Machine Learning and Artificial Intelligence in Online Fake Transaction Alerting

Naresh Babu Bynagari

Andriod Developer, Keypixel Software Solutions, 777 Washington rd Parlin NJ 08859, Middlesex, **USA**

*Corresponding Contact:
bynagari.gs@gmail.com

ABSTRACT

Artificial Intelligence (AI) is one of the most promising and intriguing innovations of modernity. Its potential is virtually unlimited, from smart music selection in personal gadgets to intelligent analysis of big data and real-time fraud detection and aversion. At the core of the AI philosophy lies an assumption that once a computer system is provided with enough data, it can learn based on that input. The more data is provided, the more sophisticated its learning ability becomes. This feature has acquired the name "machine learning" (ML). The opportunities explored with ML are plentiful today, and one of them is an ability to set up an evolving security system learning from the past cyber-fraud experiences and developing more rigorous fraud detection mechanisms. Read on to learn more about ML, the types and magnitude of fraud evidenced in modern banking, e-commerce, and healthcare, and how ML has become an innovative, timely, and efficient fraud prevention technology.

Key words

Machine Learning (ML), Artificial Intelligence (AI), Fraud Transaction, Cyber Attacks, Algorithms Technology

12/31/2015 **Source of Support:** None , **No Conflict of Interest:** Declared

INTRODUCTION

As the world makes technological advancements and the internet, businesspeople have moved with the trend, taking their businesses online scammers have followed suit, devising new, and smart ways to defraud people. Fake online transactions have become an increasing problem, and the truth is, every year, billions are lost to these scammers (Vadlamudi, 2015). This raised the question of how to solve this daunting problem. Artificial intelligence features have been used to carry out the task to ease and reduce the workload on humans. Machines through technology advancement can be programmed to simulate human intelligence. They are programmed to mimic human actions and think like humans as well.

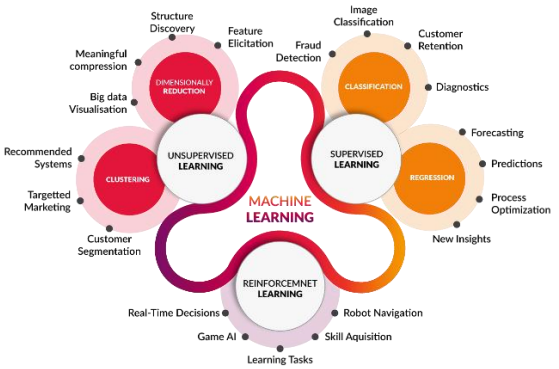

Figure 1: Machine Learning (Source: towardsdatascience.com)

MACHINE LEARNING

The term "machine learning" in the year 1959 was coined by Arthur Samuel, an American computer scientist. The term machine learning is defined as the ability of a computer to learn without explicit programming. Machine learning, also known as predictive modeling, is a subtype under artificial intelligence. In its case, it allows software applications to advance in their accuracy in determining outcomes without being explicitly programmed to do so (Bynagari, 2014). It works like a human, adapting to changes by learning new behaviors and evolving based on its experiences. This happens without human guidance, that is, without explicit programming. Machine learning algorithms use historical data as input to predict new output values.

Common uses of machine learning include fraud detection, business process automation, predictive maintenance, malware threat detection, spam filtering, and recommendation engines. (Gmail spam filtering as an example). Today, top companies, including Google and Facebook, utilize machine learning for their operations. It helps businesses or enterprises see customer behavior trends as well as patterns of business operation. Machine learning is different from traditional programming because traditional programming requires input data and a properly written and tested program for the machine to generate output (Taher-Uz-Zaman et al., 2014). However, this is not the case with machine learning, as input and output data are fed into the machine during the learning phase. Also, it works out a program for itself. The following are the following types of machine learning method:

a) Supervised Machine learning

A training dataset is provided for the machine learning algorithm in supervised learning, which supervises and corrects until the algorithm achieves a required level of accuracy. Supervised machine learning uses examples and preset guides to teach the machine. That is, machines use examples to learn. The programmer develops the algorithm for machine learning using an already prepared dataset that contains the wanted input and output data. The algorithm is must then follow the established command in arriving at the input and output. The machine learning algorithm will follow the path set by the programmer to identify patterns in data and learns from observing the operator's selection which it can also use to make future predictions. The operator may correct the ML algorithm when it makes

a prediction, and this process will continue until the machine learning algorithm accuracy and performance levels are high enough. Types of supervised machine learning include:

- **Classification:** machine learning algorithms in classifying tasks must learn from observing the operator and determine the category of observed data. It can group a transaction as fraudulent and non-fraudulent.
- **Regression:** in regression, machine learning algorithms must, through the estimation, understand the connection between variables. This makes the regression feature very important in forecasting.
- **Prediction:** this is the process of forecasting the future using past and currently collected datasets. It can be used to carry out an analysis of trends.

b) Semi-supervised machine learning

This is very similar to supervised machine learning. It combines both labeled and unlabeled data. Data with important and useful tags, which the machine learning algorithms can comprehend, is labeled data, while unlabeled data are data without tags or information.

c) Unsupervised machine learning

The machine learning algorithms here analyses and study's data pattern to understand and identify them. There is no supervision or human operator to assist it. Instead, the machine uses the data available to determine the connections and relationships of the dataset. The more the data available to analyze, the more advanced and improved it becomes with higher accuracy. Unsupervised machine learning is categorized into clustering and dimension reduction.

d) Reinforced machine learning

This type of machine learning focuses on rigid learning processes. A group of actions, parameters, and instructions are provided in the machine learning algorithms. The ML algorithm tries to go through several possibilities, options, and results through defined rules, then monitors them to determine the best. This method uses the trial-and-error method, uses past experiences, and begins adaptation in its processes in reaction to the situation for the best possible outcome.

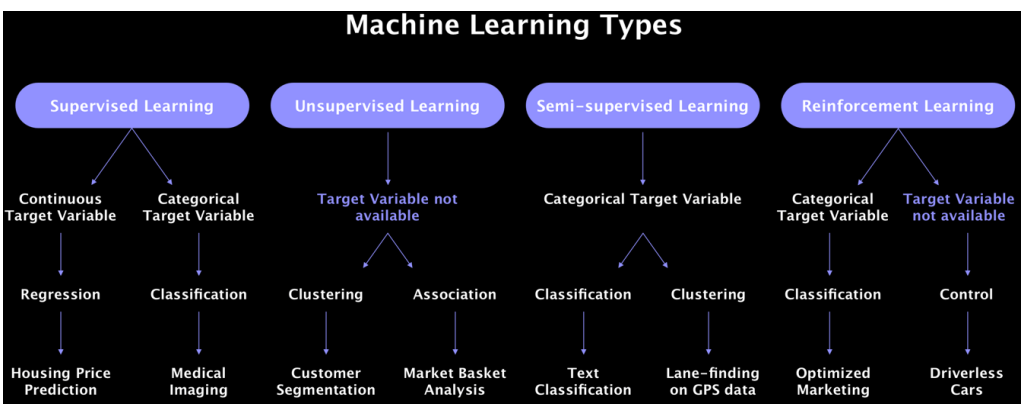

Figure 2: Machine learning types (Source: litslink.com)

MACHINE LEARNING IMPORTANCE

Machine learning today has become quite popular as several repetitive tasks and functions can be automated. Especially those tasks that need innate human intelligence without emotional or subjective judgments. Mimicking human intelligence into the machine can only be done using machine learning methods. Artificial intelligence can be programmed to function and carry out tasks like humans use machine learning programming algorithms. Businesses and other industries can automate jobs using machine learning features. Big companies and industries require big amounts of data to enhance their services and operations. Through machine learning methods, large amounts of data can be analyzed and processed with high accuracy. By developing accurate machine learning models, businesses can take advantage of profitable opportunities and avoid unforeseen risks. Machine learning features have been applied in text generation and image recognition. This is also an opportunity for machine learning development experts to become highly sought-after professionals.

In a nutshell, one may treat ML as one of the applications of AI as it is based on pattern recognition and computer learning without their deliberate programming for doing that (Paruchuri, 2015). Techniques that make ML happen are Bayesian methods, neural networks, inductive logic programming.

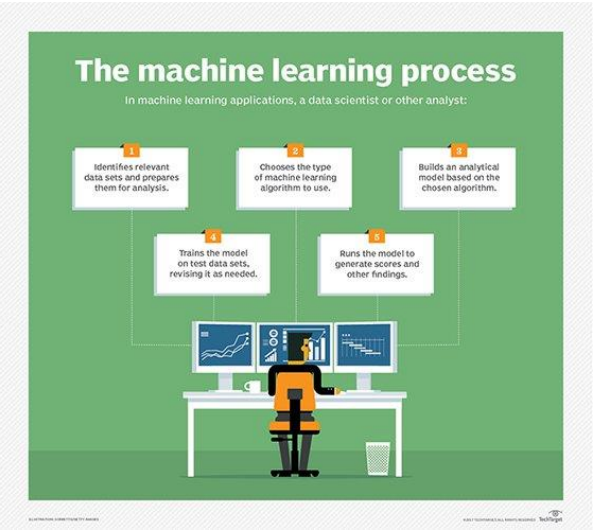

Figure 3: Machine learning Processes
Source: searchenterpriseai.techtarget.com

ARTIFICIAL INTELLIGENCE

Artificial intelligence is one of the technological wonders today that has been broadly used for various tasks, from smartly selecting music on personal devices, driving a car to detect, and averting fraudulent transactions. Technology has made it possible for machines to exhibit human intelligence in their behavior. They now can think like humans and take over activities or jobs that initially had to be done by humans. Simply put, artificial intelligence refers to machines that exhibit human-like behavior.

After being provided with the initial data, AI machines learn from it and evolve, smartly learning from the initial data input. The more data is provided, the more it learns and adapts. The ability of an AI machine to operate like the human mind enables it to process data and make the best possible action in solving problems without human interference.

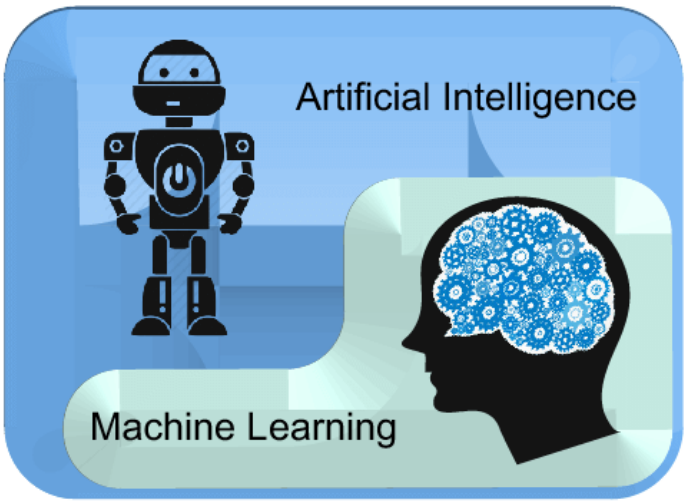

Figure 4: AI and ML
Source: javatpoint.com

- **Applications of Artificial Intelligence**

AI can be applied in different industries and sectors, from healthcare, financial to the automobiles industry. The list of applications is simply endless.

Popular examples of how AI has been applied include the invention of self-driving cars and computers playing games. These individual AI machines analyze every action taken and respond accordingly to give the best possible result.

In the financial industry, Artificial Intelligence has been used to detect fraudulent transactions like flagging accounts where unusual activities like large deposits and withdrawals take place. Trading is also made easier with AI as it estimates supply, demand, and securities pricing more streamlined.

- **Categorization of Artificial Intelligence**

AI is categorized into two: Weak and Strong AI.

- **Weak Artificial Intelligence**: Weak artificial intelligence is designed to carry out more simple tasks. For example, Apple's Siri, which works as a personal assistant, listens to questions, and helps you answer them.
- **Strong Artificial Intelligence:** Strong artificial intelligence systems take on more complex tasks and are the real definition of "work like the human mind." These AI systems are programmed to step in and solve problems that would normally require human intervention. Strong AI systems can be found in self-driving cars and surgery equipment.

➢ **Advantages of Artificial Intelligence**

Using AI has pushed the boundaries of machine functionalities. Some advantages of using Artificial intelligence include.

- **Reduces Errors by humans**: From time to time, humans make mistakes. "Human Error" is a phrase that came about because of human mistakes over time. However, computers, systems, and machines do not make human-like mistakes with the right programming and commands. Instead, AI gathers data and information by applying algorithms and making decisions based on them. This way, mistakes, and errors are reduced significantly with a higher level of precision and accuracy. For instance, the use of AI in weather forecasting has increased the accuracy of forecasts and reduced human error.
- **Reduces the need for humans to take risks**: Artificial intelligence machines can be programmed to carry out various types of jobs. Moreover, they can be programmed to handle risky tasks. It is a huge advantage as this can save human life. For instance, AI robots can be programmed to defuse a bomb, explore highly dangerous places like Mars and the deepest parts of the oceans, and so on.
- **Availability:** Machines can work for more hours than humans. An average human may for a maximum of 6hrs per day aside from the breaks. Humans need to take time out for rest, refresh themselves, and prepare for a new workday.AI can be used to manage machines maximize working hours. This is because machines can work 24/7 and do not take breaks like humans. For instance, AI has been used by websites, educational institutions, and customer service centers to help solve customers' issues and queries.
- **Helping in reoccurring jobs:** There are so many reoccurring jobs that humans do liking emailing, document verification, checking for errors, and so on. This task could be automated using AI and free human time for humans to engage in other less boring jobs.
- **Quicker decisions:** Through algorithms and other technological networks, AI can make decisions quicker than an average human being. Humans will need to conduct research and analysis before considering several things to reach a decision. The emotional and bias aspects will also be considered. Artificial intelligence machines work solely through their programming and reach conclusions and results without bias or emotions. For instance, games like chess-powered AI are almost impossible to beat because of the AI. It makes the best-calculated move in a short time as programmed by the Algorithms.
- **Innovations:** Artificial intelligence is enabling so many innovations in every aspect of life. It will help solve most very complex issues. For instance, artificial intelligence has been used to predict breast cancer at the earliest stages.

➢ **Disadvantages of Artificial Intelligence**

- **Expensive to create**: Artificial intelligence is a highly complex machine; this makes it highly expensive to create and costs a considerable amount to make. Aside from creating an AI, machines require maintenance from time to time. Maintenance like installing new software updates to prevent security breaches and repairing faults is usually needed. This will usually cost some more.
- **It makes humans lazy:** As a result of its ability to automate and reduce human workload, artificial intelligence has made many humans lazy. Many people have passed on their

Jobs to an AI to carry out. More tasks would be passed on to automated machines by humans as we become addicted to innovations that can solve problems and reduce the workload. This may cause problems for future generations.

- **Job loss:** As more AI is invented to handle tasks usually handled by humans, the need for human personnel reduces significantly. AI will replace most of the reoccurring, and few humans may be needed for only monitoring. Also, many organizations are open to replacing human personnel with automated machines that efficiently handle the same task. However, it would leave many unemployed and make organizations more dependent on machines in the long run.
- Lacks emotions: Emotions, in a way, bring about team connection. But unfortunately, artificial intelligence cannot have emotions for that connection even though humans perform tasks more efficiently.
- **No thinking outside the box:** Artificial intelligence performs based on its programming and algorithms. This means that they don't do anything outside their programming or the scripts. They might crash when they try to carry out an unknown operation. There are good sides and wrong sides to every invention. It is the job of whoever wants to use AI to decide whether to go on with the use by weighing the opportunities presented and the drawbacks.

Application of Artificial Intelligence and Machine Learning in Online Fake Transaction Alerting

With the advancement of technology, machine learning and artificial intelligence features in fraud detection will become possible. The artificial intelligence-enabled through the machine learning algorithms will use historical sequence and patterns of fraud-related data to detect fraud or possible fraudulent transactions.

- **Works faster:** Data processing speed and accuracy are much higher in AI and ML algorithms-enabled machines than when humans do them. Artificial intelligence and Machine Learning Algorithms can detect deep and highly sophisticated fraud patterns that humans may not detect. Fraud prevention frameworks design the codes and rules that instruct the machine learning algorithms on the types of operations that are fraudulent and non-fraudulent. It distinguishes the allowed and normal transactions from those that may be fraudulent and not allowed because they are suspicious.
- **Machine Learning Scaling**: Although it takes a lot of time to write rules and design an algorithm for artificial intelligence and machine learning. Also, the manual Ecommerce pattern of interaction is highly dynamic easily changes sharply within a short period. The application of machine learning techniques will become even more useful in detecting and learning new changes. Through Machine learning, artificial intelligence learns and develops based on received data and information. This means that the larger the volume of fraudulent data they receive and learn from, the better they get in fraud detection.
- **Efficiency:** This is, however, not applicable to systems that are rule-based as far as they don't evolve. Artificial intelligence enables machines to carry out mundane and repetitive tasks, functions like manual analysis of fraud, and allows human experts to carry out a more important task. According to research by Google Trends, using machine learning features for fraud detection is becoming increasingly popular in 2021.

Through machine learning features, the data scientist can detect fraudulent transactions and reduce false positives immensely. This method allows for automated and unsupervised pattern discovery within many connected transactions, which makes it highly effective in detecting and preventing fraud. As mentioned earlier, a well-programmed machine learning algorithm will separate the fraudulent transactions from the legitimate ones and use its machine learning feature to adapt to the new kinds of fraud schemes. This feature may become even more complex as the need for interpreting data patterns and continuously improve the ability to differentiate behaviors by applying data science (Neogy & Paruchuri, 2014). This needs many computations that must be accurately carried out in milliseconds. A computer with a bad domain understanding and lack of fraud-specific data science methods the ML algorithm can get to learn from the wrong data and information.

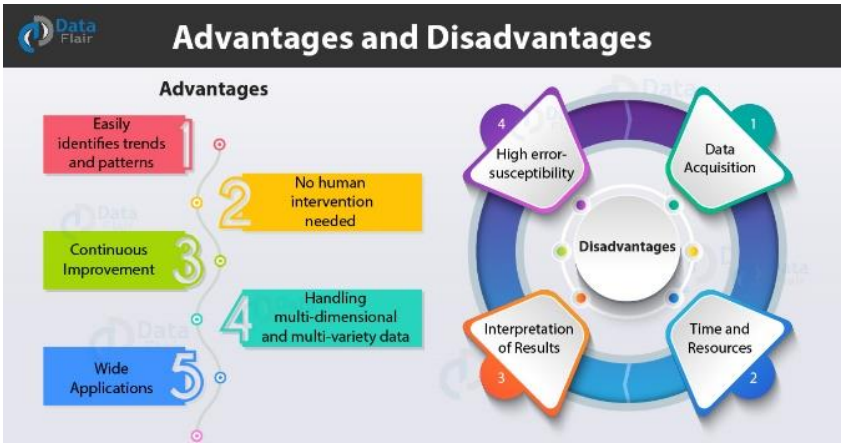

Figure 5: Advantages and disadvantages of artificial intelligence
Source: data-flair.training

Definition, Types, and Scale of Modern Fraud

With so many human activities transferring online, crime and fraud have also adapted to the digitization trend. Cyber-attacks are reported to be the fastest-growing crime in the USA, with increases in magnitude, sophistication, and cost to businesses and individuals. Some notable examples of large-scale fraud include the 2017 Yahoo hack of 3 billion accounts and the hack of Equifax compromising the data of 145.5 million customers. The volume of cybercrime-related damage is projected to rise to $6 trillion by 2021 globally, which is twice more than in 2015 ($3 trillion).

Cyberattacks are varied in manifestations, commonly including attacks with ransomware and malware, identity theft, violation of privacy, weapons, and drug sales online, and data theft, leakage, and intellectual property hacks. Most cybercrime is conducted on social media, giving $3.25+ billion in revenues to criminals every year. In 2019 alone, 85% of business organizations reported detecting phishing or social engineering threats, while another 75% of organizations are afraid of insider threats as a significant fraud risk.

The most alarming about fraud is that it may take too long to detect it. In the financial institutions conducting most of their operations offline, fraud detection may take 40+ days, leaving zero chances for criminals' identification and funds' recovery.

Figure 6: ML in fraud Detection
Source: sdk.finance

a) How Can You Apply Machine Learning for Fraud Detection?

The logic underlying the use of AI for fraud detection is simple. At the same time, machines are known to be capable learners. They may be taught based on the historical fraud protocols to identify suspicious user behavior suggesting fraud and anticipate fraud efforts before the actual attack occurs. In other words, ML helps data scientists determine potentially fraudulent transactions, thus helping to minimize the number of successful attacks. The benefit of ML for this purpose is its ability to discover fraud patterns across huge masses of streaming transactions in an automated way without human guidance. Moreover, with more data becoming available, machines learn to make subtle distinctions and adopt more sensitive and sophisticated fraud detection algorithms.

b) Machine Learning vs. Rule-based Systems in Fraud Detection.

Before ML fraud detection tools emerged, the rule-based approach was a dominant fraud identification and prevention method. It presupposes the use of 300+ explicit scenarios for detecting evident fraud signals and issue alerts to block such transactions. Despite the broad spectrum of fraud detection scenarios, it results in user dissatisfaction with numerous verification steps, unable to process masses of data in real-time.

Rule-based vs ML-based Fraud Detection Systems

Rule-based fraud detection	ML-based fraud detection
Catching obvious fraudulent scenarios	Finding hidden and implicit correlations in data
Requires much manual work to enumerate all possible detection rules	Automatic detection of possible fraud scenarios
Multiple verification steps that harm user experience	The reduced number of verification measures
Long-term processing	Real-time processing

Figure 7: Rule based vs ML Basd Fraud detection Systems (Source: sdk.finance)

In contrast to the rule-based method that works quite rigidly regarding fraud detection and analysis, ML techniques introduce quicker, automated processing of a much larger number of fraud scenarios. Besides advanced computational speed and real-time big data

processing, ML systems enable better user experiences with smaller verification steps and learn to identify even hidden or implicit fraud signals. Thus, ML systems are better equipped to work with ambiguous data that rule-based algorithms will not detect.

HOW TO DETECT FRAUD USING MACHINE LEARNING?

Understanding how ML enables a fraud detection dataset is impossible without learning the fraud-specific data science techniques (Donepudi, 2014). Otherwise, ML may go in the wrong direction, failing the initial task of fraud detection and letting fraudulent activities pass unnoticed. Here are some popular approaches to designing ML-enhanced fraud detection tools.

- **Cohesive integration of supervised and unsupervised AI models into an ML fraud detection algorithm.** Supervised models learn efficiently if they have a mass of tagged transactions based on which they tag new transactions as malicious or non-malicious. Unsupervised models are useful in cases with non-existent or scarce tagged data because of their profound self-learning ability.
- **Application of behavioral profiling and analytics in the ML systems for fraud detection.** Behavioral analytics is a helpful approach to fraud prevention and detection. ML systems store and analyze data about transaction participants' behaviors, including merchants, individuals, accounts, and devices. The behavioral profiles of each are updated upon each successive transaction, enriching the database, and making the prediction of fraud more precise.
- **Use of large datasets for AI model development.** Evidence proves that the volume of data available for machines to initiate sufficient ML is the most crucial success factor. Thus, by feeding more data into the system, you can increase its predictive accuracy. The process works similarly to the physical training of people; the more they are exposed to identical exercises, the more endurance and precision they exhibit each new time. The same goes for machines able to refine their fraud detection alerts and become more sensitive to detect even non-evident, new kinds of fraud.
- **Integration of self-learning AI with the help of an adaptive analytics setup.** The bonus of adaptive analytics is that of refining the algorithms upon every successful fraud detection case. In such a way, the AI system becomes more complex and dynamic, evolving with the changing fraud patterns and approaches. As a result of self-learning and adaptation, ML enables machines to make more precise decisions in marginal cases.
- **Machine Learning in Fraud Detection: Industry Experience.** Fraud identification has become imperative not only in traditional commercial spheres such as e-commerce or banking. It has gone far beyond economics, reaching such aspects of human lives as medical care, insurance, and personal data. When personal data becomes the most asset, fraud detection with sophisticated (and continually improving) algorithms is imperative to meet the challenge of the coming years – the rise of cybercrime. Here are some industry experiences regarding fraud detection and failures within the past years in the healthcare, banking, and e-commerce sectors – the ones most exposed to cybercriminal activities.

a) Fraud detection for medical claims and healthcare

Manipulations with healthcare insurance are the most common type of fraud in this sector, mainly because of the bureaucracy and complexity of the healthcare system. Criminals can steal money by:

Making false claims

- Sending duplicate claims
- Exaggerating the cost of medical coverage
- Including unnecessary tests or a wrong diagnosis into the claim

ML systems can help detect fraud in the medical/healthcare sector through:

- Identifying the upcoding of procedures by automatic identification of unexpected digits in the datasets
- Automatic reconciliation of bills for fake bill total prevention
- Improving personal identity verification procedures with the help of smart image recognition techniques

b) Fraud detection in banking and credit card payments

While customers strive for greater mobility and accessibility of payments, such simplified verification inevitably causes greater vulnerability to cyber-fraud. ML systems offer several intelligent solutions for the banking industry, such as:

- Automated data credibility assessment by comparing historical transaction data with each new transaction's elements.
- Elimination of duplicate transactions.
- Blockage of account theft attempts.
- Alerts about potentially fraudulent, suspicious activities.
- Fraud prevention in e-commerce

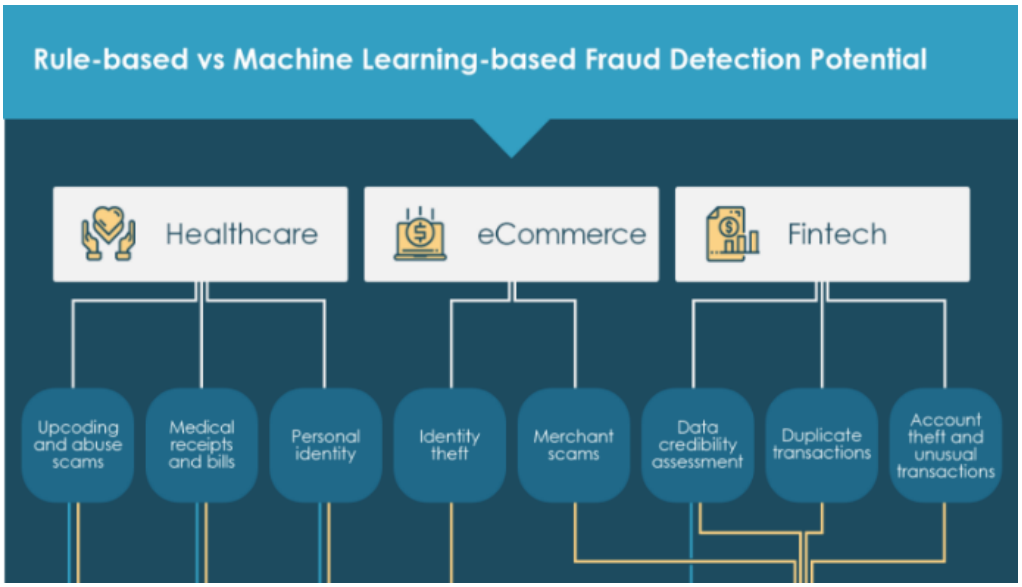

Figure 8: Fraud detection (Source: bitcoininsider.org)

Ecommerce fraud prevention has a long history of development, given that this sector is directly linked to financial transactions. Here, the two most popular fraudulent schemes include identity theft and scams. In both cases, the customer is a victim of fraud as their data

are compromised, and money is stolen, either via a fraudulent merchant scheme or directly from a bank account. Ecommerce fraud prevention techniques are sensitive to the type of offense. For instance, identity theft is prevented via ML with the help of behavior analytics. ML systems develop smart algorithms for dubious activity identification and compare historical and current data during any transaction's initiation, completing it only after obtaining a positive comparative outcome. Merchant scams can also be identified with the help of behavior analytics that locates suspicious activities and alerts users about the merchant's doubtful reputation.

Machine learning is part of artificial intelligence components where machines can learn automatically from input and output data and find a way to adapt to new data. Machine learning brings AI machines to a point where they no longer need human interference. A subset of machine learning, deep learning copies the working pattern of the human brain. It processes the data and creates patterns for actions. Deep learning in AI, the system gathers data and learns about the data automatically without human assistance. These data are random or already in patterns. Deep learning is also called Deep Neural Network (DNN).

CONCLUSION

The potential of Machine learning and artificial intelligence is vast today; some vivid examples of how they work in everyday human lives include the use of Alexa, traveling with Uber, and dealing with digital education. A vivid example of how far the Machine learning and AI process can go is the AlphaGo Zero machine that learned to play checkers by playing with itself and soon surpassed the top human talent in playing this game. These examples show that machines can learn infinitely, with ML applications limited only by human imagination. The potential application of this unique technologies in fraudulent transaction detection will go a long way in limiting the impact of fraud. It would improve user trust in the system as well. Artificial intelligence and machine learning processes will grow beyond current day application.

REFERENCE

Bynagari, N. B. (2014). Integrated Reasoning Engine for Code Clone Detection. *ABC Journal of Advanced Research*, *3*(2), 143-152. https://doi.org/10.18034/abcjar.v3i2.575

Donepudi, P. K. (2014). Voice Search Technology: An Overview. *Engineering International*, *2*(2), 91-102. https://doi.org/10.18034/ei.v2i2.502

Neogy, T. K., & Paruchuri, H. (2014). Machine Learning as a New Search Engine Interface: An Overview. *Engineering International*, *2*(2), 103-112. https://doi.org/10.18034/ei.v2i2.539

Paruchuri, H. (2015). Application of Artificial Neural Network to ANPR: An Overview. *ABC Journal of Advanced Research*, *4*(2), 143-152. https://doi.org/10.18034/abcjar.v4i2.549

Taher-Uz-Zaman, M., Ahmed, M. S., Hossain, S., Hossain, S., & Jamal, G. R. A. (2014). Multipurpose Tactical Robot. *Engineering International*, *2*(1), 21-27. https://doi.org/10.18034/ei.v2i1.204

Vadlamudi, S. (2015). Enabling Trustworthiness in Artificial Intelligence - A Detailed Discussion. *Engineering International*, *3*(2), 105-114. https://doi.org/10.18034/ei.v3i2.519

--0--

Online Archive Link: https://abc.us.org/ojs/index.php/ei/issue/archive