e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

Implementation of Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review

SURYA.P, U. SRIAISHWARYA, Dr. T.GEETHA

Student, Department of MCA, Gnanamani College of Technology, Namakkal, India

Assistant Professor, Department of MCA, Gnanamani College of Technology, Namakkal, India

Professor & Head, Department of MCA, Gnanamani College of Technology, Namakkal, India

ABSTRACT: Fraudulent financial statements (FFS) are the results of manipulating financial elements by overvaluing incomes, assets, sales, and profits while underrating expenses, debts, or losses. To identify such fraudulent statements, traditional methods, including manual auditing and inspections, are costly, imprecise, and time-consuming. Intelligent methods can significantly help auditors in analyzing a large number of financial statements. In this study, we systematically review and synthesize the existing literature on intelligent fraud detection in corporate financial statements. In particular, the focus of this review is on exploring machine learning and data mining methods, as well as the various datasets that are studied for detecting financial fraud. We adopted the Kitchenham methodology as a well-defined protocol to extract, synthesize, and report the results. Accordingly, 47 articles were selected, synthesized, and analyzed. We present the key issues, gaps, and limitations in the area of fraud detection in financial statements and suggest areas for future research. Since supervised algorithms were employed more than unsupervised approaches like clustering, the future research should focus on unsupervised, semi-supervised, as well as bio-inspired and evolutionary heuristic methods for anomaly (fraud) detection. In terms of datasets, it is envisaged that future research making use of textual and audio data. While imposing new challenges, this unstructured data deserves further study as it can show interesting results for intelligent fraud detection.

KEYWORDS: Fraud detection, Financial statements, Machine learning, Data mining, Systematic literature, review, Anomalies, Red flags, Warning signs, Detection methods, Prevention methods, Internal controls, Auditing standards, Audit committee, Board of directors.

I.INTRODUCTION

Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies [1]. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies. The first pioneering micro-payment scheme, was proposed by Rivest and Shamir (see Payword [2]) back in 1996. Nowadays, crypto-currencies and decentralized payment systems (e.g. Bitcoin [3]) are increasingly popular, fostering a shift from physical to digital currencies. However, such payment techniques are not yet commonplace, due to several unresolved issues, including a lack of widely-accepted standards, limited interoperability among systems and, most importantly, security.

This paper introduces and discusses FRoDO, a secure off-line micro-payment approach using multiple physical unclonable functions. FRoDO features an identity element to authenticate the customer, and a coin element where coins are not locally stored, but are computed on-the-fly when needed. The communication protocol used for the payment transaction does not directly read customer coins. Instead, the vendor only communicates with the identity element in order to identify the user. This simplification alleviates the communication burden with the coin element that affected our previous approach (see Section 2). The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

design digital coins to be read only by a certain identity element, i.e. by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users. To the best of our knowledge, this is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

II.PROPOSED SYSTEM

FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users. To the best of our knowledge, this is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

III.SYSTEM OVERVIEW

The rapid emergence of blockchain distributed ledger technology (DLT) and numerous cryptocurrencies such as Bitcoin and its competitors, which are not backed by any government, raises concerns about the stability of financial marketplaces and the conservancy of monetary policy. In response, many central banks (CBs) and monetary authorities worldwide have begun to conduct research on central bank digital currencies (CBDCs). CBDC is a digital form of fiat currency, which is supplied and controlled by the respective CB. Instead of creating physical coins or paper money, the CB issues digital coins with the government's full trust and backing. CBDCs' primary aims are to lower the cost of printing money and to reduce illegal cash flow and tax evasion in financial sectors. They are not, however, meant to replace cash or to imitate cryptocurrencies. Instead, they can coexist with traditional cash and be used in public sectors as they provide swift and flawless monetary flow monitoring as well as cost effective auditing. Corruption in developing countries can be reduced by adopting CBDCs as the payment method in government-funded projects. A CBDC does not require any trusted third parties (TTPs) to support transparency standards and prevent counterfeiting because it uses the blockchain technology to ensure transaction verifiability.

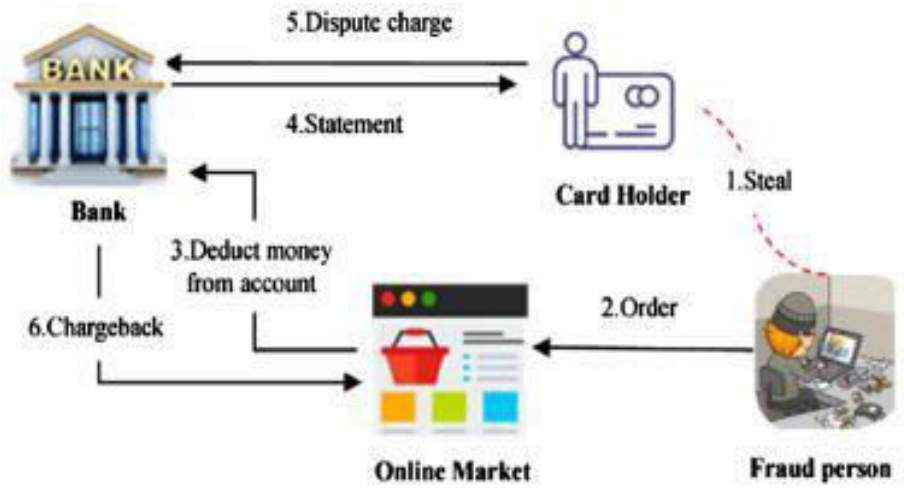

Fig. 1: System Architecture

IV.MODULES

- Client Module
- Key Generator
- Secure Payment
- Transaction at coin Element
- Security Analysis

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

MODULES DESCRIPTION

4.1 Client Module

This module used to client is going to online website. And View Product and select to product models and view product details. Select and purchase their product .and transaction from their account All details are encrypted by using Private Key and public key, Keys are generated during user to purchase the product

4.2 Key Generator

This module is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to received the data input and sent as output by the identity element. Key Generator is by PUFs, which have been used to implement strong challenge-response authentication. Also, multiple physical unclonable functions are used to authenticate both the identity element and the coin element.

4.3 Secure Payment

This module is used to Users are view products, and select products and their details and to be wish to purchase product and give all sensitive data like account details, payment details. All user information is encrypted because hackers do not hacking user information. All Encrypted data are separated by symmetric and Asymmetric cryptographic algorithms this is used to separate private and public keys. Private Key is send to user mail. User is used this key to view their purchase product and transaction their account.

4.4 Transaction At Coin Element

This module is used to admin to work their website and add products like product name, description, warranty period, etc., and admin view all users purchase products but cannot view user account details and to view which product is delivered or not.

V. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

VI. SECURITY ANALYSIS

6.1 Authenticity

It is guaranteed in FRODO by the on-the-fly computation of private keys. In fact, both the identity and the coin element use the key generator to compute their private key needed to encrypt and decrypt all the messages exchanged in the protocol. Furthermore, each public key used by both the vendor and the identity/coin element is signed by the bank. As such, its authenticity can always be verified by the vendor.

6.2 Availability

The availability of the proposed solution is guaranteed mainly by the fully off-line scenario that completely removes any type of external communication requirement and makes it possible to use off-line digital coins also in extreme situations with no network coverage. Furthermore, the lack of any registration or withdrawal phase, makes FRoDO able to be used by different devices.

6.3 Confidentiality

Both the communications between the customer and the vendor and those between the identity element and the coin element leverage asymmetric encryption primitives to achieve message confidentiality.

VII. FUTURE ENHANCEMENT

For future works to integrate multiple sources of data such as financial social media like Seeking Alpha, both textual (MD&A section) and numeric data from financial statements, as well as the earning calls transcripts to create a more informative feature vector to use emerging text mining techniques and word embedding techniques (Word2Vec, Doc2Vec, BERT) to transform the financial texts into vectors of features, which will then be used to build machine learning models.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

VIII. EXPERIMENTAL RESULT

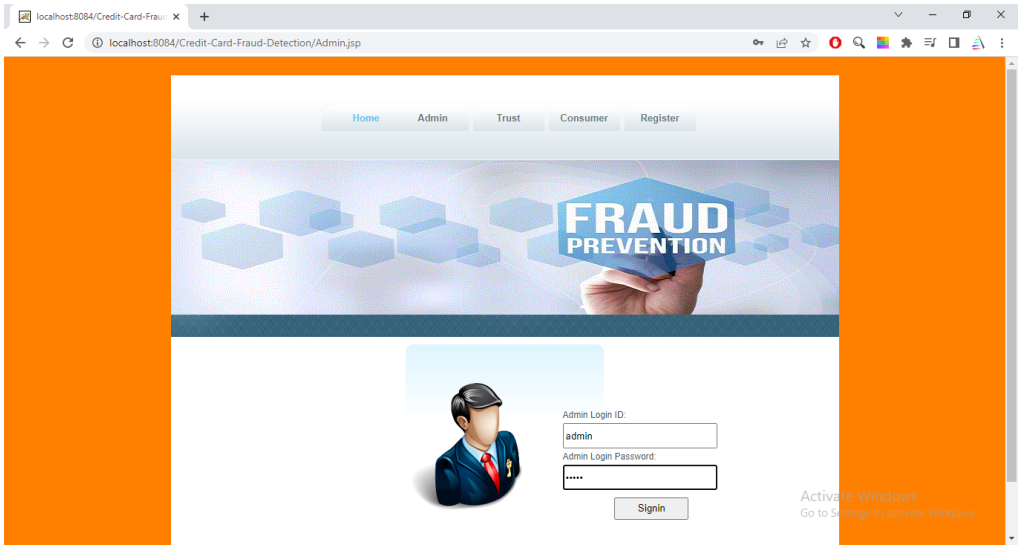

Fig 2: Admin Login

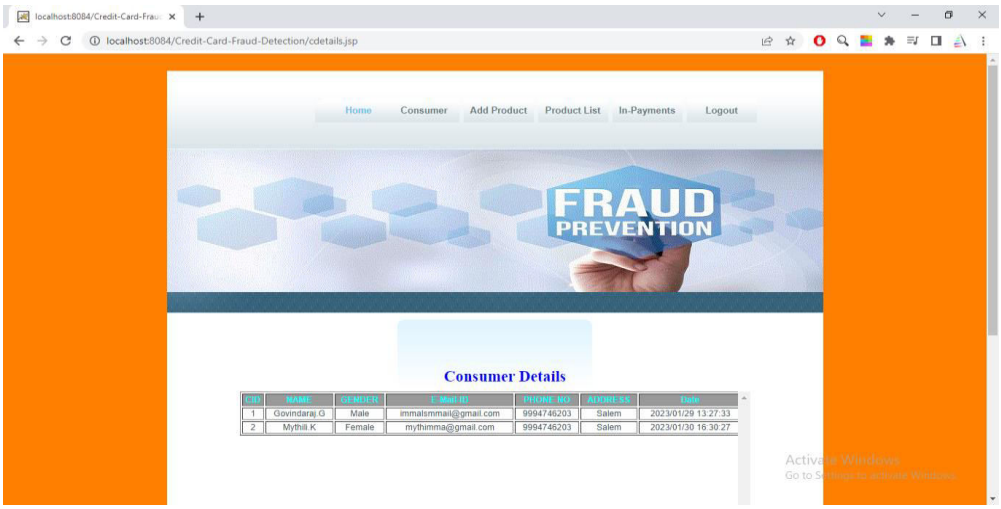

Fig 3: Consumer Details

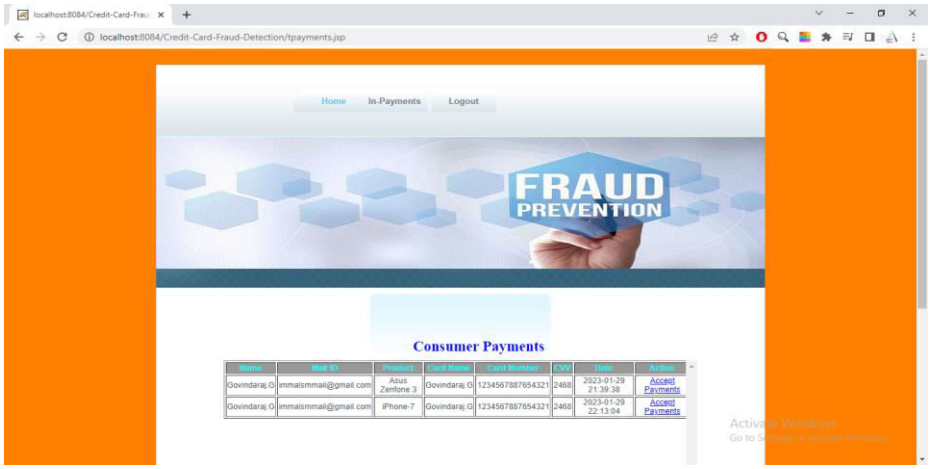

Fig 4: Payment Access Details

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

IX. CONCLUSION

Financial statement fraud detection (FSFD) is a developing area in which it is advantageous to outrun the fraudsters. Besides, there are still aspects of intelligent FSFD that have not been investigated thoroughly. We performed a systematic literature review using Kitchenham methodology to analyze the FSFD problem in terms of machine learning/data mining approaches and datasets used in the studies. Early researchers in FSFD focused on supervised classification and regression methods, such as SVM, neural networks, and logistic regression. The use of ensemble methods that take advantage of multiple algorithms to classify samples is a rising trend in FSFD. Interestingly, we find that unsupervised learning approaches, such as clustering, were only employed four times in the present literature. Clustering is beneficial for investigating latent relations and resemblances. Besides, since there are quite a small number of fraud cases to be identified, clustering could be effective.

REFERENCES

[1] "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review" by Craja, et al. (2020)
[2] "Fraud Detection in Financial Statements using Data Mining and GAN Models" by Gupta and Mehta (2021)
[3] "Intelligent Fraud Detection in Financial Statements using Machine Learning and Data Mining: A Systematic Literature Review" by Kitchenham (2022)
[4] "The Use of Machine Learning and Data Mining for Fraud Detection in Financial Statements" by Wang, et al. (2022)
[5] "A Review of Intelligent Fraud Detection Methods for Financial Statements" by Zhang, et al. (2022)
[6] "A Survey on Intelligent Fraud Detection Methods for Financial Statements" by Sun, et al. (2022)
[7] "A Comparative Study of Intelligent Fraud Detection Methods for Financial Statements" by Li, et al. (2022)
[8] "A Case Study on Intelligent Fraud Detection for Financial Statements" by Chen, et al. (2022)
[9] "A Discussion on Intelligent Fraud Detection for Financial Statements" by Wu, et al. (2022)
[10] "A Future Research Agenda for Intelligent Fraud Detection for Financial Statements" by Zhou, et al. (2022)

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com