LTIMindtree

PoV

# Stay Ahead of the Game

## Leveraging AI, ML, NLP, & EL for Smarter Fraud Detection, Risk Assessment & Compliance

# TABLE OF CONTENTS

# Abstract

Artificial Intelligence (AI) and Machine Learning (ML) are integral in today's modern banking era for expediting the realization of use cases. In this POV, we will take you through the influence of AI/ML on the financial industries.

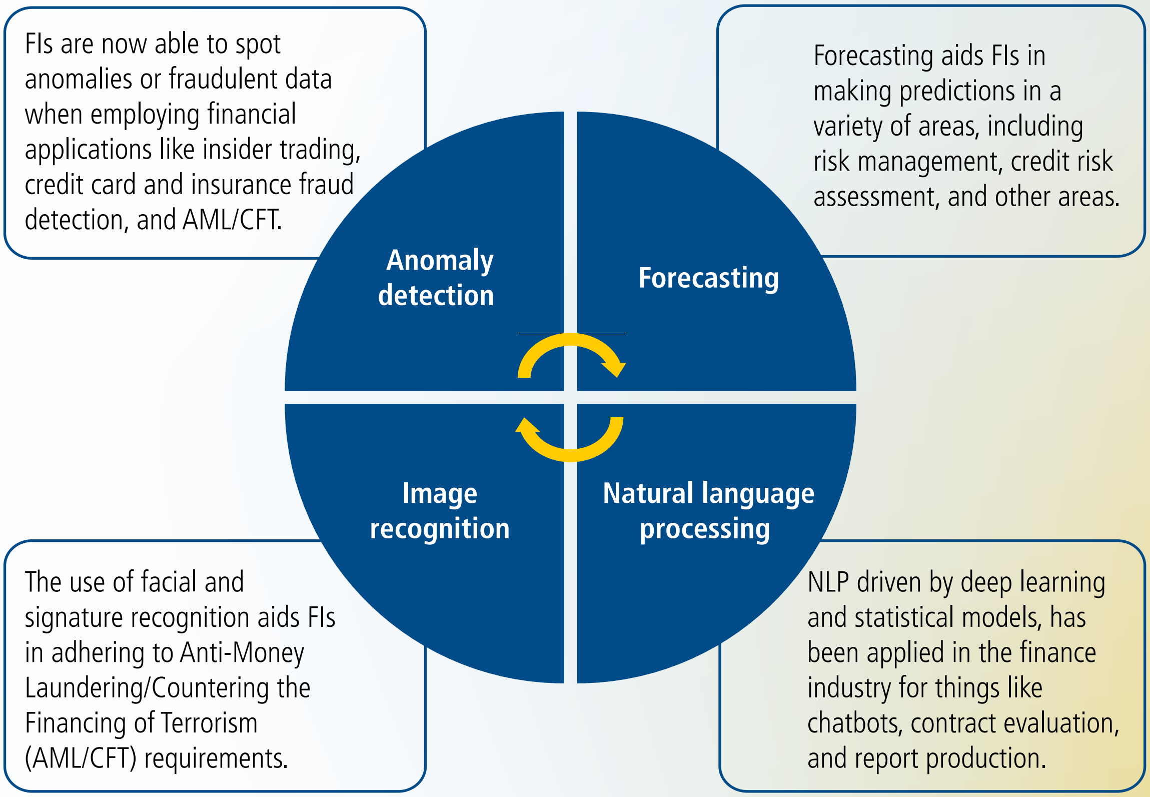
# Problem statement

Over the past decade, AI/ML systems have advanced significantly. Although, it is not the right time to say a machine that can comprehend or learn each intellectual work that a human performs. However, modern AI systems can carry out well-defined tasks that would typically need human intellect. A crucial part of most AI systems' learning process is Machine Learning (ML), which is based on analytics, mathematics, and probabilistic reasoning.

# Introduction

The adoption of AI/ML technologies has been growing rapidly in the financial industry, driven by fintech businesses. The financial industry has recently adopted big data and cloud computing, and this, together with the growth of the digital economy, has made it viable to use AI/ML systems effectively. AI/ML capabilities (Figure 1) are transforming the financial sector. Financial Institutions (FIs) can save significant money by automating processes, using predictive analytics to improve product offerings, and providing more efficient risk and fraud management processes and regulatory compliance. Lastly, AI/ML technology gives central banks and regulatory authorities new capabilities to enhance systemic risk detection and bolster prudential oversight.

The eagerness for AI/ML adoption in the banking sector has grown even more due to the COVID-19 epidemic. To manage huge amounts of loan applications during the pandemic, AI/ML has played a crucial role in the financial sector to improve their underwriting process and fraud detection. Similarly, in the post-pandemic era, supervisors who relied on intense off-site supervision efforts during the pandemic should further investigate AI/ML-supported tools and processes.



FIs are now able to spot anomalies or fraudulent data when employing financial applications like insider trading, credit card and insurance fraud detection, and AML/CFT.

Anomaly detection

Forecasting aids FIs in making predictions in a variety of areas, including risk management, credit risk assessment, and other areas.

Forecasting

Image recognition

Natural language processing

The use of facial and signature recognition aids FIs in adhering to Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) requirements.

NLP driven by deep learning and statistical models, has been applied in the finance industry for things like chatbots, contract evaluation, and report production.

# Can AI/ML help to detect fraud/anomalies?

The financial and insurance sectors have seen the most attacks for the sixth consecutive year. According to the FBI's 2021 Internet Crime Report, in the United States alone, a record-breaking 847,367 reports of online fraud were made, resulting in a loss of USD 6.9 billion. Credit cards, loan payback, fraudulent claims, identity fraud, and document forgery were just a few of the topics covered by these fraud claims. However, instances of financial fraud are not limited to the internet. Unfortunately, fraud in the financial and insurance industries is quite common, both online and offline. This demonstrates how fraud and cyberattacks negatively influence the financial sector, causing significant losses every year. The rapid adoption of online banking and payment digitalization has led to a substantial spike in transaction volume, demanding an urgent need for FIs to implement improved fraud protection methods. Each year, cybercrime costs both consumers and businesses billions of dollars.

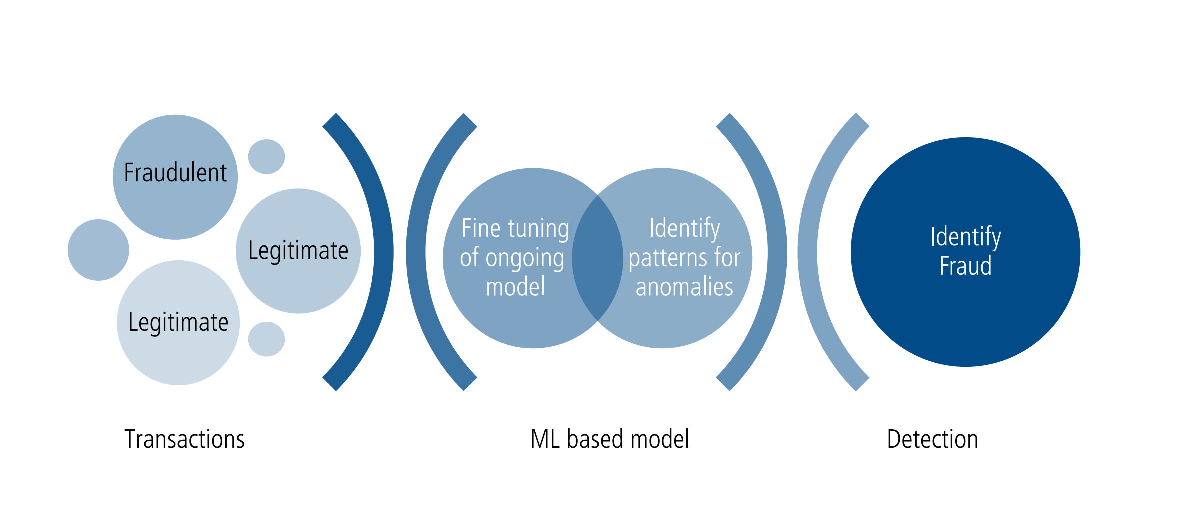


Figure 2. Artificial Intelligence & Machine Learning Capabilities

Organizations are already using ML to detect email spam and generate tailor-made product recommendations for millions of online shoppers. ML, particularly DL, blends with big data, develops at a great scale, and improves significantly over a very short time. ML-based classification and clustering algorithms are widely used in the banking sector to identify fraud in real-time, prevent it before it occurs, and assist in fraud investigation. ML algorithms, fed enormous amounts of data, allow organizations to find hidden relationships between many data points and quickly identify anomalies (figure 2).

Finding the most suitable algorithm or "margarita" of algorithms to analyze fraud-related datasets is not an easy job because it often depends on the type of data/ fraud, the environment in which we perform, the price at which it can be deployed, etc. A few well-known ML-based models/ techniques (figure 3) are widely available and used in a variety of fraud scenarios, including money laundering, credit card fraud, identity theft, forged insurance claims, tax fraud, etc.

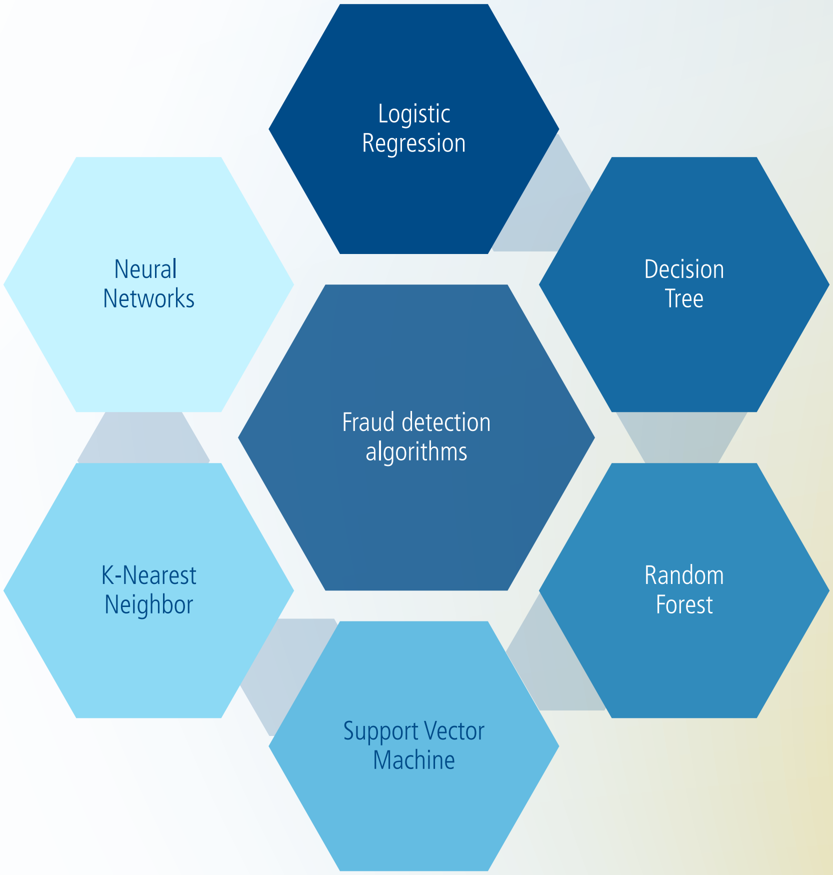


Figure 3. ML based models/ techniques

# Use cases of AI/ ML in fraud detection

1. **Money laundering:** It is considered the most pressing issue in the banking sector. ML algorithms would recognize the same patterns when they repeat in future scenarios by analyzing data such as the senders' and recipients' backgrounds or their past transaction histories, thereby discriminating between legitimate and criminal activities.

2. **Credit card fraud:** It is a prevalent type of electronic payment fraud in the retail industry. ML-based models for payment fraud detection would update card users' behavioral profiles after each transaction to improve future predictions and reduce false positives.

3. **Identity theft:** FIs might evaluate identification documents using machine learning-driven computer vision, or they might add other forms of verification, including face recognition and biometrics, to spot falsified loan applications and online fraud.

4. **Tax fraud -** By checking the general ledger in search of odd entries that might indicate attempted fraud, ML's capabilities in spotting strange patterns can efficiently be utilized to improve audit and tax compliance.

# What are the risks?

How we approach financial risk management is evolving and will soon undergo a revolution courtesy of AI/ML. The evolution of AI-driven solutions opens a world of opportunities for risk management, from determining how much a bank should lend to a customer to informing traders on the financial markets about position risk to identifying consumer and insider fraud and enhancing compliance.

In the financial industry, credit risk, market risk, and operational risk are the three primary categories of financial risk management. The ML-based models are exploring more opportunities to look at potential use cases, including credit underwriting, financial forecasting, market analysis & target campaigns, and so on across the financial sector.

1. **Credit risk:** Credit risk is the potential for financial loss resulting from a counterparty's failure to uphold its contractual duties, such as timely payment of interest or principal, or an elevated risk of default during the transaction. By leveraging AL/ML, one may determine the cost of default if a default occurs and the probability of a default event (a credit event). ML has become quite significant in the consumer and SME lending domain to make better credit decisions.

2. **Market risk:** Results from exposure to financial markets, whether through trading or investment. ML might assist in market risk management by highlighting the advantages at each stage, including data preparation, modelling, stress testing, and giving a validation trail for model explanation. ML is particularly well suited for stress-testing market models to identify unintended or developing risks in trading behavior.

3. **Operational risk:** Whether internal to the organizations (such as inefficient workflow, people, and capabilities) or from external events (such as frauds, failure in controls, an operational error, overlooked procedure, or a natural disaster), has directly or indirectly affected the FIs and ended up causing financial loss. FIs might benefit from AI/ML at different phases of the risk management process, including detecting risk exposure, evaluating, forecasting, and analyzing its consequences.

## Here are some use cases of AI/ML in risk management

1. Credit underwriting: ML-based algorithms can quickly decide on underwriting and credit scoring, saving organizations time and money. The algorithm may be trained to assess customer data, including age, income, occupation, credit behavior, and default, loan repayment and foreclosure histories.

2. Financial forecasting: By anticipating changes in market interest fluctuations, automating and optimizing insurance renewals, analyzing international exposure and assets, and reporting cost allocation justification for businesses, AI and ML can streamline numerous processes and point out areas to reduce financial risks.

3. Market analysis and target campaigns: Marketing professionals may benefit from AI/ML by assessing their target audience, evaluating engagement rates on various types of content, discovering supply and demand gaps, forecasting reputational hazards, and receiving advice on how to deal with problems and uphold their image.

## Are we not in safe hands?

The financial services industry is heavily safeguarded by regulatory compliance. FIs spend billions on regulations to adhere to the ever-changing compliance policies and standards and to stay current. Otherwise, FIs have to pay incredible fines and suffer reputational damage. According to an article from The Banker, financial institutions were penalized with 176 fines totaling USD 5.37 billion in 2021 alone for compliance violations.

The relevance of Regulatory Technology (Reg-Tech) has increased because of regulatory tightening and growing compliance costs following the global financial crisis of 2008. Recent breakthroughs in AI/ML are redefining risk and compliance management by employing large data sets, frequently in real-time, and automating compliance judgments. Both expenses and the quality of compliance have increased as a result.

The Regtech is discovering more chances to investigate potential use cases across banking, securities, insurance, and other financial sectors. Identity verification, anti-money laundering and combating the funding of terrorism, keeping track of regulatory obligations and latest compliance policy changes, and adherence to COVID-19 relief criteria are some of them.

Here are some use cases of AI/ML in regulatory compliance

1. AML/CFT compliance: AI/ML-powered technologies help reduce false positives encountered during AML/CFT checks by analyzing unstructured data and consumer behavior. It enables financial institutions to invest more time and money in cases more likely to be fraudulent.

2. Regulatory obligations and compliance policy changes: To keep up to date on the regulatory obligations and latest compliance policy changes, the internal compliance teams at the bank combed through thousands of internal documents, newspapers, and government websites. NLP-based AI solutions sniff through different websites and new regulation documents to highlight the necessary regulatory requirements and identify the most pertinent to each organization.

3. Optimizing stress testing: Financial institutions and banks must regularly define and disclose their solvency as per financial authorities' guidelines following the 2008 financial market crisis to remain compliant. Machine learning may aid compliance authorities in explicitly identifying which value combinations pose concerns, improving the reporting accuracy and reducing the time needed to execute these tests.

# Few obstacles to be wary of

According to an Economist Intelligence Unit (EIU) study, 86% of financial services executives want to increase their ML and AI spending through 2025. These startling figures demonstrate how financial institutions are beginning to understand the type of effect that cutting-edge technologies like AI and ML provide. On the other hand, while using AI/ML solutions, banks, and FIs also experience certain difficulties.

As ML models are fed with enormous datasets to train them, data security and privacy are the areas that cause the most anxiety. There is a possibility that the integrity of the data collected from millions of people worldwide might be compromised.

Training ML models with low-quality training data carries risks since biases might appear from time to time. Racial, gender, regional, and ethnic discrimination frequently accompany this low-quality data.

ML, especially DL, employs hidden layers between the input data and the output, causing a lack of transparency. This type of black box technology makes it challenging to manage risks efficiently and may be incompatible with regulatory compliance, especially when exhibiting model validity.

Legacy systems sometimes lack the adaptability or ability to meet the data processing or deployment constraints that ML and DL might necessitate for effective model training.

# Conclusion

According to Forbes, the market for AI will grow to USD 15.7 trillion by 2030 and reach USD 500 billion in investments by 2024. To achieve ML's full potential financial institutions are already seeking to restructure their organizational workflows, redefine data storage and processing standards, and help employees to understand business needs. Leading organizations adopt machine-learning algorithms and fully use smart data to improve the precision of fraud detection. The following step aims to reduce noise (false positives) and the risk of overlooking fraudulent transactions (false negatives). Model-validation procedures should be revised to overcome algorithmic bias to ensure that the appropriate algorithms are used for each circumstance. Financial regulators also propose new rules and hefty penalties in response to data breaches. According to the Fair Credit Reporting Act, even financial institutions might face penalties for failing to explain the model's predictions.

# References

1. https://www.itransition.com/machine-learning/banking
2. Machine Learning for Fraud Detection: 6 Use Cases & ML Types (itransition.com)
3. Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance in: Departmental Papers Volume 2021 Issue 024 (2021) (imf.org)
4. 6 Ways To Use Machine Learning for Data-Driven, Risk-Based Decision Making in Your Organization (ventivtech.com)
5. Machine Learning and AI for Risk Management | SpringerLink
6. Machine Learning in Finance - Overview, Applications (corporatefinanceinstitute.com)
7. Deep Learning & Machine Learning Uses in Financial Services (dominodatalab.com)
8. Top 10 AI Development and Implementation Challenges | Spiceworks

# Author profiles

## Arpan Roy

Associate Principal - Business Analysis

Arpan Roy is an Associate Principal - Business Analysis, BFS Consulting at LTIMindtree. He has over 15 years of experience in the core/retail banking sector and has worked on several consulting projects. He has contributed to transformation programs for many eminent banks, and he is currently working in the BFS practice, aiding clients with their digital transformation journey.

## Saura Roy

Senior Specialist - Business Analysis

Saura Roy is a Senior Specialist in Business Analysis, BFS Consulting at LTIMindtree. He has ten years of expertise in core banking, lending, and global IT consulting services. He is now active in the BFS practice, emphasizing digital channels and digital banking verticals. He has participated in transformational programs for leading global banks.