External fraud detection through big data: towards a pro-active operational risk management

di Giacomo Petrini

Abstract

In anni recenti, l'utilizzo di reti neurali artificiali ha condotto alla formulazione di modelli econometrici euristici, la forma strutturale dei quali evolve in tempo reale, man mano che i dati disponibili crescono nel corso del tempo. Tali approcci hanno beneficiato anche della crescita esponenziale delle capacità tecnologiche di calcolo, nonché della crescente disponibilità di dati pubblicamente disponibili.

In particolare, il recente sviluppo di reti neurali artificiali auto-adattive consente di disporre di modelli econometrici, la specificazione dei quali evolve in tempo reale, che possono essere tra l'altro utilizzati per identificare in tempo continuo eventi che si realizzano raramente e che mutano nel corso del tempo; per tali ragioni, le reti neurali auto-adattive possono essere impiegate dalle istituzioni finanziarie anche per identificare gli stream comportamentali associati ad eventi esterni di frode, offrendo il vantaggio di consentire un rapido riconoscimento di nuove fattispecie non appena queste si manifestano, senza tuttavia tralasciare l'identificazione di eventi pregressi.

Le istituzioni finanziarie sono infatti particolarmente esposte ad eventi esterni di frode, che di norma presentano la peculiarità di accadere in tempi ristretti e che sempre più, negli ultimi anni, si relazionano con la crescente evoluzione tecnologica, ad esempio per quanto concerne il sistema dei pagamenti.

Pertanto, un efficace ed efficiente sistema di identificazione e gestione di tali eventi richiede sia velocità nell'esecuzione dei controlli, sia l'esistenza di processi e procedure efficaci per l'adozione di idonee azioni di mitigazione.

Le funzioni di controllo interno, specificamente Risk Management e Internal Audit, possono pertanto rappresentare gli attori primari nel guidare le attività di disegno, sviluppo e gestione di moderne soluzioni di identificazione delle frodi esterne, che consentano di identificare velocemente nuove tipologie di frode al loro primo manifestarsi e di definire altrettanto rapidamente azioni di mitigazione efficaci, in modo da ridurne gli impatti economici attuali e prospettici, che potrebbero rappresentare rischi per la profittabilità e la reputazione di una istituzione finanziaria.

1 An introduction to artificial neural networks

In recent years, the exponential growth of calculation capacity has enabled the use both of longer time series and of more and more variables; the use of artificial neural networks has given rise to econometric models, evolving on a real-time basis as available data grow over time.

These artificial neural networks are particularly useful to make forecasts respecting a data universe that changes and/or grows quickly over time, particularly where the foreseen events are rare ones.

Generally speaking, an artificial neural network (ANN) is *"a massively parallel combination of* [connected] *simple processing unit which can acquire knowledge from environment through a learning process and store the knowledge in its connections"* [1]; these connections sometimes are called "synapses", and the learning process is usually defined as the modification of synaptic weights to capture information. Indeed, an ANN requires three more basic elements to work: (i) a summing function, to combine input with respect to corresponding synaptic weights, (ii) an activation function, to produce a computed output to be compared with environmental evidences, and (iii) a feedback function, to modify backward the synaptic weights by reason of the difference between the computed output and the environmental evidences.

Thus, an ANN is basically an iterative computational approach that employs a dataset of explanatory variables to fit given environmental evidences in a multidimensional, unconstrained data universe: *"ANNs are distributed, adaptive, generally nonlinear learning machines built from many different processing elements (PEs). Each PE receives connections from other PEs and/or itself. The interconnectivity defines the topology. The signals flowing on the connections are scaled by adjustable parameters called weights. The PEs sum all these contributions and produce an output that is a nonlinear (static) function of the sum. The PEs' outputs become either system outputs or are sent to the same or other PEs."*[2]

Therefore, the learning process of an ANN is a closed, dynamic computation. It has a beginning, once the four above mentioned basic elements have been created and once a dataset of input and output data has been prepared (so-called training dataset); it has a dynamic learning phase, during which the synaptic weights are iteratively modified by reason of the difference between the computed output and the environmental evidences; and it has an end, once the feedback function does not produce any further modification of the synaptic weights.

Thus, the ANN learning process outputs a closed (training-data driven) specification, i.e. a stable relation between input and output variables. This closed specification may then be applied to data, other than the training dataset, to obtain a model that explains environmental evidences.

[1] See Haykin S.; "Neural Networks: A Comprehensive Foundation", Prentice Hall, New Jersey, 1999.

[2] See Rojas R.; "Neural Networks: A Systematic Introduction", Springer-Verlag Berlin Heidelberg, 1996.

A new learning process is necessary whenever the computed output no longer represent an adequate fitting of the environmental evidences. For example, this happens when the analysis of the confusion matrix shows a declining capacity of correct classification over time.

Due to the exponential growth of calculation capacity, most recent developments allow to obtain "adaptive ANNs", as the so-called Self-Organizing Maps (SOMs), or Kohonen Maps: SOMs can modify their specification on an ongoing basis, while the training dataset grows over time with the inclusion of the most recent data.

Thus, they can be applied to a dataset that grows in size over time, as they produce a dynamic specification that evolves over time. At every moment, if the dataset does not change, a SOM can calculate the best-fitting specification in relation to the given dataset: this specification is usually called "a map".

Therefore, a SOM basically is *"a class of neural-network algorithms in the unsupervised-learning category"*[3] that is trained through unsupervised learning to produce a low-dimensional, discretized representation of the input space; SOMs operate in two ways: training and mapping: "training" builds the map using input examples, while "mapping" automatically classifies a new input vector.

In the SOM, the goal of learning is to cause different parts of the network responding similarly to certain input data. The synaptic weights are initialized either to small random values or sampled evenly from the subspace spanned by the two largest principal component eigenvectors.

The training uses competitive learning: when a training example is fed to the network, its Euclidean distance to all weight vectors is computed, and the PE whose weight vector is most similar to the input is called the "Best Matching Unit", or BMU. The weights of the BMUs and PEs, in the SOM grid, are adjusted towards the input vector. The magnitude of the change (or learning rate) decreases with time and with the grid-distance from the BMU.

Thus, SOMs differ from other ANNs because they apply competitive learning opposed to error-correction learning (such as back-propagation with gradient descent). They use a neighborhood function to preserve the topological properties of the input space, even if a SOM (unlike an ANN) can evolve its own topology over time.

To a greater level of detail, in the SOM algorithm, a Hebb-like learning rule is usually used, with time decreasing learning parameters. For all the PEs, the learning rate and the magnitude of its change decrease with time during the training phase, as the map stabilizes and learns the topographic map of the training dataset. At the final step, the learning-rate parameter usually has a very small value and so does the neighborhood function.

Therefore, the SOM algorithm cannot learn with adequate speed the new environmental evidences that may be different in statistical characteristics from the previously learnt training data: the time-decreasing learning rate and neighborhood function of the basic SOM algorithm reduce its capability to adapt weights for a varied environment.

A specific extension of the basic SOM is represented by the Time-Adaptive Self-Organizing Map (TASOM): it employs adaptive learning rates and neighborhood functions as its learning parameters, and every PE has its own learning rate and neighborhood size. For each new input vector, the neighborhood size and learning rate of the winning PE and the learning rates of its neighboring PEs are updated.[4]

Therefore, the learning parameters of every PE are time-independent and they change their values with the conditions of the incoming data, not with the elapse of time. Moreover, the learning parameters of each PE are adjusted independently for each PE, as the learning rate of each PE follows the values of a function of distance between the input PE and its synaptic weight. A similar updating rule is used to automatically adjust the width of the neighborhood function of each PE. The width of each output PE follows the distance between the PE synaptic weight and the weight of its neighboring PEs.

The operation of the TASOM algorithm may be summarized in eight steps:

1. Initialization: as in the case of a SOM, the synaptic weights are initialized either to small random values or sampled evenly from the subspace spanned by the two largest principal component eigenvectors;
2. Sampling: as in the case of a SOM, the training dataset is fed to the TASOM;
3. Similarity matching: the best-matching (or winning) PE is found, using the minimum-distance Euclidean norm as the matching measure:
4. Updating the neighborhood width: the neighborhood width of the winning PE is adjusted, while the neighborhood widths of the other PEs do not change;
5. Updating the learning-rate parameters: the learning rate parameters of all PEs in the network are adjusted independently for each PE;
6. Updating the synaptic weights: the synaptic weights of all PEs in the network are updated;
7. Updating the scaling values: the scaling values of all output PEs in the network are updated. A TASOM normalizes all distance calculations so as each distance calculation in the network algorithm is normalized by a scaling vector, composed of standard deviations of input vectors' components;

[3] See Kohonen, Kaski, Somervuo, Lagus, Oja, Paatero, 2004.

[4] See Shah-Hosseini, Safabakhsh, 2002, and Shah-Hosseini, Safabakhsh, 2003.

8. Continuation: the procedure restarts form step 2.

SOMs and TASOMs are particularly useful to make forecasts with respect to a data universe that changes and/or grows quickly over time, particularly where the events to be foreseen are rare ones.

2 Detecting external frauds in the financial sector with Data Analytics

A recent line of research deals with the application of SOMs and Data Analytics to the detection of external frauds.[5] External fraud events in the financial sector are usually not so frequent events, even if they can imply significant actual and perspective economic impacts, as they involve significant financial risks which may threaten profitability, and the image of a company.

Moreover, external frauds may assume several specific forms (e.g. credit cards forgery, identity theft, phishing, skimming, mobile SIM swapping, account hijacking, check-kiting schemes), but events usually happen in a short period of time and the technology side is more and more involved as payment systems evolve towards new technologies.

Thus, external fraud detection has to be fast to be effective, and usually the detection process requires the acquisition of several real-time raw data[6] to be managed under time pressure.

In these circumstances, the development of appropriate IT applications plays a central role in the creation of an effective detection process, as this issue can no longer be manually performed because it requires the use of data analysis tools and programs to be applied to large volumes of data.

Conventional fraud detection is sometimes ineffective, for example in online fraud, because online fraud is very dynamic and also technology development for conducting fraud is very dynamic and constantly changing.

Therefore, most recent evolutions are turning towards processes of continuous monitoring to identify potentially fraudulent anomalies in the data stream or in behavioral patterns, and to apply the result to prevent external frauds:[7] anomalies are identified starting from the activities or behavior typically observed in a single user (e.g. geospatial localization of the login site; identification of the computer model used to login; identification of the internet service provider used to login; activities performed after login; etc.), as this behavioral pattern can be used to establish an online behavior model of the user which is very specific and unique to him.[8]

This makes fraud easier to detect, because typically the fraudster does not know how the user behaves online, so it may be very difficult for the fraudster to appear like the account owner.

Such a behavioural analysis can also be integrated using other observable parameters of the session (e.g., IP address, HTTP header information, page views, etc.):

- the IP address provides an estimate of geospatial location, and information like country, city, network block, internet service provider;
- the HTTP header provides information of the operating system, user agent string, referrer string and browser type of the computer used to login;
- session time, session timeslot and session duration;
- amount, counterparty and details of the transaction, if any;
- etc.

On the analytical market, there is a wide spectrum of specialized tools that can support and enhance the antifraud activity. Anyway, their use is still limited, even if a proactive data monitoring/analysis remains one of the most effective tool for antifraud control, to reduce fraud losses and fraud scheme duration.[9]

Most recent continuous monitoring processes use SOMs and Data Analytics, combining specific methods and techniques from computer science, mathematical sciences, statistical, economic, psychology, law and other cognitive sciences. Usually, these processes apply operational analysis on short term, exploiting data and current information to detect fraud events with maximum efficiency.

[5] For a decade review from 2004 to 2015, see Albashrawi, Mousa, “Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015”, Journal of Data Science, Vol. 14, 2016.

[6] Nowadays text data, pictures, audio, video etc. comes from everywhere, from many different sources like contracts, customer interactions, call centers, social media, phones, emails, faxes, and others.

[7] A significant part of the involved data may also have to be stored, should it be later used in direct investigations. The Internal Audit should also access these data to make recommendations to improve the control activities.

[8] For present purposes, a "behavioral pattern" may be defined as a time sequence of actions, each of which produces measurable effects; the sequence always happens in the same chronological order, so that the chronological sequence of actions is relevant.

[9] For a review of the application of ANNs and SOMs to credit card fraud detection, see: Seeja, K. R.; Zareapoor, Masoumeh; “FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining”, Hindawi Publishing Corporation, The Scientific World Journal, Vol. 2014; Akhilomen, John, “Data Mining Application for Cyber Credit-card Fraud Detection System”, Proceedings of the World Congress on Engineering, Vol. 3, 2013.

Data analysis, in operational form, becomes also a tool for improving workplace conditions: most manual activities are avoided, especially for operations that require to process a significant amount of data.

In daily activities, the main role of operational analysis is to help detecting and fighting illegal activities, examining: (i) the links between suspects, (ii) their characteristics (director/and indirect subordination relations, positions in the hierarchy of the group, key positions that impact decision-making etc.), (iii) the movement of goods, money or other valuables, (iv) the way of communication (email, social networking), (v) the sequence of certain events, (vi) the modus operandi etc.

For example:

- sub (i) and (ii), the examination of the links between suspects and their characteristics may be relevant to identify "payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee (s.c. 'manipulation of the payer')";[10]
- sub (iii), the examination of the movement of goods, money or other valuables may be relevant to identify trade-based money laundering schemes, i.e. the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins; in practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports;
- sub (iv), the examination of the way of communication may help to discover potential illegal actor networks cases, where fraudsters pretend to be part of, or authorised by, a company and in doing so attempt to carry out 'scams' or frauds; these may involve offering a large sum of money to the recipient such as an inheritance or unclaimed bank funds, either in return for paying a modest sum (often referred to as transaction fees or brokering costs) or requiring the recipient's identity details;
- sub (v), the examination of the sequence of certain events may be relevant to identify the anomalies of the current spending pattern of a customer, with respect to his or her past spending behavior, so as to properly intercept new transactions that deviate from the learned profiles;
- sub (vi), the examination of the modus operandi may help to identify payment frauds through unauthorized access to mobile phone and/or online transactions, and to identify the precautions that need to be taken.

The success of this approach typically lies in the quality and variety of data sources.

Data mining, as an analytic process, is designed to explore data and to extract information from data sets, in order to discover patterns and relations.

It can be defined as *"the nontrivial extraction of implicit, previously unknown, and potentially useful information from data"*[11], or *"the science of extracting useful information from large data sets or databases"*[12].

Data mining shall include (but not be limited to):

a. analysis of the data-text, known as exploitation of data such as text, or "text mining"; it refers to the process of extraction of knowledge from documents, because information can be mostly found in text format, and it is considered one of the most important area in the database system;

b. geospatial analysis and visual analysis; they are important to understand the relevance of the location where events happened, to determine and discover patterns in fraud behavior.

In fact, successful implementation of an antifraud analytical system highly depends on the manner of retrieving data from a variety of sources, considering that most of them have different formats.

The data collected should be interpreted in the same way, using the same techniques and the same methodology, so that creation of data bases to be homogeneous.

3 A Self-Organizing Map for external fraud detection

We assume that nothing is known about external frauds, i.e. we don't have any aprioristic theory explaining the phenomenon. We also assume that we have a (scarce) history regarding external fraud events that hit our customers in the past (m events), and a (wider) history regarding legal transactions performed by the same customers (n events, n>m). Each transactions (legal or not) is accompanied by the time of its occurrence. Moreover, before each transaction occurrence, we can retrieve:

[10] See European Banking Authority, "EBA/GL/2020/01 - Guidelines amending Guidelines EBA/GL/2018/05 on fraud reporting under the Payment Services Directive (PSD2)", January 22, 2020.

[11] See Frawley, William J.; Piatetsky-Shapiro, Gregory; Matheus, Christopher J.; "Knowledge Discovery in Databases: An Overview".

[12] See Hand David J.; Mannila, Heikki; Smyth, Padhraic; "Principles of Data Mining".

- a set Γ of unstructured private data regarding the behavior of each customer of the bank;

- (through the access to customers' publicly available data, e.g. public profiles of their social media) a set Λ of unstructured public data.

The only variable that can let us organize Γ and Λ is the time: every piece of data embed the time of its occurrence, so that Γ and Λ can be ordered by the time of occurrence.

Thus, the dependent variable is represented by a vector Ψ composed of (n+m) rows, where every row assume the value 1 in the case of a fraud event, and 0 in the case of a legal transaction. It is a question of finding those relations between (current and lagged) data included in Γ and Λ that define the multidimensional hyper-surface (not necessary a hyperplane) that divides the estimation space between fraud events and legal transactions, as every transaction can be related to the actual observable parameters (including time, IP address,[13] browser, operating system, HTTP header,[14] etc.) corresponding to an event.

Although this approach sounds similar to the one applied to estimate models for credit risk parameters, the main difference is that the scope is not to estimate a model for forecasting fraud events.

Rather, it is to discover those multidimensional behavioral patterns, across time, that can be associated unambiguously to fraud events. Sometimes, the solution may be quite easy, considering any particular activity carried out in the account while logged into the account, as for example:

- an ATM withdrawal recorded in a certain country, while geo-localization data embedded in a public post on a social media show that the customer was in another country at the same time of the withdrawal;
- a credit card payment made from a masked IP address, while behavioral data of our customer show that he never used IP-masking in the past;
- an online banking transaction made from an IP address of a certain country, while geo-localization data, embedded in a public post on a social media, show that the customer was in a faraway place at the same time of the transaction;
- an online banking transaction made from a different computer ID, and/or with a different HTTP header information.

Indeed, detection can prove a more difficult task for fraud events different from those related to the payment system. All of these concern more structured behavioral patterns, sometimes involving groups of connected customers.

Anyway, the exact time sequence of the fraudster actions becomes important using this approach. In fact, the analysis focuses on the kinds of things users generally do before a fraud event, thus detecting specific known fraud patterns.

For these reasons, a heuristic neural network approach seems preferable, as it does not necessarily require linear relations between dependent (Ψ) and independent (Γ and Λ) variables, neither it requires an aprioristic model identification[15].

Instead, this approach lets the data identify those structural relations that can offer the better explanation of fraud events.

Furthermore, fraud events do not represent a close universe over time: both technology evolution and the adoption of effective mitigation techniques can modify the set of events to be detected, or because new types of external fraud arise, either because some kind of them are effectively mitigated[16].

Thus, a TASOM can be applied for detection purposes of external fraud events, as it upgrades on an ongoing basis, while the training dataset grows over time with the inclusion of the most recent data.

In fact, as the adaptive capabilities of a SOM or a TASOM modify when the magnitude of the changes decreases with time, these algorithms (when developed recursively over time) could be particularly useful to identify the behavioral patterns of external frauds, compared to most recent data, without neglecting the peculiarities of most ancient data.

Thus, this approach can detect new kinds of frauds, even though these new frauds have never been seen before, because it is based on the user's behavior, while old fraudulent activities and events are still taken into account, with their specific known rules, patterns, and/or indicators.

This approach can be used to generate alerts or warnings for real-time events where applied to real time transactions. Every event starts with someone, either a user or a fraudster, initiating an observed event that includes, for example, someone logging in to the user's account and/or any activity taken during an online session (e.g., checking account balance, transferring funds between accounts, viewing account information, etc.).

[13] Usually, the IP address provides an estimate of location information like country, state, city, network block, and internet service provider.

[14] Usually, the HTTP header provides information of the operating system, user agent string, referrer string, and browser type of a computer used for an event.

[15] In econometrics, the identification problem consists in identifying both the exogenous and endogenous variables and the relation between them.

[16] For example, at the beginning of the century, the frauds involving cloning ATM cards were effectively mitigated through the introduction of micro-chipped cards, so that related external frauds were considerably reduced.

The observed event may or may not be an online event. Each event includes or corresponds to one or more event parameters, collected by the set of unstructured private data. Event parameters are directly observable parameters of an event, or raw data that can be measured and/or observed. Examples of event parameters incorporate, but are not limited to:

- network information that include parameters of the network by which an online event is occurring (e.g., IP address, and country, state, city are derived parameters derived from network information),
- user agent parameters (operating system and browser of device or computer used for the event),
- event or session time,
- time sequence of deposits and withdrawals and/or of other incoming and outgoing bank records,
- time sequence of the banking transactions and operations conducted from, to or via one or more bank accounts or by specified persons during a specified period.

4 Potential contribution to Operational Risk Management (ORM) and Audit functions

According to their respective attributions, both the ORM and the Internal Audit functions are in some way involved in the detection and monitoring processes of external frauds. On one hand, the Operational Risk Management (ORM) is liable with regard to monitor and measure over time the loss events, including external frauds, and to coordinate the design of appropriate and effective mitigation actions. On the other hand, the Internal Audit function is liable with regard to the evaluation of the continuous effectiveness of the internal control system.

External frauds events usually happen in a short period of time and the technology side is more and more involved as payment systems develop new technologies. Therefore, external fraud detection has to be fast to be effective, and usually the detection process needs to acquire several real-time raw data to be managed under time pressure.

In this respect, TASOMs can be effectively applied for detection purposes, because they can apply operational analysis and exploit data and current information to detect fraud events with maximum efficiency.

Moreover, they can keep memory of previously identified fraudulent behavioral patterns, while upgrading on an ongoing basis, as the training dataset grows over time with the inclusion of the most recent data; they can therefore detect new kinds of frauds, even though these new frauds have never been seen before, while old fraudulent activities and events are still taken into account.

Thus, at the design stage, the ORM function may liaise with the IT function to draw up the application architectures, considering properly that the IT applications should be strictly interlinked with transactional data and databases, rather than with summary databases. Moreover, the same ORM function may also liaise with the Organization function to define the whole process of external frauds identification and management, which should ensure high effectiveness to be achieved in a limited period of time.

On the other hand, still at the design stage, the Internal Audit function may review the project activities, both to get comfortable with the IT and organizational developments and to ensure that all the relevant information is acquired and treated in a proper way.

During the operational phase, both the above mentioned functions can analyze the SOM results to decide which action is needed: the ORM function may focus on high frequency and/or high impact external fraud events (to coordinate the design of appropriate and effective mitigation actions), while the Internal Audit function may focus on emerging external fraud schemes, to evaluate the continuous effectiveness of the internal control system and, where appropriate, to address suitable evolutionary actions. A similar approach could be applied more generally by the Audit function to other areas of interest for its activities. Examples of potential application could be, but not limited to:

- the detection and the prevention of internal fraud events; TASOMs could be applied to identify the fraudulent behavioral patterns of company’s employees, and the application could employ also the accounting information recorded through internal front-end procedures and the detailed data contained inside the so-called “giornale di fondo”;
- the identification of the behavioral patterns related to money laundering phenomena; TASOMs may be applied to identify the customers’ behavioral patterns that are related to the concealment of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses;[17]
- the accounting audit activities, to analyze accounting data and identify unsustainable forecasting accounting variable time-series (such as cash flows or earnings) and/or anomalous accounting entries.[18]

In the above mentioned areas of interest, the application of TASOMs represent an effective analytical instrument to quickly identify behavioral sequences that are related to given output phenomenona; these behavioral patterns, once identified through

[17] See for example the series “Quaderni dell'antiriciclaggio” published by the “Unità di Informazione Finanziaria per l'Italia” (s.c. UIF), which includes several examples of misconduct aimed at “washing” illegally obtained money; these behavioral schemes can be easily translated in a chronological set of actions inside a TASOM.

[18] See Kokina J.; Davenport T. H.; “The Emergence of Artificial Intelligence: How Automation is Changing Auditing”.

the training dataset, give shape to the learning parameters that, from then on, may increase or decrease for adaptation to a changing environment with non-stationary input distributions.

Moreover, in the same areas of interest, it is relevant to keep memory of previously identified behavioral patterns, while the detection framework upgrades on an ongoing basis, as most recent data are included in the training dataset; TASOMs can vouch for that, taking into account old behavioral patterns, and they can also detect and identify new kinds of events, even though they have never been seen before.

Anyway, to a more general level, TASOMs and other ANNs could be employed both by Risk Management and Audit functions in many other fields, for example (but not limited to):

- the risk assessment activities: through the use of data extracted from real cases, the Audit function could identify higher-risk processes and evaluate the effectiveness of the internal control system.[19] Similarly, the Risk Management could employ external data to identify higher-risk credit or financial sub-portfolios, and to define suitable mitigation actions;
- the scenario analysis: ANNs could be used both to generate a plethora of stochastic scenarios and to identify the transmission mechanism to final control variables;
- the project risk management: ANNs could be used in the scheduling of complex projects, to identify hidden relation between single tasks and to help the project management; unlike the use of PERT charts, the use of ANNs could consider iterations and feedbacks, where tasks may have to be reworked, so as to take note of task iterations and iterative development processes.

5 Concluding remarks

Recent developments in econometric research can take advantage of both the exponential growth of calculation capacity and the growing availability of public data. Recently, new procedures are quickly establishing: the use of artificial neural networks is giving rise to econometric models that evolve on a real-time basis, as available data grow over time. These may be used to identify rare events at any particular time, on the basis of the information available until that moment.

SOMs and TASOMs are more and more used to identify the behavioral patterns of external frauds, with respect to most recent data, without neglecting the peculiarities of most ancient data.

Thus, this approach can detect new kinds of frauds, even though these new frauds have never been seen before, because it is based on the user's behavior. Furthermore, old fraudulent activities and events are still taken into account, with their specific known rules, patterns, and/or indicators.

Financial institutions are particularly exposed to external frauds: external fraud events usually happen in a short period of time and the technology side is more and more involved as payment systems evolve towards new technologies.

Therefore, external fraud detection has to be fast to be effective, and usually the detection process requires to acquire several real-time raw data to be managed under time pressure.

The internal control functions, primarily ORM and the Internal Audit, can be involved in the design, development and operational phases of any modern solutions that quickly identify and manage emerging external fraud schemes, so as to swiftly define and apply effective mitigation actions, and to reduce actual and perspective economic impacts which may threaten profitability and the image of a financial institution.

Giacomo Petrini

[19] See Ramamoorti, S.; Bailey, A. D. Jr; Traver, R. O.; “Risk Assessment in Internal Auditing_ A Neural Network Approach”.

Bibliography

AIFIRM – Associazione Italiana Financial Industry Risk Managers, “Position Paper N° 14 - Intelligenza Artificiale: l’applicazione di Machine Learning e Predictive Analytics nel Risk Management”, February 2019

Akhilomen, John, “Data Mining Application for Cyber Credit-card Fraud Detection System”, Proceedings of the World Congress on Engineering, Vol. 3, 2013

Albashrawi, Mousa, “Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015”, Journal of Data Science, Vol. 14, 2016

Baldwin, Amelia A.; Brown, Carol E.; Trinkle, Brad S,; “Opportunities for Artificial Intelligence Development in the Accounting Domain: The Case for Auditing”, Intelligent Systems in Accounting, Finance and Management, Vol. 14, 2006

Banarescu, Adrian, “Detecting and Preventing Fraud with Data Analytics”, Procedia Economics and Finance, Vol. 32, 2015

European Banking Authority, “EBA/GL/2020/01 - Guidelines amending Guidelines EBA/GL/2018/05 on fraud reporting under the Payment Services Directive (PSD2)”, January 22, 2020.

Fletcher, H. Glancy; Surya, B. Yadav; “A computational model for financial reporting fraud detection”, Decision Support Systems, Vol. 50 (3), February 2011

Frawley, William J.; Piatetsky-Shapiro, Gregory; Matheus, Christopher J.; “Knowledge Discovery in Databases: An Overview”, AI Magazine, Vol. 13, Number 3, 1992

Hand David J.; Mannila, Heikki; Smyth, Padhraic; “Principles of Data Mining”, MIT Press, 2001

Haykin S.; “Neural Networks: A Comprehensive Foundation”, Prentice Hall, New Jersey, 1999

Kohonen, Teuvo, “Exploration of very large databases by self-organizing maps”, Proceedings of International Conference on Neural Networks (ICNN'97), June 1997

Kohonen, Teuvo; Kaski, Samuel; Somervuo, Panu; Lagus, Krista; Oja, Merja; Paatero, Vesa; “Self-organizing map”, CIS Biennial Report 2002-2003, Ch. 8, 2004

Kokina, Julia; Davenport, Thomas H.; “The Emergence of Artificial Intelligence: How Automation is Changing Auditing”, Journal of Emerging Technologies in Accounting, Spring 2017, Vol. 14, No. 1, pp. 115-122

Ramamoorti, Sridhar; Bailey, Andrew D. Jr; Traver, Richard O.; “Risk Assessment in Internal Auditing: A Neural Network Approach”, International Journal of Intelligent Systems in Accounting, Finance & Management, Vol. 8, 1999

Rojas R.; “Neural Networks: A Systematic Introduction”, Springer-Verlag Berlin Heidelberg, 1996.

Seeja, K. R.; Zareapoor, Masoumeh; “FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining”, Hindawi Publishing Corporation, The Scientific World Journal, Vol. 2014

Shah-Hosseini, Hamed; Safabakhsh, Reza; "TASOM: A New Time Adaptive Self-Organizing Map", IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, Vol. 33 (2), April 2003

Shah-Hosseini, Hamed; Safabakhsh, Reza; "The Time Adaptive Self-Organizing Map for Distribution Estimation”, International Journal of Engineering, Vol. 15, No. 1, February 2002

Zhang, Bin; Zhou, Yi; Faloutsos, Christos; “Toward a Comprehensive Model in Internet Auction Fraud Detection”, Proceedings of the 41st Hawaii International Conference on System Sciences, 2008

RISK MANAGEMENT MAGAZINE

Anno 15, numero 1 **Gennaio – Aprile 2020**

Poste Italiane - Spedizione in abbonamento postale – 70% aut. DCB / Genova nr. 569 anno 2005

TESTATA INDIPENDENTE CHE NON PERCEPISCE CONTRIBUTI PUBBLICI (legge 250/1990)

In collaborazione con REFINITIV

IN QUESTO NUMERO

Rivista accreditata AIDEA

Risk Management Magazine
Anno 15 n° 1 Gennaio - Aprile 2020

Direttore Responsabile:
Maurizio Vallino

Condirettore
Corrado Meglio

Vignettista: Silvano Gaggero

Proprietà, Redazione e Segreteria:
Associazione Italiana Financial Industry Risk Managers (AIFIRM), Via Sile 18, 20139 Milano

Registrazione del Tribunale di Milano n° 629 del 10/9/2004

ISSN 2612-3665

E-mail: risk.management.magazine@aifirm.it; Tel. 389 6946315

Stampa: Algraphy S.n.c. - Passo Ponte Carrega 62-62r 16141 Genova

Le opinioni espresse negli articoli impegnano unicamente la responsabilità dei rispettivi autori

SPEDIZIONE IN ABBONAMENTO POSTALE AI SOCI AIFIRM RESIDENTI IN ITALIA, IN REGOLA CON L'ISCRIZIONE

Rivista in stampa: 8 Aprile 2020