Webology (ISSN: 1735-188X)
Volume 16, Number 2, 2019

Machine Learning Fraud Detection System In The Financial Section

Satyanarayan kanungo[1] , Pradeep Kumar[2]

[1]Independent Researcher, USA. https://www.linkedin.com/in/kanungosatyanarayan

[2]Independent Researcher, USA https://www.linkedin.com/in/pradeep017

Abstract: Financial fraud is a deliberate distortion of an organisation's financial statements, through exaggeration to provide a positive impression of the organisation's financial condition and cash flow. A committee of senior management in the cybercrime section are activated to catch these types of financial fraud transactions. The anti-fraud systems are associated with detecting the largest and most suspicious transactions. Small crimes may cause big losses in the financial transition sector. This proposed antifraud approach provides benefits because it can easily detect harmful operations.

Keywords: Fraud detection, CSIRT, architecture, machine learning.

Introduction

Nowadays, financial fraud cases are increasing through electronic banking facilities. Finally, transaction systems are tracked and monitored by the specialist in the cybercrime sector. The financial sector workers can detect thread which provides security and protects the network from hackers. The banking system which operates financial transactions throughout the day, provides security audits and insight tests to apply new security policies which should implement insight into the organisation to detect and respond to the current thread. Hackers are not only the target of the banking sector, but they also attack the mobile phones of individuals to decrepit OTP SMS codes. In order to detect these types of threats, financial organisations are investing capital to hire antifraud software. This capital helps to hire more employees in the "Computer Security Incident Response Team (CSIRTs)" Department [11]. The main task of this organisation is to provide modern types of solutions which will help to reduce the risk of financial transition.

Related Work

Financial organisations are looking for modern solutions with the help of specialists from CSIRT to react to threats of personal money and data of clients on an ongoing basis [1]. Different types of methods are used to identify the threats. The CSIRT method investigates different types of fraud cases through an anti-fraud system. The team has the authority to write the anti-fraud rules to block these threats. Otherwise, these types of threads are the main reason for rising internet traffic to find anomalies. As per the network rules on the firewall system, every organisation can deactivate these threads. The thread detection methods depend on post-mortem debugging, which can detect the actual fraud which is already happened [12]. The banking sector banks want to minimise these attacks on financial transition so that their customers cannot be affected. In the case of 0-day fraud, CSIRT's methods need more time to ready their defence system against these threats which run non-stop, it is the main target of CSIRTs to create 0-day fraud [2].

The media describes the types of fraud cases as “breaking into a bank”, which affects its trustworthiness and credibility. Creating these rules is not only the solution to these financial translation problems. A few transactions are known as “grey” scoring, which the banking sector cannot authorise because it is not possible for insufficient workers in a call centre. The bank’s operation roughly calculated this risk and its bears on its outcomes in financial losses. In this literature, an effective Machine-Learning scoring system is developed, which applies the previous warning system against the fraud in banking sector [13]. This system helps to analyse the login system from the customer side to monitor the banking transaction system depending on anti-fraud rules. This method can decrease fraud and enhance call centre chain management [19].

Modern antifraud scoring architecture system: CISIRT

Depending on a modern antifraud, a new type of scoring architecture system is proposed. Figure 1 represents the scoring architecture which is known as CSIRTs and used in the banking sector. The main approach of the traditional machine learning module with the help of an “external scoring system” can provide the possibilities of the expert systems which follow the anti-fuad rules [14]. The banking sector architecture does not want to advance their systems. The data flow of the proposed architecture is defined below:

Modules

There are a total of twelve modules in this architecture which follow machine learning scorning extension.

Channels: The electronic channels which operate by the customers of the banking sector, use the platform provided by the banks to do non-financial and financial transactions.

Balance the loads: This method has an application which cuts down traffic into different individual web application firewall illustrations to provide services. The infrastructure of the banks including software can handle sudden, occasional and drastic which can maximise the traffic [18].

Web application firewall: The main task of a firewall is to check the outsider’s request to know which one is a thread and which one is authentic and provide a channel to access these. In order to do this HMAC or other types of algorithms are used in this method.

Antifraud system: This system is associated with a processing module, rules testing, rules editor, interface for administrators and validation module [3].

The processing of this module is responsible for following the anti-fraud rules depending on the processing request which follows the business actions. These actions are written below:

“OK”: This indicates that the request is shifted to the financial sector (core). It is known as a white button.

“NOT OK”: This indicates that the system rejects the request automatically and performs several actions which are present in programs such as informing the user about the instructions depending on notification and shifting the report to CSIRT. This is known as the black button [15].

“MANUAL”: At the time, when the system provides meaningful information to CSIRT to mention their demand manually by providing specific operations. It is known as a grey button.

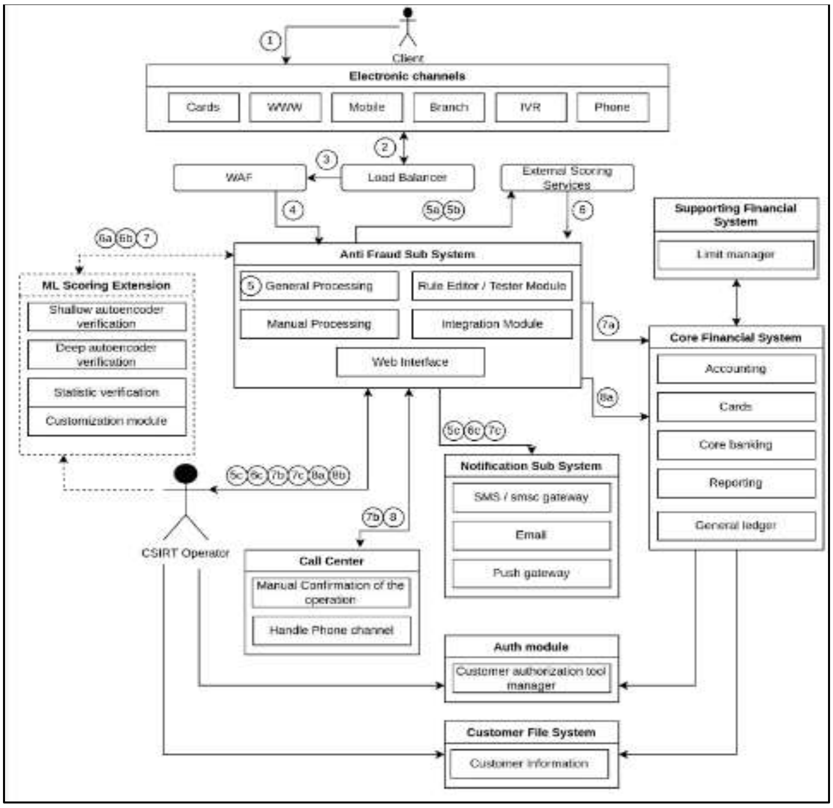

Figure 1: Machine learning depends on the Scoring System.

Source: [3]

Machine Learning Scoring Extension

In this part, the modules used in the ML scoring system are described properly. In Figure 2 the dataflow of this model is shown.

External gateways: The task of this gateway is to receive all the requests from outer and rectify which requests are authentic and which are related to the thread. The authentic requests are forwarded to the integration part of the module. The technological structure of the IT sector obliges modern systems to adapt to the systems which are already used. Modern systems with additional features can easily implemented in the current structure [16]. Because total development is costly, time-consuming and risk-associated.

Integration Module: In order to implement modern and advanced software, the suppliers are responsible for doing this. In this situation, fintech/startup organisations are exceptions because these organisations take responsibility for integration. This part of the module receives the information from external gateways and then converts this information into internal Machine Learning scoring [4].

External API: This part wants to incorporate external software. Organisations get benefits when they use external API in external gateways. Data and services follow a popular ML scoring format. In this format, the organisation ignores the loss in the process of transformation between various formats and provides easy solutions. Using external API with the help of modern technology such as AMQP (RabbitMQ) and REST API (NodeJS). The external API, known as internet API, creates different layers separated from the core section of the implementing module [17].

Internal API: In this particular system, each service has a particular scheme and this scheme uses OpenApi. Each part of this module directly communicates with the core section of the module. The services of internal API arrange the missing data from different services and make complex types of core requests.

Core: It is the main part of this module uses CPP language. This part maintains the operations, controls and executes nonsynchronous repeated operations. The function of the core section includes router services. This section of API forwards the request to the proper module.

Reporting module: This section creates reports on a daily or periodic basis. The service issues which affect ion the report is allowed by this module. This module creates a completely different database which creates reports and does not disturb the whole system[20].

Scoring module: This module provides a solution based on machine learning. Its cooperation is associated with the responses received from the user such as MANUAL, OK and NOT-OK.

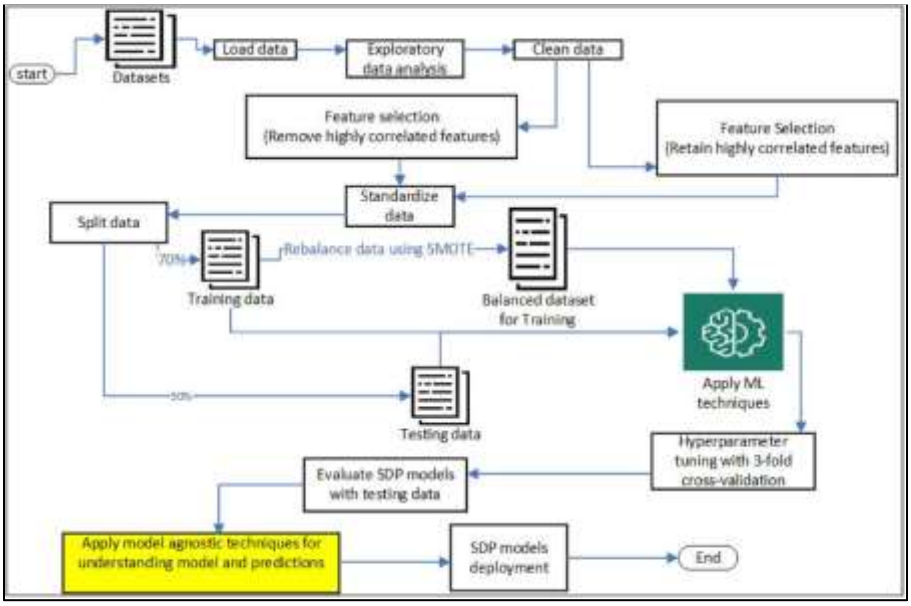
start
Datasets
Load data
Exploratory data analysis
Clean data
Feature selection (Remove highly correlated features)
Feature Selection (Retain highly correlated features)
Standardize data
Split data
70%
Training data
Rebalance data using SMOTE
Balanced dataset for Training
Apply ML techniques
30%
Testing data
Hyperparameter tuning with 3-fold cross-validation
Evaluate SDP models with testing data
Apply model agnostic techniques for understanding model and predictions
SDP models deployment
End

Figure 2: ML scoring module architecture.

Source: [4]

Machine Learning Execution Module

In this approach, an ML-based module for data scoring banking systems is proposed which will work at the time when users operate the banking system. Depending on the data, a modern approach is proposed. This approach is described below.

Data Acquisition

Depending on the ML the information is collected based on real-world information such as the number of logging attempts over three months from Poland’s bank server.

Training dataset	
Data collection time	28th January to 28th March 2018
Number of discarded records (heartbeat)	Roughly 3.7 million
Number of records	Oliver 5.6 million
Number of trainings	1,918,338
Features effective engineered	● User's "Autonomous System Number (ASN)" ● Timestamp from server side ● User's browser type ● User's operating system type ● User's browser version ● Time of operation (like evening, afternoon, working hours) ● The IP address of the user ● Working/nonworking days
Features raw extracted	● ID session ● User's operating type ● User's IP address ● User's browser version and type ● User's operating system type
Number of features (including encoding)	35
Training or test of database (%)	80.18

This survey directly obtains the user's IP address depending on data collection data but these data are used to find the "autonomous system number (ASN)" and the user's physical location depends on commercial databases [8].

Description of ML Model

This study is related to two autoencoder models:

(a) Classical (AE), also known as shallow, consists of input layer I which has a total of 36 inputs and the feature of encoding data vector. Here the code represents layer C which is associated with 3 neurons and regular output layer O. This is associated with 36 neurons [7].

(b) Deep AE is associated with additional layers H1 and H2 which are hidden and symmetrical.

It consists of 10 neurons which take part in the encoder or decoder section. This ML model follows the "Keras Version 2.2.4" and depends on the "TensorFlow framework (Version

1.13.1)”. These two models are applied sigmoid as the active function in the last section of the layer. Intermediate and input layers are used to test both Swish and ReLU. These are the active functions for all layers, but not the last models [9]. For these models, the Swish function is used because it is a faster merging of the outputs.

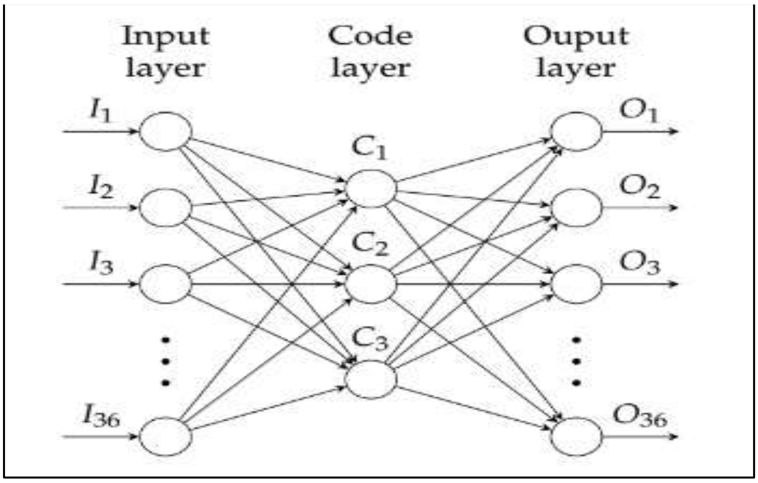

Figure 3: Shallow autoencoder model(a)
Source: [5]

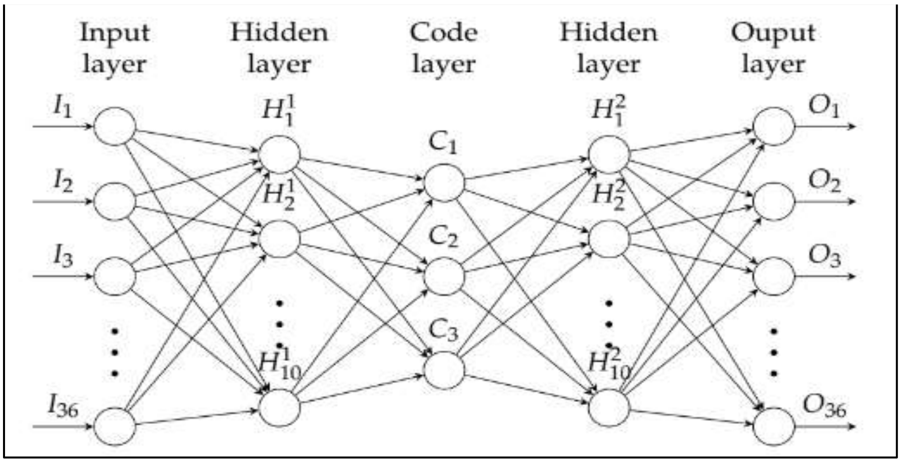

Figure 4: Deep autoencoder model (b)
Source: [6]

Training Procedure

At the time of training, autoencoder model (a) for forty to fifty responses is gained to reach convergence by gaining an MSE of 0.01558 on the test. The deep model (b) demanded more training approaches from the autoencoder model [10]. These models are used for regularisation of the code layer which is important for autoencoders and use an adaptive moment estimation algorithm. This training is focused on 1024 records. The “Mean-Squared Error (MSE)” is calculated as the loss of both models.

Results

From the deep autoencoder model (b), the total reconstruction error is 0.0127, it is smaller than the shallow autoencoder model and provides high representation learning power and higher restoration capacity depending on the more complicated structure.

Conclusion and Future Work

In this literature, modern architecture proposes an antifraud system based on an ML scoring module. These modules take a part in data flow and architecture. This module is associated with classifying operations, and decision-making like black, white or grey. This module is created as an unsupervised method to differentiate between legitimate and rogue login attempts with the help of two types of autoencoder models (deep and shallow). These models are helping to detect fraud attacks depending on real information. The outputs provide autoencoders which use an ML-based scoring application to detect fraud in the banking sector. In future, this system will expand depending on behavioural models which can able to find out the issues from the user side. This expansion is associated with knowing the user behaviour, identifying the user and profiling this.

References

[1] Homan, D., Shiel, I. and Thorpe, C., 2019, June. A new network model for cyber threat intelligence sharing using blockchain technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.

[2] Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T. and Pérez, E., 2017. An integral model to provide reactive and proactive services in an academic CSIRT based on business intelligence. Systems, 5(4), p.52.

[3]Saragih, M.G., Chin, J., Setyawasih, R., Nguyen, P.T. and Shankar, K., 2019. Machine learning methods for analysis fraud credit card transaction. International Journal of Engineering and Advanced Technology (IJEAT). ISSN, pp.2249-8958.

[4]Rashid, R.A., Chin, L., Sarijari, M.A., Sudirman, R. and Ide, T., 2019, July. Machine learning for smart energy monitoring of home appliances using IoT. In 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 66-71). IEEE.

[5]Tian, Q., Li, J. and Liu, H., 2019. A method for guaranteeing wireless communication based on a combination of deep and shallow learning. IEEE Access, 7, pp.38688-38695.

[6]Qi, Y., Shen, C., Wang, D., Shi, J., Jiang, X. and Zhu, Z., 2017. Stacked sparse autoencoder-based deep network for fault diagnosis of rotating machinery. Ieee Access, 5, pp.15066-15079.

[7]Gao, X., Shan, C., Hu, C., Niu, Z. and Liu, Z., 2019. An adaptive ensemble machine learning model for intrusion detection. Ieee Access, 7, pp.82512-82521.

[8]Hardjono, T., Lipton, A. and Pentland, A., 2019. Toward an interoperability architecture for blockchain autonomous systems. IEEE Transactions on Engineering Management, 67(4), pp.1298-1309.

[9]Beyer, M., Morozov, A., Ding, K., Ding, S. and Janschek, K., 2019, October. Quantification of the impact of random hardware faults on safety-critical ai applications: Cnn-based traffic sign recognition case study. In 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (pp. 118-119). IEEE.

[10]Zhang, L., Luo, T., Zhang, F. and Wu, Y., 2018. A recommendation model based on deep neural network. IEEE Access, 6, pp.9454-9463.

[11]Johansson, E. and Elvin, G., 2017. The impact of organizational culture on information security during development and management of IT systems: A comparative study between Japanese and Swedish banking industry.

[12]Tsakalidis, G. and Vergidis, K., 2017. A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), pp.710-729.

[13]Xue, D., Li, J., Lv, T., Wu, W. and Wang, J., 2019. Malware classification using probability scoring and machine learning. IEEE Access, 7, pp.91641-91656.

[14]Shan, C., Weng, C., Wang, G., Su, D., Luo, M., Yu, D. and Xie, L., 2019, May. Component fusion: Learning replaceable language model component for end-to-end speech recognition system. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 5361-5635). IEEE.

[15]Valladares, P., Fuertes, W., Tapia, F., Toulkeridis, T. and Pérez, E., 2017, July. Dimensional data model for early alerts of malicious activities in a CSIRT. In 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS) (pp. 1-8). IEEE.

[16]Hanif, A., Jamal, F.Q. and Imran, M., 2018. Extending the technology acceptance model for use of e-learning systems by digital learners. Ieee Access, 6, pp.73395-73404.

[17]Akasiadis, C., Pitsilis, V. and Spyropoulos, C.D., 2019. A multi-protocol IoT platform based on open-source frameworks. Sensors, 19(19), p.4217.

[18]Tekerek, A. and Bay, O.F., 2019. DESIGN AND IMPLEMENTATION OF AN ARTIFICIAL INTELLIGENCE-BASED WEB APPLICATION FIREWALL MODEL. Neural Network World, (4).

[19]Hossain, E., Khan, I., Un-Noor, F., Sikander, S.S. and Sunny, M.S.H., 2019. Application of big data and machine learning in smart grid, and associated security concerns: A review. Ieee Access, 7, pp.13960-13988.

[20]Satish, Karuturi S R V, and M Swamy Das. "Review of Cloud Computing and Data Security." IJAEMA (The International Journal of Analytical and Experimental Modal Analysis) 10, no. 3 (2018): 1- 8.

[21]. Satish, Karuturi S R V, and M Swamy Das. "Multi-Tier Authentication Scheme to Enhance Security in Cloud
Computing." IJRAR (International Journal of Research and Analytical Reviews) 6, no. 2 (2019): 1-8.

[22]Dhankhad, S., Mohammed, E. and Far, B., 2018, July. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In 2018 IEEE international conference on information reuse and integration (IRI) (pp. 122-125). IEEE.