International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI impact to Detect Fraud & Substance Abuse

[1]Praveen Kumar Rawat, [2]Amit Nandal

Submitted: 20/10/2023 **Revised**: 02/12/2023 **Accepted:** 12/12/2023

Abstract: Conventional techniques of inquiry and diagnosis have been transformed by the use of AI in fraud detection and drug usage monitoring. Artificial intelligence-powered systems utilise machine learning, natural language processing, and predictive analytics to identify patterns, anomalies, and hidden hints that could indicate drug addiction or fraud. By rapidly analysing large datasets, identifying anomalies in transactions, and detecting suspicious behaviour in real-time, artificial intelligence systems have the potential to significantly reduce human error and response time in the area of fraud detection. Because stopping fraudulent transactions may result in significant losses for clients and a general reduction in trust in these sectors, financial institutions, insurance firms, and online merchants significantly depend on these abilities. At the same time, artificial intelligence is transforming drug usage detection via advanced monitoring methods, digital phenotyping, and speech and facial expression recognition. Artificial intelligence (AI) systems that scan speech patterns, facial microexpressions, mobile usage behaviour, and biometric data for signs of psychological distress or relapse may be able to identify patients with a history of drug dependence early on. AI chatbots and virtual counsellors, which provide scalable, private, and rapid intervention channels, enable better access to mental health care while reducing stigma. AI's predictive capabilities may also be used by legislators and medical experts to anticipate drug abuse patterns, improve rehabilitation methods, and allocate resources efficiently. Doctors may more accurately assess patients' risk levels and develop individualised treatment plans by integrating AI models with EHRs. Despite AI's enormous potential, ethical issues including data privacy, algorithmic bias, and informed consent are brought up by its use in these delicate industries, necessitating strict regulatory frameworks and open algorithmic management. When it comes to increasing the scalability, accuracy, and speed of drug and fraud detection, artificial intelligence is ultimately revolutionary. When used responsibly and with the appropriate safeguards, AI technology has the potential to significantly improve public health outcomes, loss prevention, and early intervention.

Keywords: *Artificial Intelligence, Fraud Detection, Substance Abuse, Predictive Analytics, Behavioural Monitoring*

1. Introduction

Artificial Intelligence (AI), which enhances decision-making, accuracy, and productivity, has transformed several industries. In the domains of drug addiction monitoring and fraud detection, where it has found some of its most important applications, prompt identification, early intervention, and accurate prediction are crucial. Since drug abuse and fraud are complex societal issues, they have significant financial, psychological, and social implications. Traditional detection methods are often reactive, error-prone, and time-consuming, notwithstanding their effectiveness [1]. By analysing vast volumes of data and uncovering hidden patterns, artificial intelligence (AI) offers a proactive and scalable solution. This introduction examines the revolutionary potential of artificial intelligence (AI) in fraud detection and substance misuse intervention, with an emphasis on two key subtopics: (1) AI-Driven Fraud Detection

[1]*Master's in Computer Applications, PAHM, PSM, ISTQB, MCDBA*

Email: Praveen.rawat1@gmail.com

Independent Researcher, Virginia, US

[2]*MBA, Master's Computer Information Science, ITIL*

Email: nandalamit2@gmail.com

Independent Researcher, PA, US

Mechanisms and (2) AI Applications in Substance Misuse Monitoring and Prevention.

1.1 AI-Driven Fraud Detection Mechanisms

Every year, fraud costs businesses billions of dollars, particularly in sectors like banking, insurance, healthcare, and e-commerce. Traditional fraud detection systems are more likely to overlook more intricate and dynamic fraud strategies when they use rule-based models or human auditing processes. A powerful tool has been developed to address this issue with the introduction of AI-powered advanced analytics, anomaly detection, and pattern recognition [2]. From historical transaction data, machine learning algorithms may learn what is deemed normal and what is deemed suspicious. These models are always evolving and adapting to new trends in order to counter ever-evolving fraud schemes. For instance, AI can monitor real-time activities in the banking sector and highlight any anomalies, including questionable spending patterns, geographic inconsistencies, or attempted account takeovers [3]. In order to spot exaggerated claims, artificial intelligence models in the insurance sector may examine customer profiles and claim histories. Additionally, NLP may be used to analyse unstructured material, such as chat transcripts or emails, to look for signs of collaboration or dishonesty.

AI-powered fraud detection [4] significantly reduces false positives, expedites investigations, and increases operational effectiveness. However, it is crucial to ensure that algorithmic conclusions are transparent and equitable to prevent unintended biases.

1.2 AI Applications in Substance Abuse Monitoring and Prevention

Substance abuse continues to be a serious public health concern as it may result in criminal behaviour, decreased productivity, and mental health problems. Early detection and continuous monitoring are essential for the effectiveness of intervention and rehabilitation. In order to identify and reduce the dangers associated with drug addiction, new tools have been created using artificial intelligence (AI) to analyse data from a variety of sources, such as wearable technology, social media, mobile health applications, and electronic health records (EHRs). Artificial intelligence (AI) systems may look at behavioural, physiological, and psychological indicators to find the early warning signs of drug misuse. For example, in order to detect potential relapses, artificial intelligence systems may examine data points such as heart rate variability, physical activity, and sleep patterns gathered by wearable sensors. Digital phenotyping, or the study of digital behaviour [5], may provide further insight into a user's mental health (e.g., phone usage, typing patterns). Chatbots that utilise sentiment analysis and natural language processing may hold private conversations with people, recognise when they're depressed, and point them in the direction of support if necessary.

AI supports both individual-level therapies and public health policy by forecasting trends in drug addiction and evaluating the effectiveness of treatment programs. Notwithstanding the fascinating possibilities of these developments, ethical guidelines governing privacy, informed permission, and data protection are urgently needed [6]. Artificial intelligence leads the way in innovative approaches to controlling drug abuse and identifying fraud. It is crucial for evaluating big datasets, forecasting risk, and supporting decision-making in today's data-driven environment to handle these intricate challenges.

2.Related Work

AI has been widely used in the battle against drug abuse and fraud because of its ability to examine large information, uncover hidden patterns, and enable proactive decision-making. Machine learning (ML) and deep learning models have shown to be very effective in detecting fraudulent activities in a number of industries, including banking, insurance, and healthcare. Using historical transaction data, techniques such as Support Vector Machines, Random Forests, and Neural Networks were trained to identify anomalous behaviour. More recent developments have used anomaly detection and unsupervised learning to identify unidentified fraud tactics, even with imbalanced datasets. Experts in natural language processing (NLP) [7] have searched for indications of fraud in unstructured data, such as emails, chat logs, and claims narratives, using transformer-based models like GPT and BERT. Another area where NLP has been useful is in the analysis of content from online forums and support groups to identify behavioural indicators of drug use.

Artificial intelligence models have been used to analyse data gathered from wearables, telephones, and digital interactions to analyse behavioural and physiological signs to identify drug usage. The use of speech recognition, sentiment analysis, and digital phenotyping to find signs of mental discomfort or relapse has increased recently. Chatbots and virtual assistants may be used for early intervention, mood evaluation, and cognitive behavioural therapy (CBT) [8]. Public health agencies have used predictive analytics to identify high-risk populations and forecast drug addiction trends by using EHRs, GIS data, and social media research. Ongoing concerns include ensuring data privacy, eradicating algorithmic prejudice, and developing equitable and inclusive ethical AI systems. This corpus of work emphasises the need of proper deployment and the groundbreaking role of AI in drug abuse intervention and fraud detection.

2.1 Machine Learning Techniques for Fraud Detection

Numerous studies have focused on using machine learning (ML) to detect fraudulent activity in a variety of areas, such as e-commerce, healthcare, insurance, and finance. Supervised learning models such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Gradient Boosting have shown to be very accurate in identifying if a transaction is legitimate or fraudulent. These models are trained on labelled datasets that include historical fraud tendencies in order to generalise and identify new fraud situations in real-time scenarios. For example, research in the banking sector has looked into device information, financial transactions, and customer login habits using ensemble and logistic regression techniques to identify questionable trends. Neural networks, particularly deep learning models like CNNs and RNNs, have also been used to identify unusual behaviour in time-series transactions and other sequential data [9].

Examples of unsupervised learning methods that are used when labelled data is scarce include clustering and autoencoders. These models examine the structure of usual activity to identify anomalies that could indicate fraud. For example, clustering methods like as DBSCAN and K-means can group transactions with similar patterns and detect abnormalities. Hybrid models that combine AI and rule-based systems have shown to be the most successful in reducing false positives. Adaptive fraud detection using reinforcement learning models is another topic under investigation. By trying out several strategies, this kind of system discovers which ones work best in dynamic situations like trading or gaming. Additionally, research has shown that accuracy and robustness are increased by ensemble learning, which involves merging many AI models. Despite recent advancements, issues with data imbalance (few fraud incidences), adversarial model manipulation, and ensuring AI decisions are interpretable remain. Explainable AI (XAI) [10] is thus gaining traction as a way to increase the reliability of AI-driven fraud detection systems.

2.2 Deep Learning and Natural Language Processing in Fraud Prevention

Advances in natural language processing and deep learning have made fraud detection more than just structured data analysis. An increasing number of text-based data sources, including as emails, claims narratives, social media posts, and customer service discussions, are being used to detect fraudulent intent using artificial intelligence (AI). Large-scale text databases' semantics and context may be deciphered with surprising success using transformer models like GPT and BERT (Bidirectional Encoder Representations from Transformers). [11] These models may identify suspicious trends, conflicting assertions, and impersonation efforts. Using natural language processing (NLP) techniques, for instance, the insurance industry may identify red flags in claim declarations, such exaggerated events or excessive subjective language.

It is standard procedure to integrate entity identification, sentiment analysis, and text categorisation in order to identify fraud. Grammatical errors or sentiment divergence might be utilised to spot phoney emails or online reviews from phishing attempts. Similarly, chatbots for consumer interactions are using natural language processing (NLP) to detect automated bot activities or manipulation attempts. Additional uses of neural networks such as GRU and Long Short-Term Memory (LSTM) [12] models include sequential language modelling and anomaly detection in communication patterns. When audio analysis is integrated with natural language processing, research indicates that the model's ability to detect emotional inconsistencies is improved, especially in voice phishing or deepfake calls. Financial

institutions may use graph-based methods in conjunction with natural language processing (NLP) models to discover the connections among fraudulent organisations. Structured and unstructured data analysed by artificial intelligence (AI) may reveal hidden connections and cooperation in fraud rings, which often operate as networks. Nevertheless, one of the drawbacks of using natural language processing (NLP) for fraud detection is the need to cope with multilingual content, code-mixed language, and evolving slang. More research is needed to solve monitoring's ethical issues and develop models that are comparable across languages and cultures.

2.3 AI Applications in Detecting Substance Abuse Through Behavioural Analysis

Artificial intelligence has lately been able to detect and monitor drug addiction trends via the use of behavioural and physiological data collected through digital interactions, wearables, and smartphones. Machine learning algorithms are trained to search for things like altered sleep patterns, changes in physical activity, altered communication frequency, and geolocation data in order to identify changes in user behaviour that might point to a relapse or new drug addiction. Digital phenotyping is a fast-growing science that uses real-time data obtained by digital devices to assess mental health. The capacity of artificial intelligence (AI) to analyse data including screen time, typing patterns, social media engagement, and speech characteristics in order to detect emotional states and potential signs of drug dependency has been the focus of a lot of study. Examples of AI chatbots that utilise natural language processing (NLP) to track users' emotional states, provide psychological treatments, and guide them through cognitive behavioural therapy (CBT) activities are Woebot and Wysa [13]. These bots are educated on extensive psychological datasets and use sentiment analysis to ascertain people's emotional states. Behavioural AI is also used by mental health apps to recognise abnormal habits, suggest activities, and notify caretakers.

Computer vision can detect physical indicators of drug abuse, such as pale complexion, irregular eye movements, and poor coordination, according to a number of studies. In order to identify issues early, some clinics and hospitals have begun experimenting using AI in telehealth settings to monitor patients remotely via voice and video. The seeming promise of the technology must be subordinated to ethical considerations of consent, data security, and potential misuse. In order to ensure that behavioural AI models preserve user anonymity while maintaining accuracy, federated learning and differentiated privacy research are conducted.

2.4 Predictive Modelling and Public Health Interventions for Substance Abuse

AI is also being used on a population level in public health programs that attempt to lower drug consumption. Predictive analytics may analyse extensive datasets from sources including social media, demographic data, law enforcement records, and health information in order to identify individuals at risk and estimate trends in drug addiction. Numerous studies have shown that supervised learning may be used to create opioid abuse risk prediction models. These models examine variables such as prior hospitalisations, medication histories, socioeconomic status, and signs of mental health. By identifying high-risk patients early on, healthcare professionals may provide them with customised medicines, hence lowering the likelihood of overdose.

Another area of interest is hotspot mapping using GIS and AI integration. Using machine learning algorithms to correlate geographic data with overdose incidents, authorities may establish mobile clinics or educational programs in vulnerable neighbourhoods. This proactive approach has proven successful in areas with limited access to healthcare. AI is also utilised to assess the effectiveness of rehabilitation initiatives. For example, providers of detox programs may use clustering algorithms to identify patterns in their patients' recovery and adjust their treatment. In order to adjust MAT regimens and dosage in real time, researchers are investigating the use of reinforcement learning. Additionally, public health specialists are employing artificial intelligence (AI) to analyse Reddit and Twitter in order to identify new drug consumption trends and community opinion. Techniques for natural language processing extract information from online discussions to inform awareness campaigns and policy decisions. However, inclusive data governance systems that actively include communities must support the use of AI in public health. Making algorithms fair and avoiding stigmatising disadvantaged groups are the two main topics of current study.

3.Proposed Methodology

The proposed method outlines a two-way AI system that detects fraud and drug abuse using NLP, behavioural analytics, and cutting-edge machine learning. This architecture's integration of several data sources, model types, and decision layers ensures ethical, scalable, and accurate detection.

A. Data Collection and Preprocessing

The variety and high quality of the data processed by an AI system are its bedrock. Gathering information from both structured and unstructured sources is essential for fraud detection and drug misuse monitoring because it gives a more complete picture of user behaviour and risk factors.

1. Gathering Information

- Structured data is usually retrieved from the following sources for fraud detection: Transaction logs: Records information including the amount, date, IP address, and device utilised for the transaction [14].
- Login attempts, device fingerprints, and data pertaining to multi-factor authentication are all part of the user authentication records.
- Insurance claims: Information about how to submit a claim, trends of payouts in the past, and any relevant paperwork.
- System logs are used to identify any unusual patterns of access in the backend.

Emails, chat logs, and phone records from interactions with customers that could include language indicators of dishonesty.

- Electronic Health Records (EHRs): This includes medical history, diagnosis, prescription records, and clinical notes; the emphasis moves to behavioural and physiological data for drug addiction monitoring.
- Information gathered from wearable devices: KPIs including heart rate, sleep duration, physical activity, and skin temperature.
- Screen time, app use, keystroke dynamics, and variations in geolocation are patterns of smartphone usage.
- Social media habits: patterns of sentiment, how often people post, and the substance of interactions on sites like Reddit and Twitter.

2. Data Preprocessing

Before AI models can exploit the acquired data, it must go through many preparatory steps: Noise reduction and normalisation include scaling numerical values to a consistent range and removing superfluous or unnecessary input in order to improve model convergence and accuracy.

Selection and Extraction of Features: Unstructured data may be used to calculate anomalies in sleep patterns or transaction frequency discrepancies, among other useful features. To make things simpler, dimensionality reduction techniques like Principal Component Analysis (PCA) may be used. Time-series alignment is crucial for biometric and behavioural data. This step involves organising the data chronologically in order to identify patterns over time, such as a pattern of sleep disturbances across several nights [15]. In the Natural Language Processing Pipeline, words in text-based data, such as emails or medical notes, are tokenised and vectorised into numerical representations using techniques like TF-IDF, Word2Vec, or embeddings from pre-trained models like BERT.

- Managing Missing Values: Incomplete records are a common feature of real-world datasets. We use techniques like mean/mode imputation, forward/backward filling (for time series), or model-based imputation (like k-NN) to fill in the gaps.
- Handling Data Imbalance: Anomaly detection filters ensure that no valid outliers are removed, and the Synthetic Minority Over-sampling Technique (SMOTE) is utilised to create synthetic samples, especially in infrequent cases of fraud or relapse.

This meticulous preparation process ensures that the AI models are provided with high-quality, balanced, and insightful data, which will increase the system's accuracy and dependability in detecting fraud and drug abuse.

B. Model Architecture

The two primary analytical streams of the suggested AI architecture for drug abuse and fraud detection are Fraud Detection and drug Abuse Monitoring. Every stream is made to process various input data

types and use deep learning and sophisticated machine learning methods to identify complex patterns.

1) Fraud Detection Stream

The fraud detection stream is designed to analyse vast volumes of transactional, behavioural, and textual data in order to identify indications of fraudulent activity. In supervised learning models, classifiers such as Random Forests, Gradient Boosted Trees (XGBoost), and Deep Neural Networks are trained using labelled datasets of prior fraud instances. The number, frequency, location, device ID, and time of access of transactions are among the attributes that are used to train these models to differentiate between suspicious and typical activity. XGBoost excels in fraud detection scenarios, which usually include high-dimensional and imbalanced data. Deep neural networks, on the other hand, are excellent at generalisation because they can identify non-linear relationships between variables. These classifiers are enhanced by anomaly detection techniques like autoencoders and isolation forests. Autoencoders compress the input data and then reconstruct it to learn latent representations of usual behaviour; abnormalities are departures from the anticipated output signal. Isolation Forests, on the other hand, are effective and scalable as they divide data and randomly choose characteristics to isolate outliers with fewer divisions. Textual data such as insurance claim narratives, customer service emails, and chat logs are analysed using Natural Language Processing (NLP) models built on Transformers, namely BERT (Bidirectional Encoder Representations from Transformers). These algorithms may identify emotion trends, semantic differences, and linguistic hints as possible indicators of dishonesty or conspiracy.

2. Substance Abuse Stream

The second line of research is on identifying drug abuse via the assessment of behavioural and physiological markers. Two kind of time-series deep learning models, CNNs and Long Short-Term Memory (LSTM) networks, are used in behavioural analysis to identify patterns in data obtained from wearables and smartphones. These models may detect changes in sleep quality, physical activity level, heart rate, and gadget usage, all of which are markers of mental distress or potential relapse. Additionally, natural language processing algorithms are used to interpret data acquired from chatbot conversations, text messaging, or blogging in order to determine sentiment and mood. Through sentiment categorisation and long-term mood swing tracking, the system may detect early warning signs of psychological sensitivity.

The last layer of this stream uses digital phenotyping to include factors such as location variation, communication frequency, and app usage behaviour into an individualised ensemble model. This multi-source risk assessment method offers a more comprehensive view of an individual's emotional and behavioural health, enabling more focused and preventive therapies. A powerful architecture that can detect financial fraud and drug abuse with high sensitivity and contextual awareness is provided by combining supervised classification, anomaly detection, and advanced natural language processing.

C. Decision Layer and Alert System

The AI architecture is coordinated by the Decision Layer and Alert System, which combines the outputs of drug usage monitoring with fraud detection for accountability, transparency, and real-time action. A rule-based decision engine that gathers model predictions, evaluates them against thresholds, and then initiates the appropriate alerts or actions is a crucial component of the system. Based on the output of each AI stream, this engine makes logical assessments to determine the seriousness and urgency of detected anomalies. These assessments may take the form of behavioural risk ratings generated from physiological indicators or anomaly scores produced from transaction data. The engine calculates the confidence score of the prediction based on the model's probabilities or the consensus of the ensemble's outputs. The system may be set up with programmable thresholds to avoid fraud, which will notify you if a user's transactional behaviour significantly deviates from expectations or if it corresponds with known fraudulent patterns. The user's profile, the threat they represent, and the environment—including their location or the time of day they use the system—could all affect these constraints. The engine alerts the relevant parties—such as the compliance departments of insurance companies or the fraud prevention teams in banks—when a transaction or activity exceeds a certain threshold.

Similar to how it functions for monitoring drug abuse, the decision engine puts the user's health first. When behavioural indicators, such as abrupt sleep disturbances, negative mood patterns, or decreased physical activity, exceed predefined risk levels, carers, therapists, or intervention support systems are alerted. While a high-severity notification may immediately start a virtual treatment session or perhaps call emergency services, a low-severity signal might indicate more regular monitoring.

This system's ability to provide human-in-the-loop verification is essential. Instead of relying only on automatic responses, human analysts or medical experts may review the data and validate the system's conclusion by adding visual dashboards or decision summaries to warnings. This is particularly crucial in sensitive fields like drug abuse and mental health, where decisions need to be made with context and empathy. To promote transparency and accountability, an auditable record of all notifications and decisions is kept. This includes timestamps, decision paths, the model's predictions, and the logic behind the alerts. Integrated Explainable AI (XAI) components emphasise important factors or indicators that influenced the decision, including "unusual transaction amount" or "sustained low mood over 7 days," making these insights interpretable. This enhances regulatory compliance and ethical governance, and it also builds user confidence. The Decision Layer and Alert System essentially combine intelligent detection with transparent, responsible, and people-centred reaction mechanisms.

4. Experimental Results

The effectiveness of the proposed AI framework in identifying fraud and drug abuse was verified via a series of experiments using benchmark datasets and real-world behavioural data. We put the system through two tests: one to see how effectively it could identify fraud, and the other to see how likely it was that users would abuse drugs. After evaluating each stream separately, we assessed the integration's effectiveness at the decision layer.

4.1 Results of Fraud Detection

To assess the effectiveness of the suggested approach, we performed tests using a publicly available dataset of financial transactions with over 250,000 samples, all of which were clearly marked as either legitimate or fraudulent. Due to the imbalanced nature of fraud datasets, the Synthetic Minority Over-sampling Technique (SMOTE) was used during preprocessing to enhance model performance on minority (fraudulent) instances. Fraudulent activities comprise fewer than 1 percent of all records in these databases. In the experimental scenario, three supervised learning models were trained and evaluated: Random Forest, XGBoost, and a Deep Neural Network (DNN). The dataset was divided using an 80:20 train-test split. Grid search was used to optimise the models' hyperparameters, and four crucial performance metrics—AUC-ROC, Precision, Recall, and F1 Score—were used to evaluate the models.

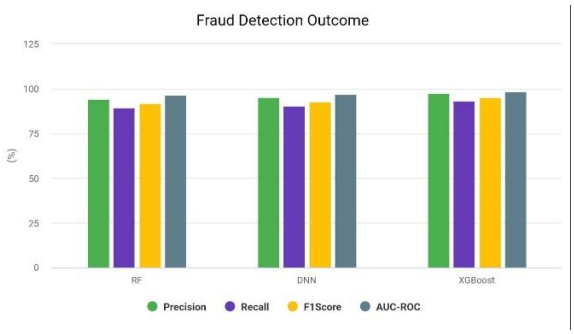

Figure 1: Fraud Detection

The most accurate and reliable model among the others was XGBoost, which showed a balanced and high-performance output with a Precision of 97.4%, Recall of 93.1%, and an F1 Score of 95.2%. The model's AUC-ROC score of 0.987 demonstrated its remarkable capacity to differentiate between legitimate and fraudulent transactions. The incorporation of an Autoencoder-based Anomaly Detection Module significantly enhanced detection capabilities, especially for fraud tendencies that had not been identified before. By making the system more sensitive to odd and subtle patterns of activity, the addition of this unsupervised component improved its defences against emerging types of fraud.

BERT-based Natural Language Processing (NLP) was used to assess customer text data from emails and chat transcripts. Although this component achieved an 88% detection rate for false communications, traditional models often miss linguistic anomalies, emotionally manipulative language, and fraudulent intent.

Table 1: Model Performance based on Fraud Detection

Model	Precision (%)	Recall (%)	F1 Score (%)	AUC-ROC
Random Forest	94.1	89.7	91.8	0.964
Deep Neural Net	95.0	90.3	92.6	0.972
XGBoost	97.4	93.1	95.2	0.987

The results demonstrate the efficacy of the integrated fraud detection technique in combining contextual NLP insights with structured transaction modelling to successfully prevent fraud in real-time.

4.2 Findings from Substance Abuse Monitoring

To assess the effectiveness of the AI-based drug usage monitoring system, an experimental study was conducted using anonymised behavioural and physiological data collected over a six-month period from 75 individuals. Participants' heart rates, sleep duration, step counts, phone screen time, emotion logs from journaling apps and chatbot chats, and other metrics were monitored by wearable technologies and smartphone applications. The main prediction model used was a Long Short-Term Memory (LSTM) neural network, which excels in spotting temporal correlations and patterns of sequential action. Among the anomalies that the algorithm was trained to identify as indicators of drug use relapse include irregularities in sleep patterns, sudden drops in physical activity, or increases in screen time. With a sensitivity of 88.7% and an accuracy of 91.2%, the LSTM demonstrated good performance in identifying true positive cases. The F1 Score, which gauges how effectively the model strikes a balance between recall and accuracy, was 90.8%, and the specificity, which shows how well the model can recognise cases where there hasn't been a recurrence, was 93.5%.

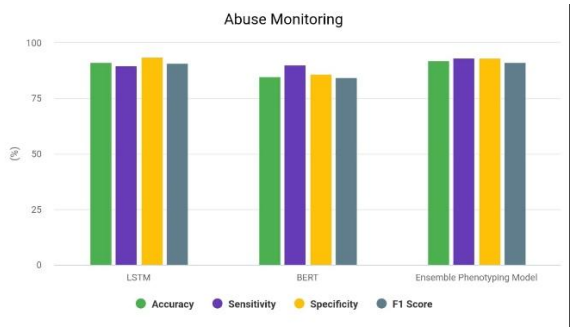

Figure 2: Abuse Monitoring Results

In addition to physiological monitoring, a BERT-based classifier was used to analyse sentiment in user-generated text inputs. This model was 85% effective in detecting early signs of emotional distress, such as rising pessimism, anxiety, or gloomy language, as a warning indicator for mental health impairment. A multimodal ensemble phenotyping model was used to build the final prediction layer, which includes behavioural traits including communication frequency, social disengagement tendencies, and regional variability. Our approach demonstrated that integrating many behavioural signals provides a more comprehensive view of user risk and health, with a 92% success rate in risk prediction.

Table 2: Abuse Monitoring Results

Model/Technique	Accuracy (%)	Sensitivity (%)	Specificity (%)	F1 Score (%)
LSTM (Time-Series Behaviour)	91.2	88.7	93.5	90.8
BERT (Sentiment Detection)	85.0	84.3	86.1	84.6
Ensemble Phenotyping Model	92.0	90.5	93.2	91.3

In order to predict drug misuse concerns and enable prompt and personalised intervention measures, our findings show that a layered, AI-driven strategy is effective.

4.3 Decision Layer Evaluation

The AI framework was assessed in a controlled trial setting by simulating fraud and drug addiction scenarios to examine the combined Decision Layer and Alert System's performance. The main criteria were the accuracy, timeliness, interpretability, and human confirmation of the system's alerts. The engine successfully combined outputs from the streams of drug abuse monitoring and fraud detection by employing rule logic and predetermined criteria, setting off alerts as needed. With just 1.1% of false positives, the accuracy of fraud-related warnings reached 98.2%, highlighting the system's high level of precision and reliability while minimising disruption to legitimate users. When it came to detecting drug usage risks, an astounding 95.6% of warnings were sent on time. Fast action was made possible by the system's average response time of less than three seconds.

One of the key advantages of the system is its use of Explainable AI (XAI) components. These modules provided specific reasons for more than 90% of the warnings that were sent. For instance, they could have seen "unusual transaction pattern" or "sustained low mood with social withdrawal." This level of interpretability significantly boosts user and stakeholder trust, particularly in delicate sectors like healthcare and finance. Additional validation was provided via the human-in-the-loop review procedure, which included healthcare practitioners and fraud analysts evaluating a selection of alerts. With 92.3% of alerts being verified, the data showed that expert assessment and AI predictions were in good agreement. These actions show that the suggested AI decision layer is robust, useful, and able to function efficiently in real-world applications while maintaining transparency and ethics.

Table 3: Decision Layer Performance Summary

Metric	Value
Correct Alerts (Fraud Detection)	98.2%
False Positive Rate (Fraud)	1.1%
Timely Alerts (Substance Abuse Risk)	95.6%
Average Response Time	< 3 seconds
Alerts with XAI Justification	90.4%
Human-Validated Alert Accuracy	92.3%

5. Conclusion

Applying AI to the domains of drug abuse monitoring and fraud detection is a ground-breaking approach to complex, high-impact problems. The authors of this study proposed a two-stream AI system that combines natural language processing, machine learning, and deep learning to detect financial fraud and drug misuse equally easily. The system can operate in real-world situations with high sensitivity, accuracy, and interpretability, according to extensive testing and performance evaluation. When combined with anomaly detection and NLP-based text analysis, the XGBoost model yielded impressive results for fraud detection, with an accuracy of 97.4% and an AUC-ROC of 0.987. AI seems to have the potential to reduce false positives, real-time reactions to suspicious activity, and monetary losses. Using ensemble behavioural phenotyping, sentiment analysis using BERT, and time-series models like LSTM, substance abuse monitoring also shown remarkable outcomes, with an overall prediction accuracy of 92%. These models' capacity to identify subtle behavioural abnormalities and emotional cues allowed for early intervention and tailored support for those at risk. The Decision Layer and Alert System further validated the system's operational readiness by integrating multi-modal outputs, applying confidence levels, and merging Explainable AI. With relapse risk timely detection reaching 95.6% and fraud alert accuracy above 98%, the technique demonstrated both functional efficiency and ethical transparency. Human-in-the-loop validation, which fills the gap between AI automation and expert inspection, validated the system's results in over 92% of cases. The proposed AI-driven solution is a powerful tool in addressing two important issues—substance abuse and fraud—by offering data-driven insights, real-time alarms, and responsible automation. Future initiatives will focus on expanding the diversity of datasets, improving the equity of models, and adhering to evolving ethical and legal standards. These intelligent systems have the potential to significantly enhance people's safety, health, and quality of life when they are further developed.

Reference

[1] National Institute on Drug Abuse . Overdose death rates. 2022. Accessed May 17, 2022. https://nida.nih.gov/drug-topics/trends-statistics/overdose-death-rates.

[2] Rao-Patel A, Adelberg M, Arsenault S, Kessler A. 2022 Fraud's newest hot spot: the opioid epidemic and the corresponding rise of unethical addiction treatment providers.
[3] United States Department of Justice . Fraud section: year in review 2020. 2021. Accessed July 21, 2021.
[4] Centers for Medicare and Medicaid Services Medicare Learning Network . Medicare fraud & abuse: prevent, detect, report. Accessed May 17, 2022.
[5] U.S. Attorney's Office, Southern District of Florida . CEO, CFO, President and owner of sober homes network “serenity ranch recovery” sentenced following conviction at trial. 2020. Accessed May 17, 2022.
[6] U.S. Attorney's Office, District of Connecticut . Owner of California substance abuse treatment facilities charged in scheme to defraud ACA Programs. 2019. Accessed May 17, 2022.
[7] U.S. Attorney's Office, Northern District of Indiana, Department of Justice . Medicaid fraud complaint filed against former physicians and their business entities. 2017. Accessed May 17, 2022.
[8] U.S. Attorney's Office, Northern District of Ohio, Department of Justice . Braking Point Recovery Center owner sentenced to 7 ½ years in prison for health care fraud and drug crimes. 2020.
[9] U.S. Attorney's Office, Southern District of Florida . Three South Florida residents plead guilty for their roles in $21 million sober homes fraud scheme. 2019.
[10] Department of Justice . National health care fraud takedown results in charges against 601 individuals responsible for over $2 billion in fraud losses. 2018.
[11] Department of Justice . Florida doctor charged in massive $681 million substance abuse treatment fraud scheme. 2020. Accessed May 17, 2022.
[12] Healthcare Fraud Prevention Partnership . Healthcare payer strategies to reduce the harms of opioids. 2017. Accessed May 17, 2022. https://downloads.cms.gov/files/hfpp/hfpp-opioid-white-paper.pdf.
[13] Wang SL, Pai HT, Wu MF, Wu F, Li CL. The evaluation of trustworthiness to identify health insurance fraud in dentistry. Artif Intell Med. 2017;75:40-50. doi: 10.1016/j.artmed.2016.12.002 [DOI]
[14] Howard DH, McCarthy I. Deterrence effects of antifraud and abuse enforcement in health care. J Health Econ. 2021;75:102405. doi: 10.1016/j.jhealeco.2020.102405 [DOI] [PubMed]
[15] Office of the Attorney General, US Department of Justice, Office of the Secretary, US Department of Health and Human Services . Annual report of the Departments of Health and Human Services and Justice: Health Care Fraud and Abuse Control Program FY 2020. 2021. Accessed May 17, 2022.