

## **Employing Artificial Intelligence to Minimize Internet Fraud**

Edward Wong Sek Khin

Faculty of Business & Accountancy, University of Malaya, Malaysia

Email: edwardwong@um.edu.my

### **ABSTRACT**

Internet fraud is increasing on a daily basis with new methods for fraudulently extracting funds from governments, corporations, businesses, and ordinary people appearing almost hourly. The increasing use of on-line purchasing and the constant and sometimes ineffective vigilance of both seller and buyer seemingly lead to the conclusion that the criminal seems to be one-step ahead at all times. Today, pre-empting or preventing fraud before it happens occurs in the manual, non-computer based business transactions because of the natural intelligence of both seller and buyer. Currently, even with advances in computing techniques, near human levels of intelligence is not the strength of any computing system, yet techniques are available which may reduce the occurrences of fraud, and are usually referred to as artificial intelligence systems. This paper provides an overview of the use of current artificial intelligence (AI) techniques as a means of combating transaction fraud. Initially this paper describes how artificial intelligence techniques are employed in systems for detecting credit card fraud (online and offline) and insider trading within the Bourses. Following this, an attempt is made to propose using the MonITARS (Monitoring Insider Trading and Regulatory Surveillance) Systems framework which uses a combination of genetic algorithms, neural nets and statistical analysis in detecting insider dealing, to be used in the detection of transaction fraud. Finally, the paper discusses future research agenda to the role of using MonITARS-type systems.

Keywords: Artificial Intelligence, Internet Fraud, Networking, MonITARS Systems

### **INTRODUCTION**

As the current systems of selling and buying goods and services over the Internet is a multi-billion dollar business, there are required assurances that the buyer and seller operate legitimately within their business dealings over the Internet. This is so that goods

and services will be supplied as per specifications, and the invoices be paid, in effect, these transactions are not different than non-Internet transactions. However, by the lack of person-to-person business contact, this has led to, at times, notable levels of distrust within the Internet marketplace. This distrust converts to raise transaction costs, costs that ought to be savings from the use of e-commerce techniques.

Artificial Intelligence (AI) is defined as ‘an intelligent computer program that uses knowledge and inference procedures to solve problems that are difficult enough to require significant human expertise for their solution’ (Holland, 1992; Giarratano and Riley, 1994).

Fraudulent uses of networked computer system are not isolated events, and it tends to mean that a successful fraud is almost certainly has occurred previously or is to be repeated elsewhere (Circular to Participating Organisations (2000a, b). In a survey conducted in 1994, by Ernst & Young of 106 UK, of the companies listed in the Times Top 1000 group of companies, nearly 50% were victims of multiple computer-based frauds during an 18 month period between January 93 and July 94, incurring an average cost of £380,000 (Card World Publications, 1994). Considering the total monetary size of computer based fraud, and this amount is considered to be an underestimate because of the corporate embarrassment of such events and to reduce “copycat” occurrences, there are technical issues surrounding the development of artificial intelligence systems that can be employed in detecting fraud. For example, ‘...the number of transactions must be screened in order to detect instances of fraud. Moreover, the types of fraud are constantly changing, which suggests that there is no specific set of patterns by which fraud can be detected’ (Card World Publications, 1994).

Here are some brief descriptions of each technology using different artificial intelligence approaches to detect fraud.

Credit View Corp (US) looks at each transaction in depth, searching for inconsistencies and indications of fraud.

- QSI Payments Inc. (US) takes a holistic approach to fraud prevention, sending all transactions through its secure servers, then stripping card information and forwarding just enough information to merchants to allow the transaction to proceed.
- Merchant Online.com markets a card reader, which encrypts all card information. The company intercepts the information, decrypts it, and presents it to the bank, making it look like a card-present sale. It then authorizes the order. (Adapted from Credit Card News, 2000)

## Detecting Fraud

Here are some technical difficulties facing service sector companies in fraud detection.

For the service sector, problems pertaining to fraud originate in the nature of the problems such as:

- ‘...the vast number of records that simultaneously need to be intelligently examined, cross-checked, and verified in order to detect instances of fraud. Furthermore, the volume of transactions also presents difficulties in developing an automated processing system, the essence of which is speed as well as accuracy. Hence, comprehensive checks on each transaction can create a severe burden on the speed and inevitably decrease the efficiency of the system, while on the other hand, too few checks are costly in terms of undetected fraud’ (Card World Publications, 1994).

Two examples outlined below illustrate the situation when high levels of data throughput occur:

- VISA International has 16 millions transactions a day, which encapsulate information relating to the place of purchase, merchant type, transaction amount, and time and date of transactions (Card World Publications, 1994).
- The Australian stock market trades an average of 200,000 trades a day, and in each trade has numbers of data fields attached. Hence, any investigation into market abuse takes place within an information background consisting of millions of trades, over 1000’s of different stocks, hundreds of brokers, and millions of clients. Thus, high volume turnovers also create a barrier for developing an effective fraud screening system (Financial Review, 2000).

Apart from the technical aspects involved in screening vast amounts of data, another problem stems from the balance of cost effectiveness of a system able to detect and eliminate actual fraud. In most instances, it may be both commercially unfeasible to detect and act on all instances of fraud (Card World Publications, 1994).

*“Both the Visa and MasterCard companies assert that problems caused by hackers who penetrate servers or databases that hold credit card numbers represent another factor, which contributes to the increasing fraud rates on credit cards (particularly on online credit card fraud)” (Gartner’s Survey Report, 2000).*

In a Gartner’s survey of 100 Web retailers, a majority found on-line Internet credit card fraud to be more common than offline fraud. Gartner found that ‘44% of e-retailers built their own antifraud software, unless they were simply manually processing card numbers off the Web and making checks through phone calls and other means. This kind

of software works by automatically submitting check-card numbers in Web-based purchases to known patterns of abuse to ascertain risk.'

For example, in the year 2000, Expedia, a US based on-line travel service, which accepts credit cards for airline tickets and hotel reservations, acknowledged that it had been victimised by gang-related card-fraud to the tune of US\$4.1 million. 'The fraud was committed by professional criminals, who obtained the card numbers, not from Expedia or Expedia customers, but from elsewhere,' said Suzi LeVine, Expedia's marketing director (Gartner's Survey Report, 2000).

As a travel agent, Expedia earns about \$10 on a \$300 plane trip booked using their services, however, if the card number is false, Expedia has to absorb the full cost of the fraudulent transaction. Expedia's card-fraud problem was not due to a computer break-in; rather the fraudulent numbers sent using the Web were not screened or examined. As a result, Expedia strengthened its fraud-screening procedures and added card risk assessment software (i.e. using an artificial intelligence system) purchased from the HNC Software Company (Gartner's Survey report, 2000).

### **OBJECTIVE OF PAPER**

Artificial Neural Networks, Genetic Algorithms, and Fuzzy Logic are the most useful artificial intelligence techniques for detecting fraud. For example, in Kingdon's report (1995c), the credit card fraud figures for the UK show a downward trend, with losses peaking in 1992 at £165 million, with £120 million in 1993 and just below £100 million for 1994

The MonITARS (Monitoring Insider Trading and Regulatory Surveillance) Systems introduced to The London Stock Exchange has been positively evaluated in investigating the importance of hybrid systems using a combination of genetic algorithms, neural nets, and statistical analysis in detecting insider dealing. With the above in mind, the objective of this paper is:

- to determine methods in exploring how Kingdon's hierarchy analysis framework within MonITARS Systems improves the detection of insider trading within Australian stock markets
- to evaluate the elements of artificial intelligence hybrid system influencing the adoption of Kingdon's hierarchy analysis framework and how these systems are able to enhance market exchange's surveillance activities.

## LITERATURE REVIEW

### Artificial Intelligence Systems

Computer based fraud discovery and the reactions to such fraud, are increasingly based upon the use of technology, particularly tools using an artificial intelligence approach (Hurley, Moutinho, & Stephens, 1995). Artificial intelligence systems refer to ‘a branch of computer science concerned with creating computer programs that can perform actions comparable with decision-making by humans’ (Giarratano and Riley, 1994). Giarratano and Riley (1994) also suggest that “increasingly, techniques such as neural nets, genetic algorithms and fuzzy logic are being applied in business paradigms for a wide range of forecasting, analysis, optimization and data base tasks. It is not surprising therefore, that these applications are increasingly being seen in the development of combating fraud” (Giarratano and Riley, 1994).

In another report by Kingdon (1995d), he asserts that there are three factors that have made AI applications particularly appropriate for combating fraud.

- ‘AI is flexible and easily adaptable to the solutions developed. For example, artificial intelligence techniques learn from experience, which means that in changing business conditions a system can adapt to new circumstances, and adjust its response accordingly.
- AI applications do not need designers to specify all the operating conditions under which they are to perform as they can learn from experience.
- AI applications create innovations, as they are capable of finding relationship hitherto unknown. This means that AI system itself can contribute creatively to the detection process, finding new links and associations between patterns of fraud’ (adapted from Kingdon, 1995d).

The development of hybrid intelligent systems for developing marketing strategies is another factor that has helped AI applications in combating fraud (Venugopal & Beats, 1994; Shuliang Li, 2000). According to Shuliang, (Ibid.), ‘neural nets and genetic algorithms are seen as being used as a means for interrogating large customer databases in order to filter customer profiles for direct marketing, credit risk evaluation, and for consumer profiled profit analysis.’

### Applications of Artificial Neural Networks, Genetic Algorithms, and Fuzzy Logic

In this section, we explore three popular types of techniques used by artificial intelligence: artificial neural networks, genetic algorithms, and fuzzy logic.

Artificial neural networks bring a number of critical competitive edges to traders, portfolio managers and trading managers. For traders, they provide a useful early warning of changing trends. For portfolio managers, they provide a faster, more accurate way of screening and selecting securities. For trading managers, they provide a way of improving overall performance, of benchmarking results against a standard customized to their particular risk profile, of monitoring compliance, and of detecting fraud (Caudill and Bulter, 1992).

In Kingdon's (1995c) paper, the author describes how the establishment of artificial neural networks were used for fraud detection in merchant banking (Fidelity Investment, Citibank), marketing (Thorn-EMI, American Express-Amex), retail banking, and insurance (TSB).

Another report by Card World Publications, (1994) maintains that artificial neural networks are largely responsible for reducing fraud substantially for Visa International. According to Northants (1994) report, 'initially the system was trialed in five Canadian and ten US banks, whose customers numbered 40 million card holders. The neural network was 'trained' to spot fraudulent activity by comparing legitimate card usage with known cases of fraud. By using patterns based on aspects such as the time of transaction, the frequency of transaction, the size of transaction, or the type of transaction (i.e. the merchant type) a comparison could be made to an existing model held for each individual cardholder. Once a pattern of behavior was judged by the system as unusual, or potentially fraudulent, the system sounded an alarm,' and the transaction was investigated further (Card World Publications, 1994).

In another report by the Intertek Group, a fraud detection system called 'Card Risk Identification Service (CHRIS)' has saved an estimated US \$18 million for Visa International. The system was able to handle 20 million authorizations a day (Intertek Group, 1994).

Intertek Group (1994) points out that HNC Software is one of the largest suppliers of artificial neural net-based credit card fraud detection software. HNC's Falcon system is used by thirty credit and transaction card suppliers world-wide, and monitors over 90 million accounts. According to HNC, users of Falcon save on average 25% more through avoiding losses resulting from fraud than other users achieved by alternative existing strategies (Intertek Group, 1994).

Nestor is another software supplier identified by the Intertek Group report (1994) as dedicated to the use of artificial neural net-based fraud detection systems. According to

the Intertek Group, Nestor supply a system called FDS, which they claim, has reduced fraud by 20-40% where it is adopted. Mellon Bank in the USA, which installed FDS in 1992, reports that the system has increased the detection rate by a factor of 20, while at the same time reducing the number of false positives by a third (Intertek Group, 1994).

The second technique is the use of genetic algorithms. According to Goldberg, D. E. (1989), 'genetic algorithms are used in a number of different application areas, especially in optimizing sequences of operations, in which the elements in the string of the chromosome encode the sequence. However, such application areas, they are seen as a class of almost intractable problems' (Goldberg, 1989).

On the other hand, in terms of fraud detection several commercial applications may also co-exist. For example, in the Netherlands the ING Bank is using genetic algorithms for signature recognition by hybridizing existing techniques (Intertek Group, 1994).

In Kingdon's (1995d) paper, he states that the US based Travelers Insurance Company has used a combination of statistical analysis, expert derived rules, and evolutionary techniques for detecting fraudulent insurance claims. He indicates that the systems detect fraud with a 43% true positive and a 16% false positive ratio on a test set of over 22,000 claims. He also points out that the systems performed its analysis by constructing profiles of claimants based on their past history and then matching the current transaction against these profiles. However, using the same sets of data, he states that it is possible for the systems to develop rules to dichotomize past cases of fraud (Kingdon, 1995d).

The third technique is fuzzy logic. The use of fuzzy logic for creating decision support and fraud detection systems is becoming popular among management and financial decision modeling experts. In Kingdon's (1995a) paper, the author explores the establishment of fuzzy logic being used for fraud detection in healthcare claims for Travelers Insurance Company. The fraud detection system uses fuzzy rule such as High, Low, Increase, and rules like 'if the number of evening office visits is Low, then the fraud like hood is decreased'.

Moreover, fuzzy logic based fraud detection systems have also reduced fraud substantially for many Japanese financial institutions, including Yamaichi and Nikko securities (Kingdon, 1995a).

## **PROPOSED THEORETICAL FRAMEWORK**

It is proposed that the analysis framework adopted from Kingdon (1995c) shown in figure 1, which incorporates the hierarchy of analysis framework within MonITARS will be applied to this study. While previous empirical research conducted by Kingdon, focused on The London Stock Exchange, in this paper a local stock exchange, organization AEX is chosen to undertake the investigation of the elements influencing the adoption of Kingdon's hierarchy analysis framework within the MonITARS Systems.

### **Overview of hierarchy analysis framework within MonITARS**

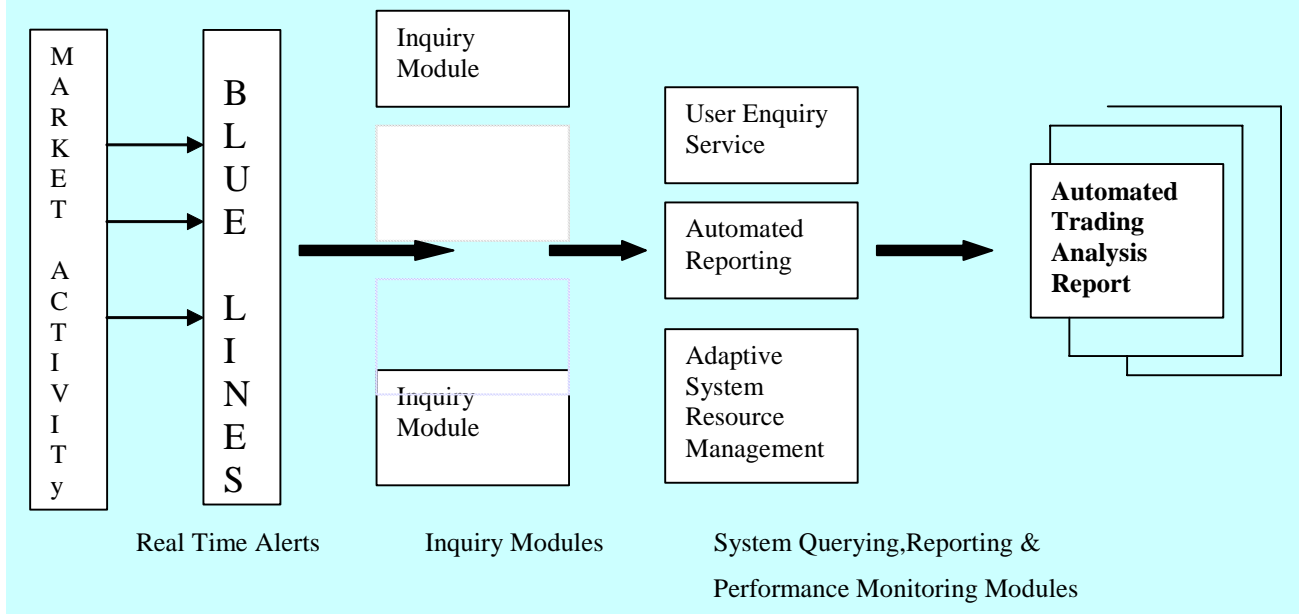
According to Kingdon's report,

*"the objectives of the MonITARS system on the London Stock Exchange was to see if there were ways of intelligently processing the massive volumes of data that passes through The Exchange with a minimum amount of human intervention, while still producing high quality relevant information, capable of being easily understood".*

In order to achieve this, Kingdon indicates that the MonITARS system should introduce a number of significant design principles describing the way the system's resources are managed and the way in which processing techniques are hierarchically combined, so as to refine, expand, and report an investigation. of this system are an Automated Trading Analysis Report, which would be used against any real and potential cases of market abuse.

In addition, the main features of Kingdon's hierarchy analysis framework are the uses of its specialist Inquiry Modules where a variety of standard and intelligent techniques are applied to infer unusual trading activity. It builds on a hybrid system from using a combination of genetic algorithms, neural networks, and statistical analysis in detecting insider dealing. MonITARS systems use three stages of filtrations. (Refer to figure 1)

Figure 1, illustrates the Kingdon's hierarchy of analysis framework within MonITARS.



**Figure 1: Model of hierarchy analysis within MonITARS (adopted from Kingdon, 1995)**

Consequently, the results

*'The first stage involves the "Blue Line", where a large number of routine (generally statistical) enquiries are conducted. These low level Alert Modules effectively patrol the large amount of traffic of incoming trading data looking for anomalies, or crisp trading violations (for example a failure to report a specific type of trade as detailed in the Exchange's list of regulatory requirements). The "Blue Line" is also responsible for screening data (removing irrelevant fields) and pre-processing data into a suitable format for the next level of analysis'.*

*'The second stage involves using the Inquiry Modules where specialist investigations are conducted such as, for example, monitoring for collective trading patterns (as in the dealing ring), or looking for specific types of trading sequences (as in possible cases of insider trading). The neural nets can be used to compress historic trading features of a market sector, a group of stocks, a market maker, an individual trader or a trading account. In addition, the statistical techniques can then be used to monitor deviations from these profiles, and genetic algorithms may be used to find collective trading patterns, or profiles indicative of trading abuse'.*

*'The third stage involves system querying, reporting and performance monitoring modules. This level allow the system to deliver a case analysis report in which the suspected abuse is described both in terms of the evidence for and against possible abuse'. (Adapted from Kingdon, J. 1995c).*

In summary, the above empirical study established that the adoption of Kingdon's hierarchy analysis framework will improve the detection of insider trading. As a result, this suggests that through effective supervision by MonITARS systems, organization

AEX will be able to enhance its reputation as a market of integrity, providing an efficient market environment based upon investor protection, and the interests of participants.

In addition, MonITARS Systems are able to tackle possible cases of insider dealing by using a combination of genetic algorithms, neural networks, and statistical analysis to produce automated trading inquiries. These inquiries will then form the basis for warranting investigations for possible civil or criminal proceedings. For example, the Australian stock market trades an average of 200,000 trades a day and any investigation into market abuse will involve a large volume of information. This information is filtered through an automated process in the form of an Automated Trading Analysis Report and this report will help organization AEX guard against any potential cases of market abuse.

Moreover, the MonITARS system also allows Surveillance analysts to review and examine a period of trading in a stock at their own personal pace. In practice, it is like watching a slow motion video replay, with every bid, offer, and trade coming onto the computer screen one by one. This means that each bid or offer matches to a particular stockbroker, and each transaction is linked with a particular client. As a result, it is possible to analyze, in full detail, the activities of a particular person trading in a given stock.

The MonITARS System is also able to generate alerts that enable Surveillance analysts to indicate the possibility of market abuse. Once an alert is generated by the MonITARS system, a referral can be made to the Enforcement department for further investigation and for possible civil or criminal proceedings.

On the other hand, the MonITARS System has been successfully detecting potentially unusual trading activities and preventing the orchestration of market abuse for The London Stock Exchange. However, these links are impossible to detect using standard computing methods. Hence, these abilities to detect orchestrated activities will also help to strengthen the routine market analysis for the organization AEX.

### **CONCLUSIONS & FUTURE RESEARCH**

In this paper, the importance of artificial intelligence technology is shown for the development of automated systems design in detecting and alerting instances of fraud. Several reasons were advanced in beginning of this paper to explain the significance of artificial intelligence in helping to combat fraud.

There are a number of other areas associated with the assessment of fraud using the MonITARS system that have a higher degree of subjectivity and consequently are more

difficult to evaluate, and are not discussed here. The visualization aspect of artificial intelligence hybrid systems will be covered in a further paper. (Edward, forthcoming). Currently, work is undertaken to evaluate the findings of using the MonITARS System, this being a hybrid system that is believed to be a pragmatic approach to system development because it can allow multiple techniques to work in combination in order to address specific sub-tasks of a complex application. This is significant for the increasingly sophisticated demands made on software solutions in particular to the decision problem of identifying fault. However, the evaluation of the perceived business implications of MonITARS Systems in helping leverage market surveillance of trading activity will be reported on at a later date.

### **Directions for further research**

The work outlined in this paper may also encourage other IS researchers to conduct future research on other fraud issues. For example, further research may be to formulate a framework of security practices to online merchants, ISPs, and third party service providers, for processing credit cards. These practices shall aim at preventing computer break-ins, the theft of card numbers from servers, and may include encrypting card data and using firewalls and antivirus software.

### **REFERENCES**

- Caudill, M., & Bulter, C. (1992). *Understanding Neural Networks: Computer Explorations*. Harvard: MIT Press.
- Circular to Participating Organisations. (2000a). *ASX Business Rules 2.2.4 Prevention of Manipulative Trading When Acting on Behalf of Clients* (No. 332), Canberra, Government Gazette.
- Circular to Participating Organisations (2000b). *ASX Business Rules 2.8 False or Misleading Appearance* ( No. 600). Canberra, Government Gazette.
- Gartner's Survey Report. (2000, Aug 21). *Online Card Fraud Target*. Framingham: Network World Press.
- Giarratano, J., & Riley, G. (1994). *Expert Systems* (2<sup>nd</sup> ed). New York: PWS Publishing Press.
- Goldberg, D.E. (1989). *Genetic Algorithms*. Boston: Addison-Wesley Publishing Press.
- Holland, J. H. (1992). *Adaptation in Natural and Artificial Systems*. Harvard: MIT Press.
- How Each Anti-fraud System Works. (2000, Oct 15). *Card Card News*, Chicago, p. A2

- Hurley, S., Moutinho, L., & Stephens, N.M. (1995). Solving Marketing Optimisation Problems Using Genetic Algorithms. *European Journal of Marketing*, 29(4), 4-5.
- Intertek Group. (1994). *Adaptive Computational Methods: Management Report*. Paris, France: Author.
- Kingdon, J. (1995a). *Redundancy in Neural Nets: An Architecture Selection Procedure using In-Sample Performance*. Technical Report, Department of Computer Science, University College London.
- Kingdon, J., & Dekker, L. (1995b). *The Shape of Space*(Tech. Rep.), London: Department of Computer Science, University College.
- Kingdon, J. (1995c). Intelligent systems for fraud detection. In Sanchez, H., Shibata, T., Zadeh, L. (Eds), *Genetic Algorithms and Fuzzy Logic Systems* (pp. 133-141). Singapore: World Scientific Publishing Co Pty Ltd.
- Dekker, L., & Kingdon, J (1995d). Development Needs of Diverse Genetic Algorithm Designs. In Stender, J., Hillebrand, E., & Kingdon, J, *Genetic Algorithms of Optimisation, Simulation and modelling* (pp. 281-288). Amsterdam: IOS Press,
- Neural Networks in Fraud Watch (1994, Sept). *Card World Publications*, p. A2.
- Responsibility of Trading Participants for Bids and Offers in SEATS. (2000, Feb 15). *Financial Review Report*, p. A7.
- Shuliang, L. (2000). The Development of a Hybrid Intelligent System for developing marketing strategy. *Decision Support Systems*, 27(1), 394-409.
- Stemming the Telemarketing Fraud Tide in Fraud Watch (1994, July). *Card World Publications*, Northants, p. A3.
- Venugopal, V., & Beats, W. (1994). Neural Networks and Statistical Techniques in Marketing Research: A conceptual Comparison. *Marketing Intelligence & Planning*, 12(7), 30-38.