

Detection of Violations in Credit Cards of Banks and Financial Institutions based on Artificial Neural Network and Metaheuristic Optimization Algorithm

Zarrin Monirzadeh

Faculty of Computer Engineering,
Department of Computer and
Electronic Engineering, University
of Eyvanekey, Semnan, Iran

Mehdi Habibzadeh

Faculty of Computer Engineering,
Department of Computer and
Electronic Engineering, University
of Eyvanekey, Semnan

Nima Farajian

Faculty of Computer Engineering,
Department of Computer and
Electronic Engineering, University
of Eyvanekey, Semnan, Iran

Abstract—Due to popularity of the World Wide Web and e-commerce, electronic communications between people and different organizations through virtual world of the Internet have provided a good basis for commercial and economic relations. These developments, although occurring for less than a century, electronic communications have always been subject to interference, cheating, fraud, and other acts of sabotage. Along with this increase in trading volume, there is a huge increase in the number of online fraud which results in billions of dollars of losses annually worldwide; this has a direct effect on customer service of banking systems, particularly electronic banking systems, and survival as a reliable financial service provider. Therefore, attention to fraud detection techniques is essential to prevent fraudulent acts and is the motive for many scientific researches. For this reason, business intelligence is used to identify financial violations in various economic, banking and other fields. Here, the focus is on algorithms and methods presented in data mining to deal with fraud by using neural networks. The main objective is to improve these methods or present new algorithms by studying the behavioral patterns of customers and the combined use of genetic algorithm to improve the performance of neural network and find the appropriate models for better decision making by implementing and testing the performance of the suggested algorithms. The results show that more strength was given to neural network by using genetic algorithm. In fact, genetic algorithm can raise our ability to control the training process. Moreover, it was concluded that criteria such as age, gender, marital status were not effective on detection; in fact, the most important effective criteria are information related to transaction.

Keywords—Financial fraud detection; neural networks; data mining; genetic algorithm

I. INTRODUCTION

Although extensive research has been conducted on fraud detection, the need for these activities still persists due to the increasing number of financial and business activities and the increased use of modern technologies. Although there are still some up-to-date articles on this matter in prestigious journals, there is a lack of appropriate resources which include the latest research in this area and there is large-scale fraud in the financial and commercial areas. KPMG's 2003 research suggests an ever-increasing rate of fraud. The research indicates that 75% of the surveyed organizations experienced

instances of fraud. This figure is 13% higher than the 1998 figures. Hence, it is important to provide techniques for detecting fraud in e-commerce and research in this area. For a long time, traditional data analysis techniques have been used for detecting fraud. This requires complex and time-consuming research and requires the use of various fields of knowledge such as finance, economics, business methods, and legal debates [1]. Here, the focus is on algorithms and methods presented in data mining to deal with fraud by using neural networks. Artificial neural networks can work like a human brain and analyze information and correctly detect the problem when properly trained. Efficiency and function of a neural network is reasonable which it is properly designed [2]. For a correct design, parameters should be initialized and set reasonably. Typically, the method used to set input parameters is to use trial and error, through which various possible combinations are tested separately to select the best combination possible. There is always a lack of a regular approach to finding the best combination among different input parameters. Therefore, this study tends to introduce a method for determining the best combination among different input parameters. Neural network is considered as a very efficient functional approximation tool, which considers structure design, followed by optimal problem or network training. Instead of gradient-based methods, evolutionary optimization methods are used to determine the neural network weights (neural network learning or training) and genetic algorithm optimization code (the most well-known and most popular optimization algorithm in the field of evolutionary computing). In the field of fraud detection research, various techniques have been evaluated by various research communities and briefly investigated by numerous studies.

Carminati [5] suggested the BANKSEALER system which is a decision support system for analyzing online banking fraud. During the training phase of this system, easy models were developed to understand spending habits of customers based on past transactions. Halvaeie et al. [6] solved the credit card fraud detection problem using an artificial immune system. They developed a new model as artificial fraud detection model (AFDM) based on artificial immune system. This model used artificial immune and its improvement for fraud detection. Olszewski [7] suggested a fraud detection

method based on user account imaging and threshold type detection. The imaging method used in this approach was self-organizing mapping (SOM).

Artificial neural networks used for classification are widely used in many fields; one of their features is the unsupervised learning (Ghasemi & Asgharizadeh, 2016). Artificial neural networks are one of the methods used to identify fraud in bank cards. The advantage of neural networks to other methods is that it can learn from past transactions and improve the results over time [17].

Nagi et al. (2016) believed that fraud is one of the most common phenomena in business. According to Section 24 of the Iranian Standards of Audit, deceptive action of one or more directors, employees or third parties for an undue advantage refers to any intentional or unlawful act. Therefore, prevention or detection of important frauds in financial statements has always been the focus of investors, legislators, standardizers, managers and auditors [18]. This study examines the effectiveness of data mining techniques in detecting fraudulent behaviors of companies reporting fraudulent financial statements to identify effective factors on these behaviors. Data mining is a bridge between statistical science, computer science, artificial intelligence, modeling, machine learning and visual representation of data. In a process framework, it is possible to extract valid, previously unknown, intelligible and reliable information from a large database. It can be used in decision-making in important business activities such as improving the usefulness of information through identification of financial fraud [19].

To implement an effective neural network, genetic algorithm is used to detect financial violations to regulate the effective parameters on efficiency of neural network. The suggested genetic algorithm can be used to decide on topology of the network, number of hidden layers, number of nodes and other factors which are effective in design and efficiency of the neural network. The main objective is to improve these methods or develop new algorithms by studying the behavioral pattern of customers and integrating genetic algorithm to improve the performance of neural network and finding a suitable model for better decision making; performance of the suggested algorithms will be assessed to predict potential behavior of customers in the future [16].

II. THEORETICAL FRAMEWORK

E-banking: E-banking is a set of services, technologies or processes used to remove time-consuming mechanisms and implement very in-house systems in banks. Electronic banking, as infrastructure of e-commerce, is one of the most important phenomena arising from information revolution and transformation of traditional ways of trading to replace it with e-commerce. Hence, electronic banking is considered as the main infrastructure of e-commerce due to the role of money and banking in commerce [3].

Types of financial violations: Financial violations are mainly carried out in two ways: direct and indirect. Directly, the physically lost or stolen card is used by other people. Indirectly, only the card number is stolen and used in phone purchases and other indirect purchasing methods, such as

Internet shopping. In the former, if the cardholder does not immediately find that the card is lost, it can only lead to financial loss. In the latter, the cardholder has no idea that he has shared his card with someone else and this may remain hidden for a long time. There is another type of indirect violation in which shared services of people are exploited; thus, the owners will have to charge their services sooner than the reasonable time or due date [4].

Expert systems: Expert systems refer to types of computational systems which are able to provide and reason in some rich areas of knowledge by solving problems and giving solutions [8]. Expert system detections encode knowledge in the form of rules; that is, they determine what should happen in what state by law. As an example, NIDES system, implemented by SRI, uses the approach of expert systems to identify attacks by using online monitoring of user activities [9]. NIDES include statistical analysis elements to detect abnormalities and rule analysis tools to detect abuses.

Transition analysis: This is an abuse detection technique in which attacks are displayed as a sequence of the monitored state transition. Activities which occur in an attack are defined as a transition between states. Attack scenarios are defined in the form of state transition diagrams. In these diagrams, nodes are system states and arcs are the related actions. In any case, if a final state is reached, it will mean the time of an attack. State Transition Analysis Tool (STAT) is a well-known regular expert system designed to search for known penetrations in an audit trail of multi-user computer systems [13]. Moreover, USTAT is also a prototype of STAT designed under the UNIX operating system [14].

Clustering: Data may contain complex structures from which even the best data mining techniques cannot extract meaningful patterns. Clustering provides a way to find the structure of complex data. Clustering refers to division of a heterogeneous population into a number of homogeneous subsets or clusters. Cluster refers to a set of information which is similar to other components of this set and is not similar to components of other sets. In clustering, there are no preset groups, and data is grouped simply by similarity, and the titles of each group are determined by the user [15].

Neural networks: Neural network is inspired by human brain; processing data is handled by many small processors which interact in parallel with each other to solve a problem. In these networks, a data structures is designed by programming methods, which can act as a neuron. This data structure is called a neuron. The network is trained by creating a network between these neurons and applying a training algorithm. By examining behavior of customers, their future behavior can be predicted. This requires a dataset consisting of characteristics of the former clients and their performance, whether they have a fraudulent and criminal function. By having this dataset and applying the right data mining techniques, one can predict the likelihood of fraud and criminal acts in new clients [15]. A neural network is a set of interconnected nodes designed by imitating human brain function. Each node has weighted communications to several other nodes on the adjacent layers [10]. In neural networks, the data structure designed by software can act as a neuron; this data structure is called a

node. Then the network is trained by creating a network between these nodes and applying a training algorithm to it. In this memory or neural network, the nodes have two active (on or 1) and inactive (off or 0) modes, and each edge (synapse or communication between nodes) has a weight. Positive weighted edges trigger or activate the next inactive node, and negative-weighted edges inactivate or inhibit the next connected node (if activated). An artificial neuron is a system with a large number of inputs and only one output. Neurons have two modes, training mode and operation mode. In training mode, the neuron learns to be triggered or fired against specific input patterns; however, the emerging trend of financial fraud is generally recognized through analyzing and extracting information (data mining) from the transaction database of financial institutions marked. This helps to formulate security policies and protocols and new authentication. In operation mode, when a detected input pattern is inserted, the corresponding output is provided. If the input is not part of the pre-identified inputs, the fire rules will decide for its triggering. Braves and Langdorff were the first to suggest an integration of continuous role-based systems and neural network-based approaches [11]. Falcon's fraud management system, a powerful tool for preventing fraudsters from abusing credit and debit cards, uses neural network algorithms. This system predicts the likelihood of fraud on an account by comparing the current transaction and past cardholder activities [12]. If this system detects a fraud-type transaction on a card, the cardholder will immediately be called by telephone; if the cardholder confirms fraud on the card, the card will be immediately blocked to prevent fraud. If the Falcon system detects any fraud, but it is not possible to call the cardholder, the card is temporarily blocked to ensure that the fraud is not committed and the cardholder must follow the situation by calling the bank; the card will remain blocked as long as the cardholder's contact is not recorded. The system is able to learn the cardholder's purchase habits by using neural networks and detect any irregularity in payment, and consider as a fraud. Machine learning techniques and technologies, adaptive pattern recognition, neural networks and statistical models have contributed in designing and developing the Falcon forecasting system.

III. HYPOTHESES

Hypothesis 1: Genetic algorithm and neural networks used to discover violations in e-commerce systems provides better results.

Hypothesis 2: Auxiliary algorithms such as genetic algorithm used along with other algorithms such as neural networks provide a stronger configuration in detecting violations.

IV. RESULTS

The data used includes various parameters such as name, gender, age, and address as personal specifications, and eventually information about transaction history, including transaction value, transaction time, and transaction status.

To test, parameters such as the number of primary population, the number of neurons, as well as the information

used can be changed to choose the best mode. All results are presented as mean. The test was iterated four times for each series of results and the mean of error and regression was presented for each iteration. This prevents random results. Moreover, variance was used to show the extent to which results of different tests were close to each other.

As it is clear, variance ranges from zero to one. The smaller and the closer numbers to zero indicate that the results of different tests are closer to each other and ultimately indicate the high reliability of results. The tables below also show regression (from the left, training regression, test evaluation regression and full regression, respectively).

First, the number of primary population was set at 30. All data available in dataset was used. The number of neurons was altered. Table I lists the results.

In Table II, only financial transaction information was used and demographic information such as name, age, and address were removed. The test mode is the same as the previous test mode and the results are presented in the Table II. Next, the number of primary population was set at 45; the results are shown in the Table III. First, all data available in dataset was used. In Table IV, a dataset of which personal data was removed was used and the results were presented. The number of primary population was set at 60. The results are presented for data with full specifications and data without personal specifications, respectively (Table V). In Table VI, data was used without personal information.

Obviously, the results of the neural network trained by genetic algorithm can be better than normal neural network. These results show that the neural network can be better trained by using optimization algorithms such as genetic algorithm (Table VII). In fact, this study indicates that optimization algorithms provide higher control on neural network training.

Genetic algorithm uses its unique features such as mutation and crossover which can be applied in a variety of ways and has a great potential in this regard. Thus, two-point crossover was used here to show capability of genetic algorithm. A finding of this study is that good results can be obtained without personal information; particularly in this method, since training time is longer than normal, the time will be longer when all data is used than the situation when this information is removed. Therefore, the latter is the final result of this study. For this purpose, these tests were run only on the data without personal information. Initially, the number of primary population was set at 30.

Table VIII shows that there was no need to increase the number of primary population, because the optimal result was obtained by this population. In fact, the need for greater population was reduced by using multiple crossovers. The greater population is required to increase overall search. However, this change can meet this need in shorter time. In fact, time is the weakness of this method, which was solved by using multiple crossovers. Better comparison is made below through diagrams. To clear the diagram, the scenarios 1 to 5 are described.

TABLE I. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 30-ALL DATA)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.86	0.85	0.87	0.86		0.81	0.81	0.81	0.81
[1,1,2]	0.022	0.0533	0.86	0.85	0.87	0.86	0.034	0.81	0.81	0.81	0.81
[1,1,3]	0.020	0.039	0.88	0.88	0.88	0.88	0.029	0.82	0.81	0.81	0.83
[1,2,3]	0.00884	0.109	0.947	0.94	0.9513	0.94649	0.0104	0.89	0.88	0.86	0.89
[2,2,3]	0.00839	0.038	0.952	0.95	0.952	0.951	0.012278	0.92	0.92	0.92	0.925

TABLE II. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 30-FINANCIAL TRANSACTION)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.875	0.84	0.88	0.86		0.82	0.815	0.83	0.82
[1,1,2]	0.0215	0.0263	0.875	0.84	0.88	0.86	0.0307	0.82	0.815	0.83	0.82
[1,1,3]	0.0198	0.0181	0.89	0.86	0.85	0.89	0.024	0.82	0.81	0.81	0.83
[1,2,3]	0.00787	0.0068	0.95	0.95	0.96	0.96	0.010	0.89	0.88	0.86	0.89
[2,2,3]	0.00809	0.0164	0.96	0.95	0.96	0.97	0.01107	0.93	0.91	0.91	0.94

TABLE III. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 45-ALL DATA)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.887	0.898	0.886	0.885		0.817	0.816	0.812	0.818
[1,1,2]	0.019	0.0071	0.887	0.898	0.886	0.885	0.057	0.817	0.816	0.812	0.818
[1,1,3]	0.00839	0.0214	0.875	0.95	0.952	0.951	0.0103	0.92	0.91	0.921	0.9396
[1,2,3]	0.00994	0.0381	0.97	0.967	0.97	0.97	0.0099	0.95	0.96	0.95	0.97
[2,2,3]	0.00717	0.037	0.98	0.98	0.978	0.98	0.00896	0.96	0.95	0.95	0.978

TABLE IV. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 45-FINANCIAL TRANSACTION)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.881	0.890	0.87	0.89		0.817	0.816	0.8122	0.818
[1,1,2]	0.017	0.046	0.881	0.890	0.87	0.89	0.051	0.817	0.816	0.8122	0.818
[1,1,3]	0.00804	0.0272	0.884	0.945	0.94	0.963	0.01	0.92	0.91	0.921	0.9396
[1,2,3]	0.00972	0.0189	0.94	0.97	0.969	0.98	0.00998	0.958	0.964	0.96	0.973
[2,2,3]	0.0067	0.0035	0.983	0.98	0.98	0.989	0.0075	0.978	0.96	0.968	0.979

TABLE V. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 60-ALL DATA)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.925	0.926	0.928	0.925		0.89	0.9	0.88	0.898
[1,1,2]	0.012278	0.0023	0.925	0.926	0.928	0.925	0.021	0.89	0.9	0.88	0.898
[1,1,3]	0.00884	0.077	0.945	0.948	0.951	0.946	0.0099	0.935	0.92	0.912	0.941
[1,2,3]	0.00387	0.024	0.968	0.969	0.9658	0.963	0.0064	0.961	0.957	0.95	0.96
[2,2,3]	0.00199	0.0041	0.89	0.982	0.981	0.993	0.0025	0.982	0.97	0.98	0.987

TABLE VI. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF GENETIC ALGORITHM (POPULATION 60-FINANCIAL TRANSACTION)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.938	0.928	0.917	0.94		0.901	0.91	0.915	0.923
[1,1,2]	0.007278	0.0014	0.938	0.928	0.917	0.94	0.011	0.901	0.91	0.915	0.923
[1,1,3]	0.00684	0.08	0.957	0.949	0.951	0.96	0.0041	0.94	0.94	0.957	0.96
[1,2,3]	0.00497	0.042	0.978	0.971	0.972	0.981	0.0047	0.97	0.972	0.97	0.975
[2,2,3]	0.00169	0.006	0.986	0.982	0.98	0.993	0.0036	0.977	0.97	0.981	0.898

TABLE VII. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF TWO-POINT CROSSOVER GA (POPULATION 30)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.88	0.871	0.87	0.886		0.84	0.82	0.827	0.83
[1,1,2]	0.0174	0.068	0.88	0.871	0.87	0.886	0.024	0.84	0.82	0.827	0.83
[1,1,3]	0.0082	0.024	0.894	0.88	0.879	0.89	0.021	0.868	0.854	0.858	0.87
[1,2,3]	0.00983	0.019	0.968	0.957	0.959	0.96	0.0097	0.938	0.94	0.94	0.94
[2,2,3]	0.00678	0.028	0.98	0.96	0.968	0.977	0.0091	0.97	0.95	0.954	0.962

TABLE VIII. COMPARISON OF ERROR OF NEURAL NETWORK AND THE OPTIMIZED ERROR OF TWO-POINT CROSSOVER GA (POPULATION 45)

Neuron No.	Suggested technique error	Error variance	Regression				NN error	Regression			
			0.927	0.9	0.89	0.91		0.878	0.87	0.869	0.88
[1,1,2]	0.00729	0.00796	0.927	0.9	0.89	0.91	0.0085	0.878	0.87	0.869	0.88
[1,1,3]	0.00692	0.078	0.948	0.945	0.994	0.963	0.01	0.92	0.91	0.921	0.9396
[1,2,3]	0.005	0.0178	0.978	0.96	0.957	0.97	0.00998	0.958	0.964	0.96	0.973
[2,2,3]	0.0017	0.0147	0.989	0.984	0.987	0.99	0.0075	0.98	0.974	0.97	0.98

Scenario 1: The neural network is trained by single-point crossover genetic algorithm; primary population is set at 30; the number of neurons is [2,2,3] and data lacks personal information.

Scenario 2: The neural network is trained by single-point crossover genetic algorithm; primary population is set at 45; the number of neurons is [2,2,3] and data lacks personal information.

Scenario 3: The neural network is trained by single-point crossover genetic algorithm; primary population is set at 60; the number of neurons is [2,2,3] and data lacks personal information.

Scenario 4: The neural network is trained by two-point crossover genetic algorithm; primary population is set at 30; the number of neurons is [2,2,3] and data lacks personal information.

Scenario 5: The neural network is trained by two-point crossover genetic algorithm; primary population is set at 45; the number of neurons is [2,2,3] and data lacks personal information.

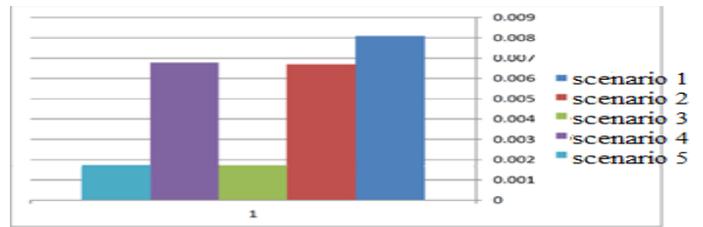


Fig. 1. Scenarios of primary population and single-point and two-point crossovers.

As shown in Fig. 1, two-point crossover could find results with smaller population to an optimal point. In this diagram, scenarios 3 and 5 are related to single-point and two-point crossovers with populations 60 and 45; the results are very close.

As shown in Fig. 2, factors such as population, bank growth, reward, salary, education are effective per unit time. Fig. 3 and 4 shows time-series prediction of multiple layer perceptron (MLP), neural networks and genetic algorithm. In these figures, the minimum time-series prediction is specified by red lines.

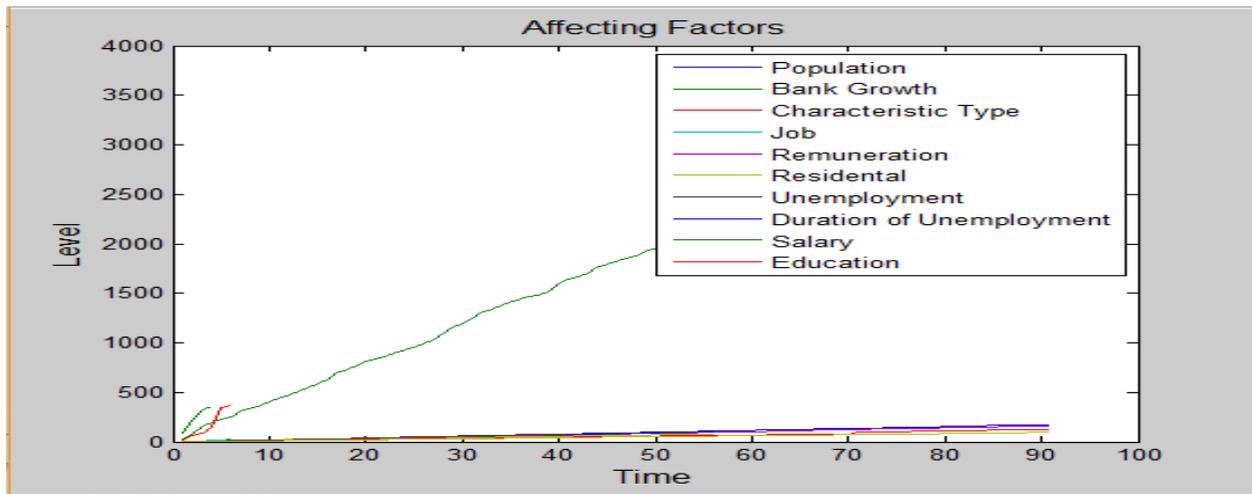


Fig. 2. Effective factors.

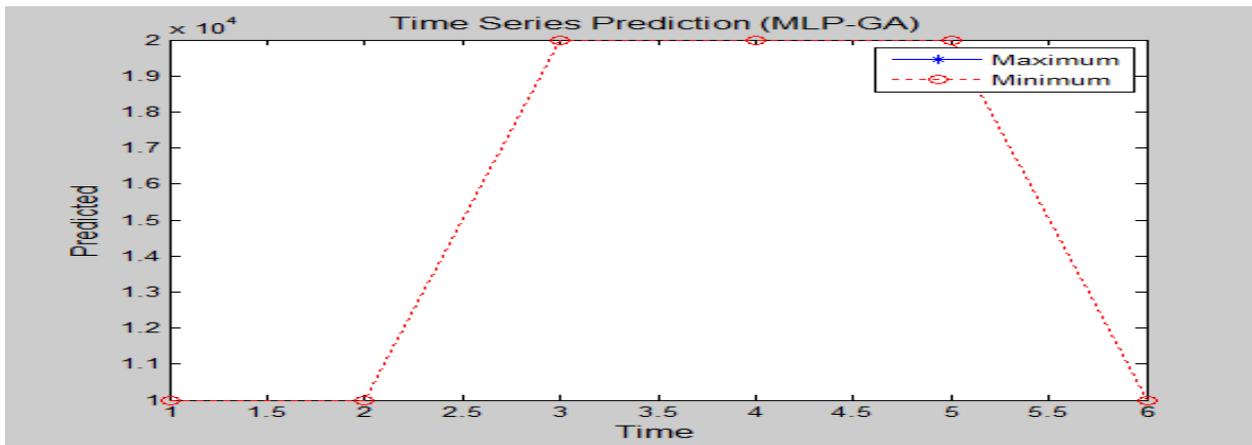


Fig. 3. Time-series prediction (MLP-GA).

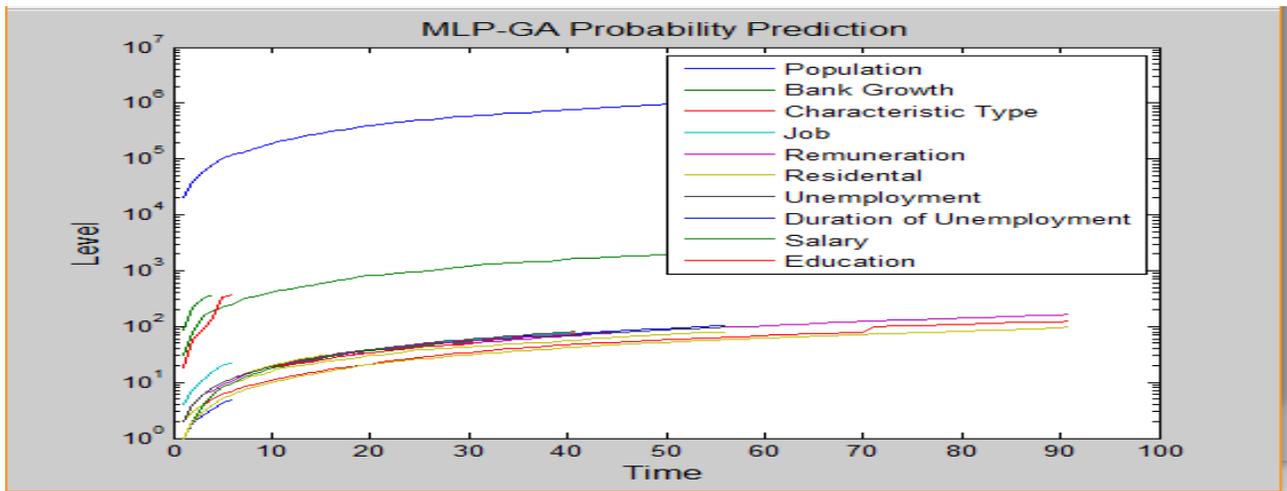


Fig. 4. MLP-GA probability prediction.

V. CONCLUSION

By historical detection using library documents and literature review, this study provides the necessary evidence to answer the questions. The results showed that first, data mining techniques are useful for detection in fraudulent financial statements; second, data mining can be considered as focus of guiding thought in business management to detect fraud.

Hybrid use of fraud detection and fault detection approaches integrates the advantages of both methods and eliminates the weaknesses of each method. Using this approach in fraud detection techniques, it is very efficient to use techniques such as neural networks. Regardless of technical discussion, it is important to note that the expansion of e-commerce and increasing growth of financial services of banks and credit and financial institutions, the increase in the number of customers and penetration rate of users, and high volume of transactions have caused new problems and challenges, such as increased tendency of fraudsters to electronic banking, which require a careful examination of data; if there are no mechanisms for detecting and preventing fraud, there will be an increase in fraud in electronic banking. However, it is not possible to accurately examine this volume of data with routine methods. On the other hand, financial and credit institutions are looking for solutions which can quickly detect criminal acts. Hardware and software capacities provided in the present century with data mining techniques can be used to examine the high volume of this kind of information. This study discussed neural network training. Neural network is one of the smart and powerful tools for prediction. Therefore, it will be useful to focus on its improvement. The main element of neural network is training. Neural network training refers to determining weight parameters and its bias. The equation of input and output is obtained by determining these parameters. For this purpose, training data is observed to reach the proper value for these parameters by iteration. This process means finding the optimal value. That is why this study used genetic optimization algorithm instead of conventional neural network training techniques. The objective function for training neural network is the same as error rate between actual output and output of the neural network. On the other hand, fault detection

in financial transactions is another aspect of this study. For this purpose, special data was used. The results show that genetic algorithm could empower the neural network to achieve better results in e-commerce. In fact, genetic algorithm increases the ability to control training process. It can be concluded that criteria such as age, gender, marital status have no effect on detection; in fact, the most important effective criteria are transaction-related information.

REFERENCES

- [1] A. Hatamirad, H. N. D. Shahriari, "fraud detection techniques in e-banking". economics new findings, vol. 134 , 2009.
- [2] S. N. D. Akbari, "financial fraud detection by data mining". AKSA IT Innovation Group, Iran, 2011.
- [3] H. Houshmand, "ecommerce and ebanking; challenges and solutions". 2010.
- [4] R. Varjini, M. Kani, "financial fraud detection techniques". Islamic Azad university of Gonabad. 2011.
- [5] M. Carminati., "BankSealer: A decision support system for online banking fraud analysis and investigation", Computers & Security., 2015
- [6] M. Halvaeie, N. Soltani, M. K. Akbari, "A novel model for credit card fraud detection using Artificial Immune Systems", Applied Soft Computing, pp. 2440-49, 2014.
- [7] D. Olszewski, "Fraud detection using self-organizing map visualizing the user profiles", Knowledge-Based Systems Vol.70, pp. 324-334, 2014.
- [8] T. F. Lunt, "A Real-Time intrusion Detection Expert System (IDES)-Final Technical Report". Technical Report. SRI Computer Science Laboratory, SRI International, from. <http://www.wenke.gtisc.gatech.edu>.1990
- [9] D. Anderson, T. Frivold, A. Tamaru , A. Valdes, "Next generation intrusion detection expert system (NIDES)", software user's manual,beta-update release, Technical Report SRIXSL-9547, Computer Science Laboratory, SRI International, from www.thc.org/root/docs/intrusion-detection/...NIDES-summary.pdf, 1994.
- [10] A. K. Ghosh, A. Schwartzbard, M. Schatz, "A Study in Using Neural Networks for Anomaly and Misuse Detection. 8th USENIX Security Symposium, from www.portal.acm.org/citation.cfm?id=1251433, 1999.
- [11] R. Brause, T. Langsdorf, M. Hepp, "Credit Card Fraud Detection by Adaptive Neural Data Mining", 11 th IEEE International Conference on Tools with Artificial Intelligence. Pp.103-106, 1999.
- [12] K. Hassibi, "Detecting Payment Card Fraud with Neural Networks", Singapore: World Scientific, ,2000.

- [13] K. Ilgun, R. A. Kemmerer, P. Porras, "A State transition analysis: A rule-based intrusion detection approach" *Software Engineering*, Vol. 21, pp. 181-199, 1995.
- [14] K. Ilgun, "USTAT A Real-time intrusion detection system for UNIX" *IEEE Symposium on Research in Security and Privacy*, pp.16-28, 2011.
- [15] I. C. Yeh, C. H. Lien, "The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients", *Expert Systems with Applications*, vol, 36, pp. 2473-2480., 2009.
- [16] A. Sharma, P. Kumar Panigrahi, "A Review of Financial Accounting Fraud Detection based on Data Mining Techniques", *International Journal of Computer Applications*, pp.0975 – 8887, Vol. 39, 2012.
- [17] Ghasemi, A. R. & Asgharizadeh, E. (2016). Presenting a hybrid ANN-MADM Method to Define Excellence Level of Iranian Petrochemical Companies. *Journal of Information Technology Management*, 6(2): 267-284.
- [18] Zakaryazad, Ashkan, and Ekrem Duman. "A profit-driven Artificial Neural Network (ANN) with applications to fraud detection and direct marketing." *Neurocomputing* 175 (2016): 121-131.
- [19] Semwal, Vijay Bhaskar, et al. "Design of Vector Field for Different Subphases of Gait and Regeneration of Gait Pattern." *IEEE Transactions on Automation Science and Engineering* (2016).