AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 3, Issue 8, 2025 ISSN (E): 2993-2637

Prevention and Prediction of Cryptocurrency Fraud Detection Using Machine Learning

P. Velavan*[1], A. Mohamed Fazil[2], K. Mohamed Saif[3], B. Samsingh[4], M. Mohamed Sameer Ali[5]

[12345]*Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India*

[*]*Correspondence: velavan@dhaanishcollege.in*

Abstract: This article talks about the growing problems that law enforcement faces because of the possibility that Bitcoin could be used for money laundering and funding terrorism. Using unsupervised machine learning, we suggest a new way to look at the whole Bitcoin user graph, which will help find suspicious people who are breaking the law. The paper's findings are very promising for improving the detection of cryptocurrency crimes, which will help fight money laundering and terrorism financing. Our main goal is to look at the whole Bitcoin user graph using a Coin Join community detection method. By studying transaction patterns and network interactions among these communities, our technique tries to detect and flag questionable people involved in criminal activities. The conclusions of our research provide enormous promise for boosting anti-money laundering efforts and strengthening counterterrorism measures through more effective bitcoin crime detection tools. We want to make a big difference in the ongoing efforts to protect financial systems and fight illegal financial activities by giving law enforcement agencies better tools and information.

Keywords: Advancing Anti-Money Laundering, Cryptocurrency Crime Detection Techniques, Bitcoin User Graph, Combat Illicit Financial Activities, Cryptocurrency-Related Crimes

Introduction

The increasing use of cryptocurrencies, especially Bitcoin, has opened up a new era of digital transactions and financial innovation. But with the benefits of these decentralised digital assets come worries about how they could be used for illegal activities like money laundering and funding terrorism [28]. Law enforcement organisations have a hard time fighting digital financial crimes because cryptocurrencies are pseudonymous and have a decentralised architecture. In light of these issues, this study examines the escalating menace of cryptocurrency-related offences, particularly emphasising the improvement of detection techniques for unlawful Bitcoin transactions [29-31]. The emergence of tools such as Coin Join, which permits the mixing of transactions to obscure the origin of funds, has further complicated the challenge of identifying suspicious actors within cryptocurrency networks. Our article seeks to improve the identification of cryptocurrency-related crimes, including money laundering and terrorism financing within Bitcoin transactions [32]. We want to find suspicious people in the Bitcoin network by using unsupervised machine learning and a Coin Join community detection method [33]. We want to improve the security and integrity of global financial systems by giving law enforcement sophisticated detection tools. This will help with anti-money laundering and counterterrorism activities in the digital finance space.

This part talks about the problems that could come up if cryptocurrencies are used for illegal things like money laundering and funding terrorism. It introduces the objectives of the paper and

the significance of adopting a community detection approach [34-37]. Talk about the several types of data that can be used to look at Bitcoin transactions, such as blockchain data, transaction history, and network interactions. Talk about preprocessing methods like normalising and cleaning data. Explore several community detection techniques ideal for recognising activity patterns inside cryptocurrency networks [38]. The document covers non-discriminatory and functional requirements [39]. The functional scope covers essential functions such as user management, catalogue browsing, and inventory management, as well as sophisticated features like reporting and analytics for analysing customer behaviour and business trends. These features are vital for efficient operations and let the system serve administrators and clients effectively [40]. From a non-functional point of view, the system is meant to be able to grow to meet the needs of more users, keep running smoothly by maintaining high performance, and use strong security measures to keep user data and transactions safe [41]. Usability and dependability are also quite important. They make sure that users have a simple and reliable experience when they use the system [42].

The technological underpinning of the article integrates both the MERN and LAMP stacks to utilise the capabilities of each technology suite. MERN (MongoDB, Express.js, React.js, Node.js) enables the front-end development and temporary server activities, enabling dynamic user interface experiences and responsive interactions [43-46]. LAMP (Linux, Apache, MySQL, PHP) is used as a permanent server solution since it is stable and has a mature environment for backend activities. The system will also feature third-party services for payment integration, hosting, and deployment to boost functionality and user experience [47-51]. The paper is restricted by various constraints, including time, budget, and resource allocation. These limits influence the paper's schedule, feature set, and resource utilisation tactics [52]. Even with these limits, the study's feasibility is looked at from three angles: technical feasibility looks at whether the current technology can support the system's development; economic feasibility looks at whether the costs are worth it and whether the investment will pay off; and operational feasibility looks at whether the solution can be added to existing workflows and managed well by the end users [53-57].

The paper also aims to integrate machine learning algorithms to enhance transaction analysis and fraud detection in cryptocurrency-related applications. One of the key goals is transaction pattern analysis, where ML algorithms can recognise anomalous behaviours that may indicate fraudulent activities such as money laundering [58-60]. For instance, clustering techniques group similar transactions, making it easier to identify those that deviate from standard patterns. Another goal is to address clustering, in which ML models group cryptocurrency addresses with similar behaviours, often uncovering networks of addresses associated with Ponzi schemes or illegal marketplaces [61-63]. Machine learning models can also be trained for fraud detection by analysing historical transaction data and identifying key indicators of fraud, including transaction size, frequency, and velocity [64].

Through supervised learning, the model can classify future transactions as legitimate or suspicious. In addition, network analysis plays a crucial role in uncovering complex criminal networks [65-67]. Graph-based ML algorithms analyse the connections and structures within cryptocurrency networks to highlight mixing services or long transaction chains that could signify attempts at laundering money [68]. Sentiment analysis is another technique that utilises natural language processing to monitor online discussions, social media posts, and forums for signs of impending or ongoing criminal activities in the crypto space [69]. Finally, risk scoring systems powered by machine learning assign each transaction or address a likelihood of criminal involvement, helping law enforcement and regulatory bodies prioritise their investigations effectively [70].

This research highlights the growing importance of machine learning in addressing cryptocurrency-related fraud. It emphasises the need for a robust data collection and preparation phase, sourcing data from blockchain logs, exchanges, and third-party services [71-73]. The dataset must include transaction history, timestamps, types, and account balances to cover a wide range of fraud indicators. The authors also recommend the inclusion of labelled data, if available, to facilitate supervised learning [74]. In the absence of such labels, unsupervised methods like

anomaly detection may be used to identify potential fraudulent activity. Feature engineering is crucial in the development of machine learning models for fraud detection [75].

The authors suggest extracting transaction-based features such as frequency, average transaction size, and time between transactions [76]. Account-based features should include metrics like account age, balance fluctuations, and connections to other accounts. Furthermore, graph-based features provide a powerful way to model and analyse relationships between addresses and transactions [77-81]. By constructing a graph of the transaction network, researchers can extract features like centrality (to determine the influence of a node), clustering coefficients (to assess how tightly nodes are connected), and perform community detection to uncover suspicious groups or patterns. These engineered features enhance the model's ability to detect and prevent fraudulent activities in a highly dynamic and complex financial ecosystem like cryptocurrency [82-84]. Overall, the integration of machine learning into transaction analysis and fraud detection significantly enhances the intelligence of modern systems. It allows for real-time monitoring, proactive threat detection, and improved allocation of investigative resources [85-89]. When paired with a robust technological stack like MERN and LAMP, and designed to be scalable, secure, and user-friendly, such systems become powerful tools not only for managing online bookstores but also for tackling broader challenges such as financial fraud in the digital economy [90].

Review of Literature

When developing a machine learning-driven approach to detect and prevent cryptocurrency fraud, it's important to understand the existing systems and methods already in place. This helps you identify potential gaps and areas for improvement [11]. Many crypto exchanges use rule-based systems to detect suspicious activities. These systems use predefined rules such as transaction limits, frequency, and patterns to flag potential fraud. While rule-based systems are simple and easy to implement, they may not adapt well to new or evolving fraud tactics [12]. Graph analytics involves modelling transactions and accounts as a graph and using graph-based algorithms to identify anomalous patterns, such as clustering, community detection, and centrality analysis. KYC and AML regulations require exchanges to verify the identity of their customers and monitor transactions for signs of money laundering [1].

These procedures are often combined with machine learning techniques to identify suspicious activities, proposing a machine learning-driven system for the detection and prevention of cryptocurrency fraud [13]. It's important to design a comprehensive and adaptable framework that leverages the latest advancements in data science and machine learning. Your proposed system should be robust, flexible, and scalable to adapt to evolving fraud tactics. Here's a step-by-step guide to designing your proposed system [2]

Develop a pipeline to ingest data from various sources, including blockchain transaction logs, crypto exchanges, and third-party APIs. Data Storage: Use a secure and scalable data storage system to handle large volumes of data. Consider using cloud-based solutions for scalability. Data Processing: Implement data cleaning and transformation processes to prepare data for analysis [14]. Transaction Features: Extract features from transaction data such as amount, frequency, type, and time of transactions. Account Features: Analyse account data such as balance changes, account age, and connected accounts. Graph Features: Create a transaction graph and extract features such as centrality and clustering coefficients [15]. Supervised Learning: Use classification algorithms like logistic regression, random forests, gradient boosting, or neural networks to identify fraudulent and legitimate transactions based on labelled data [3].

Unsupervised learning methods play a critical role in identifying anomalies in cryptocurrency transactions. Techniques such as clustering, isolation forests, and autoencoders can be employed to detect unusual patterns or behaviours in transaction data and user accounts without requiring labelled data. These methods are particularly effective in uncovering unknown fraud types and emerging criminal tactics [16]. To further enhance detection accuracy and adaptability, hybrid approaches that combine supervised and unsupervised learning techniques are recommended.

Supervised learning uses labelled datasets of legitimate and fraudulent activities to train classification models, while unsupervised techniques help detect unknown or novel fraud behaviours [17]. Model training is an essential phase where the system learns from historical data. It is followed by a thorough evaluation using metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. Cross-validation techniques are implemented to ensure robustness and prevent overfitting [4].

Once models meet performance criteria, they are deployed into production environments where they can monitor real-time transactions. Real-time monitoring enables the system to immediately analyse incoming data and flag suspicious activities [18]. In response to such events, alert mechanisms are triggered to notify administrators, investigators, or users about potentially fraudulent transactions. There are several advantages to implementing a machine learning-driven system for detecting and preventing cryptocurrency fraud compared to traditional rule-based systems [19]. These benefits include improved accuracy due to pattern recognition and adaptive learning capabilities, real-time detection that enhances response times, and scalability that accommodates increasing transaction volumes [20]. Machine learning models excel at anomaly detection by identifying subtle deviations from normal behaviour [5].

They are dynamic and can adapt to changing fraud tactics over time, resulting in fewer false positives and a better user experience. Additionally, predictive capabilities help forecast future fraudulent activities, while explainability techniques provide transparency into model decisions [21]. Customisation allows models to be tailored to specific organisational needs, and collaborative learning across institutions enhances threat intelligence. Furthermore, compliance with regulatory standards such as Know Your Customer (KYC) and Anti-Money Laundering (AML) is supported through automated checks and logging [6].

The system requires both hardware and software components to perform efficiently. The architecture has a strong data pipeline for collecting, cleaning, and changing data from a software point of view. The data is collected from blockchain logs, cryptocurrency exchanges, and third-party services, then cleaned to resolve missing values, duplication, and abnormalities [22]. Transformed data is standardised and encoded to produce adequate input features for model training. Data is kept utilising safe and scalable storage systems, with robust encryption and access control methods assuring data privacy. Good data management makes it easy to find information and follow security rules. Feature engineering is an important aspect of the system [7].

It takes raw data and finds useful features at both the transaction and account levels. Graph-based analysis provides understanding by describing the transaction network and determining metrics such as centrality or community structure. Feature selection approaches are then utilised to reduce dimensionality and increase model efficiency [23]. The type of problem determines which machine learning models are best. Supervised models learn on data that has been labelled, while unsupervised models look for strange patterns. As more data becomes available, these models are always being tested and improved [8].

Real-time monitoring systems look for evidence of fraud by watching transactions and how accounts behave. The alerting system sends out warnings with customizable levels to cut down on false alarms when it finds something strange. A feedback loop is built where users and analysts can provide input on false positives and false negatives [24]. We utilise this feedback to make models better and keep them in line with changing fraud practices. The system uses explainability tools like SHAP (Shapley Additive Explanations) to make things clearer. These tools assist users in comprehending why certain transactions are highlighted [25]. There are ways for users to talk to each other about how to respond to alerts and defend themselves from fraud. Security elements include encryption, secure access control, and adherence to data protection regulations. The system's workflow includes making sure that it follows rules like KYC and AML [9].

Users can also get help from instructional materials that describe common fraud techniques and how to stay away from them. Customer support teams are there to help users with questions about

transactions that have been reported. Working with other people in the business helps to share data, methodologies, and best practices, which makes the system better at finding complicated fraud [26]. Working with the police and other regulatory organisations makes the fight against fraud even stronger on a larger scale. Finally, all transactions and system operations are recorded for compliance and auditing purposes [27]. These records aid in forensic investigations and ensure that fraud detection activities are open and honest. Logging also makes it possible for businesses to show that they are following both internal policies and government rules [10].

Methodology

The Data Ingestion Module collects transaction data from various sources and passes it to the Feature Engineering Module. The Feature Engineering Module processes the data and extracts relevant features, which are then forwarded to the Machine Learning Model. This model is responsible for classifying transactions as either legitimate or fraudulent based on the processed data and extracted features. If a transaction is classified as suspicious, the result is transmitted to the Alerting System, which generates an alert and promptly notifies the Administrator for further action. Upon receiving an alert, the Administrator reviews and investigates the flagged transaction. Based on this investigation, they may confirm the fraudulent nature of the transaction or dismiss it as a false positive. Additionally, the Administrator provides valuable feedback on the alert, which is essential for refining the model's accuracy over time.

This feedback loop plays a critical role in the continuous improvement of the system. The feedback, especially regarding false positives and false negatives, is used to retrain and update the Machine Learning Model to enhance future performance and adapt to evolving fraud patterns [91]. The activity flow begins with data collection, involving the gathering of transaction data from blockchain logs and cryptocurrency exchanges. This raw data undergoes cleaning and transformation processes to prepare it for effective analysis [92]. Feature engineering is then performed to extract and select meaningful attributes from the data that are crucial for training machine learning models. The model then makes predictions, classifying transactions as either legitimate or potentially fraudulent [93-96]. Real-time transaction monitoring ensures that all activities are constantly checked against the model’s predictions. Suspicious transactions are flagged, leading to the generation of alerts which are handled by appropriate users or administrators. These users investigate the flagged activities and take necessary actions [97]. They also provide feedback on the model’s performance, contributing to ongoing system refinement and improvement.

In terms of machine learning models suitable for this application, several supervised learning models can be effectively employed. Random Forest is highly effective for classification tasks and can handle high-dimensional datasets. It captures complex feature relationships and is robust to noise and overfitting. Support Vector Machines (SVMs) are also effective for binary classification, utilising hyperplanes to distinguish between classes and employing kernel tricks for handling non-linear relationships. Logistic Regression is a simple yet powerful model for binary classification, modelling the probability of an event based on predictor variables. It is both interpretable and efficient for large-scale datasets. Gradient Boosting Machines (GBM) use an ensemble of weak learners, typically decision trees, to sequentially correct errors, resulting in a strong model capable of handling complex data types.

Unsupervised learning models also offer powerful tools for fraud detection. K-Means Clustering can group similar transactions or addresses based on shared features, while DBSCAN excels at detecting outliers and forming clusters in noisy, irregular datasets. Isolation Forests, designed for anomaly detection, isolate anomalies quickly and efficiently, making them suitable for high-dimensional datasets. Deep learning approaches are equally valuable in this domain. Convolutional Neural Networks (CNNs) can be applied to sequential or image-like data, extracting features automatically for tasks such as image-based fraud detection. Recurrent Neural Networks (RNNs) are designed for analysing sequential data and are useful for detecting temporal patterns in transactions. Graph Neural Networks (GNNs), specialised for graph-structured data like cryptocurrency transaction networks, can learn complex representations and are well-suited for

node classification or link prediction tasks.

Ensemble approaches improve prediction accuracy by merging the results of several base models. Bagging (as in Random Forests) and boosting (as in Gradient Boosting Machines) are two methods that help combine the strengths of several models and reduce their weaknesses. Meta-learning approaches further boost adaptability by training a meta-model that learns how to optimally mix or pick among base models depending on the properties of the data. This dynamic selection process makes sure that the best model or combination is utilised for each data subset, which improves performance as a whole. In the study "Prediction and Prevention of Cryptocurrency Crimes Using Community Detection Approach," linear regression may be constrained by the intrinsic non-linearity and complexity of the data. Nonetheless, linear regression can still be utilised to examine trends or conduct a preliminary exploratory study. It might not be able to capture all the details of transaction patterns or user behaviours, but it can be used as a starting point or to add to more advanced models in a hybrid analytical framework.

Result and Discussion

Logistic regression is a simple and popular way to classify things. It can be used in a machine learning system to find and stop cryptocurrency fraud. It is a supervised learning algorithm that predicts the likelihood of an event happening, which makes it perfect for binary classification tasks like determining if a transaction is real or fake. Integrating logistic regression into a fraud detection system begins with the establishment of a robust data pipeline. This pipeline collects data from a number of places, such as transaction records on the blockchain, bitcoin exchanges, and other platforms that are important. Once collected, the data undergoes a cleaning and transformation procedure, which includes resolving missing values, removing duplicates, correcting outliers, and standardising the data to ensure consistency for the model's input.

Next comes feature engineering, which uses statistical methods like correlation analysis or feature importance scoring to find and choose relevant transaction features like amount, frequency, time of day, and type to make the model work better. The cleaned and reformatted dataset is then used to train the logistic regression model to guess how likely it is that a transaction is fake. To see how well the model works, it is tested with a validation dataset, and metrics like accuracy, precision, recall, F1-score, and AUC-ROC are used. To improve the model and stop it from overfitting, hyperparameter tuning is done, which includes changing the strength of the regularisation. After training, the model is put into a system that monitors transactions in real time. Transactions reported as possibly fraudulent are recognised for further examination, and notifications are created to notify relevant users or administrators.

An interface helps administrators handle warnings, see reports, and change system settings. Feedback on model performance, especially about false positives and negatives, is collected to permit continual model improvement. This continuing development includes regular updates of the logistic regression model and modification of the feature engineering process based on feedback and growing data trends.

System logging and auditing are important parts of keeping things open and following the rules. We keep track of all transactions and system operations so we can check them later. The system is also checked on a regular basis to make sure it works as well as possible. The primary aim of utilising logistic regression in this context is to forecast binary events, such as fluctuations in cryptocurrency prices. To back this information, historical bitcoin price data is collected via financial databases, APIs, or exchange platforms. Features could be price, volume, market cap, and technical indicators. They could also include news sentiment or macroeconomic data. Cleaning, moving averages, and normalisation are all important steps in data preprocessing. The data is divided into three sets: training, validation, and testing. The ratio is usually 70-15-15.

To keep the model simple while keeping significant information, dimensionality reduction methods like PCA are used. Logistic regression is chosen for its efficacy in binary classification and interpretability. Training a model involves choosing the best parameters and fitting the model to the training data. Cross-validation and hyperparameter adjustment make sure that the model

works well on data it hasn't seen before. The trained model employs a probability threshold to make classifications and predict outcomes for additional data. To measure performance, we employ evaluation measures and a confusion matrix. The model is connected to trading or analytical platforms when it is deployed. It is then monitored and retrained as needed. Ethical issues include being open and honest, following the rules, and reducing bias in data and forecasts. It is very important to check for convergence, keep an eye on training metrics, and make sure the model can accurately classify transactions during model training.

We test the system's connection with cryptocurrency platforms to make sure it can make predictions in real time. We also check how fast the prediction is to make sure it meets the criteria of time-sensitive fraud detection. Keeping up with changing fraud patterns is part of model maintenance, which includes using version control and retraining the model with new data on a regular basis. Error handling techniques are used to find problems in model training and predictions, and strong logging and monitoring tools keep track of important system performance indicators. White box testing approaches are used to make sure that all logical paths are followed, all decision points are examined, and all loops work as they should. It is very important to make sure that input parameters match function arguments and that global variable definitions are the same everywhere. We check the validity of the logistic function, cost computations, and gradient descent by going over the implementation of logistic regression.

Feature engineering is inspected to confirm adequate selection, transformation, and scale of key variables. The source code receives examination to guarantee adherence to coding standards, and code coverage techniques measure the breadth of test coverage across essential components. To protect the system's integrity, boundary value analysis is used to test how the system behaves when it receives extreme input and how well it handles errors. Finally, performance and scalability tests look at how well a computer can handle training time, prediction latency, and memory utilisation. We do scalability tests to see how well the system can handle more and more transaction data. The tests look at things like response times, throughput, and resource use under different scenarios. This thorough integration of logistic regression, accompanied by rigorous testing and continual refinement, enables a strong and adaptive solution for detecting and combating cryptocurrency fraud.

Conclusion

In summary, the article "Prediction and Prevention of Cryptocurrency Crimes Using Community Detection Approach" shows a lot of promise for using sophisticated analytics to fight illegal activity in cryptocurrencies. Through the synthesis of community detection algorithms and comprehensive data analysis, this study intends to provide insights that can improve the detection and prevention of numerous forms of financial crimes, including money laundering, fraud, and illicit transactions. This research aims to aid in the formulation of proactive methods to prevent cryptocurrency-related crimes by analysing current literature, collecting pertinent data sets, and employing community detection algorithms to discern patterns and clusters within cryptocurrency networks. Using blockchain data, transaction records, network metrics, and metadata gives you a complete picture of how cryptocurrency transactions work and lets you find suspect behaviour. However, it's necessary to realise the problems and limitations inherent in this attempt.

Some of the things that could affect how well and how widely the proposed technique works are the availability of data, privacy issues, algorithmic difficulties, and legislative limits. Also, the cryptocurrency environment is always changing; therefore, analytical methods need to be updated and improved all the time to stay useful and relevant. Even with these problems, being able to accurately forecast and stop cryptocurrency crimes could have a big positive effect on society. Determine future plans for reducing the dangers that come with cryptocurrencies and making sure they are used responsibly in the global financial system.

References

[1] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the Bitcoin ecosystem," J. Cybersecurity, vol. 5, no. 1, 2019, Art. no. tyz003.

[2] D. Y. Huang et al., "Tracking ransomware end-to-end," in Proc. IEEE Symp. Secure. Privacy, California, United States of America, 2018.

[3] C. Sas and I. E. Khairuddin, "Design for trust: An exploration of the challenges and opportunities of bitcoin users," in Proc. CHI Conf. Hum. Factors Comput. Syst., Denver, Colorado, United States of America, 2017.

[4] J. Weber and E. W. Kruisbergen, "Criminal markets: The dark web, money laundering, and counterstrategies—an overview of the 10th research conference on organised crime," Trends Organised Crime, vol. 22, no. 3, pp. 346–356, 2019.

[5] D. K. Sharma and R. Tripathi, "4 Intuitionistic fuzzy trigonometric distance and similarity measure and their properties," in Soft Computing, De Gruyter, Berlin, Germany, pp. 53–66, 2020.

[6] D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. Kalyan Chakravarthi, "Applications of two separate methods to deal with a small dataset and a high risk of generalization," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.

[7] D. K. Sharma, B. Singh, M. Anam, K. O. Villalba-Condori, A. K. Gupta, and G. K. Ali, "Slotting learning rate in deep neural networks to build stronger models," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.

[8] K. Kaliyaperumal, A. Rahim, D. K. Sharma, R. Regin, S. Vashisht, and K. Phasinam, "Rainfall prediction using deep mining strategy for detection," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.

[9] A.J. John Joseph, F.J. John Joseph, O.M. Stanislaus, and D. Das (2022). Classification methodologies in healthcare, Evolving Predictive Analytics in Healthcare: New AI techniques for real-time interventions, p 55-73. IET.

[10] F. J. J. John Joseph, "Twitter Based Outcome Predictions of 2019 Indian General Elections Using Decision Tree," in Proceedings of 2019 4th International Conference on Information Technology, 2019, no. October, pp. 50–53.

[11] F. J. John Joseph and P. Anantaprayoon, "Offline Handwritten Thai Character Recognition Using Single Tier Classifier and Local Features," in 2018 International Conference on Information Technology (InCIT), 2018, pp. 1–4.

[12] F. J. John Joseph and S. Auwatanamongkol, "A crowding multi-objective genetic algorithm for image parsing," Neural Comput. Appl., vol. 27, no. 8, pp. 2217–2227, 2016.

[13] F. J. John Joseph and S. Nonsiri, "Region-Specific Opinion Mining from Tweets in a Mixed Political Scenario," in International Conference on Intelligent and Smart Computing in Data Analytics, 2021, pp. 189–195.

[14] F. J. John Joseph and V. R. T, "Enhanced Robustness for Digital Images Using Geometric Attack simulation," Procedia Eng., vol. 38, no. Apr 2012, pp. 2672–2678, 2012.

[15] F. J. John Joseph, "IoT-Based Unified Approach to Predict Particulate Matter Pollution in Thailand" The Role of IoT and Blockchain: Techniques and Applications, 145-151, 2022.

[16] F. J. John Joseph, R. T, and J. J. C, "Classification of correlated subspaces using HoVer representation of Census Data," in 2011 International Conference on Emerging Trends in Electrical and Computer Technology, Mar. 2011, pp. 906–911.

[17] F.J. John Joseph, (2022). IoT Based Aquarium Water Quality Monitoring and Predictive Analytics Using Parameter Optimized Stack LSTM. In 2022 International Conference on Information Technology (InCIT). IEEE

[18] F.J. John Joseph, (2023). Time series forecast of Covid 19 Pandemic Using Auto Recurrent Linear Regression. Journal of Engineering Research.

[19] J. F. Joe, T. Ravi, A. Natarajan and S. P. Kumar, "Object recognition of Leukemia affected cells using DCC and IFS," 2010 Second International conference on Computing, Communication and Networking Technologies, 2010, pp. 1-6.

[20] Razeghi, M., Dehzangi, A., Wu, D., McClintock, R., Zhang, Y., Durlin, Q., ... & Meng, F. (2019, May). Antimonite-based gap-engineered type-II superlattice materials grown by MBE and MOCVD for the third generation of infrared imagers. In Infrared Technology and Applications XLV (Vol. 11002, pp. 108-125). SPIE.
[21] Meng, F., Zhang, L., & Chen, Y. (2023) FEDEMB: An Efficient Vertical and Hybrid Federated Learning Algorithm Using Partial Network Embedding.
[22] Meng, F., Jagadeesan, L., & Thottan, M. (2021). Model-based reinforcement learning for service mesh fault resiliency in a web application-level. arXiv preprint arXiv:2110.13621.
[23] Meng, F., Zhang, L., Chen, Y., & Wang, Y. (2023). Sample-based Dynamic Hierarchical Transformer with Layer and Head Flexibility via Contextual Bandit. Authorea Preprints.
[24] Aryal, I. Stricklin, M. Behzadirad, D. W. Branch, A. Siddiqui, and T. Busani, "High-quality dry etching of LiNbO3 assisted by proton substitution through H2-plasma surface treatment," Nanomaterials (Basel, Switzerland), vol. 12, no. 16, p. 2836, 2022.
[25] R. L. Paldi, A. Aryal, M. Behzadirad, T. Busani, A. Siddiqui, and H. Wang, "Nanocomposite-seeded single-domain growth of lithium niobate thin films for photonic applications," in Conf. Lasers Electro-Optics, Washington, D.C.: Optica Publishing Group, 2021.
[26] S. M. Z. Shifat, I. Stricklin, R. K. Chityala, A. Aryal, G. Esteves, A. Siddiqui, and T. Busani, "Vertical etching of scandium aluminum nitride thin films using TMAH solution," Nanomaterials (Basel, Switzerland), vol. 13, no. 2, 2023.
[27] I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization,” International Journal of Computer Applications, vol. 80, no. 13, pp. 18–23, 2013.
[28] I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization for Kidney Transplantation,” International Journal of Computer Applications, vol. 92, no. 6, pp. 25–29, 2014.
[29] M. M. Abbassy and A. Abo-Alnadr, “Rule-based emotion AI in Arabic Customer Review,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 9, p.12, 2019.
[30] M. M. Abbassy and W. M. Ead, “Intelligent Greenhouse Management System,” 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020.
[31] M. M. Abbassy, “Opinion mining for Arabic customer feedback using machine learning,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP3, pp. 209–217, 2020.
[32] M. M. Abbassy, “The human brain signal detection of Health Information System IN EDSAC: A novel cipher text attribute based encryption with EDSAC distributed storage access control,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP7, pp. 858–868, 2020.
[33] M. M. and S. Mesbah, “Effective e-government and citizens adoption in Egypt,” International Journal of Computer Applications, vol. 133, no. 7, pp. 7–13, 2016.
[34] M.M.Abbassy, A.A. Mohamed “Mobile Expert System to Detect Liver Disease Kind”, International Journal of Computer Applications, vol. 14, no. 5, pp. 320–324, 2016.
[35] R. A. Sadek, D. M. Abd-alazeem, and M. M. Abbassy, “A new energy-efficient multi-hop routing protocol for heterogeneous wireless sensor networks,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 11, 2021.
[36] S. Derindere Köseoğlu, W. M. Ead, and M. M. Abbassy, “Basics of Financial Data Analytics,” Financial Data Analytics, pp. 23–57, 2022.
[37] W. Ead and M. Abbassy, “Intelligent Systems of Machine Learning Approaches for developing E-services portals,” EAI Endorsed Transactions on Energy Web, p. 167292, 2018.
[38] W. M. Ead and M. M. Abbassy, “A general cyber hygiene approach for financial analytical environment,” Financial Data Analytics, pp. 369–384, 2022.
[39] W. M. Ead and M. M. Abbassy, “IoT based on plant diseases detection and classification,” 2021 7th International Conference on Advanced Computing and Communication Systems

(ICACCS), 2021.
[40] W. M. Ead, M. M. Abbassy, and E. El-Abd, “A general framework information loss of utility-based anonymization in Data Publishing,” Turkish Journal of Computer and Mathematics Education, vol. 12, no. 5, pp. 1450–1456, 2021.
[41] A. M. El-Kady, M. M. Abbassy, H. H. Ali, and M. F. Ali, “Advancing Diabetic Foot Ulcer Detection Based On Resnet And Gan Integration,” Journal of Theoretical and Applied Information Technology, vol. 102, no. 6, pp. 2258–2268, 2024.
[42] M. M. Abbassy and W. M. Ead, “Fog computing-based public e-service application in service-oriented architecture,” International Journal of Cloud Computing, vol. 12, no. 2–4, pp. 163–177, 2023.
[43] H. AbdulKader, E. ElAbd, and W. Ead, "Protecting online social networks profiles by hiding sensitive data attributes," Procedia Computer Science, vol. 82, pp. 20–27, 2016.
[44] I. E. Fattoh, F. Kamal Alsheref, W. M. Ead, and A. M. Youssef, "Semantic sentiment classification for COVID-19 tweets using universal sentence encoder," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–8, 2022.
[45] W. M. Ead, W. F. Abdel-Wahed, and H. Abdul-Kader, "Adaptive fuzzy classification-rule algorithm in detection malicious web sites from suspicious URLs," International Arab Journal of e-Technology, vol. 3, pp. 1–9, 2013.
[46] M. A. Abdelazim, M. M. Nasr, and W. M. Ead, "A survey on classification analysis for cancer genomics: Limitations and novel opportunity in the era of cancer classification and target therapies," Annals of Tropical Medicine and Public Health, vol. 23, no. 24, 2020.
[47] F. K. Alsheref, I. E. Fattoh, and W. M. Ead, "Automated prediction of employee attrition using ensemble model based on machine learning algorithms," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–9, 2022.
[48] S. Bhoumik, S. Chatterjee, A. Sarkar, A. Kumar, and F. J. John Joseph, “Covid 19 Prediction from X Ray Images Using Fully Connected Convolutional Neural Network,” in CSBio ’20: Proceedings of the Eleventh International Conference on Computational Systems-Biology and Bioinformatics, Nov. 2020, pp. 106–107.
[49] T. Pichaibunditkun, F.J. John Joseph, (2023). Private Permission Blockchain for Optimized Invoice Management System. In 2023 International Conference on Business and Industrial Research (ICBIR). IEEE.
[50] V. Pattana-anake, F.J. John Joseph, P. Pachaivannan, (2022). Data Wrangling for IoT Based Aquarium Water Quality Management System. In 2022 International Conference on Data Science, Agents and Artificial Intelligence (ICDSAAI). IEEE.
[51] I. Nallathambi, R. Ramar, D. A. Pustokhin, I. V. Pustokhina, D. K. Sharma, and S. Sengan, “Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach,” Environ. Pollut., vol. 304, no. 7, p. 119182, 2022.
[52] H. Sharma and D. K. Sharma, “A Study of Trend Growth Rate of Confirmed Cases, Death Cases and Recovery Cases of Covid-19 in Union Territories of India,” Turkish Journal of Computer and Mathematics Education, vol. 13, no. 2, pp. 569–582, 2022.
[53] A. L. Karn et al., “Designing a Deep Learning-based financial decision support system for fintech to support corporate customer’s credit extension,” Malays. J. Comput. Sci., vol.36, no.s1, pp. 116–131, 2022.
[54] A. L. Karn et al., “B-lstm-Nb based composite sequence Learning model for detecting fraudulent financial activities,” Malays. J. Comput. Sci., vol.32, no.s1, pp. 30–49, 2022.
[55] P. P. Dwivedi and D. K. Sharma, “Application of Shannon entropy and CoCoSo methods in selection of the most appropriate engineering sustainability components,” Cleaner Materials, vol. 5, no. 9, p. 100118, 2022.
[56] A. Kumar, S. Singh, K. Srivastava, A. Sharma, and D. K. Sharma, “Performance and stability enhancement of mixed dimensional bilayer inverted perovskite (BA2PbI4/MAPbI3) solar cell using drift-diffusion model,” Sustain. Chem. Pharm., vol. 29, no. 10, p. 100807, 2022.
[57] A. Kumar, S. Singh, M. K. A. Mohammed, and D. K. Sharma, “Accelerated innovation in developing high-performance metal halide perovskite solar cell using machine learning,” Int.

J. Mod. Phys. B, vol. 37, no. 07, p.12, 2023.
[58] G. A. Ogunmola, M. E. Lourens, A. Chaudhary, V. Tripathi, F. Effendy, and D. K. Sharma, “A holistic and state of the art of understanding the linkages of smart-city healthcare technologies,” in 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022.
[59] P. Sindhuja, A. Kousalya, N. R. R. Paul, B. Pant, P. Kumar, and D. K. Sharma, “A Novel Technique for Ensembled Learning based on Convolution Neural Network,” in 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, Tamil Nadu, India, pp. 1087–1091, 2022.
[60] A. R. B. M. Saleh, S. Venkatasubramanian, N. R. R. Paul, F. I. Maulana, F. Effendy, and D. K. Sharma, “Real-time monitoring system in IoT for achieving sustainability in the agricultural field,” in 2022 International Conference on Edge Computing and Applications (ICECAA), Tamil Nadu, India, 2022.
[61] Srinivasa, D. Baliga, N. Devi, D. Verma, P. P. Selvam, and D. K. Sharma, “Identifying lung nodules on MRR connected feature streams for tumor segmentation,” in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Tamil Nadu, India, 2022.
[62] C. Goswami, A. Das, K. I. Ogaili, V. K. Verma, V. Singh, and D. K. Sharma, “Device to device communication in 5G network using device-centric resource allocation algorithm,” in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Tamil Nadu, India , 2022.
[63] M. Yuvarasu, A. Balaram, S. Chandramohan, and D. K. Sharma, “A Performance Analysis of an Enhanced Graded Precision Localization Algorithm for Wireless Sensor Networks,” Cybernetics and Systems, pp. 1–16, 2023, Press.
[64] P. P. Dwivedi and D. K. Sharma, “Evaluation and ranking of battery electric vehicles by Shannon’s entropy and TOPSIS methods,” Math. Comput. Simul., vol. 212, no.10, pp. 457–474, 2023.
[65] P. P. Dwivedi and D. K. Sharma, “Assessment of Appropriate Renewable Energy Resources for India using Entropy and WASPAS Techniques,” Renewable Energy Research and Applications, vol. 5, no. 1, pp. 51–61, 2024.
[66] P. P. Dwivedi and D. K. Sharma, “Selection of combat aircraft by using Shannon entropy and VIKOR method,” Def. Sci. J., vol. 73, no. 4, pp. 411–419, 2023.
[67] P. Das, D. Datta, S. S. Rajest, L. M. M. Visuwasam, A. Thakare, and J. Cypto, "Application of multi-criteria decision-making approach using TOPSIS to identify the vulnerable time zone of earthquake time series signal," Int. J. Crit. Comput.-Based Syst., vol. 11, no. 1/2, pp. 30–47, 2024.
[68] G. Kumaresan and L. M. Visuwasam, "Enhanced in-line data deduplication and secure authorization in hybrid cloud," Int. J. Innov. Res. Sci. Eng. Technol., vol. 4, no. 2, pp. 466–471, 2015.
[69] S. Gomathy, K. Deepa, T. Revathi, and L. M. M. Visuwasam, "Genre specific classification for information search and multimodal semantic indexing for data retrieval," SIJ Trans. Comput. Sci. Eng. Appl. (CSEA), vol. 1, no. 1, pp. 10–15, 2013.
[70] K. Kishore, D. Dhinakaran, N. J. Kumar, S. M. U. Sankar, K. Chandu, and L. M. M. Visuwasam, "Fish farm monitoring system using IoT," in Proc. 2021 Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN), 2021, vol. 10, pp. 1–6.
[71] L. M. V., A. Balakrishna, N. S. R., and K. V., "Level-6 automated IoT integrated with artificial intelligence based big data-driven dynamic vehicular traffic control system," EAI Endorsed Trans. Energy Web, p. 164176, 2018.
[72] N. J. K., M. Shoba, D. Dhinakaran, L. M. M. V., and G. Elangovan, "Bio-inspired optimization to enhance the performance in 6G networks of reconfigurable intelligent surfaces," in Advances in Computational Intelligence and Robotics, pp. 409–444, 2025.
[73] N. J. Kumar, R. Premkumar, L. M. M. Visuwasam, G. Arjunan, G. Yuyaraj, and C. T. Kumar, "Hybrid K-means and firefly algorithm-based load balancer for dynamic task scheduling in fog computing for postoperative healthcare systems," in Proc. 2025 Int. Conf.

Adv. Comput. Technol. (ICoACT), Sivalasi, India, 2025, pp. 1–6.
[74] N. J. Kumar, R. Premkumar, L. M. Michael Visuwasam, G. Arjunan, A. Shiny, and K. Dharani, "Adaptive optimization and resource allocation (AORA) model for IoT-edge computing using hybrid Newton-Raphson and dolphin echolocation algorithm (HNR-DEA) technique," in Proc. 2025 Int. Conf. Adv. Comput. Technol. (ICoACT), Sivalasi, India, 2025, pp. 1–6.
[75] R. Premkumar, N. J. Kumar, L. M. Michael Visuwasam, G. Arjunan, A. Vinothini, and C. T. Kumar, "Hybrid gradient descent and sea lion optimization algorithm (H-GD-SLnO) to optimize task scheduling in fog computing environment," in Proc. 2025 Int. Conf. Adv. Comput. Technol. (ICoACT), Sivalasi, India, 2025, pp. 1–6.
[76] K. Singh, L. M. M. Visuwasam, G. Rajasekaran, R. Regin, S. S. Rajest, and S. T., "Innovations in skeleton-based movement recognition bridging AI and human kinetics," in Advances in Computational Intelligence and Robotics, pp. 125–141, 2024.
[77] D. Soundararajan, "A novel deep learning framework for rainfall prediction in weather forecasting," Turk. J. Comput. Math. Educ. (TURCOMAT), vol. 12, no. 11, pp. 2685–2692, 2021.
[78] T. B. Sivakumar, L. Maria Michael Visuvasam, V. Sangeetha, S. Bhuvana, K. S. Kumar, and K. Sachet, "Hybrid spotted hyena and simulated annealing optimization algorithm (HSHOSAA-1) for efficient task scheduling in a clustered cloud environment," in Proc. 2024 3rd Int. Conf. Smart Technol. Syst. Next Gener. Comput. (ICSTSN), Villupuram, India, 2024, pp. 1–6.
[79] L. M. M. Visuwasam and D. P. Raj, "NMA: integrating big data into a novel mobile application using knowledge extraction for big data analytics," Cluster Comput., vol. 22, no. S6, pp. 14287–14298, 2018.
[80] L. M. M. Visuwasam and D. P. Raj, "A distributed intelligent mobile application for analyzing travel big data analytics," Peer-to-Peer Netw. Appl., vol. 13, no. 6, pp. 2036–2052, 2019.
[81] L. M. M. Visuwasam and D. P. Raj, "Spatio temporal tourism tracking system based on adaptive convolutional neural network," Comput. Syst. Sci. Eng., vol. 45, no. 3, pp. 2435–2446, 2022.
[82] L. M. M. Visuwasam, S. V. Deshmukh, N. R. Paul, M. a. M. Raja, S. Kanimozhi, and A. Thakare, "Security and data privacy systems concerns in IoT using consensus algorithm," Int. J. Syst. Syst. Eng., vol. 14, no. 6, pp. 654–675, 2024.
[83] L. M. M. Visuwasam, K. Dhinakaran, G. Kalpana, A. Balakrishna, V. Kowsalyaa, and S. R. N. Keerthana, "SMART—stockpile management with analytical regulation technology," in Cognitive Science and Technology, pp. 835–845, 2022.
[84] L. M. M. Visuwasam, M. Geetha, G. Gayathri, K. Divya, and D. Elakkiya, "Smart personalised recommendation system for wanderer using prediction analysis," Int. J. Intell. Sustain. Comput., vol. 1, no. 3, p. 223, 2021.
[85] L. M. M. Visuwasam, A. K. Gupta, R. Chaudhary, S. C. Gupta, P. Borah, and M. K. Chakravarthi, "Innovative turned and collaborative technology using simulated IoT applications," in Proc. 2022 4th Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), 2022, pp. 369–374.
[86] L. M. M. Visuwasam, G. Kalpana, K. Dhinakaran, N. K. Kumar, and V. Manigandan, "Implementation of unusual human activity detection in warehouse using SSD," in Cognitive Science and Technology, pp. 847–857, 2022.
[87] L. M. M. Visuwasam, D. Paulraj, G. Gayathri, K. Divya, S. Hariprasath, and A. Jayaprakashan, "Intelligent personal digital assistants and smart destination platform (SDP) for globetrotter," J. Comput. Theor. Nanosci., vol. 17, no. 5, pp. 2254–2260, 2020.
[88] L. M. M. Visuwasam, M. Srinath, V. S. A. Raj, A. Sirajudeen, S. S. Maharaaja, and D. Raja, "Tourist behaviour analysis using data analytics," in Advances in Business Information Systems and Analytics, pp. 343–355, 2023.
[89] L. M. M. Visuwasam, S. Swaminathan, S. Rajalakshmi, and K. P. Kumar, "A hotspot framework for analyzing geolocated travel data using SPARK," Ann. Rom. Soc. Cell Biol.,

pp. 1956–1966, 2021.
[90] L. M. M. Visuwasam, M. Srinath, V. S. Raj, A. Sirajudeen, S. Sudhir Maharaaja, and D. Raja, "Tourist behaviour analysis using data analytics," in S. Singh, S. Rajest, S. Hadoussa, A. Obaid, and R. Regin, Eds., Data-Driven Decision Making for Long-Term Business Success. IGI Global Scientific Publishing, 2024, pp. 343–355.
[91] N. J. Kumar, R. Premkumar, L. M. Michael Visuwasam, G. Arjunan, A. Shiny, and K. Dharani, "Adaptive optimization and resource allocation (AORA) model for IoT-edge computing using hybrid Newton-Raphson and dolphin echolocation algorithm (HNR-DEA) technique," in Proc. 2025 Int. Conf. Adv. Comput. Technol. (ICoACT), Sivalasi, India, 2025, pp. 1–6.
[92] P. Das, D. Datta, S. S. Rajest, L. M. M. Visuwasam, A. Thakare, and J. Cypto, "Application of multi-criteria decision-making approach using TOPSIS to identify the vulnerable time zone of earthquake time series signal," Int. J. Crit. Comput.-Based Syst., vol. 11, no. 1/2, pp. 30–47, 2024.
[93] S. A. Karthik, S. B. Naga, G. Satish, N. Shobha, H. K. Bhargav, and B. M. Chandrakala, “AI and IoT-infused urban connectivity for smart cities,” in Future of Digital Technology and AI in Social Sectors, D. Ertuğrul and A. Elçi, Eds. IGI Global Scientific Publishing, 2025, pp. 367–394.
[94] S. Rashmi, B. M. Chandrakala, D. M. Ramani, and M. S. Harsur, “CNN based multi-view classification and ROI segmentation: A survey,” Global Transitions Proceedings, vol. 3, no. 1, pp. 86–90, 2022.
[95] K. S. N. S. Nischal, N. S. Guvvala, C. Mathew, G. C. S. Gowda, and B. M. Chandrakala, “A survey on recognition of handwritten ZIP codes in a postal sorting system,” International Research Journal of Engineering and Technology (IRJET), vol. 7, no. 3, pp. 1–4, May 2020.
[96] B. M. Chandrakala and S. C. Linga Reddy, “Proxy re-encryption using MLBC (Modified Lattice Based Cryptography),” in Proc. Int. Conf. Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil, India, 2019, pp. 1–5.
[97] H. S. Supriya and B. M. Chandrakala, “An efficient multi-layer hybrid neural network and optimized parameter enhancing approach for traffic prediction in Big Data Domain,” The Journal of Special Education, vol. 1, no. 43, pp. 94–96, 2022.