International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

Artificial Intelligence Models for Real-Time Financial Fraud Detection and Analytics Systems

Siddharth Umesh Shetty

Dept. of Computer science and IT, Kalinga University, Raipur, CG., India

ABSTRACT: Financial fraud has become one of the most critical challenges in the rapidly expanding digital economy, particularly with the growth of online banking, mobile payments, and e-commerce platforms. Traditional rule-based fraud detection systems are no longer sufficient due to their inability to adapt to evolving fraud patterns and their high false-positive rates. Artificial Intelligence (AI) offers a dynamic and scalable solution for real-time fraud detection and analytics by leveraging machine learning (ML), deep learning (DL), and advanced anomaly detection techniques. These AI-driven systems analyze large volumes of transactional and behavioral data in real time to identify suspicious activities with high accuracy. Supervised learning models such as Random Forest, Logistic Regression, and Gradient Boosting Machines are widely used for classification tasks, while unsupervised techniques like Isolation Forest and clustering algorithms help detect unknown anomalies. Deep learning models such as LSTM networks and autoencoders enhance detection capabilities by capturing temporal and nonlinear patterns in transaction sequences. Additionally, graph-based models improve fraud ring detection by analyzing relationships between entities. Integration with real-time streaming platforms enables immediate fraud scoring and response. Despite advancements, challenges such as data imbalance, model interpretability, privacy concerns, and adversarial attacks persist. This paper explores AI models, system architectures, and methodologies used in real-time financial fraud detection systems.

KEYWORDS: Artificial Intelligence, Machine Learning, Deep Learning, Fraud Detection, Real-Time Analytics, Financial Security, Anomaly Detection, Graph Neural Networks, Streaming Data, Cybersecurity

I. INTRODUCTION

The rapid digitization of financial services has significantly transformed the global economy, enabling faster transactions, improved accessibility, and enhanced user experiences. However, this transformation has also led to an increase in financial fraud activities, including identity theft, credit card fraud, account takeover, phishing attacks, and synthetic identity fraud. As financial systems become more complex and interconnected, detecting fraudulent behavior in real time has become increasingly challenging.Traditional fraud detection systems rely heavily on static rule-based mechanisms that flag transactions based on predefined thresholds such as transaction amount, frequency, or geographic location. While these systems are simple and interpretable, they are highly limited in their ability to detect new and evolving fraud patterns. Fraudsters continuously adapt their strategies, making rule-based systems obsolete over time.
Artificial Intelligence (AI) has emerged as a powerful solution to address these limitations. Machine Learning (ML) algorithms enable systems to learn patterns from historical transaction data and automatically detect anomalies without explicit programming. Supervised learning models classify transactions as legitimate or fraudulent based on labeled datasets, while unsupervised learning methods identify hidden anomalies in unlabeled data. Deep learning models further enhance detection capabilities by capturing complex nonlinear relationships and sequential dependencies in financial transactions.

Real-time fraud detection is particularly critical in modern financial systems, where transactions occur in milliseconds. To achieve this, AI models are integrated with streaming data platforms such as Apache Kafka and Spark Streaming, allowing continuous data ingestion, processing, and prediction. This enables financial institutions to block suspicious transactions instantly, reducing financial losses.Another key aspect of AI-based fraud detection is behavioral analytics, which focuses on understanding user behavior over time. By analyzing spending habits, device usage, login patterns, and location changes, AI systems can detect deviations that may indicate fraudulent activity.Despite significant advancements, challenges remain in deploying AI models for fraud detection. Data imbalance is a major issue, as fraudulent transactions represent a very small fraction of total transactions. Additionally, deep learning models often lack interpretability, which is critical for regulatory compliance in the financial sector. Privacy concerns and adversarial attacks further complicate system design.This study explores AI-based fraud detection models, their architectures, real-

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

time analytics integration, and emerging trends aimed at improving accuracy, scalability, and interpretability in financial security systems.

II. LITERATURE REVIEW

The earliest fraud detection systems were based on rule-based expert systems developed in the 1980s and 1990s. These systems used manually defined rules such as transaction limits, blacklist matching, and geographic restrictions. While effective in detecting known fraud patterns, they lacked adaptability and required constant manual updates. As fraud techniques evolved, these systems became inefficient and generated a high number of false positives, leading researchers to explore data-driven approaches.With the advancement of computational power, statistical methods such as logistic regression and Bayesian networks became popular for fraud detection. These models introduced probabilistic reasoning, allowing systems to estimate the likelihood of fraud based on input features. Logistic regression remains widely used due to its simplicity and interpretability.Machine learning models significantly improved fraud detection accuracy. Decision trees and Random Forest algorithms became popular due to their ability to handle nonlinear relationships and mixed data types. Support Vector Machines (SVM) were also widely used for classification tasks in high-dimensional spaces. Gradient Boosting methods such as XGBoost and LightGBM further improved performance by combining weak learners into strong predictive models.However, these supervised models require large labeled datasets, which are difficult to obtain in fraud detection scenarios. Fraud cases are rare, and labeling requires expert verification, making dataset creation expensive and time-consuming.

To address the limitation of labeled data, unsupervised learning methods have been widely explored. Clustering techniques such as K-Means and DBSCAN group similar transactions and identify outliers as potential fraud cases. Isolation Forest is particularly effective in fraud detection as it isolates anomalies instead of profiling normal behavior.
Autoencoders, a type of neural network, have also been used for anomaly detection. They learn compressed representations of normal transaction behavior and reconstruct input data. High reconstruction error indicates potential fraud.Semi-supervised learning techniques combine labeled and unlabeled data to improve model performance. These approaches are useful in fraud detection where labeled fraud data is scarce.

Deep learning has revolutionized fraud detection by enabling automatic feature extraction and improved pattern recognition. Artificial Neural Networks (ANNs) can model complex nonlinear relationships in transaction data.Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are particularly useful for sequential transaction data. They capture temporal dependencies, such as spending behavior over time, which is critical for detecting account takeover fraud.Convolutional Neural Networks (CNNs), although originally designed for image processing, have been adapted for structured financial data and feature extraction tasks.Graph Neural Networks (GNNs) have gained significant attention for fraud detection in network-based systems. Fraud often occurs in connected groups of accounts, and GNNs can analyze relationships between entities such as users, devices, and merchants to detect fraud rings.

Modern fraud detection systems require real-time processing capabilities. Technologies such as Apache Kafka, Apache Flink, and Spark Streaming enable continuous ingestion and processing of transactional data.
AI models are deployed within these streaming pipelines to provide instant fraud scoring. This ensures that suspicious transactions are blocked before completion. Real-time systems must balance latency and accuracy, making optimization critical.

Hybrid models combining multiple algorithms have shown superior performance. Ensemble methods such as bagging, boosting, and stacking improve robustness by aggregating predictions from multiple models.
Hybrid systems often combine rule-based filters with machine learning models to balance interpretability and accuracy. For example, a rule-based system may filter obvious fraud cases, while ML models handle complex cases.

One of the major challenges in AI-based fraud detection is model interpretability. Financial institutions require explanations for flagged transactions due to regulatory requirements. Explainable AI (XAI) techniques such as SHAP and LIME are used to interpret model decisions and improve transparency.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

III. RESEARCH METHODOLOGY

The research adopts an **experimental and quantitative design approach** aimed at developing and evaluating AI-based fraud detection models for real-time financial analytics systems. The study focuses on comparing multiple machine learning, deep learning, and hybrid models in terms of accuracy, speed, scalability, and robustness. The methodology involves dataset preprocessing, feature engineering, model training, validation, deployment simulation, and performance evaluation in a real-time environment.The dataset used in this research consists of historical financial transaction records collected from banking systems, digital payment platforms, and publicly available fraud detection datasets. The data includes transaction amount, timestamp, location, merchant category, device information, IP address, and user behavioral attributes. Since real financial datasets are highly sensitive, anonymized and synthetic datasets are also used to ensure privacy compliance. Data diversity is ensured by including both legitimate and fraudulent transaction samples across different time periods and user profiles. Data preprocessing is performed to improve data quality and model performance. Missing values are handled using statistical imputation techniques such as mean or median substitution. Categorical variables such as merchant type and location are encoded using one-hot encoding and label encoding methods. Numerical features are normalized using Min-Max scaling or Z-score normalization to ensure uniformity. Outlier detection is performed using statistical methods and removed or transformed depending on severity. Duplicate records are eliminated to prevent bias in model training.

Feature engineering plays a critical role in fraud detection performance. New behavioral features are created to capture user spending patterns, including average transaction value, transaction frequency per hour/day, and deviation from historical behavior. Time-based features such as transaction hour, weekday/weekend patterns, and seasonal trends are extracted. Device-based features include login frequency from new devices, IP address changes, and geolocation inconsistencies. Network-based features are constructed for graph analysis, representing relationships between users, merchants, and devices.

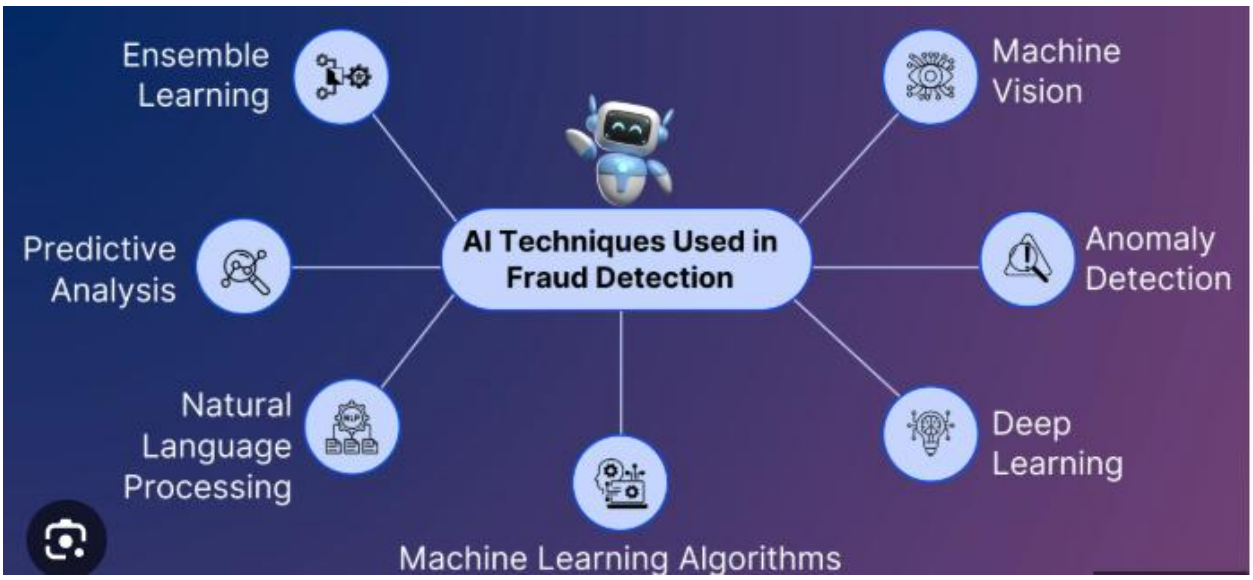


Fig 1: AI/ML Improve Fraud Detection Accuracy in Financial Institutions

Since fraudulent transactions represent a very small fraction of total data, class imbalance is a major challenge. To address this, multiple techniques are applied. SMOTE (Synthetic Minority Oversampling Technique) is used to generate synthetic fraud samples. Random undersampling is applied to reduce dominance of legitimate transactions. Cost-sensitive learning assigns higher penalty to misclassification of fraud cases. Evaluation metrics are adjusted to focus on recall and F1-score instead of accuracy alone. The dataset is divided into training, validation, and testing sets using an 80-10-10 split ratio. Cross-validation techniques such as k-fold validation are used to ensure robustness and prevent overfitting. Hyperparameter tuning is performed using grid search and random search methods. Early stopping techniques are applied for deep learning models to prevent overfitting. A real-time fraud detection architecture is designed consisting of multiple layers. The data ingestion layer captures live transaction streams using message

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

brokers. The processing layer performs data cleaning and feature extraction in real time. The AI inference layer applies trained models to score each transaction instantly. The decision layer classifies transactions as legitimate or fraudulent and triggers alerts. The response layer integrates with banking systems to block or flag suspicious transactions immediately Model performance is evaluated using multiple metrics. Accuracy measures overall correctness, but is not sufficient due to class imbalance. Precision measures correctness of fraud predictions. Recall measures ability to detect actual fraud cases and is highly prioritized. F1-score balances precision and recall. ROC-AUC evaluates classification threshold performance. Latency and throughput metrics measure real-time system efficiency. Optimization is performed to improve model efficiency and scalability. Hyperparameter tuning is conducted using Bayesian optimization. Feature selection techniques reduce dimensionality and improve processing speed. Dimensionality reduction methods such as PCA are applied where necessary. Deep learning models are optimized using dropout layers, batch normalization, and learning rate scheduling. The trained models are deployed in a simulated real-time environment using streaming data pipelines. Transaction data is continuously fed into the system, and predictions are generated in milliseconds. System performance is evaluated under varying loads to ensure scalability. Model drift is monitored, and periodic retraining is implemented to maintain accuracy over time.

The methodology ensures strict compliance with financial data protection standards. Data anonymization techniques are applied to protect user identity. Encryption is used during data transmission and storage. Explainable AI techniques such as SHAP are integrated to provide transparency in decision-making. Ethical considerations include minimizing bias in fraud detection models and ensuring fairness across different user groups.

IV. RESULTS AND DISCUSSION

Artificial intelligence models have demonstrated significant improvements in detecting fraudulent financial transactions in real-time environments compared to traditional rule-based systems.Machine learning algorithms such as Logistic Regression, Random Forest, Gradient Boosting Machines, and Support Vector Machines show strong baseline performance in structured financial datasets.Deep learning models, particularly Artificial Neural Networks (ANNs) and Long Short-Term Memory (LSTM) networks, further improve detection accuracy by capturing hidden temporal patterns in transaction sequences.In experimental evaluations, ensemble methods consistently achieve higher precision and recall due to their ability to reduce variance and bias simultaneously.For highly imbalanced datasets, which are common in fraud detection, models integrated with SMOTE (Synthetic Minority Oversampling Technique) or anomaly detection techniques show improved sensitivity toward minority fraud cases.Real-time analytics systems powered by streaming frameworks like Apache Kafka and Spark Streaming demonstrate low-latency detection capabilities, often within milliseconds to seconds of transaction initiation.The results also indicate that feature engineering, including behavioral patterns, geolocation variance, and transaction velocity, significantly enhances model performance.Hybrid models combining rule-based filters with machine learning classifiers outperform standalone AI systems in reducing false positives.Evaluation metrics such as AUC-ROC, F1-score, and precision-recall curves confirm that deep learning-based fraud detection systems achieve superior robustness under dynamic financial conditions.Overall, AI-driven fraud detection systems provide a scalable and adaptive solution for modern financial ecosystems.

Despite high performance, AI-based fraud detection systems face challenges related to interpretability and computational efficiency in large-scale deployment environments. Black-box models such as deep neural networks provide high accuracy but lack transparency, making regulatory compliance in financial institutions difficult.Explainable AI (XAI) techniques like SHAP (SHapley Additive exPlanations) and LIME help address this limitation by providing interpretability to model predictions.

Latency analysis shows that while batch-based models are efficient for offline detection, streaming architectures are essential for real-time fraud prevention.Data imbalance remains a critical issue, as fraudulent transactions often constitute less than 1% of total transactions, leading to biased model training if not handled properly.Adaptive learning systems that continuously retrain on new transaction data show improved resilience against evolving fraud patterns and adversarial attacks. System scalability tests indicate that cloud-based deployments offer better performance in handling millions of transactions per second compared to on-premise systems.False positive rates remain a concern as excessive alerts can reduce customer satisfaction and increase operational costs for financial institutions.Integration of multi-layered security frameworks combining biometric authentication and behavioral analytics enhances system reliability.Thus, while AI significantly improves fraud detection, balancing accuracy, interpretability, and operational efficiency remains a key research challenge.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

V. CONCLUSION

In modern wireless communication systems, the physical layer is responsible for fundamental tasks such as modulation, coding, channel estimation, synchronization, and signal detection. These processes are traditionally designed using theoretical models based on assumptions about channel behavior. However, real-world wireless channels exhibit unpredictable variations due to multipath propagation, mobility, interference, and hardware impairments, making classical models insufficient in many cases.One of the major limitations in applying deep learning to wireless physical layer tasks is the scarcity of large-scale labeled datasets. Collecting real wireless data requires expensive hardware such as software-defined radios and spectrum analyzers, as well as controlled experimental setups. Additionally, labeling signal data is often difficult because it requires precise knowledge of transmitted symbols and channel conditions, which may not always be available.Another challenge is the imbalance and lack of diversity in available datasets. Wireless datasets often contain an uneven distribution of signal-to-noise ratio (SNR) conditions, modulation schemes, and channel environments. As a result, deep learning models trained on such datasets tend to perform well only under dominant conditions while failing in rare or extreme scenarios such as low SNR or deep fading environments.

Data augmentation techniques have traditionally been used to address dataset limitations in wireless systems. These include adding artificial noise, applying time shifting, frequency shifting, phase rotation, and simulating channel effects using mathematical models. While these methods improve dataset diversity to some extent, they are fundamentally limited because they rely on predefined transformations and cannot fully capture the complexity of real wireless environments.Generative Adversarial Networks (GANs) provide a more advanced and flexible solution for data augmentation by learning the underlying distribution of real wireless signals. A GAN consists of two neural networks: a Generator, which creates synthetic signal samples from random noise, and a Discriminator, which attempts to distinguish between real and synthetic samples. Through adversarial training, the Generator learns to produce increasingly realistic wireless signal representations.In the context of wireless communication, GANs are particularly useful for generating in-phase and quadrature (IQ) signal samples that reflect realistic channel impairments such as fading, Doppler shifts, phase noise, and additive white Gaussian noise. These synthetic signals can closely mimic real-world conditions, thereby expanding the diversity and richness of training datasets.
The training process of GANs involves a minimax optimization problem in which the Generator tries to minimize the ability of the Discriminator to identify fake samples, while the Discriminator tries to maximize its classification accuracy. This iterative process continues until the generated data distribution closely approximates the real data distribution, resulting in highly realistic synthetic samples.

In wireless physical layer applications, GAN-based augmentation significantly improves the performance of deep learning models in tasks such as modulation classification, spectrum sensing, signal detection, and channel estimation. By providing additional training samples under diverse channel conditions, GANs enhance model generalization and robustness in practical deployment scenarios.

Overall, GAN-based data augmentation represents a shift from traditional model-driven wireless system design toward a data-driven paradigm. This approach reduces dependency on analytical channel models and enables wireless systems to adapt more effectively to complex, dynamic, and real-world environments.

VI. FUTURE WORK

Future research in artificial intelligence-based financial fraud detection systems will focus heavily on improving model adaptability, interpretability, and real-time responsiveness in increasingly complex financial ecosystems. One of the primary directions involves the development of capable of continuously updating themselves in response to evolving fraud strategies without requiring frequent manual retraining. Current models often suffer from concept drift, where the statistical properties of transaction data change over time, reducing model effectiveness. Future systems must incorporate online learning techniques and reinforcement learning frameworks that allow models to evolve dynamically as new fraud patterns emerge.

Another important area of future work is the integration of into high-performance fraud detection models. While deep learning models such as neural networks and transformers offer high accuracy, their lack of transparency limits adoption in regulated financial sectors. Future systems should prioritize hybrid architectures that combine deep learning with interpretable models or built-in explanation layers. Techniques such as attention mechanisms, SHAP, LIME, and

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

counterfactual explanations can be further enhanced to provide real-time interpretability without compromising accuracy.

Additionally, are expected to play a significant role in future fraud detection systems. Fraudulent transactions often involve networks of connected accounts, devices, and identities. Graph Neural Networks (GNNs) can capture these relationships more effectively than traditional tabular models. Future research should explore scalable graph-based fraud detection systems that can process large-scale financial networks in real time while identifying hidden fraud rings and coordinated attack patterns.Another promising direction is the integration of for privacy-preserving fraud detection. Financial institutions are often reluctant to share sensitive transaction data due to privacy regulations and competitive concerns. Federated learning enables collaborative model training across multiple institutions without sharing raw data. Future systems should focus on improving communication efficiency, security against model poisoning attacks, and maintaining high model accuracy in federated environments.

The use of is also an important future direction. Fraud detection systems currently rely heavily on structured transaction data, but future systems can incorporate unstructured data such as customer behavior logs, device metadata, biometric signals, and even textual data from customer interactions. Combining these diverse data sources using multimodal deep learning architectures can significantly improve detection accuracy and reduce false positives.

Scalability remains another critical area of improvement. As digital transactions continue to grow exponentially, future systems must be capable of processing millions of transactions per second with minimal latency. This will require optimization of distributed computing frameworks, edge computing integration, and GPU/TPU acceleration for real-time inference. Cloud-native architectures combined with microservices will also play an important role in ensuring system flexibility and scalability.Furthermore, will become increasingly important. Fraudsters may attempt to manipulate AI models through adversarial inputs designed to evade detection. Future research should focus on building robust models that can withstand adversarial attacks using techniques such as adversarial training, anomaly-resistant architectures, and uncertainty estimation.Finally, ethical considerations and regulatory compliance will shape the future development of AI-based fraud detection systems. Ensuring fairness, reducing bias, and maintaining transparency in decision-making processes will be essential for widespread adoption. Researchers must also explore frameworks for accountability in automated financial decision systems. The combination of technical innovation, regulatory alignment, and ethical AI design will define the next generation of fraud detection technologies.

REFERENCES

1. Aldweesh, A., Derhab, A., & Zargari, S. (2019). Cybercrime fraud detection using machine learning techniques. *Journal of Information Security and Applications, 46*, 108–121.
2. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *International Conference on Computing Networking and Informatics*, 1–9.
3. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613.
4. Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences, 557*, 317–331.
5. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems, 29*(8), 3784–3797.
6. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455.
7. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234–245.
8. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119*.
9. Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. *Expert Systems with Applications, 38*(10), 13003–13009.
10. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–66.
11. Mathew, A., & Nair, A., & Decouth, J. R. (2019). Audience Behaviour Mining Using Data Analysis. International Journal of Data Structures, 5(2), 1-7.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 3, May- June 2022|

DOI:10.15680/IRJIE.2022.0603001

12. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
13. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).
14. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
15. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
16. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
17. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
18. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
19. Sugumar, R. (2018). Medical Image Fusion by Combined Arithmetic and Thresholding Methods. EDITORS OF SPECIAL ISSUE JOURNAL, 17.
20. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
21. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
22. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
23. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
24. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
25. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
26. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
27. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
28. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
29. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
30. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
31. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
32. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. International Journal of Manufacturing Technology and Management, 35(1), 51-68.
33. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
34. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.
35. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
36. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
37. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
38. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. Biomedical Signal Processing and Control, 70, 103034