International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

Fraud Detection in Banking Transactions Using Machine Learning

M. Pooja
Deparment of Computer Science Engineering (AI & ML),
CMR Engineering College, Hyderabad, Telangana, India

A Venkat Koushik
Deparment of Computer Science Engineering (AI & ML),
CMR Engineering College, Hyderabad, Telangana, India

Abstract: Fraud in banking has been around for a long time. It started a time ago back in the 19th century when people made fake checks and fake documents that caused problems for banks. Now we are in an age and fraud is a big problem. Every year people lose a lot of money because of fraud. The losses are huge over 30 billion United States Dollars. This happens around the world. When people do banking transactions the losses can get even bigger. Fraud, in banking transactions is an issue that people should be aware of. Banking transactions can be risky because of fraud. The number of transactions is going up. This will make the industry figure go up too. Reports are saying that the transactions figure will be than 30 billion United States Dollars all around the world. This is a deal for the transactions industry because the number of transactions is really increasing. The transactions are getting bigger and bigger every day. This means that the transactions industry will get a lot bigger. The figure, for the transactions industry will be very high because of all the transactions that are happening.

As things get more digital lots of places are using automated detection mechanisms. The old ways of doing security like following a set of rules do not work well when things change. These old methods also miss a lot of threats. It is the same with systems that only use one way of doing things. These security methods and systems that only use one way do not change so they cannot find threats as they come up. Automated detection mechanisms and security methods, like these have to deal with evolving threats so it is a problem that these systems do not adapt and they cannot capture evolving threat patterns of automated detection mechanisms.

Fraud schemes can be really tricky to catch. The ways we try to detect fraud schemes can miss signs of new fraud schemes, which means we get a lot of wrong answers. This is a deal because it means fraud schemes can go on without being detected.

The methods we use to detect fraud schemes are not always right. Sometimes they say something is fraudulent when it is not or they say something is safe when it is really a fraud scheme. This happens a lot, with fraud schemes. Fraud schemes can go undetected. That is a problem. The methods we use to detect fraud schemes need to be able to catch fraud schemes. Fraud schemes are ways that people try to cheat others. These schemes can be very tricky and tough to figure out. That is why you need to be really careful and watch out for any signs of fraud. Fraud schemes are an issue. Emerging fraud schemes are particularly bad because they can get you into a lot of trouble. Emerging fraud schemes are the ones that you have to worry about the most because emerging fraud schemes can cause a lot of problems.

Learning rates are really important. We have a big problem to solve when it comes to learning rates.

One way to deal with this problem is to use a solution that combines machine learning approaches and other machine learning approaches.

This solution uses machine learning techniques and other machine learning techniques to perform fraud detection in an effective way when it comes to fraud detection and machine learning techniques.

Machine learning is used to find transactions that do not seem right. When you try out machine learning on a set of data you get a model that is really good at finding suspicious transactions. This model gets it 98 percent of the time which is very good. The system that uses machine learning is also very good, at dealing with information to detect fraud. Machine learning helps the system to find fraud cases.

The system is a web site that people can use. It lets people log in. It watches what is happening with transactions right now.

The web site does a lot of things like checking who the users are and watching what is happening in time so it knows what people are doing as they do it.

The web application is really complete. It gives users these things in a way that is helpful, for the web application users.

By comparing a suite of algorithms such as Random Forest, XG-Boost, and others, the study sheds light on the most effective techniques while also exposing their limitations. The study clearly demonstrates the need to move away from outdated methods and adopt advanced approaches to ensure safety. Advanced methods are essential for safeguarding the integrity of modern banking transactions.

Keywords: Machine Learning, Fraud Detection, Banking Security, Supervised Algorithms, Transaction Analysis.

1. INTRODUCTION

Fraud spotting in bank dealings matters more every day, not just to money handlers but also to people who own accounts. As

Folks now spend more time buying things online, thanks to how fast digital money moves. Banking apps help people pay without cash, making it smooth to shop from phones. Easier access means more clicks than trips to stores.

Folks now handle money stuff online without thinking twice - phones make it happen fast. Transactions slide through apps like notes passed in class, quiet but constant.

Fear grows when scams spread fast, messing with trust in digital cash moves. People start doubting every tap and swipe on their phones.

Shopping and managing money from home now happens more often because banks and stores moved online. Yet criminals found new ways to trick others using those same tools like phone payments and digital accounts.

Hard for old systems to spot money crimes fast. This work tries something new about catching fraud in banks

Something people talk about is using machine learning for handling transactions. This means letting smart algorithms take charge of certain tasks. These systems learn patterns instead of following fixed rules. Tasks that once took time now happen faster because of them. Automation comes into play without someone watching every step. Decisions get made based on past data rather than guesses. The whole process changes how payments move behind the scenes. Efficiency shows up where delays used to be common. Systems adapt when new transaction types appear over time. What seemed complex becomes routine through repetition.

Faster deals happen when machines learn what to do

Faster computers spot odd patterns before trouble shows up

Finding new paths through data, machine learning shapes how deals move today. Ways to improve exchanges appear when systems learn over time. Future swaps between parties will quietly rely on these patterns. While it does many jobs, shifting how we handle payments stands out clearly.

Fraudulent banking moves show up fast - systems spot them instantly, then block access before damage spreads. Alerts trigger when odd patterns emerge, stopping theft mid-step. Real-time checks run nonstop, cutting risks as they happen.

This work focuses on methods tied to teaching computers how to decide. One part deals with sorting data into groups, another spots odd patterns that do not fit. Learning happens as systems adjust through examples. At its core, it explores tools such as grouping setups and finding irregularities - ways machines grow smarter by doing tasks over time.

What makes this work is how it leans on classification models - those tools from machine learning. Important? Absolutely, they’re central to what happens here. Getting things finished relies heavily on them, truth be told.

A twist happens when patterns break - machines notice. Spotting odd behavior? That task often lands on algorithms. Unusual means stand out, so systems flag them fast.

Machine learning guides how the system works. Supervised learning fits into that mix. It belongs among the methods shaping the outcome. These approaches matter, with supervision playing its role quietly.

What drives the project? Machine learning methods. These shape how things move forward, nothing else. Methods that learn from data - those are central. They aren’t just tools; they’re the core of what happens here.

Looking back at old transactions helps spot unusual activity. These systems learn what fraudulent behavior looks like over time. Instead of reacting after the fact, they predict risks before damage occurs. Patterns emerge when similar cases repeat across months. One sign alone might mean nothing. Yet together, small details build a clearer picture. Machines notice what humans often miss. Over time, accuracy improves with more examples. Past mistakes guide future corrections. Recognition grows sharper with each update

Something spots odd payments, then signals the bank to take a closer look. When unusual activity shows up, the bank receives a notice right away. Checks happen faster because updates come through automatically. Alerts pop up if anything stands out during regular flows. Banks stay aware thanks to constant updates on payment patterns.

Looking back at old financial records is what this work focuses on. One tool used here includes decision trees - these help sort patterns out. Instead of guessing, systems like support vector machines step in to clarify things. Other algorithms join them, working behind the scenes without drawing attention. Each model plays its role quietly within the bigger effort.

Patterns tied to fraud get picked up by neural networks. Because these systems study data, they start recognizing odd behavior. Suspicious actions stand out once the model has learned what to look for. As training progresses, spotting irregularities becomes more accurate. What makes them effective is how they adapt through examples. Over time, alerts go off when something feels off based on past cases.

Spotting shady deals might get easier when machines take over, cutting down mistakes people often make. That app

Working well comes from how fraud detection systems are set up, even if accuracy does not always improve. Efficiency shows up when they fit into larger setups. These tools matter a lot once you see where they operate. Helping them adapt changes what they can do. Companies rely on such systems more than expected these days.

Handling many transactions fast matters for organizations. Yet security cannot take a back seat when moving quickly. Staying safe while scaling up is part of the task. This work ties directly into how those groups operate. Their ability to perform gets support through this effort.

Finding ways to catch dishonest actions comes down to using information wisely. A system built on facts can cut down on lost funds, quite effectively. Stopping theft before it grows turns out to be the core reason behind such tools. Preventing loss isn’t just helpful - it shapes how these methods evolve.

Finding fraud means checking data carefully. It needs tools that watch patterns closely. Spotting odd details helps catch problems early. This kind of work relies on steady observation.

Hidden signs often show up in how numbers behave. Watching those shifts makes a difference. Results depend on consistent tracking over time

Fraud detection aims to cut down on losses, making it easier to spot issues early. Still, success depends on how well systems adapt over time.

Aim high when spotting fraud - catching it fast means less money lost. Success shows up in fewer scams slipping through. Focus stays sharp because the target never moves. Wins come quietly, one alert at a time.

Falling numbers hit both lenders and those who rely on them.

A fresh approach begins here: building a tool trained to spot odd moments in bank activity. Not every transfer fits the pattern - some slip sideways. Machines learn what looks wrong, then act. Watching numbers closely means catching tricks early. Banks gain quiet helpers that never blink. Learning keeps growing as new moves appear. Hidden signals rise into view. Protection shifts from slow checks to smart watches. Money flows safer when eyes are sharp.

A collection of data pulled from Kaggle set the stage. Different methods guided by labeled examples took shape - among them, Support Vector Machine made an appearance. Each approach followed its own path through the numbers

Logistic Regression Decision Tree Gradient Boosting Ada-Boost, XG-Boost ,Random Forest, K Nearest Neighbors.

A fresh look at KNN begins here. One goal stands out - spotting payments gone wrong. Instead of guessing, tests show how well it catches shady deals. Watching each move helps measure true performance. What fits one case might fail another. Results come from real checks, not theories. Every trial tweaks the approach just a bit. Outcomes shift when conditions change slightly. Pay attention to getting things right most of the time.

2. PURPOSE OF THE PROJECT

One goal behind the project "Fraud Detection in Banking Transactions using Machine Learning" sits in building a smart, automatic setup that spots fake moves in bank activity - fast and right. Digital money actions grow. So do clever tricks used by scammers aiming at weak points regular checks miss. Instead of sticking to old methods, this work turns to machine learning tools digging into huge piles of past deals, sniffing out signs something's off. These models learn from years of records, getting sharper over time. They change shape when new cheating styles pop up, staying one step ahead simply by watching what came before. Aiming to cut down hours lost to hand-checking payments, this work targets fewer errors in spotting shady deals. Real threats get caught faster because smart software learns how scammers shift tactics over time. Legit moves stay under less suspicion when systems stop misreading them as risky. Banking walls grow tougher right when hackers probe harder. Customers gain quieter minds knowing cash moves safely behind digital locks. Alerts pop up quicker than before thanks to live monitoring loops built into daily operations. Money trails once hard to trace now show red flags earlier in the game. Fewer mistaken alarms mean staff focus energy where it counts most. Risk levels dip not just in theory but on front-line screens too. One way the system gets better at spotting issues is by using many different models, so banks can act quickly when something looks off. Because it puts all algorithms on the same playing field, comparing them becomes straightforward - making it easier to pick the best one for each job. From pulling in raw information to showing clear visuals at the end, every stage fits together without gaps. Instead of staying fixed, the setup learns from fresh examples over time, shifting as scams change shape. With updates built into its routine, the tool doesn’t fall behind even when tactics grow sneakier

3. EXISTING SYSTEMS AND THEIR DISADVANTAGES

Back when banks first started spotting shady deals, they leaned on fixed rules. Such setups mark odd moves by checking against a list of do-not-do’s. Yet spot-on though they might be for clear-cut scams, sneaky new tricks often slip through. True, those old-school filters did help at the start. Still, today’s sharper fraud finds ways around rigid checklists too easily. One big issue with rule-based setups? They struggle when scams get tricky or shift over time. Since crooks keep changing how they operate, rigid rules can’t keep up fast enough. Take fake identities or sneaky takeovers of accounts - these slip through until someone writes fresh rules. Imagine a scammer testing an account with tiny purchases that look harmless; the system ignores them since those actions aren’t on its checklist. When tricks evolve, old rules lose power. Staying current means constant updates, which takes serious effort and time. A single misstep in judgment can trigger alerts where none are needed. When rules stick too closely to fixed limits, normal activity slips through cracks and gets labeled suspicious. Transactions that fall outside routine habits - like buying something big or spending overseas - are often caught in the net. Legitimate actions mistaken for fraud cause holdups, frozen access, or extra checks just to prove nothing's wrong. Customers face hassle without reason, simply because their behavior changed slightly. Banks spend time untangling cases that never should have been raised. A trip abroad could set it off, even when everything is above board. A large number of incorrect alerts creates real problems - not just for the bank, but also for people using it. Delays happen. Lives get disrupted. Sometimes access to money stops completely while checks take place, leaving users annoyed and less likely to trust the service. Staff must step in, one by one, reviewing every alert that pops up, which eats up hours and adds pressure on teams already busy. Because older rule-driven tools often miss the mark, employees end up doing much of the work by hand. Each case needs attention, paperwork, follow-up, stretching out the process longer than needed. Delays pile up when spotting fraud takes too long, leaving room for more damage before anyone notices. Sluggish methods stretch out checks done by hand, widening gaps where scams slip through unseen. People handling these tasks get stretched thin, particularly as transaction numbers climb higher each day. Digital banking keeps growing, pushing institutions to juggle ever-larger flows of activity and information. Handling every odd-looking case without help isn’t practical anymore - speed and size have changed the game completely. More people want smarter tools because old methods struggle today. Since basic rules fail under heavy transaction loads, better options are needed. Instead of sticking to rigid setups, many now turn to systems that learn on their own. These models adjust quickly when scams change shape. They handle huge amounts of data without constant human help. Accuracy improves when machines spot suspicious behavior early. As tricks get sneakier, outdated checks fall behind. Automated approaches catch what rules miss. Security gets stronger while users feel safer. Better detection doesn't just block fraud - it builds trust over time. Out there, older setups just lag behind when faced with today's flood of bank transactions, both in number and type - so scams slip through, honest users get flagged. A different path emerges when machines learn from masses of info, spotting tangled clues people often miss. Imagine noticing a shift - a sudden purchase far away, spikes in activity at odd hours, rhythms gone out of sync - all signs a smart tool might catch fast. Change comes alive as these tools adapt on their own, minute by minute, learning fresh tricks crooks invent before rules can be rewritten. Speed shows its face again when mountains of records get sorted in moments, decisions made sharp and right, cutting delays dead. Banks face growing piles of data, constant streams of transactions, sudden spikes in user demands - so smart tools that learn on the fly now matter more than ever. These systems spot suspicious activity faster, hit fewer dead ends, work without slowing things down. Accuracy climbs when algorithms adapt instead of sticking to old rules. Fewer mistakes mean less frustration, smoother experiences for people using their accounts daily. Trust builds quietly when problems vanish before they start. Security tightens not through force but by staying one step ahead. Efficiency gains aren't just numbers - they shape how safe users feel. A single slip can shake confidence, so getting it right matters beyond code and servers.

Disadvantages:

One downside? They're too stiff to catch fresh tricks fraudsters come up with. Because rules stay fixed, real purchases sometimes get stopped - slowing things down for users and banks alike. Every red flag needs a person to check it out - a slow process that eats up staff hours without pause. When scams mix several steps or fake identities, these setups usually miss the signs completely. Changing rules all the time and paying for extra checks adds up fast in daily running expenses. When transaction numbers climb, rule-driven setups slow down, becoming clunky to handle, which complicates spotting fraud across big operations. Instead of tapping into broad information pools, these systems stick to narrow inputs, skipping deeper patterns hidden in richer, varied records.

developing Intelligent Tutoring Systems. Neural networks can also be used in automated grading systems and virtual labs, and are advantageous for their ability to provide accuracy and adaptability over more traditional methods. Additionally, neural networks can process data types that were previously unavailable to educators in the form of datasets of greater complexity (e.g., video files, images, etc.) [1][2].

4. PROPOSED SYSTEM AND ITS ADVANTAGES

One way to tackle fraud better is through smarter software that learns from past data. Instead of relying on old rules, this method uses real examples of bank activity pulled from a public source online. What stands out is how it tests many smart models at once - ones with names like Decision Tree, XGBoost, or Logistic Regression. Each model sees the same numbers but finds its own clues in things like transfers, account totals, and odd flags. Some spot sneaky changes fast. Others catch slow leaks others miss. Together they cover more ground than any single one alone. Accuracy matters because mistakes can wrongly accuse honest users. The trick lies in catching cheats without troubling regular customers. Patterns shift when crooks adapt. Good systems must keep pace quietly. Models trained together often see what one might overlook. Results show some learn faster. Others stay steady under pressure. Working hand in hand, these methods lift both precision and reliability when spotting fraud. Instead of just piling up data, careful steps like rebalancing and transforming values help the system respond fairly to different kinds of transactions. A structure built around user roles shapes how people interact - admins get deeper tools, while everyday users see only what matters most. As scams shift over time, constant observation paired with routine updates keeps the model sharp and ready. It learns fresh tricks without losing past knowledge. Better results come from smarter math behind the scenes - machine-driven choices beat rigid rules every time when catching suspicious behavior. Fewer mistakes spotting fraud: This setup works to catch only real threats, so normal purchases do not get wrongly stopped. Not stuck in old ways: Instead of fixed rules, it learns new tricks scammers use, catching fresh kinds of scams others miss. Stays current without help: Because it checks itself often and updates its knowledge, it keeps pace with how fraud changes over time. Handles messy data well: It uses smart sorting and coding methods to manage uneven datasets, letting every kind of payment get fair analysis. Grows when needed: Built to manage huge amounts of payments daily, it scales smoothly as bank activity increases. Clear dashboard for everyone: Admins get deep tools, regular staff see clean views, shaped by who is logging in. Less human work required: Machine smarts take over most checking, cutting down on slow hand reviews and saving effort for tougher jobs.

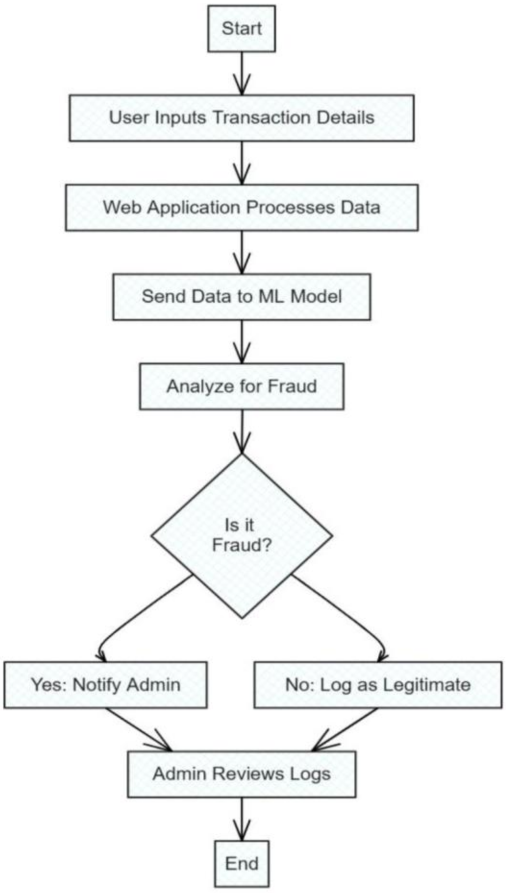


Fig: Simple Activity Diagram of Fraud Detection

5. RESULT

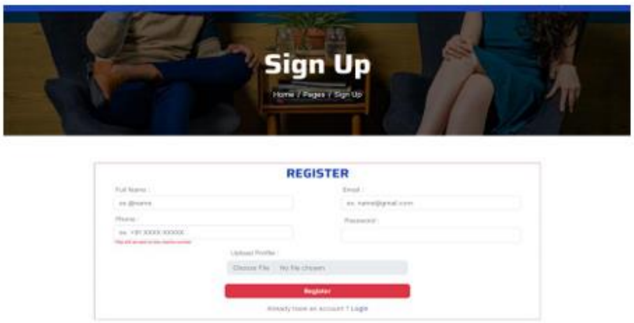


Fig: Sign Up Page

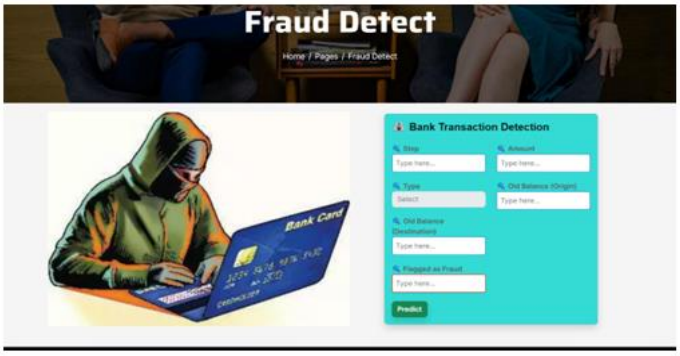
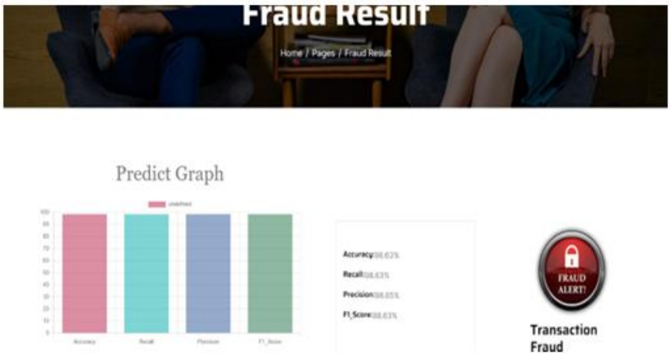


Fig: Bank Transaction Detection Page



Accuracy:98.63%
Recall:98.63%
Precision:98.65%
F1_Score:98.63%

Fig: Fraud Result Prediction Graph

6. CONCLUSION

Out in front, old-school fraud rules start to lag when scams shift shape overnight. Machine smarts jump into the gap, learning patterns while staying sharp through constant change. Instead of one-size-fits-all models, stacking different learners brings better results - especially after cleaning and shaping data just right.

Built from the ground up, the app gives power users and staff alike a clear view, making it easier to spot odd behavior fast. At the back end, structure matters; decisions get support before things spiral. Even with stubborn problems like overfitting, too many false alarms, or growing pains, this method steps out of old routines into something flexible, shaped by real data flow. Close to 98 percent precision shows it works - wildly complex information becomes manageable. What counts most? Cutting fraud losses right now while slowly rebuilding confidence in how money moves online. Thanks to smart spotting tools paired with designs that actually consider people, banking shifts toward being clearer, less risky. The result feels steady, grounded, not flashy but reliable.

REFERENCES

[1] Sharma and V. Gupta, “Comparative Analysis of Machine Learning Techniques for Fraud Detection,” IEEE Access, vol. 8, pp. 206347–206359, 2020.

[2] J. Liu, C. Ma, and R. Zhao, “Gradient Boosting in Financial

Fraud Analytics," in Proc. IEEE Int. Conf. Big Data, 2021, pp. 984–990.

[3] D. Martins, F. Santos, and B. Jones, "Performance Assessment of KNN in Real-Time Transaction Monitoring," IEEE Trans. Knowl. Data Eng., vol. 35, no. 2, pp. 223–235, 2023.

[4] R. Sundaram, V. Pillai, and A. Rao, "Deep Autoencoder Approaches to Fraud Detection in Financial Transactions," IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 2, pp. 754–763, 2023.

[5] L. Williams and T. Carter, "Privacy-Preserving Techniques in Financial Fraud Detection," IEEE Trans. Inf. Forensics Security, vol. 18, pp. 345–358, 2023.

[6] T. Ogawa, S. Kim, and H. Nishimura, "Adaptive Drift Detection for Evolving Fraudulent Activities," IEEE Access, vol. 11, pp. 99320–99334, 2023.

[7] F. Navarro and L. Chen, "AdaBoost-Based Money Laundering Detection in Banking Flows," in Proc. IEEE Symp. Security and Privacy, 2022, pp. 556–563

[8] T. Johnson and C. Rhodes, "Machine Learning for E-Commerce Fraud: A Comparison of Decision Tree vs. XGBoost," IEEE Access, vol. 10, pp. 11246–11257, 2022.