Fraud detection system in payment systems

Lynx, created by the *Instituto de Ingeniería del Conocimiento (IIC –Institute of Knowledge Engineering),* is used to effectively detect fraud in payment systems in real time with a multichannel focus. It allows intervening in the authorization process of the transaction taking into account the specific characteristics of the channel where it originates from (ATM, commerce, internet banking, telephone banking, branch office, etc.). The risk analyst is also offered a global vision of the client's bank account movements. The system is the result of their own behaviour patterns detection technology, based on statistic models and particularly on neural networks.

PRODUCT

The Lynx fraud detection system allows financial entities to act online on a current transaction, taking into account the fraud risk level assigned and complementing it with other parameters associated to business variables.

Its goal is to lessen the impact of fraud in the entities' results. To do this, it analyses the transaction's features to detect possible fraud behaviour patterns and, additionally, identify those transaction access points (commerce, cash point, telephone, etc.) suspected of conniving with fraud and particularly the possible sources where information is copied.

Lynx combines the advantages of the **parametric** and **statistical models:** the former allow including rules that reproduce the expert analysts' behaviour and the latter detect and include fraudulent behaviour patterns through the historical analysis of the data, providing a better false/positive ratio and higher execution performance.

COMPONENTS

Lynx consists of a set of modules or components described below:

Clients/Accounts Module: this is the system's main component. It monitors in **real time** the bank transactions carried out across all the client's accounts and originated from different entry channels, informing the authorising system of the risk level of said transactions. The Lynx fraud detection system is reinforced by its **multichannel** approach. This module also stores the fraud alerts in a database to aid analysts when consulting them and to be used by the rest of the system modules.

Location Module (channel access points): this component allows the analysis of the transaction access point's behaviour in order to detect fraudulent transactions. In the specific case of card transactions, it detects the point of compromise (POC), potential places where card copies could have been made and conniving businesses or points of use. In the case of internet banking the IP access transmission is analysed; in call centres the number of received calls and/or the operator if there is one. In short, any element which may be susceptible of being a hub of fraud.

Alert communication to an external system: this interface allows establishing a link with an external system to help to automate alerts. This external system can use the information provided by Lynx to implement any type of procedure such as sending a SMS or communicating with a call centre.

eLynx: this component is included to boost fraud detection made with cards not present in ecommerce. It allows all parties or agents involved to intervene in the fraud identification process: card issuer, acquirer and retailer where the purchase is made.

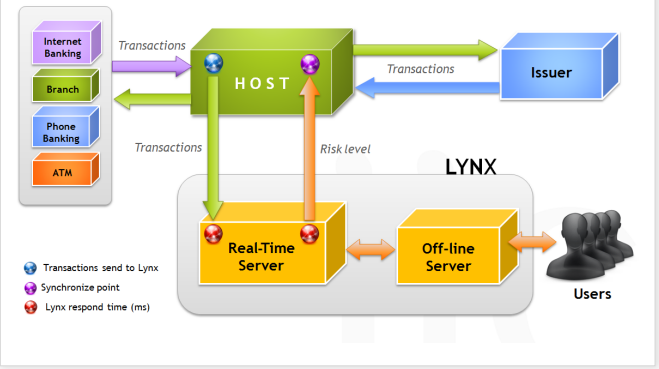
LYNX ARCHITECTURE

Lynx directly receives from the host the transaction information, qualifying it and generating a response message with the recommended action based on the risk level or the business own rules. When a transaction is alerted it is stored in a database for future consultation and review by the analysts. They access the alerts via a web page using a secure and encrypted connection to the server. Lynx has a hierarchy of users (administrator, supervisor, analyst, etc.) and allows different security levels when accessing the information.

TECHNICAL REQUIREMENTS

The server is available on IBM pSeries AIX and Intel Linux RedHat architectures. The supported database platforms are Oracle Enterprise Edition y DB2 UDB. The client equipment only needs a network connection and an Explorer or equivalent web browser.

Architecture: Lynx real-time transactions flow



Original product property of:

adic
asociación para el desarrollo de la ingeniería del conocimiento

C/ Francisco Tomás y Valiente, nº 11
EPS, edificio B, 5ª planta
UAM Cantoblanco.
28049 Madrid, Spain

Tel.: (+34) 91 497 2323
Fax: (+34) 91 497 2334
iic@iic.uam.es
www.iic.uam.es