INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 1 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY TO DETECT FINANCIAL CRIMES IN CORPORATE

AUTHOR - DRISHTI KAMALAKSHA KOTIAN, STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY

BEST CITATION - DRISHTI KAMALAKSHA KOTIAN, THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY TO DETECT FINANCIAL CRIMES IN CORPORATE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (1) OF 2025, PG. 546-553, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

In the era of expedited globalization and technological advancement in every aspect of the economic and social growth, the growth of financial crimes in the corporate alongside is very evidently increasing. Such frauds can be prevented, tracked and detected through the usage of Artificial Intelligence more proficiently than the traditional methods available in today's world that cannot keep up with the anomalies in financial transactions, since dealing with complex algorithms and layered financial activities is best done through Artificial Intelligence.

Collectively, this research paper gives an intricate insight on the multi-faceted aspects of Artificial Intelligence in the detection of financial crimes in the corporate, its impact, benefits, ethical implications and need for constant evolution of the Artificial Intelligence in itself.

A more adaptable approach is needed for the pace at which the financial world is growing and Artificial Intelligence, currently, fits the role well.

Keywords: Artificial Intelligence, Financial crimes, Machine Learning, Risk Management, Natural language processing, blockchain technology

.Introduction

Artificial Intelligence is a bunch of various technologies that help computers perform a diverse range of activities and functions, comprising of abilities such as comprehension, translations of vocal and written language, provide suggestion and furthermore. Artificial Intelligence although budding is truly the backbone for innovative approach towards computing and unleashing the potential for the people as well as the corporate. For instance, OCR i.e., Optical Character Recognition. This a type of technology that serves as a foundation for the conversion of typed, handwritten or printed text from pictorial format to machine-coded texts. Artificial Intelligence technology is a scientific field that is related to computers as well as machines that can reason, comprehend and behave in a way that requires the human mind or that consists of data that exceeds the human analytical skills. Artificial Intelligence includes different aspects since it is a broad field, it includes philosophy and psychology, data analytics, data science and statistics, hardware and software engineering, linguistics as well as neuroscience.

As for the usage of Artificial Intelligence for business practices it is a set of various technologies that are essentially depended on machine learning and deep learning which is used for analytics, prediction and forecasting, suggestions and more.[978]

One element of a multi-layered fraud detection technique should involve artificial intelligence. To build a complete defence against fraudulent activity, combine it with additional fraud protection strategies like encryption, multi-factor authentication, and anomaly detection

[978] https://cloud.google.com/learn/what-is-artificial-intelligence#

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

systems. This all-encompassing strategy guarantees that the extra security measures offer a fallback to guard against fraud even in the event that one layer is breached.

The frequency and sophistication of fraudulent acts have increased as a result of the growth in online transactions. Advanced schemes that try to evade traditional detection techniques are always testing cybersecurity safeguards. Although still vital, human inspection is no longer enough to stop the sheer number of security breaches; it's difficult to stay up with the speed and slyness of contemporary cyberthreats. According to DigitalOcean's 2023 Currents report, 37% of respondents raised their cybersecurity expenditures in order to purchase more sophisticated security software. An extremely remarkable development in the battle against digital fraud is Artificial Intelligence fraud detection. Artificial Intelligence systems can swiftly sort through enormous information using complex algorithms to find odd patterns and abnormalities that can point to fraudulent activity. Over time, this technology improves its prediction skills by learning from every encounter and refining the detection process.[979]

This technology protects consumer trust, lowers financial losses, and preserves the integrity of business operations while strengthening security measures.

Financial crimes in the Corporate

Any unlawful activity involving money or financial transactions intended to achieve financial benefits through dishonest means is referred to as financial crime. It includes a broad spectrum of illegal actions, most of which are driven by monetary gain. These operations, which frequently take advantage of financial systems, institutions, or regulatory gaps, are carried out by criminal groups, companies, and individuals in order to either hide illegal funds or unlawfully grow their fortune. It can be difficult to discover and prosecute activities that entail intricate transactions spanning several jurisdictions.[980]

As long as people have been trading money for goods and services, there has been financial crime. In particular, financial crime refers to offenses against other people's property. Since practically all businesses now primarily conduct their operations and provide their services online due to the rapid advancement of digitalization, they are prime targets for cybercrime. For businesses, this implies that thieves are creating ever-more-advanced techniques to steal crucial financial information.

Regretfully, these crimes are not always committed by third parties. On the contrary, internal companies are responsible for a significant number of financial crimes. Because of this, these individuals are not only aware of the simplest methods to obtain crucial information, but they also know how to ideally hide their identities when interacting with banks, other financial institutions, or clients, or when working in the supply chain.

Both internal staff members and external assailants are capable of committing financial crimes.[981]

Among the corporate financial crimes are fraud, a general term that refers to a variety of tactics used to defraud individuals of their money. One of the most popular and straightforward is offering to give someone a large amount of money (say, $10,000) in exchange for sending the scammer a lesser amount (say, $300); the scammer may claim that the smaller amount is a processing or finder's fee. Naturally, the scammer receives the money that is paid to him but never distributes the promised funds. Two of the most common computer crimes are identity theft and "hacking" of computer systems.

An employee taking a few dollars out of a cash drawer or a sophisticated plan to move millions

[979] https://www.digitalocean.com/resources/articles/ai-fraud-detection

[980] https://www.quantexa.com/resources/financial-crime/

[981] https://www.lexisnexis.com/in-en/glossary/compliance/financial-crime?srsltid=AfmBOor3bbZ7rqg1-Y90aniygQcFwjP0lqZY49DW03R9pXJWxI_lSnt8

of dollars from a company's accounts to the embezzler's accounts are both examples of embezzlement, which is a theft or larceny offense. In addition to these crimes, money laundering is another well-known financial crime. It is a service that criminals who handle large sums of money require; it entails transferring the money through multiple accounts and ultimately into legitimate businesses, where it is mixed with the actual profits of the legitimate business and no longer distinguishable as having originated from the commission of a crime. A certain amount of white-collar criminality takes place at the corporate level.

For instance, a brokerage company might permit insider trading by its trading desk staff. Corporate entities may also engage in money laundering.

Transactional fraud monitoring systems can train AI algorithms for automated fraud detection to identify data trends that point to fraudulent behaviour. Unusual transaction quantities, several transactions from the same device, or purchases made from several locations in a brief period of time are examples of these trends. When the AI finds a discrepancy, it can mark the transaction for additional examination.[982]

The use of Artificial Intelligence Technology in corporate fraud detection

A collection of statistical methods known as artificial intelligence enables computers to recognize connections, draw conclusions, and forecast outcomes using patterns discovered in vast volumes of data. AI is being used by financial services firms to automate back-office tasks, such as preventing credit card fraud, customizing product offerings, advising sales teams, and stopping money laundering.

The practice of individuals or criminal organizations transferring revenues from their illicit operations into the global financial system to make them appear as though they were acquired legally is known as money laundering. About $25 billion is spent year by US banks on anti-money laundering procedures, and in 2023, penalties for banks globally that do not prevent money laundering exceeded $6 billion.

The intrinsic characteristics of the blockchain could be used by a blockchain-based anti-money laundering system to identify and stop illicit transactions. Let's say AI with machine learning capabilities is incorporated into the AML software that tracks transactions. The software program might then examine data strings to see if money laundering is occurring. Because AI is capable of machine learning, it can identify patterns in vast amounts of data and adjust to changes in criminal activity over time.

The transaction monitoring procedure would become much more effective and efficient with the use of these instruments, which would help automate it. Additionally, suspect activity can be warned, highlighted, and stopped for additional investigation if it is found. Additionally, the blockchain would permanently record all of this behaviour.[983]

Artificial intelligence (AI)-based systems that can identify the behavioural indicators of money laundering are replacing traditional rules-based systems that search for indications of criminal activity or questionable transactions based on preprogrammed patterns. AML software has historically searched for red flags that might point to criminal activity in addition to supplementary data like a bank customer's listing on an international sanctions list, bank deposits that fall below the threshold that necessitates government reports, or transfers of funds out of an account that resemble recent payments made into the account.

The problem is that criminals use increasingly sophisticated strategies to launder their gains through what seem to be genuine financial

[982] https://corporatefinanceinstitute.com/resources/esg/white-collar-crime/

[983] https://www.merklescience.com/3-reasons-why-the-future-of-anti-money-laundering-rests-on-blockchain#:~:text=Blockchain%20Technology%20for%20AML%20Compliance&text=In%20that%20case%2C%20the%20software,to%20its%20machine%20learning%20capabilities.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

transactions. They invest in already-existing businesses that mostly conduct business in cash and then exaggerate their sales, in addition to creating shell corporations to make ownership more difficult to track down. Additionally, they channel their money through nations with loose rules and deposit tiny sums of money in a variety of financial institutions. This indicates that conventional AML techniques frequently produce a large number of false positives and are ineffective, which can cost banks up to tens of millions of dollars annually.

In addition to assigning risk scores to customers based on their past behaviour and Know Your Customer (KYC) information, AI-based systems can identify hidden transaction patterns among networks of people, compare behaviours with those that are historically common for an organization or its peers, and triage events to close low-risk investigations. Because the vast majority of alarms their tracking software raises for inquiry are actually related to benign transactions, banks are having difficulty identifying actual money laundering activities, while criminals are becoming more adept at circumventing restrictions. Money and effort are wasted on those false positives. More advanced AI-powered software is now being used by financial institutions to either replace or complement anti-money laundering (AML) software that is based on predetermined criteria. This software more fully checks for suspicious behaviour, grades clients according to their risk of money laundering, and is more adept at uncovering hidden patterns in transactions and links between individuals and businesses. Reduced false positive alarms, improved defence against criminal activity and fines from the government, and cheaper compliance expenses are possible outcomes. [984]

With more financial transactions taking place online, traditional rule-based systems are losing their ability to detect fraud as the usage of artificial intelligence (AI) in financial fraud detection grows. Artificial intelligence (AI)-driven fraud detection systems analyse enormous volumes of data in real time using machine learning algorithms, spotting trends and abnormalities to highlight possible fraudulent activity. Over time, these systems' accuracy and efficacy can be increased by training them on historical data.

The capacity of AI-powered fraud detection systems to identify extremely sophisticated fraudulent behaviours that are challenging to identify with conventional rule-based systems is one of their main advantages. They are able to identify fraud that spreads across various channels, including online and in-person transactions, or that involves numerous accounts, devices, and places.

Furthermore, real-time AI-powered bank fraud detection systems are essential for spotting card-not-present criminal activity. These devices have a millisecond detection time for potential fraud. However, these methods are not perfect and can produce inaccurate findings, such false negatives or false positives.

To guarantee these systems' dependability and efficacy, it is crucial to regularly train and enhance them. Generally speaking, the growing application of AI in financial fraud detection has promise for greatly reducing the negative effects of fraud on both individuals and businesses.[985]

Artificial intelligence Technology can analyse patterns of consumer behaviour over time to spot anomalous conduct. For instance, the AI system has the ability to identify questionable transactions if a customer starts making significant purchases out of the blue.

NLP can be used by AI systems to analyze customer communications, including chat transcripts and emails, and find signs of fraud. For instance, the AI system can detect a possible fraud attempt if a consumer sends an email asking for a password reset after abruptly changing their account details.

[984] https://www.oracle.com/in/financial-services/aml-ai/

[985] https://www.fraud.com/post/artificial-intelligence

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

New data can be used to train AI algorithms, increasing their efficacy and accuracy over time. This ongoing learning makes it possible for fraud detection systems to remain current with the newest techniques and trends in fraud. All things considered, AI's function in fraud detection is to instantly spot suspicious activity and fraudulent transactions, lowering the possibility of monetary losses for companies and safeguarding client information.

In the battle against financial fraud and banking, artificial intelligence (AI) has become a potent weapon. Large volumes of data may be processed in real time by AI-powered fraud detection systems, which can then spot trends and abnormalities that might point to fraudulent behaviour. Machine learning techniques are used to continuously improve the accuracy and effectiveness of these systems over time. Deep learning, a subfield of machine learning that focuses on training neural networks to recognize patterns in data, is one example. Because of its capacity to analyse enormous volumes of data and spot intricate patterns that human analysts might not notice right away, it has been effectively employed in the detection of financial fraud.

One of the key benefits of AI-powered fraud detection systems is their ability to spot incredibly complex fraudulent activities that traditional rule-based systems might miss.

They are able to identify bank fraud that spreads across various channels, including online and in-person transactions, or that involves numerous accounts, devices, and places.

Artificial Intelligence can also help avoid fraud by enabling better fraud risk management. Financial institutions can be warned about possible fraudulent activity before it happens by using predictive analytics algorithms to identify high-risk clients or transactions.

AI-powered fraud detection tools, however, are not infallible and may result in false positives or false negatives. To guarantee the accuracy and efficacy of these systems, ongoing training and improvement are required. All things considered, applying AI to banking and financial fraud protection might greatly lessen the negative effects of fraud on both consumers and enterprises.[986]

Financial fraud risk management and its need

Fraud risk management is the barrier that protects a company from dishonesty and fraud. The possibility that a person or organization would become a victim of fraud is known as fraud risk.

Fraud risk can take several forms, including external fraud committed by parties outside the company, such cybercriminals or fraudsters, and internal fraud committed by staff, managers, or contractors. These threats can take many different forms, from simple theft or embezzlement to intricate schemes like financial statement manipulation and identity-theft.

Fraud risk affects the firm in a number of ways and extends beyond monetary losses. It involves reputational injury, a decline in consumer confidence, and legal repercussions, all of which can be equally detrimental and occasionally irreparable. The first step in creating a comprehensive fraud risk management plan is comprehending the complexities of fraud risk.

The practice of implementing safeguards against fraud before it happens is known as fraud risk management. It entails implementing a strong fraud risk management program, a thorough fraud management plan, and a fraud strategy that takes internal controls and fraud awareness into account. Fraud can have serious consequences, including monetary losses, reputational damages, and even legal issues. In essence, controlling fraud risks means erecting obstacles to stop fraud from damaging the company. It is comparable to having a solid defence system in place.

[986] https://www.fraud.com/post/artificial-intelligence

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Businesses and corporations can reduce the danger of becoming victims of fraudulent activity by putting in place efficient strategies and procedures. Strong internal controls must be put in place in order to stop and identify fraudulent activity. Segregation of roles, frequent audits, permission procedures, and supervision systems to guarantee adherence to rules and procedures are a few examples of these controls. Training programs should address subjects including identifying red flags, reporting suspicious activity, and comprehending corporate policies and procedures linked to fraud prevention, even if teaching staff members about fraud dangers and prevention techniques is essential. Businesses should evaluate their fraud risks on a regular basis in order to find weaknesses and rank areas that need development. These evaluations could entail looking back at past fraud instances, assessing possible dangers, and studying internal procedures.

A business may suffer large financial losses as a result of fraudulent activity. Identity theft, money laundering, and other fraudulent activities can have serious financial repercussions. Companies build a financial buffer that lessens possible losses by putting in place a fraud risk management program.

For any firm, a damaged reputation may be disastrous. Trust can quickly deteriorate when stakeholders, partners, and customers believe your company is susceptible to fraud. Retaining your business reputation as a reliable organization by controlling fraud threats shows your dedication to moral and safe business operations.[987]

The benefits of the usage of Artificial Intelligence Technology in the detection of Financial Crimes in Corporate

Businesses may enhance customer service, productivity, and security by utilizing artificial intelligence. Artificial intelligence can keep an eye on transactions around-the-clock, ensuring that any questionable activity is detected early on and can be addressed right away. Additionally, it facilitates prompt discovery, which is essential for thwarting scammers and reducing possible losses. Artificial intelligence's quick response time gives companies a strong weapon to prevent fraud before it affects their bottom line. Artificial intelligence fraud detection systems can increase their monitoring capabilities as transaction volumes rise without requiring corresponding staffing increases. This scalability is crucial for growing businesses because it enables them to maintain high levels of fraud detection and prevention without incurring significant additional costs.

Larger datasets bring with them more complexity, which artificial intelligence systems can manage to keep organizations safe as they grow. By preventing fraud losses, using artificial intelligence to detect fraud saves money. By eliminating the need for large manual review teams, it also lessens the financial strain on companies. The staff of a business may concentrate on strategic duties that call for human expertise when fraud detection operations are automated, which results in a more resource-efficient operation. For the same, it may be essential to assemble a specialized team of personnel from IT, data science, compliance, legal, and operations. The money saved over time by utilizing artificial intelligence can be put back into other aspects of the company, such as developing a product roadmap or funding marketing campaigns. Because artificial intelligence can analyse data more precisely than humans, fraudulent transactions can be identified with greater accuracy.

These systems are less likely to make mistakes than manual reviews. Over time, the system's ability to detect fraud increases as a result of artificial intelligence algorithms' constant learning and improvement from fresh data. Customers are more inclined to stick with a company when they feel safe doing business with them. By keeping clients safe, artificial

[987] https://www.fraud.com/post/fraud-risk-management

intelligence fraud detection increases their trust and happiness with the business's offerings. Gaining new clients that value the protection of their financial and personal data can be facilitated by establishing a solid reputation for security.[988]

Despite having an advanced ERP financial reporting system in place, the London-listed UAE healthcare business was able to understate debts totalling US$4 billion in the 2020 NMC Health scam. The likelihood of such misreporting would have been reduced if an AI fraud detection technology had been integrated into the ERP software and utilized in tandem with expert supervision.[989]

The of the disadvantages of using Artificial Intelligence Technology in the detection of Financial Crimes in Corporate

There are some difficulties with using AI for fraud detection. The quality of the data is one of the main problems. Large volumes of data are essential for AI systems to identify trends in fraudulent activity. It might be challenging for smaller financial institutions or financial technology firms to collect the required amount and calibre of data. AI systems may not be as successful without complete and accurate data, thus failing to detect fraudulent activity or mistakenly flagging valid transactions.[990]

The inability of AI systems' algorithms to be transparent or interpretable is another difficulty. Even while AI is quite good at spotting fraud, it can occasionally be challenging to explain the choices made by AI models or the reasons behind the conclusions that AI systems arrive at.

For AI and ML to work well, massive volumes of data are needed, which can be problematic for smaller companies. Additionally, they necessitate a substantial hardware and software investment, which limits their accessibility for smaller businesses. [991]

AI systems require access to relevant and high-quality data in order to detect fraud. But occasionally, data may be erroneous, out-of-date, or incomplete, which might impair how well AI algorithms work. Regulations and privacy concerns may also restrict the amount of data that is available, which makes it challenging for AI systems to learn from a large dataset. A careful balance must be struck between protecting access to essential data and guaranteeing data integrity while adhering to privacy regulations.

It can be challenging to integrate AI fraud detection into an organization's current infrastructure. The newest machine learning and AI business technologies might not work with legacy systems, necessitating major updates or even total redesigns. Downtime or decreased functionality during the transition phase may result from this resource-intensive and disruptive integration process. To lessen these effects, businesses must carefully design and implement the integration of AI technologies.

False positives, in which valid transactions are reported as fraudulent, can still be produced by AI systems. Customers may become frustrated and the customer-business relationship may suffer as a result of this friction. A constant problem is striking a balance between the desire to deliver a seamless client experience and sensitivity to fraud. AI models must be continuously improved in order to lower the number of false positives and preserve consumer happiness.

Companies must make sure their AI fraud detection systems abide by all applicable rules, such as those pertaining to data protection and privacy, such as the General Data Protection Regulation (GDPR). Ethical questions are also brought up by the use of AI in decision-making processes. For example, algorithms may be

[988] https://www.digitalocean.com/resources/articles/ai-fraud-detection#

[989] https://abmagazine.accaglobal.com/global/articles/2024/oct/business/ai-risk-in-internal-audit.html#:~:text=In%20the%20case%20of%20Chinese,not%20by%20the%20AI%20software.

[990] https://cms-lawnow.com/en/ealerts/2024/11/the-role-opportunities-and-challenges-of-ai-in-detecting-financial-fraud

[991] https://www.gdslink.com/the-future-is-now-the-benefits-and-limitations-of-using-ai-and-machine-learning-for-fraud-detection/

biased, which could result in the unfair treatment of some clientele groups. To stay in compliance and preserve moral principles, businesses need to carefully negotiate these ethical and regulatory environments.[992]

Fake paperwork and inflated sales numbers were used to represent US$300 million in revenue for the Chinese brand Luckin Coffee in 2020. An anonymous human whistleblower, not the AI software, discovered the scam even though the corporation was utilizing AI-driven financial analytics tools. AI cannot consider the broader business environment or the ramifications of decisions that deviate from the pre-established parameters since it is limited to the limits established during software development. Furthermore, unstructured and extremely complicated data, such financial agreements spanning numerous jurisdictions or legal contracts, cannot be decoded by the majority of AI systems.[993]

Conclusion

Machine Learning, Natural Language Processing and Blockchain as a part of Artificial Intelligence can help increase security in the corporate and not just detect financial crimes in the corporate but also prevent it. Artificial Intelligence helps detect threats in a jiffy, making it easier for the corporates to prevent and regulate the possibilities of financial frauds with and outside their vicinity that would affect it otherwise. Artificial Intelligence Technology can be expensive but overtime it proves to be a good decision since it enhances the transparency with all financial activities.

Artificial Intelligence Technology can be helpful when it comes to financial fraud detection since it has the ability to sift through heavy and layered data in a very short span of time, in literal milliseconds.

As and when the evolution of such technologies occur, corporates can install such Artificial Intelligence Technology in their daily routines for financial governance whilst providing safety from the possibility of the occurrence of financial crimes and even detection of financial crime as and when the take place.

Overall, in a corporate world, technology, social and economic development is taking place at a very fast pace, followed by which is the growth of financial crimes in the corporate. Here, Artificial Intelligence Technology can help with adapting to such fast pace development by detecting financial crimes which is very important in aiding such growth.

[992] https://www.digitalocean.com/resources/articles/ai-fraud-detection
[993] https://abmagazine.accaglobal.com/global/articles/2024/oct/business/ai-risk-in-internal-audit.html#:~:text=In%20the%20case%20of%20Chinese,not%20by%20the%20AI%20software.