skills development programs and partner with various universities in South Africa to develop IT curricula and upskilling programs to acquaint their staff with the emerging new IT business models (Standard Bank Group Ltd., 2016, p. 60). According to the Annual Report of the Standard Bank Group Ltd. (2016, p. 60),

Standard Bank places a high premium on the development of human capacity to keep their staff abreast of advanced technology and techniques to enhance effective operation and customers' satisfaction.

In two separate reports by Ernst and Young (2003) and KPMG (2001), the findings show apathy towards the act of reporting cybercrime incidents to the police for investigation. The reasons stated for this were that some organisational managers perceive this as an undue exposure of the weakness or vulnerability of the system to the public, which may undermine the integrity of the organisation and erode public confidence. The extant South African law on cybercrime is the law applicable to cybercriminals, indicating a maximum number of five years of imprisonment for culprits (Ajayi, 2016, p. 9); hence, the involvement of police in the process of investigation and prosecution is justifiable.

2.2 Cyberfraud Mitigation in financial institutions

Saddiq and Bakar (2019, p. 911) reported that the effect of cyberfraud on the financial institutions and the global economy is detrimental. Cyberfraud can be committed internally or outside an organisation (Modugu and Anyaduba, 2013, p. 282). An employee of the organisation can take advantage of easy access to the banks and customer information as well as weak internal controls to commit fraud.

This can be traced to the fact that internal employees have direct access to information and have a better knowledge of the control architecture of the organisation. This knowledge can be leveraged to invent cover-up schemes that can promote the affinity for continuous crime perpetration. However, the development of robust internal control measures, such as transaction approvals, close monitoring, intermittent monitoring, forensic investigation, periodic staff shuffles or redeployments may help curb internal fraud perpetration.

On the other hand, people outside an organisation can also exploit the weak security and anti-fraud measures of financial institutions to commit fraud. Some take advantage of customers' ignorance to commit fraud (Modugu and Anyaduba, 2013, pp. 282–283).

Balan *et al.* (2017, pp. 64–65) explain that customers are vulnerable to cyberfraud because of the lack of information, poor awareness, lack of online monitoring systems and poor real-time responses. This lends more credence to the fact that the banks need proper reinforcement of the existing security apparatus and intelligent systems to make them more proactive rather than being reactive to cyberfraud incidences:

> It was estimated that 80% of the cyber security breaches result directly or indirectly (i.e. through collaboration with external bodies) by the people within the organisation (Hinde, 2003, p. 664).

Skalak *et al.* (2011, p. 19) stated that auditors cannot prevent the occurrence of fraud but forensic accounting has a preventative capacity to stop fraud from occurring. Gray (2008, p. 116) indicates that the auditors can identify and prevent errors in financial statements but lack the capacity for fraud identification and mitigation, unlike the forensic accountants. The auditors can respond to fraud risk, while forensic accountants can investigate allegations, suspicions and evidence of fraud cases (Skalak *et al.*, 2011, p. 13). Likewise, Golden *et al.* (2006, p. 3) describe forensic accountants as knowledgeable investigators with a sound understanding of legal and financial frameworks, majorly employed for the detection, investigation and prevention of fraudulent-related activities. A forensic accounting investigator is a trained and experienced professional who specialises in the process of investigation and resolving suspected or alleged fraud cases through the analysis of document analysis which may include financial and nonfinancial information, cross-examination and third-party inquiries (Golden *et al.*, 2006, p. 3). Hence, the roles of forensic accounting have been identified as detection, investigation and deterrence of fraud

(Golden *et al.*, 2006, p. 22). Fraud-related cases can be handled by forensic accountants since fraud encompasses deliberate misappropriation of resources, acquisition of property via deception, misrepresentation of reports or concealment.

Hopkin (2010, pp. 255–256) indicates that financial institutions that do not have the required expertise to combat cyberfraud-related risks may consider outsourcing risk managers. According to Van der Voort *et al.* (2019, p. 376), a risk manager can manage the link between the risk regulation system, which places premium on public values, and the organisation. Risk managers are saddled with the responsibilities of implementing the processes of risk assessment and management, hence, they manage the expectations from the organisation, regulatory bodies and the environment (Van der Voort *et al.*, 2019, p. 377). The accounting officer has the ultimate responsibility for fraud risk management, and in a situation where the third-party risk management service is not provided as expected, the organisation may be vulnerable.

2.3 Multi-objectives integer programming model for effective allocation of resources for cyberfraud mitigation

Considering the dynamic nature of the business environment, there is a need for the optimisation of human capital and employees' expertise to effectively contain cyberfraud. Hence, the main objective of this study is to investigate the feasibility of employing a MOIP for effective allocation of resources for cyberfraud mitigation. Many works have been reported on the use of the MOIP model, GA, Pareto fronts and evolutionary algorithms for solving real life problems such as the minimisation or maximisation of variables such as time, revenue, cost and risk (Certa *et al.*, 2009; En-nahli *et al.*, 2015; Geng *et al.*, 2018; Amaral and Elias, 2019; Dong *et al.*, 2022). The results obtained from these studies indicates the feasibility of the MOIP, genetic algorithm (GA) and Pareto front techniques for selection of non-dominating solutions. Zhang *et al.* (2007) found that the use of NSGA-II, a fast-sorting multi-objective genetic algorithm outperform other techniques such as the Pareto algorithms, single-objective GA, Pareto GA and random search. Some authors reported that the use of Z3 and SMT [1] solvers boast of specialised algorithms for effective search of optimum solutions (Pitangueira *et al.*, 2016, 2017). However, the use of the MOIP–GA model for the allocation of anti-fraud capacities aimed at cyberfraud mitigation has not been sufficiently highlighted by the existing literature.

3. Methodology

This section is divided into two subsections, the first sub-section presents the research methodology in general (MOIP and GA) and the second one presents the model specifications in terms of the objectives and constraints.

3.1 Multi-objective interger programming model and the genetic algorithm

An MOIP model is employed for the optimisation of the employed capacities for cyberfraud mitigation to ensure the effective allocation and utilisation of human resources. Thus, the MOIP model, validated by a GA solver, is employed for the efficient allocation of human resources during cyberfraud mitigation. The reason for this is that MOIP involves the use of integer variables for discrete representations in which decision-makers have to deal with several objectives. It finds application in supply chain management, logistics, scheduling and financial planning (Özlen and Azizoğlu, 2009, p. 25). MOIP problems are usually in the form of a *go–no-go* integer problem (Caramia and Dell'Olmo, 2008, p. 11). Thus, in the context of this study, it is considered to be that either there is a cyberfraud occurrence or not. In addition, the decision to mobilise resources to tackle cyberfraud could also be categorised

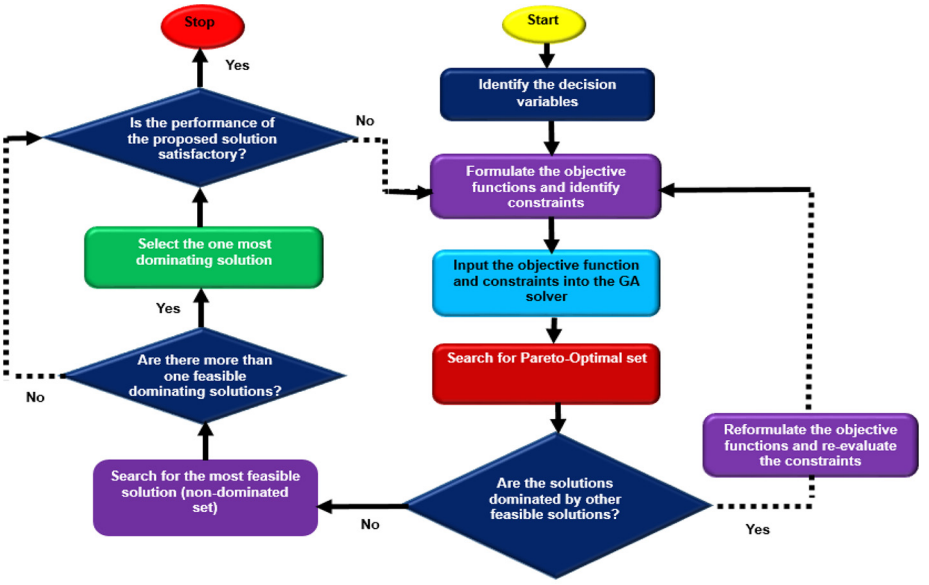
as a *go–no-go* integer problem. Hence, an MOIP may be suitable for the optimisation of the employed capacities for cyberfraud mitigation.

With respect to cyberfraud mitigation, there are conflicting objectives; hence, a MOIP approach was considered to ensure effective allocation and utilisation of the human resources. The development of a multi-objective integer programming approach may allow the decision-makers to achieve a balance between the objectives to make an informed decision relating to cyberfraud mitigation. The validation of the developed MOIP model, using the GA, determines the applicability of the proposed solutions in achieving the stated objective functions.

For this study, the formulated objectives are the minimisation of the total allocation cost of the anti-fraud capacities and the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots. The choice of the two objectives stems from the fact that, some financial institutions face challenges of inadequate resources relating to staffing and extended workloads, as well as financial resources (Dzomira, 2015, p. 9). Mac (2015) highlights effective employee allocation and human capacity development as part of the sustainable steps to cyberfraud mitigation.

Figure 1 presents the framework for the validation of the developed multi-objective integer programming model. This study demonstrates how a multi-objective problem relating to cyberfraud mitigation can be solved using the MOIP model. Therefore, it provides a practical guided approach of dealing with MOIP model with two objectives geared towards cyberfraud mitigation and presents an example. However, it can easily be extended to a general MOIP (or an multi objective mixed integer problem) with (many) more objectives.

The first step is the identification of the decision variables. These are captured in Table 1. Next is the formulation of the objective functions and the identification of the constraints.



Source: Authors' own

Figure 1.
Framework for the MOIP model validation

Notation or parameter	Description
G	Organisation's finance department
F	Internal audit committee
R	External risk manager
A	Accountant
Fa	Forensic accountant
Z	Nature of human resources for the investigation of cyberfraud (Index z): g, f, r, a and fa, where g, f, a and fa are internal anti-fraud personnels while r is external
N_c	Number of available human resources of types c, ∀c
I	Number of bank's branches, $i = 1, 2. \ldots I$
J	Number of shift of anti-fraud personnel, $j = 1, 2, 3$, i.e. $J = 3$
S	Types of cyberfraud occurrences, s = 1, 2,. . .. . .p
A_{ijz}	Minimum number of total human resources of type z to be allocated to i-th bank's branches and j-th shift
C^{α}	The cost of the employed capacities (both the hiring and operational cost of the anti-fraud personnel of type z). In this case, C^{g}, C^{f}, C^{r}, C^{a} *and* C^{fa} for the cost for the organisation's finance department, internal audit committee, risk manager, accountant and forensic accountant
RC_s^z	Average number of reported or suspected cyberfraud cases of type s by the anti-fraud personnel of type z
P_{ij}	P_{ij} is considered to be 1 if there is a possibility of a cyberfraud occurrence in i-th bank's branches and j-th shift, otherwise P_{ij} is taken as zero
d_{ij}	Minimum number of external risk managers and forensic accountants for cyberfraud investigation in i-th bank's branches and j-th shift
e_{ij}	Minimum number of forensic accountants for cyberfraud control in i-th bank's branches and j-th shift
SO_{ijs}	Cyberfraud occurrence of type s at in i-th bank's branches j-th shift $SO_{ijs} \in \{0, 1\}$. If cyberfraud occurs it takes the value of 1 otherwise 0
M_s	Minimum number of anti-fraud personnel to be deployed for cyberfraud incidences of type s
h_{ij}	Duration of cyberfraud investigation in i-th bank's branches and j-th shift

Table 1.
Notations and the parameters employed for the MOIP model

For this study, the formulated objectives are the minimisation of the total allocation cost of the anti-fraud capacities and the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots. The objective functions are given as in-outs into the GA solver in a MATLAB 2020 environment to search for the Pareto fronts. The constraints represent the minimum requirements of antifraud personnel allocated to the bank's branches and shifts as well as the mininum or manximum numbers of the anti-fraud capacities. The presence of a feasible solution that is not dominated by other feasible solutions indicates the feasibility of the developed MOIP model in achieving the set objectives. Otherwise, the objectives need to be reformulated with the constraints re-evaluated. This non-dominated set of solutions also represents the feasible ones.

A GA solver is stochastic in nature:

> A GA solver is a stochastic, population-based algorithm for solving optimisation problems that searches randomly by mutation and crossover among population members (Deep *et al.*, 2009, pp. 505-506).

It is perceived as an efficient tool for obtaining near-optimal or optimal solutions for a wide range of problems (Esbensen, 1995, p. 173; Barbozaa *et al.*, 2015, p. 563). Moreover, the GA solver is simpler for solution generation because it does not consider some of the constraints

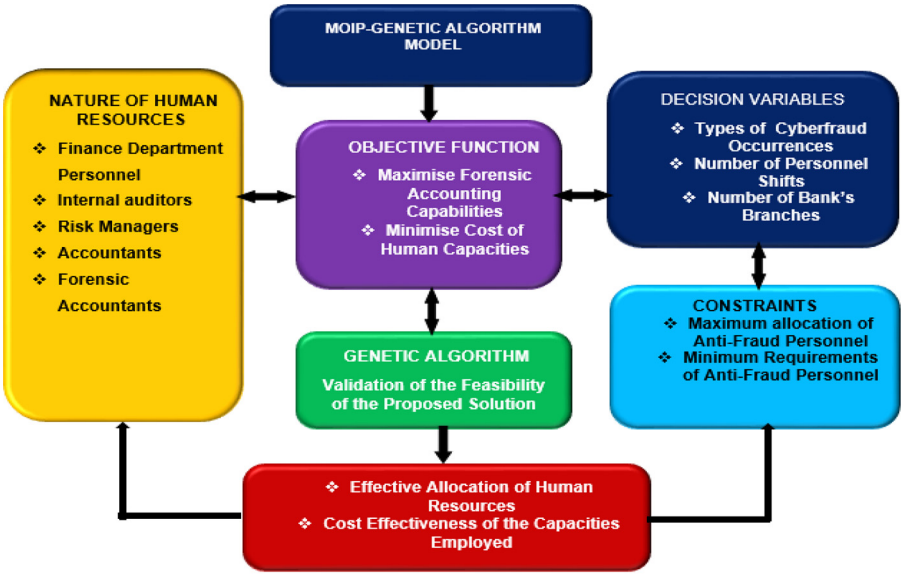
related to the conventional research techniques. In addition, it is capable of generating a solution to problems which cannot be resolved by other optimisation techniques (Barbozaa *et al.*, 2015, p. 563). The advantages of GA solvers, as indicated by Barbozaa *et al.* (2015, p. 563), inform the choice of the GA technique for solving the MOIP model developed in this study. The GA solver was employed in this study to determine the existence of feasible solutions. In other words, to determine the feasibility of:

- either simultaneously achieving the minimisation of the total allocation cost of the anti-fraud capacities and the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots; or
- the trade-off between them, if they cannot be reached simultaneously.

For the MOIP, the GA was also employed to search for a Pareto-optimum solution without the violation of the identified constraints. Hence, in case that a solution that optimises all the objective functions simultaneously does not exist, a GA solver finds the Pareto-optimal trade-offs between the two objective functions, i.e. the set of solutions that are not dominated by other feasible solutions (Deb, 2001). On the other hand, the Pareto front still represents feasible choices, indicating the suitability of the MOIP to achieve the set objectives without the violation of the stated constraints (Deb, 2001). In other words, the Pareto front shows the boundary defined by the set of all the points mapped by the Pareto optimal set (Deb, 2001).

The framework for the MOIP–GA model is presented in Figure 2.

3.1.2 Multi-objectives integer programming model specifications. Table 1 presents the notations and the parameters employed for the MOIP model. From the literature survey conducted, the suggested fraud investigators are the organisation's finance department, the internal audit committee, the external risk manager, accountants and forensic accountants (Ramaswamy, 2005; Skalak *et al.*, 2011, p. 19; Van der Voort *et al.*, 2019, p. 376;



Source: Authors' own

Figure 2.
MOIP–GA framework

Akinbowale *et al.*, 2020; Akinbowale *et al.*, 2021). Furthermore, a survey was carried out across the 17 licenced banks in South Africa on the fraud investigator. The primary qualitatitative data gathered from the survey identified the organisation's finance department, the internal audit committee, the external risk manager, accountants and forensic accountants as the major fraud investigators in the South African banking industries. This outcome of the survey was found to be in agreement with the literature; thus, these five human resource capacities were considered for the formulation of the MOIP models.

For the decision variables, $x^{z}_{ijk_z} = 1$, if k_c anti-fraud personnel of type z is to be allocated to i-th bank's branches and j-th shift; otherwise, $x^{z}_{ijk_z} = 0$.

From Table 1, the following mulit-objective functions are formulated to deal with the efficient allocation of human resources for mitigating cyberfraud and to minimise the cost of the employed capacities.

The first objective function (Z_1) is to minimise the total allocation cost of the antifraud capacities in all the bank's branches and shifts in a day (1).

$$min.Z_1 = \sum_{i=1}^{I}\sum_{j=1}^{3}\sum_{k_g=1}^{N_g} C^g x^g_{ijk_g} + \sum_{i=1}^{I}\sum_{j=1}^{3}\sum_{k_f=1}^{N_f} C^f x^f_{ijk_f} + \sum_{i=1}^{I}\sum_{j=1}^{3}\sum_{k_r=1}^{N_r} C^r x^r_{ijk_r} + \sum_{i=1}^{I}\sum_{j=1}^{3}\sum_{k_a=1}^{N_a} C^a x^a_{ijk_a} + \sum_{i=1}^{I}\sum_{j=1}^{3}\sum_{k_{fa}=1}^{N_{fa}} C^{fa} x^{fa}_{ijk_{fa}} \quad (1)$$

The essence of the first objective function (Z_1) according to (1) is to minimise the cost of the employed capacities (C^g, C^f, C^r, C^a *and* C^{fa}) for the organisation's finance department, internal audit committee, risk managers, accountants and forensic accountants.

The second objective function (Z_2) is to maximise the forensic accounting capacities in all cyberfraud incident prone spots (2).

$$max.Z_2 = \sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{k_{fa}=1}^{N_{fa}} \frac{P_{ij}}{h_{ij}}\ x^{fa}_{ijk_{fa}} \quad (2)$$

The essence of the second objective function (Z_2) according to (2), is to optimise the forensic accounting capacities for cyberfraud prevention and investigation.

The objective functions (Z_1 *and* Z_2) are subject to the following equation:

The first group of constraints (3) addresses the maximum allocation of the personnel to the shifts in a day.

$$\sum_{j=1}^{J} x^{c}_{ijk_c} \leq H,\ \forall H,\ k_c,\ c = g,\ f,\ r,\ a,\ fa \quad (3)$$

where H is the maximum number of shifts (H ≤ J).

These first constrainsts implies that any anti-fraud personnel from any of the five categories cannot be allocated to more than two shifts in a day out of the maximum possible three shifts (assuming an average of eight working hours in a shift per day). The model proposes a real time response to cyberfraud activities throughout the 24 h in a day.

The equations (4)–(8) represent the minimum requirements of antifraud personnel z allocated to i-th bank's branches and j-th shift. The assumption is based on the fact that the anti-fraud personnel have unique roles and responsibilities; hence, they are not substitutable.

The equation (4) indicate the minimum requirements for the organisation's finance department allocated to i-th bank's branches and j-th shift.

$$\sum_{k_g=1}^{N_g} x_{ijk_g}^{g} \geq A_{ijz} \quad i \in \{1,2\ldots,I\},\ j \in (1,2,3\},\ k_z \in N_z \tag{4}$$

The equation (5) stand for the minimum requirements for the internal audit committee allocated to i-th bank's branches and j-th shift.

$$\sum_{k_f=1}^{N_f} x_{ijk_f}^{f} \geq A_{ijz} \quad i \in \{1,2\ldots,I\},\ j \in (1,2,3\},\ k_z \in N_z \tag{5}$$

The equation (6) denote the minimum requirements for the risk managers allocated to i-th bank's branches and j-th shift.

$$\sum_{k_r=1}^{N_r} x_{ijk_r}^{r} \geq A_{ijz}\ i \in \{1,2\ldots,I\},\ j \in (1,2,3\},\ k_z \in N_z \tag{6}$$

The equation (7) indicate the minimum requirements for the accountants allocated to i-th bank's branches and j-th shift.

$$\sum_{k_a=1}^{N_a} x_{ijk_a}^{a} \geq A_{ijz}\ i \in \{1,2\ldots,I\},\ j \in (1,2,3\},\ k_z \in N_z \tag{7}$$

The equation (8) stand for the minimum requirements for the forensic accountants allocated to i-th bank's branches and j-th shift.

$$\sum_{k_{fa}=1}^{N_{fa}} x_{ijk_{fa}}^{fa} \geq A_{ijz}\ i \in \{1,2\ldots,I\},\ j \in (1,2,3\},\ k_z \in N_z \tag{8}$$

The equation (9) indicate the maximum allocation of z-th type of anti-fraud personnel to manage s-th type of cyberfraud occurrence in a j-th shift in i-th bank's branches.

$$\sum_{k_g=1}^{N_g} RC_s^g x_{ijk_g}^{g} + \sum_{k_f=1}^{N_f} RC_s^f x_{ijk_f}^{f} + \sum_{k_r=1}^{N_r} RC_s^r x_{ijk_r}^{r} + \sum_{k_a=1}^{N_a} RC_s^a x_{ijk_a}^{a} + \sum_{k_{fa}=1}^{N_{fa}} RC_s^{fa} x_{ijk_{fa}}^{fa} > SO_{ijs} M_s \quad i \in \{1,2\ldots,I\},\ j \in (1,2,3\} \tag{9}$$

The equation (10) indicate the minimum number of risk managers and forensic accountants for cyberfraud investigation in i-th bank's branches and j-th shift.

$$\sum_{k_r=1}^{N_r} x_{ijk_r}^{r} + \sum_{k_{fa}=1}^{N_{fa}} x_{ijk_{fa}}^{fa} \geq d_{ij}\ \forall i,j \tag{10}$$

The equation (11) indicate the minimum number of forensic accountants for cyberfraud control in i-th bank's branches and the j-th shift.

$$\sum_{k_{fa}=1}^{N_{fa}} x_{ijk_{fa}}^{fa} \geq e_{ij} \ \forall i,j \tag{11}$$

The non-negativity and integer equation are expressed under (12).

$$x_{ijk_c}^{c} \geq 0, x_{ijk_c}^{c} \text{ are integers} \tag{12}$$

These equation ensure that some of the identified anti-fraud personnel of type z are allocated to each of the branches of a bank and shifts.

4. Results and discussion

The results presented in Figure 3 show the validation of the MOIP model. The formulated objectives are the minimisation of the total allocation cost of the anti-fraud capacities and the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots. However, usually, it is impossible to obtain optimal solutions for a MOIP, which concurrently optimises all of the objective functions. Thus, the feasibility of the objectives is usually evaluated by Pareto-optimal solutions. The Pareto front represents the set of all the non-dominated feasible solutions, i.e. the best possible trade-off between the two objectives in trying to optimise them. Hence, the GA was employed to obtain these Pareto-optimum solutions (Pareto front) as presented in Figure 2 without violation of the identified constraints.

The points comprise the set of feasible solutions non-dominated by any other feasible solution. These are the feasible choices indicating the suitability of the MOIP to achieve the set objectives. Figure 3 shows that the Pareto front satisfies the stated constraints.

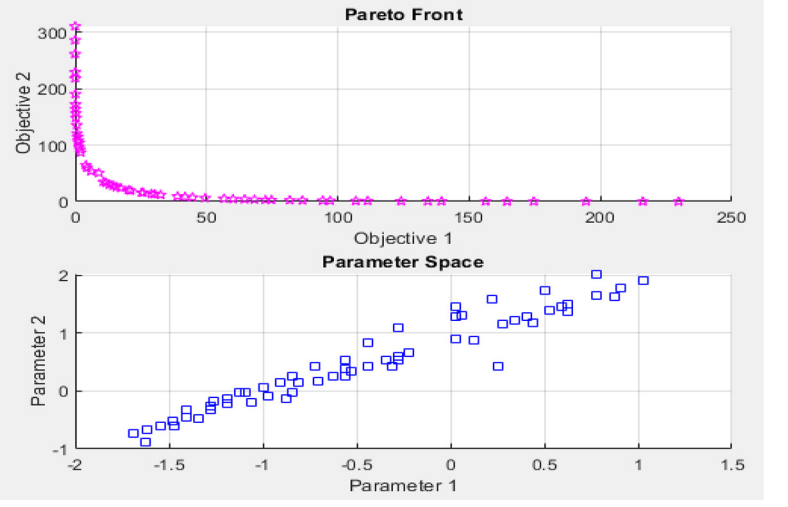


Figure 3.
Pareto front for the MOIP model

Table 2 presents the results obtained using the GA solver for obtaining the optimal solution for the MOIP model. The GA solver iterates by repeating the search to obtain the feasible ones. The total number of iterations carried out by the GA solver before obtaining the optimum set of solutions was 10. The F-count indicates the total number of points where evaluations take place in the search for optimum solution. The values of the F-count range from a minimum value of 60 at the first iteration to a maximum value of 2,312 at the tenth iteration. This denotes the number of evaluations carried out for each of the iterations. The total number of feasible solutions for each of the iterations varies from a minimum number of six at the first iteration to a maximum number of 60 at the tenth iteration.

The presence of the sets of solution from the Pareto fronts show the feasibility of the MOIP to achieve the set targets without the violation of the stated constraints (i.e. to simultaneously minimise the cost of employed human capacities and maximise the total number of available anti-fraud capacities, internal and external, for the mitigation of cyberfraud).

5. Conclusion and policy implications

The GA solver indicates the feasibility of simultaneously achieving the minimisation of the total allocation cost of the anti-fraud capacities, or the maximisation of the forensic accounting capacities in all cyberfraud incident prone spots – or the trade-off between them, if they cannot be reached simultaneously. Hence, the implementation of an MOIP model like the presented one for effective allocation and utilisation of human resources to combat cyberfraud is recommended.

For effective response to cyberfraud incidences in all cyberfraud incident prone spots, the decision-makers can use such an iterative MOIP framework to aid their decision-making on human resources allocation. This allows them to develop a work plan and schedule the anti-fraud capacities per shift on a daily basis based on their unique expertise. If implemented properly it may address the problem of shortage of human resources to respond in real time to cyberfraud incidences.

This may also enable the reinforcement of the existing security apparatus and intelligent systems thereby making it more proactive rather than being reactive. Future works can consider further validation of the developed MOIP model with the use of a quantitative data set.

Table 2. Results obtained from the optimal solution for the MOIP model

Iteration	Function count (*F* count)	No. of solutions	Spread	Volume
0	60	6	–	187,950
1	366	6	–	121,720
2	651	10	–	74,449
3	942	19	–	103,160
4	1,231	29	0.99969	103,680
5	1,523	36	0.14288	103,860
6	1,831	53	0.3962	104,000
7	2,012	60	0.9922	997,920
8	2,114	60	0.4404	113,230
9	2,210	60	0.99094	73,341
10	2,312	60	0.34173	89,643

Note

1. Z3 and SMT are solvers with specialized algorithms for solving background theories and opitmisation problems.

References

Ajayi, E.F.G. (2016), "Challenges to enforcement of cyber-crimes laws and policy", *Journal of Internet and Information Systems*, Vol. 6 No. 1, pp. 1-12.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020), "An innovative approach in combating economic crime using forensic accounting techniques", *Journal of Financial Crime*, Vol. 27 No. 4, pp. 1253-1271.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2021), "The integration of forensic accounting and the management control system as tools for combating cyberfraud", *Academy of Accounting and Financial Studies Journal*, Vol. 25 No. 2, pp. 1-14.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2022), "Analytical hierarchy process decision model and Pareto analysis for mitigating cybercrime in the financial sector", *Journal of Financial Crime*, Vol. 29 No. 3, pp. 884-1008.

Amaral, A. and Elias, G. (2019), "A risk-driven multi-objective evolutionary approach for selecting software requirements", *Evolutionary Intelligence*, Vol. 12 No. 3, pp. 421-444.

Balan, S., Otto, J., Minasian, E. and Aryal, A. (2017), "Data analysis of cybercrimes in businesses", *Information Technology and Management Science*, Vol. 20 No. 1, pp. 64-68.

Barbozaa, O.A., Junior, F.N., Bortolottia, S.L.V. and De Souza, R.A. (2015), "Mixed integer linear programming and genetic algorithm applied to storage and transportation problems in an oil industry", *Systems and Management*, Vol. 10, pp. 561-574.

Barclays Africa Group Ltd (2017a), "Integrated report", available at: www.barclaysafrica.com/content/dam/barclays-africa/bagl/pdf/results/annual/2017-integrated-report.pdf (accessed 16 November 2020).

Barclays Africa Group Ltd (2017b), "GRI report", available at: www.barclaysafrica.com/content/dam/barclays-africa/bagl/pdf/results/annual/2017-gri-report.pdf (accessed 16 November 2021).

Caramia, M. and Dell'Olmo, P. (2008), *Multi-Objective Management in Freight Logistics Increasing Capacity, Service Level and Safety with Optimization Algorithms*, 1st ed., Springer, London, XVI, p. 187.

Certa, A., Enea, M., Galante, G. and La Fata, C.M. (2009), "Multi-objective human resources allocation in R&D projects planning", *International Journal of Production Research*, Vol. 47 No. 13, pp. 3503-3523.

Ch, R., Gadekallu, T.R., Abidi, M.H. and Al-Ahmari, A. (2020), "Computational system to classify cyber crime offenses using machine learning", *Sustainability*, Vol. 12 No. 4087, pp. 1-16.

Dalla, E.H. and Geeta, M.S. (2013), "Cybercrime a threat to persons, property, government and societies", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3 No. 5, pp. 997-1002.

Deb, K. (2001), *Multi-Objective Optimization Using Evolutionary Algorithms*, John Wiley and Sons, Inc.

Deep, K., Singh, K.P., Kansal, M.L. and Mohan, C. (2009), "A real coded genetic algorithm for solving integer and mixed integer optimization problems", *Applied Mathematics and Computation*, Vol. 212, pp. 505-518.

Detica Limited (2011), *The Cost of Cybercrime*, United Kingdom, pp. 1-32.

Dlamini, Z. and Modise, M. (2012), "Cyber security awareness initiatives in South Africa: a synergy approach", *7th International Conference on Information Warfare and Security*, Seattle, USA, pp. 1-10.

Dong, S., Xue, Y., Brinkkemper, S. and Li, Y.-F. (2022), "Multi-objective integer programming approaches to next release problem – enhancing exact methods for finding whole Pareto front", *Information and Software Technology*, Vol. 147 No. 106825, pp. 1-14.

Dzomira, S. (2014), "Electronic fraud (cyber fraud) risk in the banking industry", *Zimbabwe. Risk Governance and Control: Financial Markets and Institutions*, Vol. 4 No. 2, pp. 16-26.

Dzomira, S. (2015), "Cyber-banking fraud risk mitigation conceptual model", *Banks and Bank Systems*, Vol. 10 No. 2, pp. 7-14.

En-Nahli, L., Allaoui, H. and Nouaouri, I. (2015), "Multi-objective modelling to human resource assignment and routing problem for home health care services", *IFAC-Papers OnLine*, Vol. 48-3, pp. 698-670.

Ernst and Young (2003), *Fraud: Unmanaged Risk. 8th Global Survey*, Global Investigations Dispute Advisory Services, South Africa, available at: www.whistleblowing.com.au/information/documents/EY8thGlobalSurvey2003.pdf (accessed 1 August 2020).

Esbensen, H. (1995), "Computing near-optimal solution to the Steiner problem in a graph using a genetic algorithm", *Networks*, Vol. 26 No. 4, pp. 173-185.

Firstrand Group Ltd (2017), "Annual integrated report", available at: www.firstrand.co.za/InvestorCentre/CurrentFSRannualreport/FirstRand/annual/integrated/report2017.pdf (accessed 16 November 2020).

Geng, J., Ying, S., Jia, X., Zhang, T., Liu, X., Guo, L. and Xuan, J. (2018), "Supporting many objective software requirements decision: an exploratory study on the next release problem", *IEEE Access*, Vol. 6, pp. 60547-60558.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on the firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.

Golden, T.W., Skalak, S. L. and Clayton, M.M. (2006), *A Guide to Forensic Accounting Investigation*, John Wiley and Sons, Inc., NJ, pp. 1-565.

Hinde, S. (2003), "Computer security: Mapping the future", *Computers and Security*, Vol. 22 No. 8, pp. 664-669.

Hopkin, P. (2010), *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, Kogan Page Limited, London, pp. 1-357.

Hunton, P. (2009), "The growing phenomenon of crime and the internet: a cybercrime execution and analysis model", *Computer Law and Security Review*, Vol. 25 No. 6, pp. 528-535.

KPMG (2001), "Global e-fraud survey, KPMG forensic and litigation services", available at: www.home.kpmg.com/xx/en/home/services/advisory/riskconsulting/forensic.html (accessed 1 August 2020).

Kraemer-Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change*, Vol. 80 No. 3, pp. 541-555.

Kshetri, N. (2019), "Cybercrime and cybersecurity in Africa", *Journal of Global Information Technology Management*, Vol. 22 No. 2, pp. 77-81.

Lagazio, M., Sherif, N. and Cushman, M. (2014), "A Multi-Level approach to understanding the impact of cybercrime on the financial sector", *Computers and Security*, Vol. 45, pp. 58-74.

Mac, F. (2015), "Fraud mitigation best practices", available at: www.freddiemac.com (accessed 7 July 2021).

Martin, N. and Rice, J. (2011), "Cybercrime: Understanding and addressing the concerns of stakeholders", *Computers and Security*, Vol. 30 No. 8, pp. 803-814.

Meephlam, P. (2017), "Challenges in internet fraud prosecution and investigation in Thailand: the perspective of Thai police officers", A Dissertation Submitted in Partial Fulfilment of Master of Science in Criminology and Criminal Justice, Durham University, pp. 1-100.

Modugu, K.P. and Anyaduba, J.O. (2013), "Forensic accounting and financial fraud in Nigeria: an empirical approach", *International Journal of Business and Social Science*, Vol. 4 No. 7, pp. 281-289.

Monni, S.S. and Sultana, A. (2016), "Investigating cyber bullying: pervasiveness, causes and socio-psychological impact on adolescent girls", *Journal of Public Administration and Governance*, Vol. 6 No. 4, pp. 1-26.

Okeshola, F.B. and Adeta, A.K. (2013), "The nature causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state", *Nigeria. American International Journal of Contemporary Research*, Vol. 3 No. 9, pp. 98-114.

Özlen, M. and Azizoğlu, M. (2009), "Multi-objective integer programming: a general approach for generating all non-dominated solutions", *European Journal of Operational Research*, Vol. 199 No. 1, pp. 25-35.

Pitangueira, A.M., Tonella, P., Susi, A., Maciel, R. and Barros, M. (2016), "Risk-aware multistakeholder next release planning using Multi-Objective optimization", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, Vol. 9619, pp. 3-18.

Pitangueira, A.M., Tonella, P., Susi, A., Maciel, R. and Barros, M. (2017), "Minimizing the stakeholder dissatisfaction risk in requirement selection for next release planning", *Information and Software Technology*, Vol. 87, pp. 104-118.

Ramaswamy, V. (2005), "Corporate governance and the forensic accountant", *CPA Journal*, Vol. 75 No. 3, pp. 68-70.

Rao, H.S. (2019), "Cyber crime in banking sector", *International Journal of Research - Granthaalayah*, Vol. 7 No. 1, pp. 148-161.

Saddiq, S.A. and Bakar, A.S.A. (2019), "Impact of economic and financial crimes on economic growth in emerging and developing countries: a systematic review", *Journal of Financial Crime*, Vol. 26 No. 3, pp. 910-920.

Saini, H., Rao, Y.S. and Panda, T.C. (2012), "Cyber-crimes and their impacts: a review", *International Journal of Engineering Research and Applications*, Vol. 2 No. 2, pp. 202-209.

Saleh, H., Rezk, A. and Barakat, S. (2017), "The impact of cyber crime on E-Commerce", *International Journal of Intelligent Computing and Information Science*, Vol. 17 No. 3, pp. 85-96.

Skalak, S.L., Alas, M.A. and Sellito, G. (2011), "Fraud: an introduction", in Golden Thomas, W., Skalak, Steven L. and Mona, M. Clayton (Eds), *A Guide to Forensic Accounting Investigation*, John Wiley and Sons. Inc., US., Hoboken, NJ, pp. 1-23.

South African Banking Risk Information Centre (SABRIC) (2020), "Annual crime statistics", available at: www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf (accessed 20 June 2022).

Standard Bank Group Ltd (2016), "Annual integrated report", available at: www.annualreport2016.standardbank.com/downloads/Standard_Bank_AIR_2016_Full_annual_integrated_report.pdf (accessed 16 November 2020).

Tiwari, S., Bhalla, A. and Rawat, R. (2016), "Cybercrime and security", *International of Advanced Research on Computer Science and Software Engineering*, Vol. 6 No. 4, pp. 46-52.

Uma, M. and Padmavathi, G. (2013), "A survey on various cyber-attacks and their classification", *International Journal of Network Security*, Vol. 15 No. 1, pp. 390-396.

Van der Voort, H., de Bruijne, M. and Steenhuisen, B. (2019), "Roles of risk managers: understanding how risk managers engage in regulation", *European Journal of Risk Regulation*, Vol. 10 No. 2, pp. 376-392.

Walden, I. (2007), *Computer Crimes and Digital Investigations*, Oxford University Press, Inc.

Zhang, Y., Harman, M. and Mansouri, S.A. (2007), "The Multi-Objective next release problem", *Proceedings of GECCO 2007: Genetic and Evolutionary Computation Conference, 2007*, pp. 1129-1137.

Further reading

Dlamini, S. and Mbambo, C. (2019), "Understanding policing of cybercrime in South Africa: the phenomena, challenges and effective responses", *Cogent Social Sciences*, Vol. 5 No. 1, pp. 1-13.

South African Banking Risk Information Centre (SABRIC) (2018), "Digital banking statistics", available at: www.icfp.co.za/article/sabric-digital-banking-crime-statistics (accessed 5 September 2020).

UK Finance (2020), "Overview of payment industry fraud", available at: www.ukfinance.org.uk (accessed 5 September 2020).

Corresponding author
Oluwatoyin Esther Akinbowale can be contacted at: oluwatee01@gmail.com