

Literature on Various Anti-Money Laundering Techniques

R. Krishna Bharathi, G. Kavitha, Mary Linda I



Abstract: Laundering money is a method in which black money is converted into white cash. Anti-money laundering is a technique or procedure for finding such laundering operations. Although anti-money attempts began at an early point, the alternatives appear to be limited to a strategic level. Mostly criminal act offenders try to create the transactions look as innocent as possible. In order to explore a appropriate solution for suspect transaction detection, extensive study has been performed. But if the exchange is really suspect or not, there is no credible mechanism to verify and the method is also very tedious. This paper examines several methods and algorithms for the anti-money laundering system that have been suggested.

Keywords: Anti Money Laundering, AROMLD, Bitcoin, Bitmap Index-based Decision Tree.

I. INTRODUCTION

Money laundering is a method of transforming irresponsible cash into responsible cash. The technology is being updated every day and many merits as well as demerits are associated with this rapidly changing technology. The world has become so globalized with the introduction of e-commerce, and the technology has made everything so user-friendly that many transactions can be made with a single click of a button. Fraud detection is compulsory as it impacts the entire country as well as the financial institution[1],[3],[5]. This criminal activity is becoming increasingly advanced and maybe this could be the main reason for the fraud detection trouble. This criminal activity results in several adverse effects ranging from drug trafficking to economic terrorism. Anti money laundering is a method in which black money is converted into white cash. Money launderers cover their behavior in most instances through a sequence of measures that make it look like cash from illegal or unethical origin has been legally gained. Anti money laundering systems refine customer information, label it to the level of suspicion and inspect it for anomalies. Any instant and significant increase in funds or a big withdrawal would include such anomalies. There may

also be smaller transactions that fulfill certain requirements as suspect[2],[4],[6].

II. ANTI-MONEY LAUNDERING IN ONLINE TRANSACTION

Kannan. S et al. (2017), prescribes the Autoregressive Outlier calculation to limit computational intricacy in ML movement identification (AROMLD). The evaluation of the Inter Quartile Range (IQR) offers the proportion of variety for obscure information set qualities.

Vikas Jayasree et al. (2017), gauges the risk of money cleaning utilizing the Bitmap Decision Tree (BIDT) strategy. At first, gaining from the Bitmap Index-based Decision Tree is utilized to make the tree of understanding that decides the peril of illegal tax avoidance for an organization and improve versatility[7],[9],[11]. The record in a table is numbered consecutively in a BIDT bitmap file with each key worth, account number, and an utilized bitmap. Utilizing the "select" inquiry yield, the BIDT calculation along these lines applies tally and bit-wise sensible activities on AND. The result of the question relates unequivocally to the development of a choice tree and all the more absolutely to the evaluation of the peril of versatility in cash cleaning job. The populace frequencies are procured for the root hub, the essential record of the choice tree, simply by checking the total measure of "1" in the bitmaps based on the component to search for tax evasion and gauge the hazard factor level[8],[10],[12]. The test is performed on factors, for example, administrative hazard rate, false positive rate, and time to distinguish danger. The coming about investigation of the BIDT procedure is contrasted and the current Smart Card-based Security Framework (SCSF) and Multilayered Detection System (MDS) utilizing Statlog German Credit Data.

Pankaj Richhariya et al. (2012), the possibility of extortion identification is disrupted by the expansion and quick acceleration of web based business, and examples of monetary misrepresentation brought together with it are additionally strengthening, prompting trillions of dollars being separated each year globally[26],[28],[30]. They gave a broad outline of different techniques, for example, discovery of charge card misrepresentation, online sale misrepresentation, recognition of broadcast communications extortion, and PC interruption. The interruption discovery framework's disservice is terrible versatility in light of the fact that the framework and its arrangement of principles must be explicit to the observing setting[13],[15],[17].

Manuscript published on 30 August 2019.

* Correspondence Author (s)

R. Krishna Bharathi, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India. Email: kribharamalingam94@gmail.com

G. Kavitha, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India. Email: kavithag90@gmail.com

Mary Linda I, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India. Email: catchlin.18@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

III. ANTI-MONEY LAUNDERING IN GOLD FARMING

Gold farming is a major virtual economy division. Gold farming was first used in online games to elaborate on economics because the imaginary world, like the true world, can contain limited resources that are subject to supply and demand legislation [14],[16],[18].

Hyukmin Kwon et al. (2017), They evaluate the features of a massively multiplayer internet role-playing (MMORPG) environment and develop a technique for GFG detection. They create a graph that characterizes transactions in the virtual economy and traces unusual trades and events. Their trading graph and physical networks extract characteristics used by GFGs to discover them in their entirety [25],[27],[29].

IV. ANTI-MONEY LAUNDERING IN BITCOIN

Bitcoin is the first digital e-cash scheme commonly embraced. All Bitcoin transactions that include sender and receiver addresses are stored in the government blockchain that may cause privacy issues. Without getting trusted third parties, the Zerocoin protocol hides the connection between individual Bitcoin transactions [19],[21],[23].

Malte Moser et al. (2013), provide a first systematic account of anti-money laundering (AML) opportunities and constraints in Bitcoin, starting with the observation that Bitcoin draws criminal activity as many say it is an anonymous transaction scheme. While this assertion does not stand up to scrutiny, several services have appeared in the Bitcoin ecosystem providing enhanced transaction anonymization – such as Bitcoin Fog, BitLaundry, and Blockchain information's Send Shared features. While Bitcoin Fog and Blockchain.info anonymize their transactions effectively, we can link BitLaundry's input and output transactions. Against the background of these results, it seems unlikely that the Bitcoin scheme will be able to enforce a Know-Your-Customer principle. Therefore, they sketch alternative AML approaches that account for incomplete understanding of real identities but exploit government data in the transaction graph and discuss the consequences as a decentralized currency for Bitcoin.

V. CONCLUSION

Anti-money laundering is a complicated and challenging job in this article. Detecting anomaly from the mass financial transaction is not simple. A thorough study is conducted on the different ways to launder cash such as internet transaction, gold farming and bitcoin and their methods. The problems identified are as follows, the allocation of fragmented nodes has not been more organized, the handling of voluminous financial institutions and time consumption is more hard, and the account analyzed is repeated every time even after a fresh method begins [20],[22],[24].

In the future, instead of considering only the frequent accounts involved in the transaction, it is necessary to take into account each and every account to investigate whether they are frequently used or not. With less effort and time taken to include improved techniques, they can also discover the suspect actions.

REFERENCES

- Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Weight ward change region plummetering change for square based image Huffman coding", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4313-4316.
- Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Image compression utilizing wavelet transform", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4305-4308.
- Kandavel, N. & Kumaravel, A. 2019, "Offloading computation for efficient energy in mobile cloud computing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4317-4320.
- Vinoth, V.V. & Kanniga, E. 2019, "Reversible data hiding in encrypting images-an system", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3051-3053.
- Selvapriya, B. & Raghu, B. 2019, "Pseudocoloring of medical images: A research", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3712-3716.
- Senthil Kumar, K. & Muthukumaravel, A. 2019, "Bi-objective constraint and hybrid optimizer for the test case prioritization", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3436-3448.
- Kavitha, G., Priya, N., Anuradha, C. & Pothumani, S. 2019, "Read-write, peer-to-peer algorithms for the location-identity split", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 445-447.
- Kaliyurthi, K.P., Michael, G., Anuradha, C. & Sundaraj, B. 2019, "Certain improvements in Alzheimer disease classification using novel fuzzy c means clustering for image segmentation", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 599-604.
- Kaliyurthi, K.P., Sundarraj, B., Geo, A.V.A. & Michael, G. 2019, "RIB: Analysis of I/O automata", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1019-1022.
- Velvizhi, R., Rajabhushanam, C. & Vidhya, S.R.S. 2019, "Opinion mining for travel route recommendation using Social Media Networks (Twitter)", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 508-512.
- Kavitha, R., Sangeetha, S. & Varghese, A.G. 2019, "Human activity patterns in big data for healthcare applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1101-1103.
- Pothumani, S., Anandam, A.K., Sharma, N. & Franklin, S. 2019, "Extended VEOT framework - Implemented in a smart boutique", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 762-767.
- Kaliyurthi, K.P., Michael, G., Krishnan, R.M.V. & Sundarraj, B. 2019, "Pseudorandom techniques for the internet", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 915-918.
- Aravindasamy, R., Jeffrin Rajan, M., Rama, A. & Kavitha, P. 2019, "Deep learning provisions in the matlab: Focus on CNN facility", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 990-994.
- Theivasigamani, S., Linda, M. & Amudha, S. 2019, "Object sensing and its identification & motion sensing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 545-549.
- Mary Linda, I., Vimala, D. & Shanmuga Priya, K. 2019, "A methodology for the emulation of IPv4", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 848-852.
- Velvizhi, R., Priya, D.J., Vimala, D. & Linda, I.M. 2019, "Increased routing algorithm for mobile adhoc networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1606-1608.
- Sangeetha, S., Anuradha, C. & Priya, N. 2019, "DNS in real world", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 937-940.

19. Geetha, C., Vimala, D. & Priya, K.S. 2019, "Constructing multi-processors and spreadsheets with SKIVE", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 516-519.
20. Yugendhar, K., Sugumar, V. & Kavitha, P. 2019, "A novel method of univac using fuzzy logic", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 435-437.
21. Kaliyamurthi, K.P., Michael, G., Elankavi, R. & Jijo, S.A. 2019, "Implementing aggregate-key for sharing data in cloud environment using cryptographic encryption", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 957-959.
22. Jeffrin Rajan, M., Aravindasamy, R., Kavitha, P. & Rama, A. 2019, "A novel method of object orientation variation in C++ and java", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 708-710.
23. Nayak, R., Dinesh, S. & Thirunavukkarasu, S. 2019, "A novel method improvement of rapid miner for the data mining applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 457-460.
24. Sivaraman, K., Krishnan, R.M.V., Sundarraj, B. & Sri Gowthem, S. 2019, "Network failure detection and diagnosis by analyzing syslog and SNS data: Applying big data analysis to network operations", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 883-887.
25. Vimala, D., Linda, I.M. & Priya, K.S. 2019, "Decoupling online algorithms from erasure coding in DNS", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 950-953.
26. Rama, A., Kumaravel, A. & Nalini, C. 2019, "Preprocessing medical images for classification using deep learning techniques", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 711-716.
27. Sangeetha, S., Srividhya, S.R., Anita Davamani, K. & Amudha, S. 2019, "A procedure for avoid overrun error in universal synchronous asynchronous receiver transmitter (usart) by utilizing dummy join and interrupt latency method", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 657-660.
28. Aravindasamy, R., Jeyapriya, D., Sundarajan, B. & Sangeetha, S. 2019, "Data duplication in cloud for optimal performance and security", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1156-1158.
29. Aravindasamy, R., Jeffrin Rajan, M., Sugumar, V. & Kavitha, P. 2019, "A novel method on developing superblocks and the transistor using apodryal", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 982-985.
30. Sasikumar, C.S. & Kumaravel, A. 2019, "E-learning attributes selection through rough set theory and data mining", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 3920-3924.

AUTHORS PROFILE



R. Krishna Bharathi Assistant Professor, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India



G. Kavitha Assistant Professor, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India



Mary Linda I Assistant Professor, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India