IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Fraud Find: Financial Fraud Detection By Analyzing Human Behavior

Dr.B Naveen Kumar[1],Eshadhari Bhavani[2], G Venkata Sai Kumar[3], Ch Satwika Pardhu[4,], Adi Adhitya Patel[5]

[2,3,4,5] UG Scholars, Department of CSE, **AVN Institute of Engineering and Technology,**Hyderabad, Telangana, India.

[1]Assoiate Professor, Department of CSE, **AVN Institute of Engineering and Technology**, Hyderabad, Telangana, India.

ABSTRACT

Financial fraud is commonly represented by the use of illegal practices where they can intervene from senior managers until payroll employees, becoming a crime punishable by law. There are many techniques developed to analyze, detect and prevent this behavior, being the most important the fraud triangle theory associated with the classic financial audit model. In order to perform this research, a survey of the related works in the existing literature was carried out, with the purpose of establishing our own framework. In this context, this paper presents Fraud Find, a conceptual framework that allows to identify and outline a group of people inside a banking organization who commit fraud, supported by the fraud triangle theory. Fraud Find works in the approach of continuous audit that will be in charge of collecting information of agents installed in user's equipment. It is based on semantic techniques applied through the collection of phrases typed by the users under study for later being transferred to a repository for later analysis. This proposal encourages to contribute with the field of cyber security, in the reduction of cases of financial fraud.

INTRODUCTION

Fraud is a worldwide phenomenon that affects public and private organizations, covering a wide variety of illegal practices and acts that involve intentional deception or misrepresentation. According to the Association of Certified Fraud Examiners (ACFE) fraud includes any intentional or deliberate act of depriving another of property or money by cunning, deception or other unfair acts. The 2016 PwC Global Economic Crime Survey report describes that more than a third of organizations worldwide have been victims of some kind of economic crime such as asset misappropriation, bribery, cybercrime, fraud and money laundering. Approximately 22% of respondents experienced losses of between one hundred thousand and one million, 14% suffered losses of more than one million and 1% of those surveyed suffered losses of one hundred million dollars. These high loss rates represent a rising trend in costs caused by fraud. In organizations, 56% of cases are related to internal fraud and 40% to external, this difference is since any individual related to accounting and financial activities is considered a potential risk factor for fraud.

When observing the behavior of people in the scope of business processes, it can be concluded that the human factor is closely linked and related to the fraud triangle theory of the Donald R. Cressey, where three basic concepts: pressure, opportunity and rationalization; are needed. Nowadays, there are different solutions in the commercial field as well as the academic field, where some works in progress had been identified aimed at detecting financial fraud. In both cases, these solutions are focused on the use of different tools that perform statistical and parametric analysis, as well as behavioral analysis, based on data mining techniques and Big Data; but none of them solve the problem of detection financial fraud in real time. Fraud Find, unlike other proposals, detects, reports and stores fraudulent activities in real time through the periodic analysis of the information generated by users for further analysis and treatment. This paper presents Fraud Find, a conceptual framework that allows detecting and identifying potential criminals who work in the banking field, in real time, based on the theory of the fraud triangle. For the design of the FraudFind framework, some software components related to the processing of information were analyzed, among them, RabbitMQ, Logstash and Elastic Search. In addition, the computerization of the triangle of fraud and the use of semantic techniques will allow finding possible bank delinquents with a lower false positive rate.

LITERATURAL SURVEY

Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem

Occupational fraud is a $652 billion problem to which disgruntled employees are a major contributor. Much security research addresses reducing fraud opportunity and increasing fraud detection, but detecting motivational factors like employee disgruntlement is less studied. The Sarbanes–Oxley Act requires that companies archive email, creating an untapped resource for deterring fraud. Herein, protocols to identify disgruntled communications are developed. Messages cluster well according to disgruntled content, giving confidence in the value of email for this task. A highly accurate naïve Bayes model predicts whether messages contain disgruntled communications, providing extremely relevant information not otherwise likely to be revealed in a fraud audit. The model can be incorporated into fraud risk analysis systems to improve their ability to detect and deter fraud.

Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit

Every year, fraud as a subset of insider threats causes billions US dollar of damage worldwide. We suggest a generic architectural model to unify the classic fraud audit approach with human behavior taking into account the fraud triangle in order to achieve better fraud detection and prevention. The human factor is extensively integrated into the audit as a qualitative component, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud audit. This provides added value because transactions examined by the auditor can be better differentiated and prioritized. It is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered using normal means by taking suspicious and non-suspicious human behavior into account. The proposed architecture is implemented using a prototype and is applied exemplary to an SAP ERP system.

An insider threat prediction model," in Trust, Privacy and Security in Digital Business

Information systems face several security threats, some of which originate by insiders. This paper presents a novel, interdisciplinary insider threat prediction model. It combines approaches, techniques, and tools from computer science and psychology. It utilizes real time monitoring, capturing the user's technological trait in an information system and analyzing it for misbehavior. In parallel, the model is using data from psychometric tests, so as to assess for each user the predisposition to malicious acts and the stress level, which is an enabler for the user to overcome his moral inhibitions, under the condition that the collection of such data complies with the legal framework. The model combines the above mentioned information, categorizes users, and identifies those that require additional monitoring, as they can potentially be dangerous for the information system and the organization.

Internal fraud risk reduction: Results of a data mining case study

Corporate fraud represents a huge cost to the current economy. Academic literature has demonstrated how data mining techniques can be of value in the fight against fraud. This research has focused on fraud detection, mostly in a context of external fraud. In this paper, we discuss the use of a data mining approach to reduce the risk of internal fraud. Reducing fraud risk involves both detection and prevention. Accordingly, a descriptive data mining strategy is applied as opposed to the widely used prediction data mining techniques in the literature. The results of using a multivariate latent class clustering algorithm to a case company's procurement data suggest that applying this technique in a descriptive data mining approach is useful in assessing the current risk of internal fraud. The same results could not be obtained by applying a univariate analysis.

SYSTEM ANALYSIS

Existing System:

A key aspect is to classify individuals by focusing on reducing the internal risk of fraud through a descriptive mining strategy. Besides, the experience of auditors plays an important role in the fight against financial fraud. Some work is proposed which points to the creation of new frameworks that provide systematic processes to help auditors to discover financial fraud within an organization by analyzing existing information and data mining techniques using their own experience and skills. Accordingly, another proposal creates generic frameworks for the detection of financial fraud FFD, to evaluate the different characteristics of FFD algorithms according to a variety of evaluation criteria.

Proposed System:

The proposed framework operates in the continuous auditing approach to discover financial fraud within an organization belonging to the banking sector which will be our main study environment and also focused on the fraud triangle theory with the human factor considered as an essential element. Fraud Find is proposed with the objective of analyzing large amounts of data from different sources of information for later processing and registration. The agent is an application installed in the workstations of the users (endpoints), in order to extract the data that they generate from the different sources of information that reside on their equipment. This application is responsible for sending the data entered by the user for ordering and classification. Later this organized information is received by Log stash for its treatment.

IMPLEMENTATION MODULES

1. Agent

The agent is an application installed in the workstations of the users (endpoints), in order to extract the data that they generate from the different sources of information that reside on their equipment. This application is responsible for sending the data entered by the user for ordering and classification.

2. Behavior analysis

If we are given a set of patterns or a set of feature vectors for some set of population then we would like to know if the data set has some relatively distinct subsets or not. In this context we can define cluster analysis as a classification technique for forming homogeneous groups within complex data sets. Typically, we do not know a priori the natural groupings or subtypes, and we wish to identify groups within a data set. We wish to form classifications, taxonomies, or typologies that represent different patterns in the data.

3. Fraud detection

Behavioral analytics solutions are designed to understand the normal behavior of each individual account holder, calculate the risk of each new activity and then choose intervention methods commensurate with the risk. The key characteristics that make behavioral analytics effective are automatically monitoring all activity for all account holders, not just devices or transactions; no requirement for prior knowledge of the specific fraud that the perpetrator is attempting; and providing detailed historical context for suspicious activity.

4. Fraud category

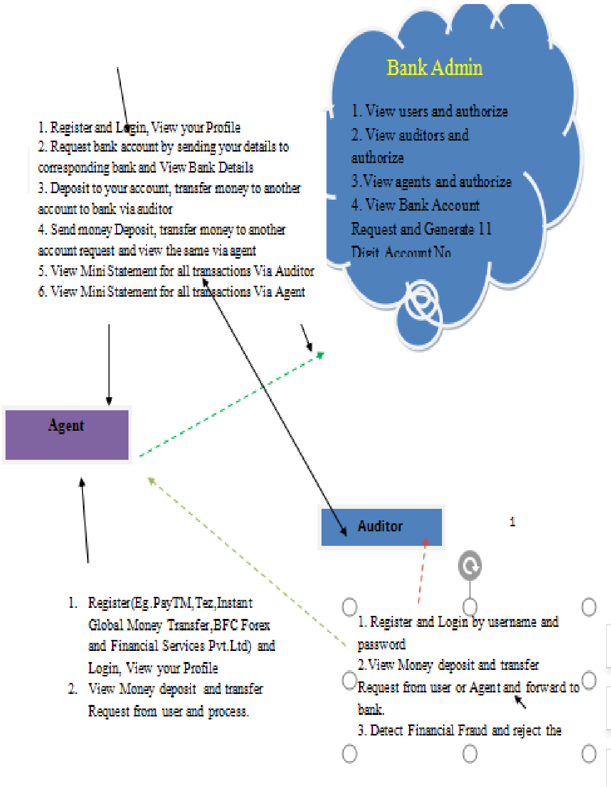
Periodically, a task that do the alert tracking, checks the information entered and compares it with a fraud triangle library to determine if there is a relation in order to generate an alert that will be stored in the database. The library of the fraud triangle is just a dictionary that contains three definitions: pressure, opportunity and justification. Under these parameters, the sentences and words associated with these behaviors are composed.

ALGORITHM:

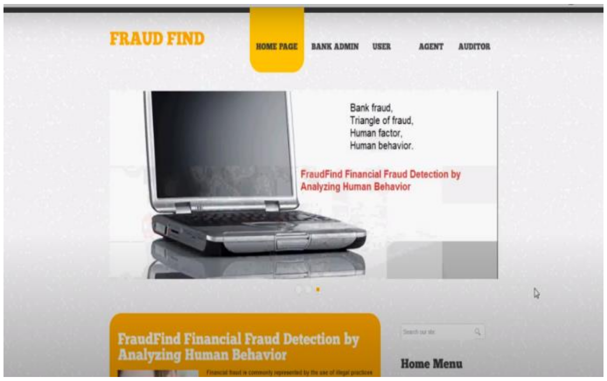
1. K means clustering

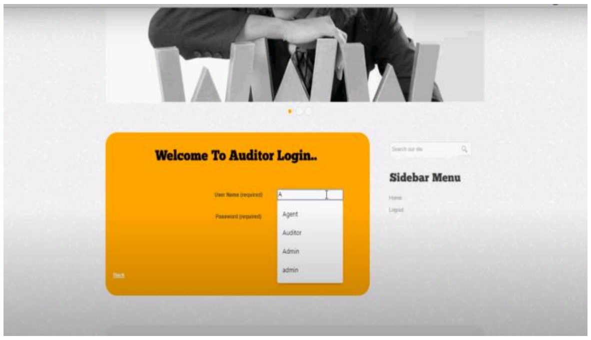
K-Means clustering intends to partition *n* objects into *k* clusters in which each object belongs to the cluster with the nearest mean. This method produces exactly *k* different clusters of greatest possible distinction. The best number of clusters *k* leading to the greatest separation (distance) is not known as a priori and must be computed from the data. The objective of K-Means clustering is to minimize total intra-cluster variance, or, the squared error function.

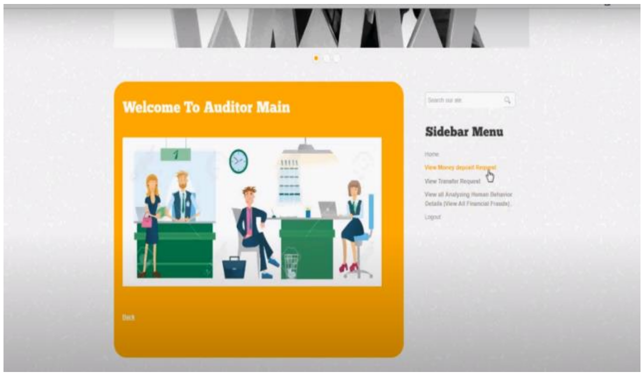
SYSTEM ARCHITECTURE

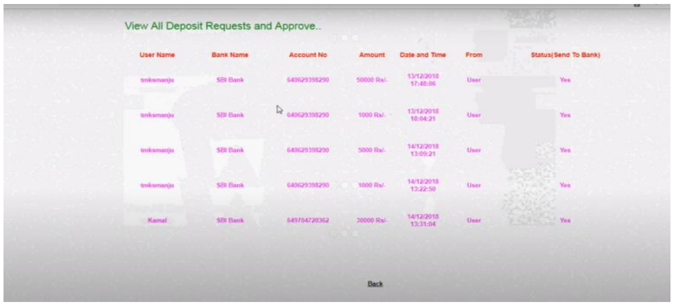

Bank Admin
1. View users and authorize
2. View auditors and authorize
3.View agents and authorize
4. View Bank Account Request and Generate 11 Digit Account No
1. Register and Login, View your Profile
2. Request bank account by sending your details to corresponding bank and View Bank Details
3. Deposit to your account, transfer money to another account to bank via auditor
4. Send money Deposit, transfer money to another account request and view the same via agent
5. View Mini Statement for all transactions Via Auditor
6. View Mini Statement for all transactions Via Agent
Agent
Auditor
1
1. Register(Eg.PayTM,Tez,Instant Global Money Transfer,BFC Forex and Financial Services Pvt.Ltd) and Login, View your Profile
2. View Money deposit and transfer Request from user and process.
1. Register and Login by username and password
2.View Money deposit and transfer Request from user or Agent and forward to bank.
3. Detect Financial Fraud and reject the

SCREEN SHOTS

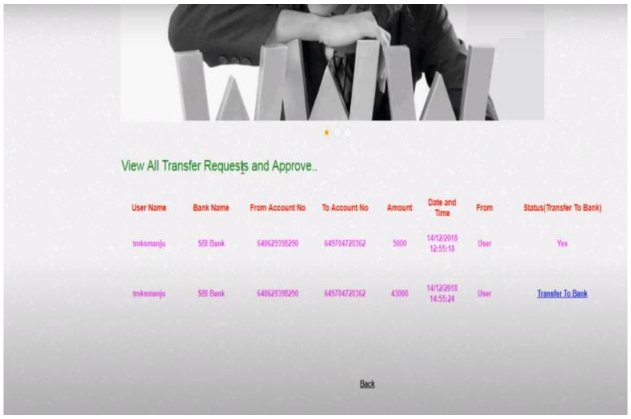

FRAUD FIND
HOME PAGE
BANK ADMIN
USER
AGENT
AUDITOR
Bank fraud,
Triangle of fraud,
Human factor,
Human behavior.
FraudFind Financial Fraud Detection by Analyzing Human Behavior
FraudFind Financial Fraud Detection by Analyzing Human Behavior
Financial fraud is commonly represented by the use of illegal practices
Search our site
Home Menu




Welcome To Auditor Main
Back
Search our site
Sidebar Menu
Home
View Money deposit Request
View Transfer Request
View all Analyzing Human Behavior Details (View All Financial Frauds)
Logout

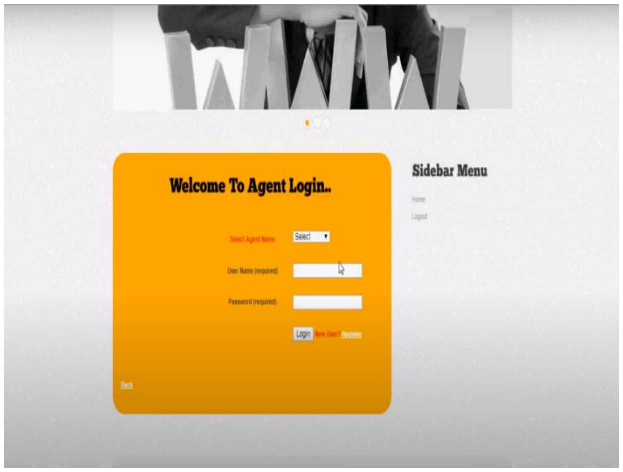

View All Deposit Requests and Approve..

User Name	Bank Name	Account No	Amount	Date and Time	From	Status(Send To Bank)
tmksmanju	SBI Bank	640629398290	50000 Rs/-	13/12/2018 17:48:06	User	Yes
tmksmanju	SBI Bank	640629398290	1000 Rs/-	13/12/2018 18:04:21	User	Yes
tmksmanju	SBI Bank	640629398290	5000 Rs/-	14/12/2018 13:09:21	User	Yes
tmksmanju	SBI Bank	640629398290	1000 Rs/-	14/12/2018 13:22:50	User	Yes
Kamal	SBI Bank	649704720362	30000 Rs/-	14/12/2018 13:31:04	User	Yes



View All Transfer Requests and Approve..

User Name	Bank Name	From Account No	To Account No	Amount	Date and Time	From	Status(Transfer To Bank)
tmksmanju	SBI Bank	640629398290	649704720362	5000	14/12/2018 12:55:18	User	Yes
tmksmanju	SBI Bank	640629398290	649704720362	43000	14/12/2018 14:55:24	User	Transfer To Bank

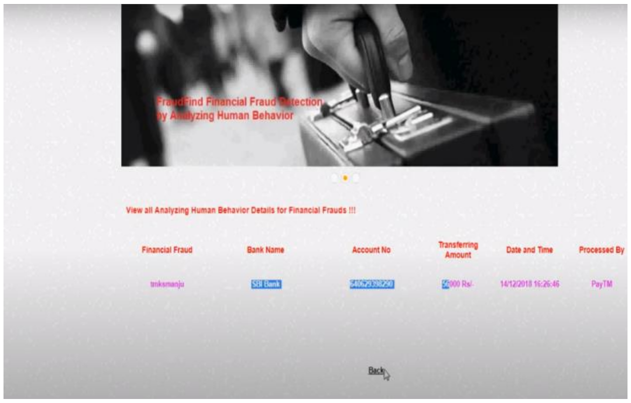


Welcome To Agent Login..

Select Agent Name: Select

User Name (required):

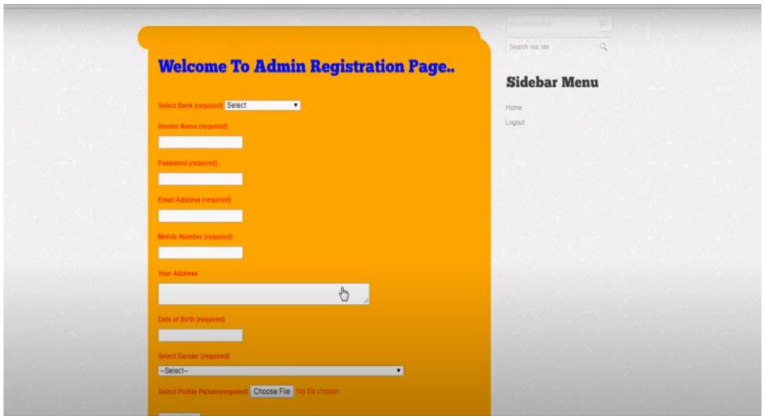
Password (required):



FraudFind Financial Fraud Detection by Analyzing Human Behavior

View all Analyzing Human Behavior Details for Financial Frauds !!!

Financial Fraud	Bank Name	Account No	Transferring Amount	Date and Time	Processed By
tmksmanju	SBI Bank	640629398290	50000 Rs/-	14/12/2018 16:26:46	PayTM



Welcome To Admin Registration Page..

Select Bank (required): Select

Vendor Name (required):

Password (required):

Email Address (required):

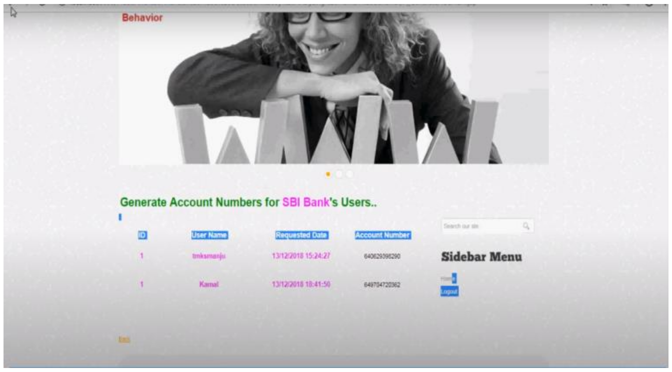
Mobile Number (required):

Your Address:

Date of Birth (required):

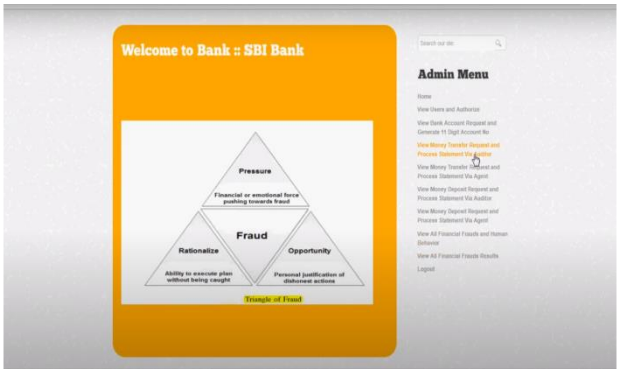
Select Gender (required): --Select--

Select Profile Picture(required): Choose File No file chosen



Generate Account Numbers for SBI Bank's Users..

ID	User Name	Requested Date	Account Number
1	tmksmanju	13/12/2018 15:24:27	640629398290
1	Kamal	13/12/2018 18:41:50	649704720362



Welcome to Bank :: SBI Bank

Pressure
Financial or emotional force pushing towards fraud
Fraud
Rationalize
Ability to execute plan without being caught
Opportunity
Personal justification of dishonest actions
Triangle of Fraud
Search our site
Admin Menu
Home
View Users and Authorize
View Bank Account Request and Generate 11 Digit Account No
View Money Transfer Request and Process Statement Via Auditor
View Money Transfer Request and Process Statement Via Agent
View Money Deposit Request and Process Statement Via Auditor
View Money Deposit Request and Process Statement Via Agent
View All Financial Frauds and Human Behavior
View All Financial Frauds Results
Logout

CONCLUSION

The present work proposes Fraud Find, a conceptual framework to detect financial fraud supported by the fraud triangle factors which, compared to the classic audit analysis, makes a significant contribution to the early detection of fraud within an organization. Taking into account human behavior factors, it is possible to detect unusual transactions that would have not been considered using traditional audit methods. These patterns of behavior can be found in the information that users generate when using the different applications on a workstation. The collected data is examined using data mining techniques to obtain patterns of suspicious behavior evidencing possible fraudulent behavior. Nevertheless, the legal framework and the different regulations that are applied in public and private institutions of a particular region represent a high risk for the non-implementation of this architecture as an alternative solution. Future work will have as its main objective the implementation and evaluation of the framework as a tool for continuous auditing within an organization.

REFERENCES

[1] "ACFE Asociaci´on de Examinadores de Fraudes Certificados," (Date last accessed 15-July-2014). [Online]. Available: http://www.acfe.com/uploadedfiles/acfewebsite/ content/documents/rttn-2010.pdf

[2] "PwC," (Date last accessed 15-July-2014). [Online]. Available: https://www.pwc.com/gx/en/economic-crime-survey/ pdf/GlobalEconomicCrimeSurvey2016.pdf

[3] N. B. Omar and H. F. M. Din, "Fraud diamond risk indicator: An assessment of its importance and usage," in 2010 International Conference on Science and Social Research (CSSR 2010). IEEE, dec 2010.

[4] "Lynx," (Date last accessed 15-July-2014). [Online]. Available: http://www.iic.uam.es/soluciones/banca/lynx/

[5] "Ibm," (Date last accessed 15-July-2014). [Online]. Available: https://www.ibm.com/developerworks/ssa/local/ analytics/prevencion-de-fraude/index.html

[6] C. Holton, "Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem," Decision Support Systems, vol. 46, no. 4, pp. 853–864, mar 2009.

[7] S. Hoyer, H. Zakhariya, T. Sandner, and M. H. Breitner, "Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit," in 2012 45th Hawaii International Conference on System Sciences. IEEE, jan 2012.