Neural networks: the panacea in fraud detection?

Maria Krambia-Kapardis
Cyprus University of Technology, Limassol, Cyprus, and
Chris Christodoulou and Michalis Agathocleous
Department of Computer Science, University of Cyprus, Nicosia, Cyprus

Abstract

Purpose – The purpose of the paper is to test the use of artificial neural networks (ANNs) as a tool in fraud detection.

Design/methodology/approach – Following a review of the relevant literature on fraud detection by auditors, the authors developed a questionnaire which they distributed to auditors attending a fraud detection seminar. The questionnaire was then used to develop seven ANNs to test the usage of these models in fraud detection.

Findings – Utilizing exogenous and endogenous factors as input variables to ANNs and in developing seven different models, an average of 90 per cent accuracy was found in the fraud detection prediction model. It has, therefore, been demonstrated that ANNs can be used by auditors to identify fraud-prone companies.

Originality/value – Whilst previous researchers have looked at empirical predictors of fraud, fraud risk assessment methods and mechanically fraud risk assessment methods, no other research has combined both exogenous and endogenous factors in developing ANNs to be used in fraud detection. Thus, auditors can use ANNs as complementary to other techniques at the planning stage of their audit to predict if a particular audit client is likely to have been victimized by a fraudster.

Keywords Neural nets, Fraud, Auditors, Financial reporting

Paper type Research paper

Economic crime is on the increase and no company is immune from falling victim to a fraudster. The recent global PricewaterhouseCoopers (2009) survey on fraud indicated that 30 per cent of the 3,000 respondents in 54 countries had fallen victim to fraud. Emerging economies appear to be at higher risk (Krambia-Kapardis and Zopiatis, 2010) and some industries are more prone to fraud than others (PricewaterhouseCoopers, 2009). Fraudulent scandals at the turn of the twenty-first century, caused by greed and fraudulent financial activities reduced public trust and the confidence of investors in annual reports and the services of auditors (Rezaee and Crumbley, 2007). Auditors play an important role “in protecting investors from receiving false, inaccurate, incomplete, and misleading financial information” (p. 45). Whilst it is not the auditor’s role to detect fraudulent financial reporting, they are expected to do so by the public. Rezaee and Crumbley argue that had the auditors had more skepticism and alertness, some of the recent audit failures could have been prevented. This alertness, however, should be prevalent from the beginning of the audit to enable auditors to plan their work in order to avoid inefficiencies in an audit.

In their The Philosophy of Auditing monograph, Mautz and Sharaf (1961, p. 131) pointed out that the probability of detecting fraud is a function of time pressures,
preventing chargeable costs from increasing, and the expectation of clients and the public alike that fraud will be identified by the auditor. By emphasizing close correlates of fraud detection, Mautz and Sharaf's work is relevant for the purpose of the present paper, because it can be said to have contributed to other researchers in later years putting forward more sophisticated prediction models of fraud detection (see below).

Fraudulent financial reporting is an intentional act which involves clever, educated individuals who are placed in a position of trust and can manipulate this trust with either political persuasion or intimidation, to benefit themselves or their company depending whether it is an occupational or organizational crime. Given the low incidence of detected fraud in companies, it is expected that auditors will lack the knowledge, skills and expertise to identify cues as far as fraud is concerned. Thus, a model needs to be developed to predict the likelihood of fraud so as to enable auditors to plan their work accordingly; furthermore, since the demand for audits in the future will be significantly affected by the extent to which auditors show themselves capable of detecting fraud (Carpenter, 2007, p. 1119). Research into fraud detection is decades old. Audit policies and procedures have been changing, the motivation for carrying our fraud research is high and the research itself constitutes a real challenge (Nieschwietz et al., 2000, p. 191). The authors of the current paper have decided to take an interdisciplinary approach with the use of artificial neural networks (ANNs) and develop a new approach into fraud detection.

Even though numerous alternative definitions exist for ANNs, one could simply define them as networks of parallel distributed processing elements (commonly referred to as “neurons”), which have a natural propensity for storing experiential knowledge and adaptively respond to inputs according to a learning process (Haykin, 2009; Ham and Kostanic, 2001). A number of inherent features of ANNs make them suitable for such a task and for a huge number of other applications (see, for example, Velido et al., 1999 and Paliwal and Kumar, 2009 for surveys). More specifically, in contrast to model-based techniques, ANNs are data-driven self-adaptive (through learning) systems, as they do not need any a priori assumptions with regards to the models of the scenarios being investigated, or if they do, they are minimal. ANNs can usually generalise pretty well after they are trained with a sample of the data, which could even be noisy (Haykin, 2009).

The term “noisy data” refers to the data that are affected by other variables. For example, a child can be trained to recognize his mother and, if the mother changes her hair style (which would make her face image “noisy”), the child would still recognize the face of his mother. Furthermore, one should note the fact that ANNs are nonlinear and universal functional approximators. For this to become clear, let us consider a particular application, such as determining the age of a person from face images (Lanitis et al., 2004). The data that are usually available for such an application is in the form of face images “input” and their corresponding ages “output”. Certainly, we know that there is a relationship between the face images and their corresponding ages, but this relationship is not immediately obvious and in mathematical terms is non-linear, i.e. we cannot find a linear function to relate the “output” to the “input”. The ANN in this sense is a non-linear functional approximator, as in this scenario, it will approximate the function that relates the face images with their corresponding ages and should be able to generalise after being trained, i.e. given a new face image (which was not part of the training set) to determine the age of the person in the image.
Moreover, ANNs are described as universal functional approximators since they can theoretically be used in any possible application where function approximation is required. As Green and Choi (1997, p. 15) explain, “The NN learns the pattern of input data in a learning fraud and nonfraud sample. The learned behavior pattern is then applied to a test fraud and nonfraud sample”. Given these advantages, ANNs have been applied to diverse real world applications including fraud detection (Lerouge et al., 1999), but in a different context to the one investigated in the current study. See below on how the current ANNs are different to the one suggested by Green and Choi (1997).

Building on the existing literature and for the first time, the present study set out to determine if NNs can be used by auditors to predict if fraud exists in their client so as to plan their audit accordingly. This model will be further discussed below. Questionnaires were given to auditors who were asked to answer it after thinking of a company which they had audited and had been victim to fraud and another one that had not been so victimized. The questions selected for the questionnaire were based on prior academic literature (Uzun et al., 2004; Makkawi and Schick, 2003; Saksena, 2003; Beasley, 1996) and from victimization studies (PricewaterhouseCoopers, 2009). The responses were then coded for analysis and, based on prior literature, a number of “questions were posed” to the NN (black box).

Literature review

The literature in the field on fraud detection has evolved over the years. Some authors have acknowledged that there are limitations in the way individual auditors make fraud judgments (Wilks and Zimbelman, 2004) and ultimately find it difficult to identify fraud (Carpenter, 2007; Knapp and Knapp, 2001; Pincus, 1989). Sorensen and Sorensen (1980) recommended the triangle approach as a method of enhancing fraud detection. The three parameters of the triangular approach are:

1. a strong, involved, investigative board of directors;
2. a sound, comprehensive system of internal controls; and
3. alert, capable independent auditors.

Whilst this sounds a logical approach, recent authors, including the present authors, have responded to the need to assist auditors further by developing fraud-risk assessment models that utilize certain cues to fraud.

Pincus (1989) was one of the first studies to investigate the usefulness of red flags in an experimental study. She found that the checklist approach resulted in greater comprehensiveness and uniformity in data acquisition but that it had no impact on no-fraud cases as well as a dysfunctional effect on fraud cases. While the red flag approach is not without its limitations (Krambia-Kapardis, 2002; Saksena, 2003), it is worth noting that utilizing such a method does raise the auditor’s sensitivity to the possibility of fraud. Despite the fact the red-flags approach has attracted a great deal of attention by researchers (Nieschwietz et al., 2000, p. 214), it should also be noted that if too many risk assessment cues with low diagnostic ability are used, then the accuracy in the auditor’s inherent risk assessment will be lower (Waller and Zimbelman, 2000). Loebbecke et al.’s (1989) assessment model is another suggested approach to assist auditors in detecting fraud. It is asserted that in order to detect fraud auditors need to assess the conditions that provide an incentive, the motives the perpetrator may have and finally the authority and responsibility the person may have that would allow him...
to commit the fraud. Similarly to the red flags approach, however, this method assumes that the auditor will be making an assessment on the environment or the individual likely to be committing the fraud.

Building on Loebbecke et al.’s (1989) work, Krambia-Kapardis’ (2001) eclectic fraud detection model asserts that in order to be able to detect fraud the auditor will need to initially utilize the rationalizations opportunity and person (ROP) risk assessment model and, second, identify the fraud risk information available. Using the ROP model, the auditor identifies the situational and company characteristics which provide the opportunity (O) for a person (P) with motives and crime-prone personality to commit the fraud and rationalize (R) his actions. The fraud risk information relates to endogenous risk factors in the auditee’s company such as internal control weaknesses, criminal record of employees, etc. Interestingly, researchers have also found that fraud is likely to be detected in the earlier years of the engagement rather than the latter (Mock and Wright, 1993; Loebbecke et al., 1989, p. 203). This may be due to the predictability of audit tests, or the fact that predecessor auditors may not have been allowed to pursue suspected frauds, emphasizing the importance of the planning process and that at the planning stage the audit team can determine the audit procedures to ensure efficiency and effectiveness in their procedures. Furthermore, if an auditor is under time pressure his awareness of fraud cues and detection decreases (Braun, 2000). Other inhibiting factors according to Bernardi (1994) are the auditors’ insensitivity to client integrity and competence.

Utilizing Statement of Auditing Standard No. 99 requirement that auditors should interact with their team members to discuss fraud and document that discussion (Carpenter, 2007) has tested the usefulness of brainstorming. The subjects were asked to perform analytical procedures on the case studies provided and then commence their brainstorming. Carpenter found that “audit teams generate more quality fraud ideas during the brainstorming session than the respective individual auditors” and that “interacting teams generally perform better than individuals” (p. 1136). One consideration as far as Carpenter’s methodology is concerned, is that the brainstorming can be useful for audit clients who are not the first-year audits and/or when the audit team is the same as prior years. In first year audits or where there has been a rotation of partners or audit team, brainstorming techniques will have some limitations.

Auditors need to assess the fraud risk accurately to avoid:

- having to carry out unnecessary audit work, thus affecting the budget of the audit; or
- not having carried out enough audit work with the risk of not having detected a material misstatement.

In considering either red flags, checklists or even assessing the likelihood of fraud, requires “knowledge, experience, reasoning” (Loebbecke et al., 1989, p. 3). Thus, assessing the level of risk and utilizing the above methods involves a high level of judgment. Wilks and Zimbelman (2004) argue that auditor’ tasks in fraud risk assessment, audit planning and audit plan implementation is inhibited when they use fraud checklists because the auditee can predict the audit procedures. They suggest auditors use strategic reasoning by taking into consideration various conditions that directly affect the auditee. One must not undermine the current economic crisis (Makkawi and Schick, 2003):
Auditors are caught on the horns of a dilemma. On one horn they are asked to do everything possible to prevent material financial statement fraud. On the other horn hangs the reality that auditing is a competitive business, subject to the same demands for profitability and the return on capital as other businesses. These economic demands create a conflict for auditors by constraining their ability to detect fraud (p. 591).

Thus, auditors need to find cost effective methods to enable them to predict at the planning stage of their audit if a prospective audit client is prone to fraud.

At this point it needs to be remembered that in securing corporate accountability, the external auditors’ responsibilities have been extended Porter (2009, p. 172). Whilst traditionally external auditors had focused their attention on “the audittees’ financial information” (p. 172), they are now explicitly expected to read “all the information that accompanies audited financial statements [...] to ensure it is not inconsistent with the financial statements and does not contain material misstatements of fact” (p. 172), including non-financial information in some jurisdictions. At a time of economic crisis, however, auditing does not cease being a competitive business subject to the same demands for profitability and the return on capital. By constraining their ability to detect fraud, the financial crisis creates a conflict for auditors as to the amount of work they should do (Makkawai and Schick, 2003, p. 591).

Regarding company characteristics that correlate with a high incidence of financial statement fraud, researchers have identified:

- companies with fewer audit committees, and where there were fewer meetings of audit committees (Saksena, 2003; Beasley, 1996);
- companies with an ineffective code of conduct, lower focus on ethical discernment and ethical misbehavior (Barlaup et al., 2009; Krambia-Kapardis and Kapardis, 2008);
- boards with proportionally fewer independent non-executive directors than executive directors (Uzun et al., 2004; Beasley et al., 2000);
- companies where there is substantial insider stock ownership (Makkawi and Schick, 2003, p. 592);
- some industries which are more prone to fraud than others (PricewaterhouseCoopers, 2009; Makkawi and Schick, 2003, p. 594);
- companies where the chief executive officer (CEO) hold a tenure position (Saksena, 2003); and/or
- companies with lower insider stock ownership (Saksena, 2003).

As will be shown below, in order to improve the effectiveness of audit plans to detect fraud, plans should be linked to risk assessment (Nieschwitz et al., 2000, p. 238). Examination of the models put forward to enhance fraud detection by auditors shows they have improved over the years from listing red flags and factors that inhibit audit effectiveness to cognitive models and the recent use of NNs.

Taking into account the merits of earlier models of fraud assessment, Nieschwitz’s et al. (2000) exhaustive list of difficulties in fraud detection (p. 207) and “empirical predictors of fraud, auditors unaided fraud risk assessments and mechanically aided fraud risk assessments” (p. 191) methods, the present authors suggest the use of NNs at the planning stage of an audit in order to enhance fraud detection.
Other studies have utilized NNs in the field of investigation (Lerouge et al., 1999; Taniguchi et al., 1998) but in a different context. However, the work thus far is limited because it addresses the usage of NN after the audit has been planned.

Green and Choi (1997) have utilized the information in financial statements as fraudulent signals in NN models. They have argued that whilst analytical procedures “possess both efficiency and effectiveness”, NN can prove useful in fraud detection. The success of NNs have already been tested in credit approval (Klimasauskas, 1991), bankruptcy prediction (Tam and Kiang, 1992), stock selection (Yoon et al., 1994) and automated trading (Trippi and DeSieno, 1992). Green and Choi have selected five ratios and used them as input variables in fraud. They have found that “NNs have significant potential as a fraud investigative and detection tool” (p. 26). To proceed to this level, however, one must wait for the year’s end to obtain all the financial information and by then it may be too late. An auditor would need to plan his audit and carry out interim audit reviews well before the year end. Analytical reviews can be used as predictors of fraud at the planning stage. However, there are two limitations to using analytical reviews. One being that management has control over the data and second external information is ignored (Nieschwietz et al., 2000).

The present authors maintain that utilizing NNs with macro rather than micro parameters, the auditors would be able to predict how probable fraud is to occur in a particular company and plan their audit accordingly. Given that the profession “has taken the approach that an auditor should plan the audit by first assessing the risk of fraud and then design the audit plan in response to that risk” (Nieschwietz et al., 2000, p. 191) it is argued that the work proposed will be very useful by auditors. Thus, it is hypothesized that audit firms may apply this innovative method of NN as complimentary to other techniques. The cost of developing/training an ANN is low and the auditors would determine at the outset if their audit client is likely to be a fraud victim by employees, management or a third party.

One can claim that just like a company would appoint an expert consultant (or forensic accountant) and provide him/her with information to determine if fraud is taking place the same could be done with ANNs. The expert will seek answers to a number of questions to predict if fraud exists. In using ANNs the auditor would answer for each of its audit client the list of questions posed in the Appendix. Once the answers are processed by the model the auditor will be told if that firm is likely to have fraud.

Methodology
The authors distributed 200 questionnaires to auditors who attended a seminar on fraud detection and prevention in Cyprus and 168 (84 per cent) completed questionnaires were returned. Of the 168 questionnaires, 30 per cent of them did not include a non-fraud case. However, since the prediction model is addressing fraud cases and not non-fraud cases it was felt that there were enough cases to train the black box. The number of responses appear adequate if one considers that Cyprus has a population of only 700,000 and only 2,500 qualified accountants. The auditors were asked to complete the questionnaire[1] by identifying one company that they had audited in the last five years that had fallen victim to a material fraud and a company that they audited which did not have fraud (A2). For the fraud companies, they were asked to state the industry (B1), the number of employees so as to distinguish small to large companies (B2), the type of fraud (B3), the opportunities provided which made
fraud easy to occur (B4) and the procedures followed when fraud was identified (B5). They were then asked to answer a series of questions regarding:

- whether a code of conduct existed in that organization (B6);
- whether an audit committee existed (B7);
- proportion of non-executive directors on the board (B8);
- proportion of independent non-executive directors on the board (B9);
- whether the CEO was tenured (B10);
- number of years the CEO was in the current position (B11); and
- total percent of share owned by management (B12).

The questions posed in the questionnaire were drawn from academic literature (Uzun et al., 2004; Makkawi and Schick, 2003; Saksera, 2003; Beasley, 1996) and from the fraud victimization study of PricewaterhouseCoopers (2009). No new questions were used since it was felt that these issues had been tested, these parameters were useful in determining if fraud is likely to occur. For the companies which did not experience fraud, the auditors were asked to state the industry (B1), the number of employees (i.e. the size of the company (B2)), the reasons why fraud was not possible (B4), what procedures did they expect would be followed if fraud was detected (B5) and, finally, the list of questions 1-7 above.

**ANNs as a fraud detection tool**

The type of the ANN used for detecting the fraud described above is the multilayer perceptron (MLP) with the error backpropagation (BP) learning algorithm (Rumelhart et al., 1986). Some basic features of this type of ANN will be given here (for a full description, see Haykin, 2009). The MLP ANN consists of an input layer of nodes or “neurons” (by analogy with their biological brain counterparts), one or two hidden layers and an output layer. Individual neurons take single or multiple inputs and produce an output which is a non-linear transformation of the product of the input values and their corresponding weights (i.e. the adjustable interconnection values). Neurons acting individually can only perform trivial functions, but in a network structure they could solve complex tasks. A typical MLP ANN architecture is shown in Figure 1.

Signal propagation through this network occurs as follows. The input vector values $x_i$ are entered through the input layer $i$. The layer $i$ neurons propagate the $x_i$ values to

![Figure 1. Typical architecture of a MLP ANN](image-url)
the hidden layer $j$ through the connecting links associated with weight vector values $v_{ij}$ that modify the propagated $x_i$ values. Every neuron of the hidden layer $j$ receives the summed product of the input values $x_i$ with the weight vector values $v_{ij}$ plus a bias term $b_j$ for each layer $j$ neuron. The result is passed through an activation function $f$, which generates the output of each hidden neuron $y_j$. Similarly, the $y_j$ values are multiplied with the weights $w_{jk}$ and summed together with a bias term $b_k$ for each layer $k$ neuron to give the final output $z_k$ of the network after passed through the activation function $f$. This can be described mathematically with the following equations:

$$y_i = f\left(\sum_i w_{ij}x_i + b_j\right)$$  \hspace{1cm} (1)

$$z_k = f\left(\sum_j v_{jk}y_j + b_k\right)$$  \hspace{1cm} (2)

Any monotonically increasing and continuously differentiable function can serve as an activation function for the MLP ANN with BP. For the work in the current study the sigmoid function is used, i.e.:

$$f(u) = \frac{1}{1 + e^{-\gamma u}}$$  \hspace{1cm} (3)

Where, $u$ stands for the terms in the brackets in equations (1) and (2) and $\gamma$ denotes the slope of the sigmoid. Owing to the fact that the values of sigmoid function operation range are within $[0, 1]$, for all $u$ values, the real (desired) output values used in both training and testing should be normalised in this range. Training in an MLP ANN means finding the right set of weight values that would give the desired output. The error BP learning algorithm has a feed-forward phase in which the external input factors passed through the neurons of the input layer are propagated forward and compute the actual output values at the output layer neurons according to equations (1) and (2). The backward phase follows, in which the weights of the ANN are modified according to the difference between the real (desired) and actual (computed) outputs at the output layer. It has to be noted that in our case the external input factors are the encoded possible answers to the relevant questions in the questionnaires, giving specific characteristics of a particular company, while the outputs encode the existence or of specific fraud problems. As mentioned in the introduction the ANN does not have any a priori knowledge regarding the solution. The weights are initialised with small random values and through an iterative training procedure they are adjusted so that the error function ($E$) which is the squared difference between the computed and the correct (as given from the data for which we have the correct answer) output ($t_k$) is minimised. More specifically, the adjustment to the weights for the output units is given by:

$$\Delta w_{kj} = \eta \delta_k y_j$$  \hspace{1cm} (4)

where:

$$\delta_k = Z_k(1 - Z_k)(t_k - Z_k)$$  \hspace{1cm} (5)
\( \Delta w_{kj} \) is the change to the weight from unit \( j \) to unit \( k \) and \( \eta \) is the learning rate. For the hidden units of the same network, through the error BP learning rule the adjustment to the weights leading to the hidden units can be written as:

\[
\Delta v_{ji} = \eta \delta_j x_i
\]

where:

\[
\delta_j = y_j (I - y_i) \sum_k \delta_k w_{kj}
\]

\( \Delta v_{ji} \) is the change to the weight from unit \( i \) to unit \( j \).

The above error BP learning equations have been derived by performing gradient descent on the \( E \) function (Rumelhart et al., 1986). Small values of the learning rate \( \eta \) in equations (4) and (5) enable the ANN to avoid oscillations in the weight adjustments, even though the number of iterations could be increased. The introduction of another term, called momentum may accelerate convergence by making the current weight change proportional to the previous weight change. In our current study the optimal values found and used for the learning rate and momentum are 0.7 and 0.6, respectively, for all the ANNs constructed.

The ANNs (MLP with BP type) constructed for the present study take as input a set of companies’ characteristics and try to determine if those companies will have fraud or not. More specifically, seven different ANNs were constructed which took as input specific characteristics of a company and attempted to give an answer to a specific question related to fraud. These seven specific questions are given in the first column (question) of Table I. The second column of Table I (input) lists the information characteristics of several companies that have been collected through questionnaires and represent the input of each ANN. In particular, each code B1-B12 (see “Methodology” section) represents a question from the questionnaire (see the Appendix) for which the answers have been encoded accordingly and used as inputs to the specific networks. Certainly, for each question of the first column of Table I (for which a separate ANN has been constructed), the relevant answers of the B questions were chosen as inputs which were considered as the factors that would affect the answer (output of the ANN) to each question. Similarly, the output column of Table I

<table>
<thead>
<tr>
<th>Question</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does fraud take place?</td>
<td>B1, B2, B6, B7, B8, B9, B10, B11, B12</td>
<td>A2</td>
</tr>
<tr>
<td>2. Which type of fraud is it?</td>
<td>B1, B2, B6, B7, B8, B9, B10, B11, B12</td>
<td>B3</td>
</tr>
<tr>
<td>3. Which industries are prone to fraud?</td>
<td>B2, B6, B7, B8, B9, B10, B11, B12, B3</td>
<td>B1</td>
</tr>
<tr>
<td>4. Small or large industries are prone to fraud?</td>
<td>B1, B6, B7, B8, B9, B10, B11, B12, B3</td>
<td>B2</td>
</tr>
<tr>
<td>5. If a company has an audit committee will it have fraud?</td>
<td>B1, B2, B6, B7, B8, B9, B10, B11, B12</td>
<td>A2</td>
</tr>
<tr>
<td>6. Which is the procedure to be followed if a company has fraud?</td>
<td>B1, B2, B6, B7, B8, B9, B10, B11, B12, B3</td>
<td>B5</td>
</tr>
<tr>
<td>7. What are the opportunities enabling fraud to occur?</td>
<td>B1, B2, B6, B7, B8, B9, B10, B11, B12, B3</td>
<td>B4</td>
</tr>
</tbody>
</table>

**Note:** See text for further details of A and B codes

---

Table I. Specific fraud-related questions which the ANNs attempt to answer and relevant inputs/outputs to the ANNs
represents the target output question for which the answers have been encoded and used as the target output for the training process of each ANN.

The encoding of the information from the questionnaires has been carried out as follows. Each question in the questionnaire (see “Methodology” section) has a specific set of possible variables/answers (through multiple-response questions). As mentioned above, the inputs to each specific ANN are a set of these answers of the relevant B questions (relevant being the ones specified at the input column of Table I). Question B1, for example, has eight possible answers[2]. This information is encoded in a binary vector of size three with possible values \{000, 001, 010, 011, 100, 101, 110, 111\}. In the same way we have encoded the answers of each B question with different vector sizes. Using this encoding, the input vectors would be specified by vector \( \mathbf{I} = (I_1, I_2, ..., I_n) \) where \( n \) is size of the input vector and \( I_i \) can either be 0 or 1 (binary). If we take the first ANN as an example which has as inputs the answers to the questions B1, B2, B6, B7, B8, B9, B10, B11, B12 (Table I), then the \( \mathbf{I} \) vector would be \( \mathbf{I} = (B1, B2, B6, B7, B8, B9, B10, B11, B12) \) with each B replaced by the appropriate vector of encoding the information of the specific answer as outlined above. In the same way, the output vector is the vector which illustrates the answer for the specific question (A or B) as listed in the output column of Table I.

The model (from now on called the black box) was to be trained to think like an expert and was to answer a number of questions (Table I). For instance, in answering the first question, if fraud is likely to take place it had to look at information provided by the respondents. Based on prior literature, the researchers identified the parameters used which would assist in determining if fraud is likely to take place. For instance, for the first question the parameters were:

- type of industry (B1) (PricewaterhouseCoopers, 2009; Makkawi and Schick, 2003);
- size of company (B2) (PricewaterhouseCoopers, 2009);
- existence of code of conduct (B6) (Krambia-Kapardis and Kapardis, 2008);
- existence of audit committee (B7) (Beasley, 1996; Saksena, 2003);
- proportion of non-executive directors on the board (B8) (Beasley et al., 2000; Uzun et al., 2004);
- proportion of independent non-executive directors on the board (B9) (Beasley et al., 2000; Uzun et al., 2004);
- whether the CEO was tenured (B10) (Saksena, 2003);
- number of years CEO in current position (B11) (Uzun et al., 2004); and
- total percentage of share owned by management (B12) (Saksena, 2003).

Thus, as mentioned in the description of the encoding of information above, for the first question, for example, the black box was trained with the answers to each of the parameters above as input and the desired output was the corresponding answer to Question 1, i.e. whether there existed fraud or not. After being trained, the black box would approximate the relationship of the input and output and would therefore be able to generalise, i.e. to determine whether fraud is likely to take place, if it were to be given a new case with similar characteristics/parameters.

Seven questions or problems were posed to each of the seven ANNs created for each question, namely: first, to determine if fraud is likely to take place; second, to work out
if employee/management fraud/or third party fraud is probable; third, if a particular industry is prone to fraud; fourth, whether the size of the audit client relates to fraud proneness; fifth, the correlation between audit committee and fraud; sixth, the likelihood of determining the procedure to be followed if a particular fraud does take place; and finally, predicting the opportunities enabling fraud.

The optimal architectural parameters found for the seven constructed ANNs (for answering the questions posed in the question column of Table I) are shown in Table II. The complexity of the problem led to the need to use two hidden layers of neurons in each constructed MLP ANN. Table II also shows the sizes of the input and output vectors of each of the seven ANNs which are determined by the inputs and outputs as specified in Table I.

**Results**

The initial results with the encoding as described in the previous section and by using two thirds of the available data for training and one-third for testing were not very accurate given that approximately only 60 per cent correct answers on average were obtained for each of the seven questions of Table I. This led to the evolving of the data pre-processing approach. More specifically, it was decided to recode the responses for questions $B3[3]$, $B4[4]$ and $B5[5]$ because of the enormous amount of information they contained in the case of a huge dataset (i.e. those questions had a lot of variables/answers).

There was also a missing value problem, caused by some unanswered questions from the 168 questionnaires available in the dataset. In the results quoted above (60 per cent) the missing value were replaced by random values within the range of the existing answers. However, this possibility did not seem realistic given the distribution of the answers within the existing data. This approach is standard for addressing missing values (Haykin, 2009). For dealing with this issue further, the distribution of each possible answer to each question was calculated and then the missing values of each question were replaced with possible answers according to the probability of having a specific answer. These two extra pre-processing procedures (also acceptable by the literature, see Haykin, 2009) increased the results to approximately 70 per cent correct answers on average for each of the seven questions of Table I.

The final set of results was taken by using the leave-one-out cross-validation procedure (Vapnik, 1998), given the small sample of the data available. With this method, the ANN is trained multiple times, using all but one of the samples of the dataset (168 questionnaires in our case, i.e. it is trained/tested 168 times). The performance of the ANN is tested on the removed data sample each time and the average is taken in the end. With the leave-one-out cross-validation the results are shown in Table III.

The percentage accuracy values are based on the probability of having a correct answer according to the real and predicted answer. Table III thus indicates that

<table>
<thead>
<tr>
<th>Type of parameter</th>
<th>NN according to Table I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of neurons for the 1st hidden layer</td>
<td>30 30 30 30 30 30 30</td>
</tr>
<tr>
<td>Number of neurons for the 2nd hidden layer</td>
<td>25 25 25 25 25 25 25</td>
</tr>
<tr>
<td>Size of input vector</td>
<td>17 17 17 17 17 20 20</td>
</tr>
<tr>
<td>Size of output vector</td>
<td>1  3  3  1  1  4  2</td>
</tr>
</tbody>
</table>

Table II. Optimal architectural parameters for the ANNs constructed and size of input/output vectors
the first ANN is 95 per cent correct in predicting if fraud is likely to take place. Thus, if
an auditor were to respond to the questions posed as parameters (Table I) for this ANN
question, the model has 95 per cent chance to provide him/her with the correct
prediction (i.e. that there exist fraud or no fraud exists). In the second question
posed ANNs will be 92 per cent accurate in predicting the type of fraud likely to take
place, etc.
These results are statistically significant (i.e. it is unlikely to have occurred by
chance) as they are averaged over ten times with the leave-one-out cross-validation
procedure, through which for our data samples the ANNs are trained/tested 168 times
(see previous paragraph). In other words, given that the results reported are effectively
obtained by averaging the outcome of the ANNs over 1,680 (168 × 10) times, it is indeed
unlikely to have occurred by chance and they are therefore statistically significant.
As shown in Table III, the accuracy level is rather high apart from the industry
variable. It is suggested that perhaps the industry accuracy response is 68 per cent and
not higher because there were many variables for ANNs to consider. If the industry
category was recoded and decreased from eight variables to say four to five then the
accuracy level would have been higher.
It can be seen that by excluding the industry question, on average the chance
of forming the wrong conclusion that there is no fraud when fraud exists is only
7 per cent on average. The fact that the current study has used both exogenous and
endogenous factors in developing fraud prediction ANNs is an advantage to Green and
Choi (1997) that have used five ratios as input variables. The input variables used in
the present study have been proven by previous researchers and professional surveys
of high correlation with fraud being present in an organization.

Discussion of findings and conclusions
Researchers thus far have used empirical predictors of fraud (e.g. Loebbecke et al.,
1989), fraud risk assessment methods (Carpenter, 2007) and mechanically fraud risk
assessment methods (Pincus, 1989). They all have had their strengths and weaknesses
yet fraud continues to be undetected and auditors are sued and run the risk of having
to pay large sums of money for failing to take reasonable care and skill. As indicated in
Table III, by using ANNs the auditors will be able to predict if fraud has taken place in
the firm they are planning an audit.
One may argue that because the study was carried out in an emerging economy the
findings cannot be representative. The global PricewaterhouseCoopers (2009) survey

<table>
<thead>
<tr>
<th>Question</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does fraud take place?</td>
<td>95</td>
</tr>
<tr>
<td>2. What type of fraud is it?</td>
<td>92</td>
</tr>
<tr>
<td>3. Which industries are prone to fraud?</td>
<td>68</td>
</tr>
<tr>
<td>4. Size of companies prone to fraud (Small &lt; 250 employees or large)</td>
<td>91</td>
</tr>
<tr>
<td>5. If a company has audit committee will it have fraud?</td>
<td>91</td>
</tr>
<tr>
<td>6. Which is the procedure to be followed if a company has fraud?</td>
<td>96</td>
</tr>
<tr>
<td>7. What are the opportunities enabling fraud to occur?</td>
<td>96</td>
</tr>
</tbody>
</table>

Note: In the Industry category there were eight variables thus it lowered the chance of accuracy. Had we recoded the data and merged industries then the percentage would have been higher.
has shown that fraud recognizes no boundaries while Krambia-Kapardis and Zopiatis (2010) have indicated that emerging economies are facing increased risks due to the size of the economy and the controls in place. Thus, fraud has no boundaries and auditors ought to begin to consider other methods to predict if fraud is likely to occur at their client since the existing methods have not proven to be very successful. The implications of the study for the auditors are that they need to look beyond existing audit procedures, and to utilize computing expertise in developing ANNs.

ANNs have been used by various companies for a variety of applications. To illustrate, Dai-ichi Kangyo Bank and Fujitsu developed a NN system for predicting the future yield of securities by predicting the interest rate on treasury bonds; Siemens/Siemens-Nixdorf developed a NN stock market prediction model for predicting the Deutscher Aktien IndeX (German Stock Exchange) as well as the DM-US$ exchange rate; Nikko Securities designed a NN system trained on the ratings of human experts (which grade debt securities with respect to the issuer’s ability to meet interest and principal requirements) for providing consultation for the ratings of convertible bonds; Sharp developed a single-touch microwave oven by training a NN to predict the correct power and time needed to re-heat pre-prepared food, on the basis of signals derived from a humidity sensor; various other consumer products using NNs on the market include, air-conditioners, electric carpets, electric fans, electric thermo-pots, desk-type electric heaters, kerosene fan heaters, induction heating cookers, Japanese word processors, etc. (Asakawa, 1993; Miyazaki, 1991); USAir uses a NN developed by BehavHeuristics to forecast airline passenger demand (BehavHeuristics press release July 8, 1994); VISA use a NN system for credit card fraud detection (NewsWeek, October 20, 1994, p. 34); Sharp are trading a NN Japanese optical character recognition system (Hammerstrom, 1993). ANNs are innovative, cost effective and as shown in this paper have high accuracy level in their predictions.

Audit firms (Big 4 or medium sized) can train ANNs to think based on their client base. The study reported in this paper has shown that ANNs and, more specifically, the current ANNs do have high accuracy level. Audit firms, however, in different countries depending on their client base can train an ANN to predict for their client if it is prone to fraud. They can respond to the questions posed in the questionnaire (since this questionnaire used international and not local literature) to train the ANNs and, before they begin planning their audit, they can input the information for a particular client of theirs and the black box will provide them with a prediction. This will assist them at the planning stage since they will assess how much work needs to be done and in which audit area.

A possible limitation of the modeling advocated in this paper is that every few years (or within a shorter period) the audit firm may need to retrain the ANNs depending on economic environments, new correlates of fraud identified, etc. Another limitation is that a generalised ANNs (unlike a check-list approach) cannot be developed by a Big 4 firm and be used by the same firm in another country. Thus, each firm in each country ought to train its own ANN. The findings obtained show that ANNs can have a high accuracy in predicting fraud and that if one were to use the same parameters as the present authors they would be able to have a 95 per cent accurate prediction. Finally, the present authors are confident that the current ANN can be applied by practitioners to save on audit costs and predict fraud cases.
Notes

1. Since a two-page front-back questionnaire was used, the researchers have no way of knowing which side the respondents completed first. The possibility of an order effect, i.e. that reading a fraud instead of non-fraud case first impacts on the results obtained cannot be excluded. However, by the same token, other respondents may well have read a non-fraud case first in which case any order effect would balance out.

2. B1 relates to the industry. The variables in this question were:
   - hospitality and tourism;
   - health;
   - automobile industry;
   - manufacturing;
   - banking and insurance company;
   - construction/defence;
   - retail/wholesale; and
   - real estate agent.

3. In B3, the types of fraud were recoded to enable the model to identify if fraud was likely to take place. For example, theft of cash was recoded to include (bounced cheques, petty cash fraud, payroll fraud and theft of cash); corruption was to include (corruption taken and given); theft of assets (comprised theft of assets and unnecessary purchases). Thus, the recoding provided only nine categories of fraud rather than 17.

4. In B4, the opportunities providing for fraud were initially six but the research team decided to separate them into endogenous and exogenous factors only thus enabling the model to have a better chance of providing accurate results. For example, endogenous factors were considered to be weak internal controls, collusion, weak information technology controls, corporate culture and type of business, whereas external factors were considered to be exogenous factors.

5. In B5, a list of 18 procedures followed by management once fraud detection was made. These variables were recoded into legal action taken, internal investigation, external investigation and no action.

References


Further reading
Appendix. Questionnaire

A. Demographics

1. Position of respondent. (please √)

<table>
<thead>
<tr>
<th>Accountant</th>
<th>Internal auditor</th>
<th>External auditor</th>
</tr>
</thead>
</table>

B. Think of one company/organisation that had material fraud being committed by its employees/management or others in the last 5 years

1. Type of organization. (please √)

<table>
<thead>
<tr>
<th>Hospitality and tourism</th>
<th>Health</th>
<th>Automobile and transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public sector/ Semi government</td>
<td>Banking/Finance/ Insurance</td>
<td>Construction/Real estate</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Retail/Wholesale</td>
<td></td>
</tr>
</tbody>
</table>

2. Number of employees. (please √)

<table>
<thead>
<tr>
<th>&lt;50</th>
<th>51-100</th>
<th>101-250</th>
<th>251-499</th>
<th>500-1,000</th>
<th>1,000+</th>
</tr>
</thead>
</table>

3. Type of fraud committed in that organization in the last 5 years (You can √ more than one)

<table>
<thead>
<tr>
<th>Employees</th>
<th>Management</th>
<th>External parties (customers, suppliers etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Bounced cheques or cheque forgery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Conflict of interest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Corruption/bribery (taken)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Corruption/bribery (offered)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Expense accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Industrial espionage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Invoice manipulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Money laundering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Overpricing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j. Payroll fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>k. Petty cash fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>l. Poor quality of goods/services provided</td>
<td></td>
<td></td>
</tr>
<tr>
<td>m. Price fixing/ collusion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Theft of assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>o. Theft of cash (Through false claims)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>p. Unnecessary purchases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>q. Window dressing/ financial statement manipulation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Total amount being victimized | | |

4. Opportunity provided which made fraud easy to occur. (You can √ more than one)

| a. Weak internal controls | d. Corporate culture that facilitates crime | |
| b. Collusion | e. External factors conducive for crime | |
| f. Type of business | f. Weak IT security/access controls | |

(continued)
5. Procedure followed when fraud was identified: Tick the steps that were taken when the fraud was identified. (You can √ more than one)

<table>
<thead>
<tr>
<th>a. Civil action for recovery</th>
<th>b. Warning/reprimand</th>
</tr>
</thead>
<tbody>
<tr>
<td>c. Disciplinary action</td>
<td>d. Permitted individual to resign</td>
</tr>
<tr>
<td>e. External investigation</td>
<td>f. Referred to appropriate authority</td>
</tr>
<tr>
<td>g. Immediate dismissal</td>
<td>h. Report to the police</td>
</tr>
<tr>
<td>i. Insurance claim</td>
<td>j. Reviewed by the audit committee</td>
</tr>
<tr>
<td>k. Internal investigation</td>
<td>l. Settled before the courts</td>
</tr>
<tr>
<td>m. Negotiated settlement</td>
<td>n. Settled out of court</td>
</tr>
<tr>
<td>o. No action or sanction</td>
<td>p. Voluntary resignation/retirement</td>
</tr>
<tr>
<td>q. Intra-company transfer</td>
<td>r. Other…</td>
</tr>
</tbody>
</table>

6. Did the organization have at the time an effective code of conduct?  
   Yes ☐ No ☐

7. Did it have at the time an audit Committee?   Yes ☐ No ☐

8. Proportion of non-executive directors on the board

   <20% ☐ 21-30% ☐ 31-40% ☐ >40% ☐

9. Proportion of Independent Non-Executive Directors on the Board

   <20% ☐ 21-30% ☐ 31-40% ☐ >40% ☐

10. CEO is tenured  Yes ☐ No ☐

11. Number of years the CEO is in current position

   <3 ☐ 3-6 ☐ 6-10 ☐ >10 ☐

12. Total % of share owned by management

   <10% ☐ 11-20% ☐ >20% ☐

(continued)
C. Think of an organization which did not have any fraud in that last 5 years

1. Type of organization. (please √)

<table>
<thead>
<tr>
<th>Hospitality and Tourism</th>
<th>Health</th>
<th>Automobile and Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Sector/ Semi government</td>
<td>Banking/Finance/Insurance</td>
<td>Construction/Real estate</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Retail/Wholesale</td>
<td></td>
</tr>
</tbody>
</table>

2. Number of employees. (please √)

<table>
<thead>
<tr>
<th>&lt;50</th>
<th>51-100</th>
<th>101-250</th>
<th>251-499</th>
<th>500-1,000</th>
<th>1,000+</th>
</tr>
</thead>
</table>

3. Reasons why fraud was not possible. (You can √ more than one)

| c. Strong internal controls | d. Corporate culture that does not facilitate crime |
| b. Collusion not possible | e. External factors not conducive for crime |
| h. Type of business         | f. Strong IT security/access controls |

4. What procedure will be followed if fraud is to be identified: Tick the steps that are likely to be followed. (You can √ more than one)

| a. Civil action for recovery | b. Warning/reprimand |
| c. Disciplinary action       | d. Permitted individual to resign |
| e. External investigation    | f. Referred to appropriate authority |
| g. Immediate dismissal      | h. Report to the police |
| i. Insurance claim          | j. Reviewed by the audit committee |
| k. Internal investigation   | l. Settled before the courts |
| m. Negotiated settlement    | n. Settled out of court |
| o. No action or sanction    | p. Voluntary resignation-retirement |
| q. Intra-company transfer   | r. Other… |

(continued)
6. Did the organization have at the time an effective Code of Conduct?
   - Yes □  No □

7. Did it have at the time an audit Committee?
   - Yes □  No □

8. Proportion of non-executive directors on the board
   - <20% □  21-30% □  31-40% □  >40% □

9. Proportion of independent non-executive directors on the board
   - <20% □  21-30% □  31-40% □  >40% □

10. CEO is tenured
    - Yes □  No □

11. Number of years the CEO is in current position
    - <3 □  3-6 □  6-10 □  >10 □

12. Total % of share owned by management
    - <10% □  11-20% □  >20% □

Corresponding author
Maria Krambia-Kapardis can be contacted at: maria.kapardis@cut.ac.cy