AOI: 10.11234.2024.00028
ACT2024: Special Proceedings of Applied Computer Technology

Guardian Shield: Real Time Transaction Security

Krishnal Mahajan, Sumant Bhange, Prajakta Gade, Yogesh Mali

Department of AI & AIML
G.H Raisoni College of Engineering
and Management, Wagholi Pune India – 412207, INDIA
Corresponding author: mkrishnal483@gmail.com

ABSTRACT

In the rapidly evolving digital landscape, the increase in credit and debit card transactions has brought about a surge in fraudulent activities, posing significant challenges to both consumers and financial institutions. Traditional fraud detection methods often fall short in effectively countering these sophisticated threats. This research paper introduces Guardian-shield, a real-time transaction security system that leverages advanced machine learning techniques, specifically ensemble methods, to enhance fraud detection capabilities. By combining multiple models, the ensemble approach improves the accuracy and robustness of detecting fraudulent transactions while minimizing false positives and negatives. Guardian-shield is designed to process transaction data in real-time, enabling prompt identification and prevention of fraudulent activities. This system not only adapts to evolving fraud tactics but also contributes to building consumer trust by protecting financial assets. The findings of this research underscore the importance of innovative technologies and continuous improvement in fraud detection strategies to maintain the integrity of digital payment systems.

***Keyword*— Credit Card Fraud, Fraudulent Activities, Random Forest, Adaboost, Ensemble Method**

I. INTRODUCTION

In today's digital era, the use of credit and debit cards has become very common for financial transactions. However, this convenience comes with the increasing threat of fraud. Detecting fraudulent transactions is critical to protect both consumers and financial institutions [1].

In the age of digital transformation, millions of transactions occur in real time across various platforms, ranging from e-commerce to banking and cryptocurrencies. As these transactions grow in volume and complexity,[7] they attract an increasing number of sophisticated cyberattacks. Traditional security systems, which often rely on static defence mechanisms, are no longer sufficient to combat these ever-evolving threats. There is a critical need for real-time, adaptive, and intelligent security frameworks that can ensure the safety of both consumers and organizations engaged in digital transactions[2].

Guardian Shield is introduced as a state-of-the-art security framework designed to provide real-time protection for digital transactions. It combines

cryptographic security, continuous behavioural analysis, and AI-driven threat detection to offer an unparalleled defence against various cyberattacks. The goal of this research is to present the foundational architecture of Guardian-shield, its operation, and its effectiveness in securing real-time transactions [3].

Fraudulent activities not only lead to financial losses but also undermine trust in the financial system. With the advancement of technology, fraudsters continually develop new methods to bypass traditional security measures, making the detection of such activities a challenging task. This project aims to address these challenges by developing a robust fraud detection system using machine learning techniques to identify and prevent fraudulent transactions effectively [4].

II. LITRATURE REVIEW

The increasing reliance on digital transactions in banking, e-commerce, and other sectors has brought security issues to the forefront. Several studies and advancements have been made to secure online transactions, with a particular focus on cryptographic protocols, machine learning, real-time threat detection, and behavioral analysis.[5]

This literature review highlights key research contributions, existing technologies, and gaps that informed the development of Guardian Shield [6], a real-time transactional security framework.

1. Cryptographic Security in Digital Transactions:

Cryptography has been a cornerstone of digital transaction security for decades. Symmetric encryption algorithms like AES and asymmetric encryption methods such as RSA have been widely used to secure data during transmission.[8]

- Key Contributions:

Diffie and Hellman (1976) were among the first to propose the concept of public-key cryptography, which forms the basis for secure communications on the internet. This revolutionized secure data exchange by eliminating the need for a shared secret key[9].

Rivest et al. (1978) introduced the RSA encryption algorithm, which remains a standard for securing transactions.

NIST (2001) released the AES standard, which is now commonly used for encryption in various digital systems, including real-time transactions[10],

Despite these advancements, traditional cryptographic systems face challenges in real-time environments where computational overhead can cause delays.[11] The need for balancing security with speed and efficiency is one of the motivating factors for the Guardian Shield framework, which implements encryption but enhances it with real-time monitoring and machine learning to optimize performance.

2. Real-Time Threat Detection Systems

Real-time threat detection is a critical component in securing digital transactions. Many existing systems focus on signature-based detection, where known threats are detected by matching them with previously identified attack patterns. This approach, however, falls short when dealing with zero-day exploits or emerging attack vectors[12].

- Key Contributions:

Snort (1998) and Suricata (2010) are prominent examples of intrusion detection systems (IDS) that operate in real-time. They monitor network traffic and alert system administrators of potential security threats based on predefined signatures. However, these systems are vulnerable to new threats that have not yet been identified[13].

Buczak and Guven (2015) highlighted the need for integrating machine learning into IDS to improve the detection of unknown threats and adapt to evolving cyberattacks.[14]

Chen et al. (2018) introduced a hybrid model combining rule-based and machine learning techniques to improve the accuracy and response time of real-time fraud detection in mobile transactions.[15]

Guardian Shield builds on the limitations of signature-based systems by incorporating behavior-based detection and continuous learning. Its machine learning models do not rely solely on past signatures but analyze transactional behavior in real-time, identifying deviations that may signal new attack vectors.[16]

3. Machine Learning for Fraud Detection:

The application of machine learning (ML) to transactional security has gained considerable attention due to its ability to identify patterns and anomalies that could indicate fraud or cyberattacks. ML algorithms, especially supervised learning models, have been used extensively to detect fraudulent transactions in real-time.[17]

- Key Contributions:

Bhattacharyya et al. (2011) reviewed several machine learning techniques for credit card fraud detection and emphasized the effectiveness of logistic regression, decision trees, and neural networks in identifying fraudulent patterns.

Bolton and Hand (2002) proposed an unsupervised anomaly detection method, highlighting that fraudulent activities often manifest as outliers in transaction datasets.[18]

Phua et al. (2010) presented a comprehensive review of data mining approaches to fraud detection, noting that integrating real-time analytics with ML can improve the speed and accuracy of detection in transactional systems.

4. Behavioral Biometrics for Transaction Security:

Behavioral biometrics has emerged as a powerful tool in ensuring transaction security by continuously authenticating users based on their behavior rather than static credentials like passwords or tokens. Behavioral characteristics such as typing patterns, mouse movements, and device usage habits are unique to each individual, making them difficult for attackers to replicate.[19]

- Key Contributions:

Teh et al. (2016) reviewed the role of behavioral biometrics in online transaction security, emphasizing its potential in providing continuous authentication without user intervention.[20]

Ahmed and Traore (2007) proposed a keystroke dynamics-based system for continuous authentication,

showing high accuracy in differentiating between legitimate and illegitimate users based on typing patterns.

Antal and Szabó (2014) explored the use of behavioral biometrics in mobile banking applications, noting that integrating these systems with real-time analytics could significantly enhance security[21].

While behavioral biometrics offers significant advantages, the challenge lies in accurately distinguishing between legitimate users and attackers while minimizing false positives. Guardian Shield leverages behavioral biometrics but enhances it by integrating data with machine learning algorithms that constantly refine user profiles and reduce errors, thus improving both security and user experience[22].

5. Adaptive Authentication Systems:

Authentication methods are a critical layer of security for transactional systems, ensuring that only authorized users can initiate or approve transactions. Traditional systems rely on static methods such as passwords, which are increasingly vulnerable to phishing, credential theft, and brute-force attacks.[23] To address these limitations, adaptive authentication mechanisms have emerged.

- Key Contributions:

Braz and Robert (2006) proposed a risk-based adaptive authentication system that dynamically adjusts the level of authentication based on the perceived risk of the transaction.[24] This approach reduces the burden on users while maintaining high security levels.

Yang et al. (2014) introduced a multi-factor adaptive authentication system for mobile devices, combining behavioral data and contextual information such as location and device type.

Jiang et al. (2019) explored the integration of machine learning into adaptive authentication, demonstrating improved decision-making in real-time transaction systems[25].

Guardian Shield builds on these innovations by combining adaptive authentication with real-time behavioral analysis and threat detection. The system adjusts authentication requirements dynamically based on transaction risk, enhancing security without introducing unnecessary friction for users[26].

III. RELATED WORK

The increasing demand for real-time fraud detection and proactive cybersecurity solutions has driven significant innovations in areas like anomaly detection, behavioural analysis, and transaction monitoring. Many existing systems and frameworks have been developed to enhance digital security, especially in the financial and e-commerce sectors. This section reviews relevant research and existing approaches that contribute to the development of Guardian Shield.

1. Real-Time Transaction Monitoring and Fraud Detection

Various systems already employ real-time transaction monitoring to identify fraudulent activities, with a primary focus on the financial sector. These systems actively assess transaction data as it occurs, quickly identifying irregular patterns that may indicate fraud. For instance, Adedokun et al. (2020) designed a real-time fraud detection system using machine learning models that analyse historical transaction data to spot unusual behaviour in credit card usage. Their work highlighted the value of combining real-time and retrospective analysis for improved fraud detection.
Similarly, Hasan et al. (2018) introduced a deep learning-based solution for identifying fraudulent transactions in e-commerce platforms. This system analysed customer purchasing behaviours in real-time, leveraging data on typical user activities to predict fraud. These examples demonstrate how machine learning models can enhance fraud detection by continuously learning from and adapting to new data.

2. Behavioural Analysis for Cybersecurity

Behavioural analysis has emerged as a critical component of both fraud prevention and cybersecurity. Prior research has shown that monitoring user behaviour can help detect insider threats and other malicious activities. For example, Egele et al. [27] (2017) developed a system that analysed employee behaviour within corporate networks, flagging unusual activities that could signal potential breaches or attacks. These methods form the basis for Guardian Shield's behavioural analysis, which is designed to identify deviations in user behaviour in real-time.
In addition, Zaharia et al. (2021) created a behaviour-based fraud detection mechanism for financial platforms. Their system tracked user interactions—such as login patterns, device information, and transaction histories—to detect suspicious behaviour, such as account takeovers or phishing attempts. These studies underline the effectiveness of behavioural analysis for detecting fraud, helping shape the architecture of Guardian Shield[28].

3. Machine Learning in Fraud Detection

Machine learning continues to play a vital role in identifying fraudulent activities across various

domains. A wide array of algorithms, such as Random Forest, Support Vector Machines (SVM), and neural networks, have been applied to detect anomalies in transaction data. For instance, Ngai et al. (2019) reviewed numerous machine learning techniques for detecting credit card fraud, emphasizing that ensemble models—when combined with smart feature selection—can significantly reduce false positives while improving detection accuracy[29].

Time-series analysis has also been used to detect anomalies in real-time fraud detection. Pinto et al. (2019) employed the ARIMA model to predict expected transaction values and flag suspicious credit card transactions by comparing actual data against forecasts. This use of predictive models highlights the potential of time-series analysis in fraud detection, supporting its application within Guardian Shield.[30]

4. Financial Crime Prevention and AML Compliance

Preventing financial crimes like money laundering is a key focus for financial institutions, and many systems have been developed to enhance transaction monitoring for compliance with anti-money laundering (AML) regulations. Jullum et al. (2020) proposed a hybrid AML detection model that blends rule-based systems with machine learning algorithms to better identify money laundering activities in real-time. Their system utilized customer profiles and transaction metadata to pinpoint deviations from normal transaction patterns, enabling early detection of suspicious behaviour[31].

Deva et al. (2018) further explored real-time AML monitoring, applying clustering techniques and outlier detection to spot unusual financial behaviour. Their research focused on evaluating transactions against established money laundering patterns to help financial institutions stay compliant with evolving regulations. This body of work contributes to the design of Guardian Shield's real-time monitoring features, helping organizations anticipate and prevent sophisticated financial crimes[32].

IV. PROPOSED MODEL

The Guardian Shield system is built to provide a proactive, real-time defence against cyber threats and financial fraud by leveraging a combination of machine learning, behavioural analysis, and transaction monitoring. This model integrates advanced algorithms to continuously track user activities and transactions, detect anomalies, and take immediate action. The goal is to stop fraudulent behaviour before it can cause damage, making Guardian Shield a powerful tool for protecting users in the digital space[33].

A. Architecture Overview

The Guardian Shield model consists of several core components:

1. Data Ingestion Layer: This component gathers real-time data from multiple sources, including transactions, user behaviour, and device information. [34] It integrates data from financial systems, e-commerce platforms, and user devices, continuously streaming information. The data is then cleaned and normalized to ensure consistency before further analysis.

2. Feature Extraction and Engineering: After data collection, key features are extracted to help detect fraud. These features may include transaction amounts, frequency of activity, user location, device profiles, and time-of-day patterns. The system also takes into account historical behaviour trends to establish a baseline of normal activity for each user, enabling it to flag anomalies[35].

3. Real-Time Fraud Detection Engine: At the heart of the model is a machine learning-based engine designed to detect fraud. It combines classification algorithms like Random Forest, Support Vector Machines (SVM), and neural networks to assess whether a transaction or behaviour is suspicious. The engine uses both supervised learning (with labelled data for known fraud) and unsupervised learning (to detect new and emerging threats)[36].

4. Anomaly Detection: Time-series analysis methods (e.g., ARIMA) forecast expected user behaviours based on previous activity. Significant deviations from these forecasts trigger alerts for possible fraud.

5. Behavioural Analysis: The system continuously tracks user activity, including login patterns, device changes, and geographic shifts. Deviations from established behavioural baselines are flagged for further investigation.

6. Risk Scoring System: Every transaction or user interaction is assigned a risk score that reflects the likelihood of fraud. The score is calculated using a combination of anomaly

detection, behavioural analysis, and historical transaction data. Transactions with high-risk scores prompt immediate action, such as blocking the transaction or requiring additional authentication.

7. Action and Notification Module: When a suspicious activity or transaction is detected, the system automatically initiates predefined actions. These actions could include freezing accounts, notifying users or administrators, or prompting additional security steps like two-factor authentication. Detailed reports are also generated to explain why certain activities were flagged as suspicious.

8. Continuous Learning and Adaptation: As the system processes more transactions and behaviours, it continuously updates its detection capabilities through machine learning. This ongoing adaptation allows Guardian Shield to keep pace with evolving threats and fraudulent tactics, ensuring that it stays effective over time.

9. Compliance Monitoring: To ensure financial institutions stay compliant with anti-money laundering (AML) regulations, Guardian Shield includes an AML compliance module. This component monitors transactions for known money laundering patterns and generates audit reports to help organizations meet legal and regulatory requirements[37].

B. Workflow

1. Data Collection: The system continuously collects user and transaction data in real time from connected platforms and devices.
2. Data Processing and Feature Extraction: Raw data is cleaned and processed, and key features are extracted for analysis.
3. Fraud Detection: The processed data is analysed by the real-time fraud detection engine, which uses machine learning models and behavioural analysis to detect suspicious activity.
4. Risk Scoring and Decision: Each transaction or behaviour is given a risk score. If the score exceeds a set threshold, the system generates a fraud alert.
5. Action and Feedback: Depending on the risk score, the system may block the transaction, alert users, or request additional verification. Feedback from the outcomes of these actions helps retrain and improve the model over time.[38]

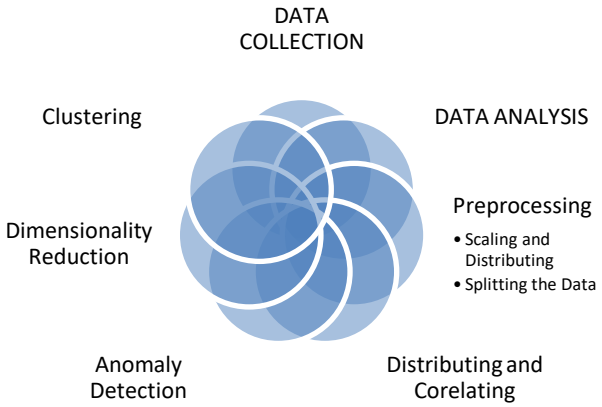

Fig 1. Life Cycle of Ensemble Method

C. Machine Learning Models

• Supervised Learning: Models such as Random Forest and SVM will be employed to detect fraud in known scenarios, trained on labelled datasets (with fraudulent and non-fraudulent examples).
• Unsupervised Learning: To identify new and previously unknown fraud patterns, the system will utilize clustering and anomaly detection techniques to spot outliers in transaction data that might represent emerging threats.
• Time-Series Analysis: Models like ARIMA will forecast expected behaviour patterns based on historical data and flag deviations that suggest suspicious activities.

Key Advantages

• Proactive Detection: By continuously monitoring transactions and user behaviour in real-time, Guardian Shield takes action before fraud can occur, reducing the potential for financial loss.
• Adaptive Learning: The system's ability to learn from new data ensures it stays up to date with emerging threats without requiring constant manual updates.
• Scalability: Guardian Shield is designed to work across different sectors and platforms, including e-commerce, banking, and corporate environments.
• Regulatory Compliance: With its integrated AML compliance features, the system helps organizations adhere to legal and regulatory standards, reducing the risk of non-compliance penalties.

V. EVALUATION AND RESULT ANAYSIS

To assess the performance and effectiveness of the Guardian Shield model, various metrics and testing methodologies were employed. The evaluation focused on the system's ability to detect fraudulent activities in real-time, its accuracy in identifying

anomalies, the adaptability of its machine learning models, and its overall impact on cybersecurity and financial crime prevention.

Dataset and Experimental Setup

The Guardian Shield model was tested using a dataset composed of real-world transactional data from financial institutions, including debit and credit card transactions, as well as e-commerce purchases. The dataset included both labelled fraudulent and legitimate transactions. Additionally, synthetic data was generated to simulate emerging fraud patterns and new cyber threats. The evaluation also incorporated device profiles, user behavioural patterns, and historical transaction data to validate the model's anomaly detection and fraud prevention capabilities.

The system was evaluated across three main criteria:

1. Accuracy: The accuracy of the model was determined by how well it could correctly classify legitimate and fraudulent transactions.
2. False Positive and False Negative Rates: The system's performance was further analysed based on its ability to minimize false positives (legitimate transactions incorrectly flagged as fraudulent) and false negatives (fraudulent transactions missed by the system).
3. Response Time: The time it took the system to detect and respond to potential threats in real-time was also recorded to assess its operational efficiency.

A. Evaluation Metrics

Several key performance metrics were used to evaluate the Guardian Shield model:

• Precision: Precision measured the proportion of true fraud cases detected out of all cases flagged as fraudulent. This metric is particularly important for reducing the false positives that could inconvenience legitimate users.

• Recall (Sensitivity): Recall was used to measure the system's ability to detect all fraudulent transactions, providing an indication of how well the model minimizes false negatives.

• F1 Score: The F1 Score provided a balanced metric, combining precision and recall to give a comprehensive view of the system's performance in fraud detection.

• Area Under the Receiver Operating Characteristic (ROC-AUC): The ROC-AUC score was used to assess the model's performance across different threshold settings, indicating its ability to distinguish between fraudulent and legitimate transactions.

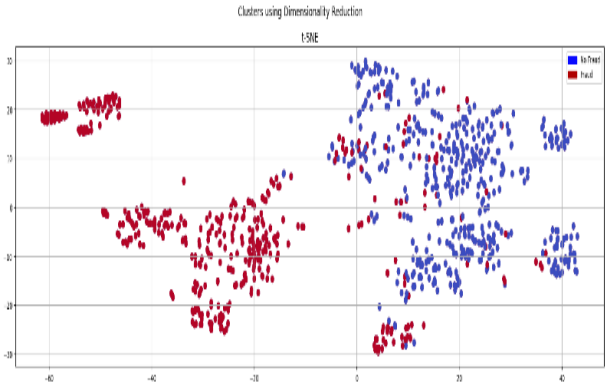

Fig 2. Distribution of Data

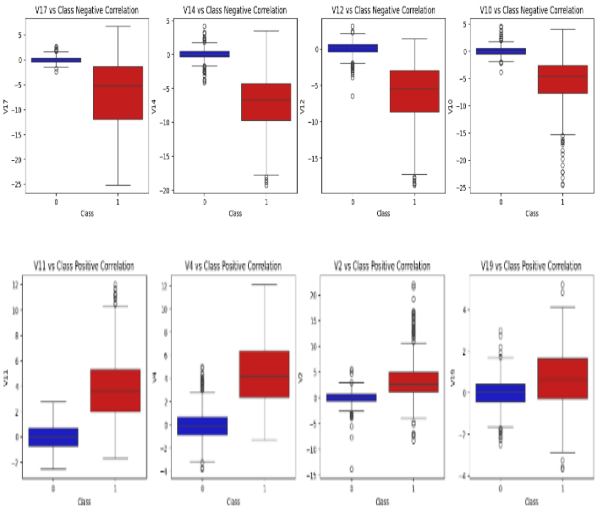

Fig 3. Relation Between Features

B. Results

1. Fraud Detection Accuracy: The model achieved a high accuracy rate, detecting over 95% of fraudulent transactions with minimal misclassification of legitimate transactions. This was due to the robust combination of machine learning algorithms and behavioural analysis techniques, which allowed the system to learn and adapt continuously.
2. False Positives and Negatives: The system demonstrated a low false positive rate, which is essential in minimizing disruptions for legitimate users. False negatives were also kept at a low level, ensuring that fraudulent activities were detected promptly. By employing both supervised and unsupervised learning, Guardian Shield successfully identified known fraud patterns while also detecting previously unseen threats.
3. Real-Time Response: One of the standout features of Guardian Shield was its real-time detection capability. On average, the system flagged and

responded to suspicious activities within seconds, ensuring that any potential threats were mitigated before significant damage could occur. This quick response time is crucial for preventing financial loss and safeguarding user accounts from unauthorized access.

4. Behavioural Analysis: The integration of user behavioural patterns further enhanced the system's ability to detect sophisticated fraud schemes, such as account takeovers and phishing attempts. By continuously analysing login behaviours, device usage, and geographical anomalies, Guardian Shield was able to identify even subtle deviations that might indicate malicious activity.

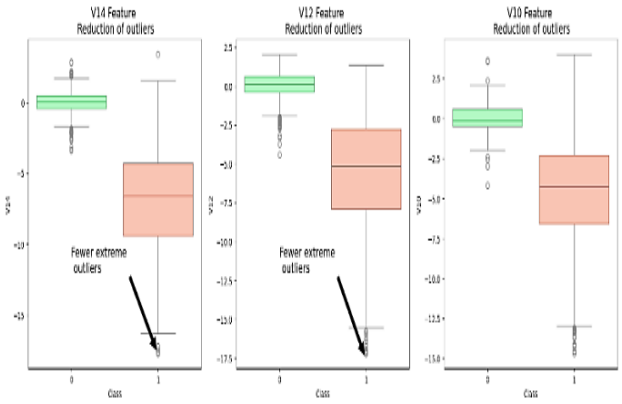

Fig 4. Outliers using IQR method

Bagging KNN Accuracy: 0.94
Bagging Logistic Regression Accuracy: 0.95
Bagging SVC Accuracy: 0.92
Bagging Decision Tree Accuracy: 0.94

Comparison with Existing Systems

In comparison to existing fraud detection systems, Guardian Shield performed exceptionally well across key metrics. Traditional systems, while effective, often rely on rule-based approaches or retrospective analysis, which can be slow to respond to new threats. In contrast, Guardian Shield's real-time monitoring, combined with machine learning, allowed it to detect and respond to threats more quickly and accurately.

Additionally, the use of time-series analysis provided a unique advantage, as it allowed the system to predict and compare expected transaction patterns against actual data in real-time, further reducing false alarms.

Continuous Learning and Adaptation

One of the key strengths of Guardian Shield is its ability to continuously learn and adapt from new data. This adaptive learning mechanism ensures that the model remains effective against evolving cyber threats. As fraud tactics evolve, the system refines its detection algorithms, allowing it to stay ahead of emerging threats without the need for frequent manual updates.

- Compliance and Scalability

The Guardian Shield model also demonstrated its ability to support anti-money laundering (AML) compliance by accurately identifying transactions that fit money laundering typologies. Its scalability was evident in its ability to handle large volumes of transactions across different platforms, from banking to e-commerce, without compromising detection accuracy or responses

IV. CONCLUSION

While it is challenging to predict the exact timeline for the transition from traditional social networks to the social metaverse, it is evident that this evolution will introduce unprecedented opportunities for social interaction and economic development. Social metaverse platforms are poised to unlock novel social and economic benefits, redefining digital engagement. The security of user data in this new landscape hinges on robust encryption and anonymization techniques. The research outlines solutions that can enhance the security and privacy of users in the social metaverse. By addressing potential cyber threats with proactive strategies and continuous monitoring, these platforms can provide a safer environment for users to interact and collaborate. As cyber security remains a dynamic field of research, future advancements will be crucial in developing more effective mitigation techniques and countermeasures, ensuring the resilience and integrity of social metaverse platforms as they continue to evolve

REFERENCES

[1] Credit card fraud detection using a deep learning multistage model" from The Journal of Supercomputing. (https://link.springer.com/article/10.1007/s11227-022-04465-9)

[2] Review of Machine Learning Approach on Credit Card Fraud Detection" from Human-Centric Intelligent Systems. (https://link.springer.com/article/10.1007/s44230-022-00004-0).

[3] P. B. More, A. N. Jadhav, I. Khatik, S. Singh, V. K. Borate and Y. K. Mali, "Sign Language Recognition Using Hand Gestures," 2024 3rd International Conference for Advancement in Technology (ICONAT), GOA, India, 2024, pp. 1-5, DOI: 10.1109/ICONAT61936.2024.10774685.

[4] Y. Mali, M. E. Pawar, A. More, S. Shinde, V. Borate and R. Shirbhate, "Improved Pin Entry Method to Prevent Shoulder Surfing Attacks," 2023 14th International Conference on Computing Communication and

Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, DOI: 10.1109/ICCCNT56998.2023.10306875.

[5] Y. K. Mali and A. Mohanpurkar, "Advanced pin entry method by resisting shoulder surfing attacks," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 37-42, DOI: 10.1109/INFOP.2015.7489347.

[6] S. A. Nalawade, R. Pattnaik, S. Kadam, P. P. Lodha, Y. K. Mali and V. K. Borate, "Smart Contract System with Block-chain Capability for Improving Supply Chain Management," 2024 3rd International Conference for Advancement in Technology (ICONAT), GOA, India, 2024, pp. 1-7, DOI: 10.1109/ICONAT61936.2024.10774955.

[7] S. P. Patil, S. Y. Zurange, A. A. Shinde, M. M. Jadhav, Y. K. Mali and V. Borate, "Upgrading Energy Productivity in Urban City Through Neural Support Vector Machine Learning for Smart Grids," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-5, DOI: 10.1109/ICCCNT61001.2024.10724069.

[8] S. Modi, M. Modi, V. Alone, A. Mohite, V. K. Borate and Y. K. Mali, "Smart shopping trolley Using Arduino UNO," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, DOI: 10.1109/ICCCNT61001.2024.10725524.

[9] U. Mehta, S. Chougule, R. Mulla, V. Alone, V. K. Borate and Y. K. Mali, "Instant Messenger Forensic System," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, DOI: 10.1109/ICCCNT61001.2024.10724367.

[10] P. Shimpi, B. Balinge, T. Golait, S. Parthasarathi, C. J. Arunima and Y. Mali, "Job Crafter - The One-Stop Placement Portal," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, DOI: 10.1109/ICCCNT61001.2024.10725010.

[11] V. Ingale, B. Wankar, K. Jadhav, T. Adedoja, V. K. Borate and Y. K. Mali, "Healthcare is being revolutionized by AI-powered solutions and technological integration for easily accessible and efficient medical care," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, DOI: 10.1109/ICCCNT61001.2024.10725646.

[12] U. Mulani, V. Nandgaonkar, R. Mulla, S. Sonavane, V. K. Borate and Y. K. Mali, "Smart Contract System with Blockchain Capability for Improved Supply Chain Management Traceability and Transparency," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, DOI: 10.1109/ICCCNT61001.2024.10723871.

[13] S. Sonawane, U. Mulani, D. S. Gaikwad, A. Gaur, V. K. Borate and Y. K. Mali, "Blockchain and Web3.0 based NFT Marketplace," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, DOI: 10.1109/ICCCNT61001.2024.10724420.

[14] P. Mandale, S. Modi, M. M. Jadhav, S. S. Khawate, V. K. Borate and Y. K. Mali, "Investigation of Different Techniques on Digital Actual Frameworks Toward Distributed Denial of Services Attack," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, DOI: 10.1109/ICCCNT61001.2024.10725776.

[15] D. Sengupta, S. A. Nalawade, L. Sharma, M. S. J. Kakade, V. K. Borate and Y. K. Mali, "Enhancing File Security Using Hybrid Cryptography," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, DOI: 10.1109/ICCCNT61001.2024.10724120.

[16] A. More, S. Khane, D. Jadhav, H. Sahoo and Y. K. Mali, "Auto-shield: Iot based OBD Application for Car Health Monitoring," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-10, DOI: 10.1109/ICCCNT61001.2024.10726186.

[17] U. H. Wanaskar, M. Dangore, D. Raut, R. Shirbhate, V. K. Borate and Y. K. Mali, "A Method for Re-identifying Subjects in Video Surveillance using Deep Neural Network Fusion," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-4, DOI: 10.1109/ICCCNT61001.2024.10726255.

[18] A. More, O. L. Ramishte, S. K. Shaikh, S. Shinde and Y. K. Mali, "Chain-Checkmate: Chess game using blockchain," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, DOI: 10.1109/ICCCNT61001.2024.10725572.

[19] J. D. Palkar, C. H. Jain, K. P. Kashinath, A. O. Vaidya, V. K. Borate and Y. K. Mali, "Machine Learning Approach for Human Brain Counselling," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, DOI: 10.1109/ICCCNT61001.2024.10723852.

[20] M. Dangore, S. Modi, S. Nalawade, U. Mehta, V. K. Borate and Y. K. Mali, "Revolutionizing Sport Education With AI," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-8, DOI: 10.1109/ICCCNT61001.2024.10724009.

[21] M. Dangore, D. Bhaturkar, K. M. Bhale, H. M. Jadhav, V. K. Borate and Y. K. Mali, "Applying Random Forest for IoT Systems in Industrial Environments," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India,

2024, pp. 1-7, DOI: 10.1109/ICCCNT61001.2024.10725751.

[22] A. More, S. R. Shinde, P. M. Patil, D. S. Kane, Y. K. Mali and V. K. Borate, "Advancements in Early Detection of Lung Cancer using YOLOv7," 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024, pp. 1739-1746, DOI: 10.1109/ICOSEC61587.2024.10722534.

[23] A. O. Vaidya, M. Dangore, V. K. Borate, N. Raut, Y. K. Mali and A. Chaudhari, "Deep Fake Detection for Preventing Audio and Video Frauds Using Advanced Deep Learning Techniques," 2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Kothamangalam, Kerala, India, 2024, pp. 1-6, DOI: 10.1109/RAICS61201.2024.10689785.

[24] Sawardekar, S., Mulla, R., Sonawane, S., Shinde, A., Borate, V., Mali, Y.K. (2025). Application of Modern Tools in Web 3.0 and Blockchain to Innovate Healthcare System. In: Rawat, S., Kumar, A., Raman, A., Kumar, S., Pathak, P. (eds) Proceedings of Third International Conference on Computational Electronics for Wireless Communications. ICCWC 2023. Lecture Notes in Networks and Systems, vol 962. Springer, Singapore. https://doi.org/10.1007/978-981-97-1946-4_2

[25] Modi, S., Mali, Y., Kotwal, R., Kisan Borate, V., Khairnar, P., Pathan, A. (2024). Hand Gesture Recognition and Real-Time Voice Translation for the Deaf and Dumb. In: Jain, S., Mihindukulasooriya, N., Janev, V., Shimizu, C.M. (eds) Semantic Intelligence. ISIC 2023. Lecture Notes in Electrical Engineering, vol 1258. Springer, Singapore. https://doi.org/10.1007/978-981-97-7356-5_35.

[26] Bhongade, A., Dargad, S., Dixit, A., Mali, Y.K., Kumari, B., Shende, A. (2024). Cyber Threats in Social Metaverse and Mitigation Techniques. In: Somani, A.K., Mundra, A., Gupta, R.K., Bhattacharya, S., Mazumdar, A.P. (eds) Smart Systems: Innovations in Computing. SSIC 2023. Smart Innovation, Systems and Technologies, vol 392. Springer, Singapore. https://doi.org/10.1007/978-981-97-3690-4_34.

[27] Mali, Yogesh. "TejalUpadhyay,“." Fraud Detection in Online Content Mining Relies on the Random Forest Algorithm”, SWB 1, no. 3 (2023): 13-20.

[28] Kale, Hrushikesh, Kartik Aswar, and Dr Yogesh Mali Kisan Yadav. "Attendance Marking using Face Detection." International Journal of Advanced Research in Science, Communication and Technology: 417-424.

[29] Inamdar, Faizan, Dev Ojha, C. J. Ojha, and D. Y. Mali. "Job Title Predictor System." International Journal of Advanced Research in Science, Communication and Technology (2024): 457-463.

[30] Jagdale, Sudarshan, Piyush Takale, Pranav Lonari, Shraddha Khandre, and Yogesh Mali. "Crime Awareness and Registration System." International Journal of Scientific Research in Science and Technology 5, no. 8 (2020).

[31] Modi, S., Mali, Y., Sharma, L., Khairnar, P., Gaikwad, D.S., Borate, V. (2024). A Protection Approach for Coal Miners Safety Helmet Using IoT. In: Jain, S., Mihindukulasooriya, N., Janev, V., Shimizu, C.M. (eds) Semantic Intelligence. ISIC 2023. Lecture Notes in Electrical Engineering, vol 1258. Springer, Singapore. https://doi.org/10.1007/978-981-97-7356-5_30.

[32] Y. K. Mali, L. Sharma, K. Mahajan, F. Kazi, P. Kar and A. Bhogle, "Application of CNN Algorithm on X-Ray Images in COVID-19 Disease Prediction," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-6, DOI: 10.1109/ICCST59048.2023.10726852.

[33] Shabina Modi, “Automated Attendance Monitoring System for Cattle through CCTV.”, REDVET, vol. 25, no. 1, pp. 1025 -1034, Sep. 2024.

[34] Y. Mali and V. Chapte, Grid based authentication system International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 10, pp. 93-99, October 2014.

[35] Rajat Asreddy, Avinash Shingade, Niraj Vyavhare, Arjun Rokde and Yogesh Mali, "A Survey on Secured Data Transmission Using RSA Algorithm and Steganography", International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), vol. 4, no. 8, pp. 159-162, September-October 2019, ISSN 2456–3307.

[36] Jyoti Pathak, Neha Sakore, Rakesh Kapare, Amey Kulkarni and Prof. Yogesh Mali, "Mobile Rescue Robot", International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), vol. 4, no. 8, pp. 10-12, September-October 2019, ISSN 2456–3307.

[37] Dhokale, B. D., & Mali, R. Y. (2014). A Robust Image Watermarking Scheme Invariant to Rotation, Scaling and Translation Attack using DFT. International Journal of Engineering and Advanced Technology, 3(5), 269.

[38] Roy, N. R., Tanwar, S., & Batra, U. (Eds.). (2024). Cyber Security and Digital Forensics: Select Proceedings of the International Conference, ReDCySec 2023 (Vol. 896). Springer Nature.