



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.488

 9940 572 462

 6381 907 438

 ijirccce@gmail.com

 www.ijirccce.com

Multi Factorial Analysis in Detecting Money Laundering Users

Varshaa V K, Paappa S, Nirmala V, Dr.B.Murugeshwari

UG Students, Dept. of CSE., Anna University, Velammal Engineering College, Chennai, India

Professor, Dept. of CSE., Anna University, Velammal Engineering College, Chennai, India

ABSTRACT: A challenge in such scenarios is that cloud vendors may offer varying and possibly incompatible ways to isolate and interconnect virtual machines located in different cloud networks. Our approach is tenant driven in the sense that the tenant provides its connectivity mechanism. We are implementing Block chain concept in this project. We implement both Public and Private cloud data storage, Private is for sensitive data storage and public cloud for normal data storage. We implement this concept for banking system, to identify overall user behaviour with personal identification. Integration of all his / her transactions like Banking, Land Registrations, Gold Purchase or any cash transactions more than Rs.20k is accounted and monitored.

KEYWORDS: cloud networks, Block chain, integration, data storage

I. INTRODUCTION

Tax evasion is a financial crime against the tax system in which taxpayers deliberately report false financial positions to deny their tax obligations. It has become a severe economic problem for many countries resulting in a significant tax gap, i.e., the difference between the tax revenue the government is entitled to and the actual revenue collected. For example, the predicted tax gap for 28 European Union countries was, on average, \$51.9 billion, nearly 7.7% of their 2015 GDP. In the United States, the estimated tax gap was at \$441 billion for 2011- 2013, or about 2.7% of their GDP. In Australia, the estimated tax gap was at \$21.9 billion in 2015, roughly 2.2% of its GDP. Aside from less revenue for government budgets, tax evasion has also led to an unfair business competition environment, especially for compliant taxpayers whose operating costs are consequently higher than their non-compliant competitors. Such a phenomenon would eventually incur more tax non-compliance to challenge the tax system. Tax authorities have expended tremendous efforts in trying to reduce the tax gap and curtail tax evasion behaviours. Many computer-aided case selection approaches have been widely used to detect individual tax evasion behaviours, such as account manipulation and false invoices. However, these approaches mainly focus on detecting individual tax evaders by designing a set of financial indicators and further training a classifier model to classify the taxpayer entities. They are not able to detect Related Party Transaction-based Tax Evasion(RPTTE) behaviours, where groups of related taxpayers are involved in illegally redistributing their profits and losses to reduce the overall tax burden. The RPTTE behaviours are often conducted through related party transactions and transfer pricing and have become a growing global trend in tax evasion. Thus, the effective mining and exploration of tax evasion groups are of significant importance in reducing the tax gap. So, to eradicate the above drawbacks, We present an interactive analytics system, to enable the quick exploration and inspection of tax evasion groups with profit analysis. The proposed intuitive and carefully-designed method provide an overview and detailed explorations of tax evasion groups. To the best of our knowledge, This method is the first visual analytics system that is designed for detecting and exploring tax evasion groups by analysing related party transaction-based tax evasion (RPTTE) behaviours.

II. LITERATURE SURVEY

2.1 Money Laundering in the Bitcoin Network: Perspective of Mixing Services

Author: Junwoo Seo, Mookyu Park, Haengrok Oh, Kyungho Lee

Various crimes using Bitcoin are highlighted. Among various crimes using Bitcoin, this paper suggests a method to detect money laundering focusing on mixing service that provides Money Laundering. This is part of the anti-money-laundering (AML) strategy, which can determine whether the mixer service is used in certain transactions by using transaction sample data using mixer. Money laundering using Bitcoin is often used to avoid fund tracking in the underground world and analyzing it is essential in situational awareness of fund tracking.

2.2: Identifying Money Laundering Accounts

Author: Chih-Hua Tai, Tai-Jung Kan

Money laundering is often associated with criminal activities. Anti-money laundering is thus regarded as an important task in many countries. However, as it is common that money launderers divide the dirty money into multiple parts and make sequences of banking transfers or commercial transactions, manually detecting activities of money laundering is challenging. To ease the task, this work establishes a two-phase intelligent method based on machine learning and data analysis techniques for identifying suspicious money laundering accounts from the transaction data. The first phase emphasizes on identifying every suspicious money laundering account while the second phase further retrieves highly suspicious ones so that both the recall and precision for the identification of money laundering accounts can be somewhat taken care of. Evaluated on the data given by Bank Sino Pac, the established intelligent method achieves a recall rate of 26.3%, which is three times the recall rate (8.6%) of the Money Laundering Control Act in Taiwan, in the first phase, and later the precision rate can be increased up to 87.04% in the second phase.

2.3: Cryptocurrency: The New Face of Cyber Money Laundering

Author: SagwadiMabunda

Virtual currencies are on the rise and so is money laundering. While there are efforts to combat money laundering through various intergovernmental bodies, many have expressed concern over the rise of virtual currencies. Some cryptocurrencies such as Bitcoin have played a major role in the proliferation of online money laundering as it possesses characteristics that criminals are fond of. Bitcoin and other cryptocurrencies are decentralized, anonymous/pseudonymous and irreversible. They provide the means to skirt the Anti-Money laundering safeguards that have been put in place. This paper discusses the intersection between Anti-Money Laundering efforts and the challenges that are introduced by cryptocurrencies such as Bitcoin. It also looks at the case of Liberty Reserve to highlight these challenges.

III. EXISTING SYSTEM

Not User Friendly: The UI is not easily understandable by every users

Lots of paperwork: In previous cases, each and every records will be written manually. It may have the chances of missing.

- **Time consuming:** Every work is done Manually, so it requires lot of time to look after the next one.

DISADVANTAGES IN THE EXISTING SYSTEM

- There is no tracking system for purchasing
- Fraudulent made while purchase property.

IV. PROPOSED SYSTEM

Public and Private cloud data storage, Private is for sensitive data storage and public cloud normal data storage. We implement this concept for banking system, to identify overall user behaviour with personal identification. Integration of all his / her transactions like Banking, Land Registrations, Gold Purchase or any cash transactions more than Rs. 20k is accounted and monitored.

ADVANTAGES:

- Tracking system for purchasing property
- Notification for income tax payment
- Cloud storage for public and private information

SYSTEM FLOW

The block diagram of our proposed system is shown in Fig 8.1

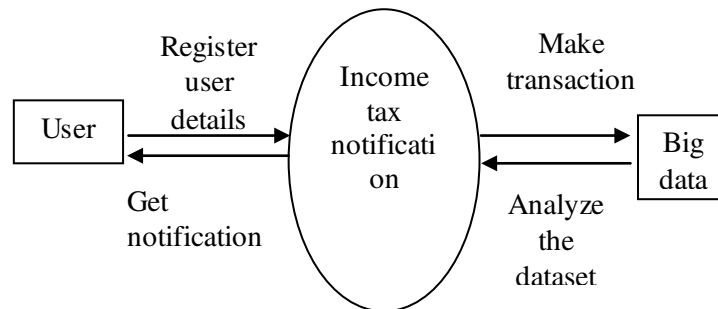


Fig . 1 System flow diagram

MODULES

1. User registration
2. Bank server
3. Land registration and gold purchase
4. Cloud deployment
5. Block chain deployment
6. Big data Analysis & black money notification

MODULE DESIGNS:

USER REGISTRATION:

In this module we are going to create a User application by which the User is allowed to access the data from the Server. Here first the User wants to create an account and then only they are allowed to access the Network. Once the User create an account, they are to login into their account and request the Job from the Server. Based on the User's request, the service Provider will process the User requested Job and respond to them. All the User details will be stored in the Database.

BANK SERVER:

Bank Service Provider will contain information about the user in their Data Storage. Also the Bank Service provider will maintain the all the User information to authenticate when they want to login into their account. The User information will be stored in the Database of the Bank Service Provider. To communicate with the Client and with the other modules of the Company server, the Bank Server will establish connection between them. For this Purpose we are going to create a User Interface Frame.

LAND REGISTRATION AND GOLD PURCHASE:

In this module we implement land registration and purchased details to be monitor. Here, user name, land documents, price and selling price land. And also we monitor the gold purchase of every user and all other property details will be monitored based on user' Id.

CLOUD DEPLOYMENT:

User will upload their data to the cloud server and request for a particular file is send to cloud server. To deploy our system we use dropbox cloud storage to store our details. Here we store sensitive and normal information on private and public cloud server respectively.

BLOCKCHAIN DEPLOYMENT:

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block an hash code will generate for security. Here we store all transaction information like land purchase, gold purchase and all other purchasing details will stored on block chain. For every transaction we a block will create with hash code to refer the other block. Transaction detail will be more secure on block chain.

BIGDATA ANALYSIS & BLACK MONEY NOTIFICATION:

Through out all transaction here we monitor proper payment of tax payment. Because, more number of forgeries were made on purchasing of land, people shows a fake price for land purchase and gold purchase. So , in this module we get the details of purchasing rate more than 20K . If user purchasing rate is increased more than 20K, system will alert the income tax notification to the user. Using aadhar number we can monitor all bank transaction also.

V. RESULTS

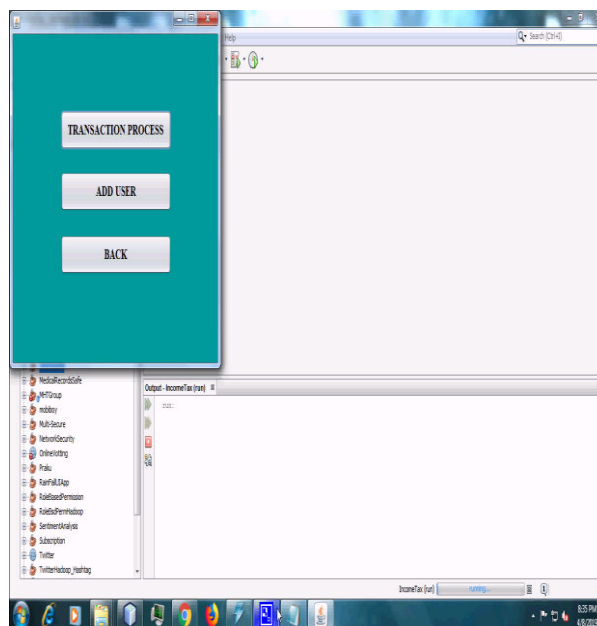


Fig .11.1.Options to add new users to register or to make a files or upload files or transaction finder by selecting appropriate actions.

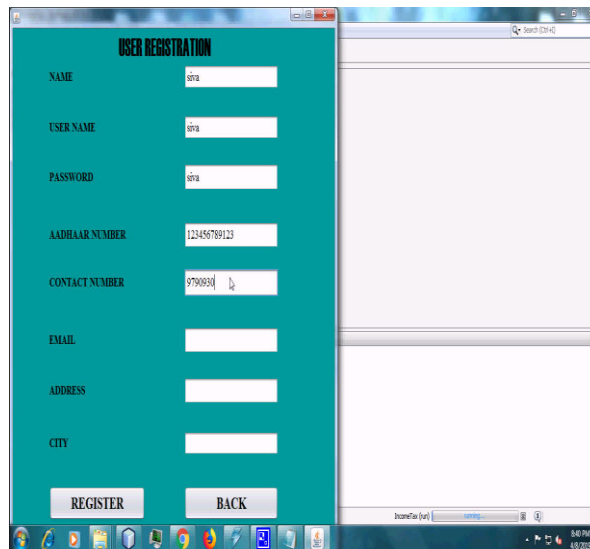


Fig . 11.2. User Interface page to register new user details

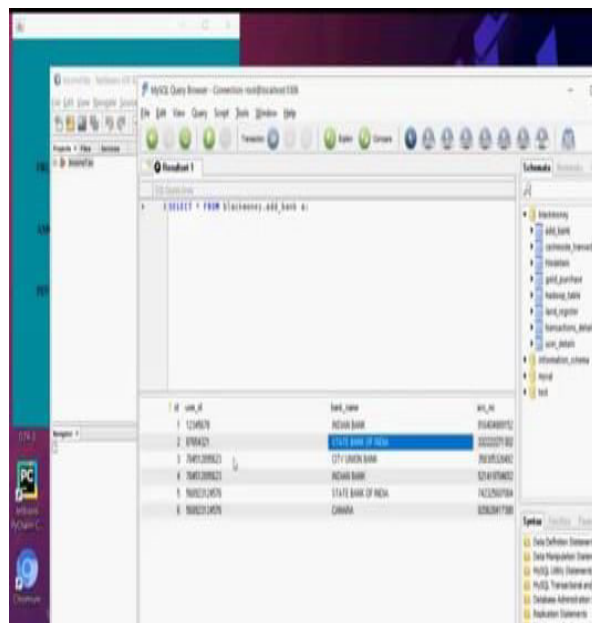


Fig.11.3 .Database connectivity to view the enrolled data

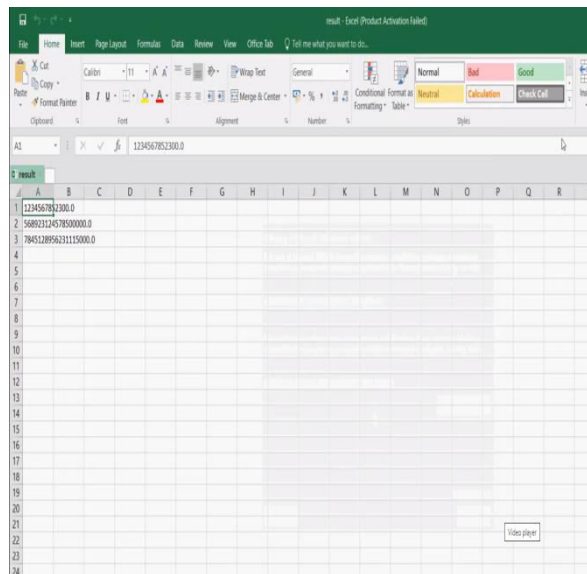


Fig.11.4. Result set created after analysing all three case

VI.CONCLUSION AND FUTURE ENHANCEMENT

We analyse the money laundering activities by all the transactions like Bank, Land and Gold purchase. Now a days, forgeries level is increasing in smarter way so to provide security we track the money using blockchain technology. In future work, we will consider acquiring the latest data source that include the unit price in the invoice data. Also, the suspiciousness indicators can be customized to discover patterns that domain experts would like to explore, such as the tax burden difference and the rate of change in profit. Furthermore, the visual summary of our glyph design can be extended by incorporating the topological patterns in investment relationships as a widely used pattern matching method. Last, we would like to advance the usefulness of our system with an additional view to portrait groups with similar features and allow users to select similar cases if they find one suspicious case.

REFERENCES

- [1] "History of Anti-Money Laundering Laws". United States Department of the Treasury. 30 June 2015. Retrieved 30 June 2015. <https://www.fincen.gov/history-anti-money-laundering-laws>
- [2] "Money Laundering Act 2012 amended". Resource Portal of OGR Legal. OGR Legal. Retrieved 2 November 2015. <https://resource.ogrlegal.com/money-laundering-act-2012-amended/>
- [3] "OPSI: Proceeds of Crime Act". Retrieved 14 February 2009. http://www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_1
- [4] "Suspicious Money Laundering Transaction: Q&A". Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice, Taiwan. Retrieved 20 November 2017. <https://goo.gl/jbu6Ln>
- [5] "Money Laundering". Wikipedia. Retrieved 18 January 2018. https://en.wikipedia.org/wiki/Money_laundering
- [6] "Suspicious Money Laundering or Terrorist Trading" Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice, Taiwan. Retrieved 30 January 2018. <https://goo.gl/SfDrvC>
- [7] "Don't Trust Your Instincts-Benford's law" PanSci. Retrieved 25 December 2017. <https://pansci.asia/archives/54264>



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details