IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# ATM FRAUD TRANSACTION WITH USER BEHAVIOUR PATTERN

**KAMAL NATH.T, JEEVAKUMAR.S**

**STUDENT PG & RESEARCH DEPT OF COMPUTER APPLICATIONS**

**HINDUSTHAN COLLEGE OF ARTS AND SCIENCE, COIMBATORE, TAMIL NADU.**

## ABSTRACT

Banking quarter has been a essential organization that contributes immensely to the sustainability and preservation of the financial system in any country the instances attributed to financial institution transaction may be bad whilst infused with the aid of using intruders or fraudsters fraud detection in on line banking transactions along with in automated teller machine atm is one of the crucial techniques applied with the aid of using banks to defend customers account fraud detection calls for numerous investments complicated algorithms schooling and testing algorithm which offers out behavioural profiling of the person financial institution account and transactions the generalization and category cappotential glad handiest at 73 degree of fraud analysis fraudsters have untiring instances making unlawful moneys at the same time as the recommend set of rules on this paintings will fight maximum efforts of illegalities concerning finances with the aid of using digital facts processing edp withinside the banking quarter this could be finished with the aid of using facts mining the bio-facts aleven though biometric combinational operations on the preliminary beginning of the money owed and as such will conform with the set of rules proposed the paper labored cautiously the usage of the present literatures and structures to mix the processes of biometric to the already present ones and creating a entire thought for a layout of atm enginethe proposed device with stpm suggests out a specific category amongst uncommon quantity of edp facts with a degree of 93 of accuracy the sequential extraction marked out every and each transaction proceeded and proven out correctly

## I. INTRODUCTION

Banks and financial institutions often use machine learning algorithms to monitor user activity on their ATM network, looking for patterns that may indicate fraud. Some examples of user behavior patterns that may indicate fraudulent activity include:

1. Abnormal withdrawal quantities: Frequent withdrawals of surprisingly big quantities of coins might also additionally suggest that a fraudster is attempting to withdraw as lots cash as feasible earlier than the account is flagged or the cardboard is blocked.

- Abnormal withdrawal quantities may be a crimson flag for ATM fraud due to the fact fraudsters might also additionally try to withdraw as lots cash as feasible earlier than the account is flagged or the cardboard is blocked. Fraudsters regularly use stolen or counterfeit playing cards to withdraw coins from an ATM, and they'll try and withdraw big sums of cash in a quick time frame earlier than the financial institution or the cardholder turns into privy to the fraud.
- Banks and monetary establishments might also additionally screen ATM transactions for odd withdrawal quantities as a part of their fraud detection and prevention strategies. If a withdrawal quantity exceeds a positive threshold, the transaction can be flagged for similarly research or declined altogether. Additionally, clients can be capable of set withdrawal limits on their ATM playing cards to save you big unauthorized withdrawals.
- It's vital to word that odd withdrawal quantities by myself do now no longer always suggest fraud. There can be valid motives why a consumer wishes to withdraw a big sum of money from an ATM, together with a deliberate buy or an emergency situation. However, whilst odd withdrawal quantities are mixed with different suspicious behaviors, together with uncommon transaction instances or locations, they'll suggest that fraudulent interest is taking place.

2. Unusual transaction instances: Transactions that arise out of doors of a patron's ordinary transaction instances or styles may also imply fraudulent hobby.

- Unusual transaction instances or styles may be some other crimson flag for ATM fraud. Transactions that arise out of doors of a patron's common transaction instances or styles may also imply that a person apart from the account holder is the usage of the ATM card, along with a fraudster who has received the cardboard via robbery or hacking.
- Banks and economic establishments may also display ATM transactions for uncommon transaction instances or styles as a part of their fraud detection and prevention techniques. If a transaction happens at a time or vicinity this is uncommon for the account holder, the transaction can be flagged for similarly investigation. Additionally, clients may also get hold of indicators for transactions that arise out of doors in their ordinary

styles, such as though a transaction happens at an uncommon time of day or in a vicinity that they've in no way visited before.

- It's crucial to observe that there can be valid motives why a patron's transaction instances or styles may also change. For example, a patron can be journeying to a brand new vicinity or may also want to withdraw coins at an uncommon time because of an emergency. However, while blended with different suspicious behaviors, along with unusual withdrawal quantities or a couple of transactions in a brief time period, uncommon transaction instances or styles may also imply that fraudulent hobby is taking place.
- To defend towards ATM fraud, clients can take numerous steps, along with frequently tracking their account hobby, placing withdrawal limits on their ATM playing cards, and retaining their ATM playing cards and PINs secure. If clients observe any suspicious hobby on their accounts, they need to right now touch their financial institution and record the difficulty.

3. Unusual transaction places: Transactions that arise in places which are uncommon for the patron, along with some other nation or country, may also imply fraudulent hobby.

- Unusual transaction places also can be a signal of ability ATM fraud. Transactions that arise in places which are uncommon for the patron, along with some other nation or country, may also imply that a person apart from the account holder is the usage of the ATM card.
- Banks and economic establishments may also display ATM transactions for uncommon places as a part of their fraud detection and prevention techniques. If a transaction happens in a vicinity this is uncommon for the account holder, the transaction can be flagged for similarly investigation. Additionally, clients may also get hold of indicators for transactions that arise in places that they've in no way visited before.
- It's crucial to observe that there can be valid motives why a patron's ATM card can be utilized in an uncommon vicinity. For example, a patron can be journeying for enterprise or excursion and want to withdraw coins from an ATM in some other nation or country. However, while blended with different suspicious behaviors, along with unusual withdrawal quantities or a couple of transactions in a brief time period, uncommon transaction places may also imply that fraudulent hobby is taking place.
- To defend towards ATM fraud, clients can take numerous steps, along with frequently tracking their account hobby, placing withdrawal limits on their ATM playing cards, and retaining their ATM playing cards and PINs secure. If clients observe any suspicious hobby on their accounts, they need to right now touch their financial institution and record the difficulty.
- 4. Abnormal transaction frequency: Frequent transactions or a couple of transactions in a brief time period may also imply fraudulent hobby.

- Abnormal transaction frequency also can be a crimson flag for ability ATM fraud. Frequent transactions or a couple of transactions in a brief time period may also imply that a person apart from the account holder is the usage of the ATM card.
- Banks and economic establishments may also display ATM transactions for unusual transaction frequency as a part of their fraud detection and prevention techniques. If there are too many transactions taking place in a brief time period, or if there are numerous transactions in a unmarried day, the transactions can be flagged for similarly investigation.
- It's crucial to observe that there can be valid motives for a patron to make common transactions or a couple of transactions in a brief time period. For example, a patron can be chickening out coins for a particular purpose, along with a huge buy or to pay for a couple of bills. However, while blended with different suspicious behaviors, along with uncommon transaction instances, uncommon transaction places, or unusual withdrawal quantities, common or a couple of transactions may also imply that fraudulent hobby is taking place.
- To defend towards ATM fraud, clients can take numerous steps, along with frequently tracking their account hobby, placing withdrawal limits on their ATM playing cards, and retaining their ATM playing cards and PINs secure. If clients observe any suspicious hobby on their accounts, they need to right now touch their financial institution and record the difficulty.

5. Transactions that arise after a card has been mentioned misplaced or stolen: Transactions that arise after a patron has mentioned their card misplaced or stolen may also imply that a person else is the usage of the cardboard.

- Transactions that arise after a card has been mentioned misplaced or stolen may be a clean indication of ability ATM fraud. When a patron reviews their card misplaced or stolen, the financial institution will generally block the cardboard to save you unauthorized transactions. If transactions arise after the patron has mentioned their card misplaced or stolen, it is able to imply that a person else is the usage of the cardboard.
- Banks and economic establishments may also display ATM transactions for transactions that arise after a card has been mentioned misplaced or stolen as a part of their fraud detection and prevention techniques. If transactions arise after the cardboard has been mentioned misplaced or stolen, the transactions can be flagged for similarly investigation.
- To save you ATM fraud withinside the occasion of a misplaced or stolen card, clients need to right now touch their financial institution to record the difficulty and feature their card blocked. Customers need to additionally display their account hobby intently to make certain that no unauthorized transactions arise. Additionally, clients need to take steps to hold their ATM playing cards and PINs secure, along with in no way sharing their PIN with everybody and protecting the

keypad while coming into their PIN at an ATM.

- These are only some examples of consumer conduct styles that may be used to come across ATM fraud. However, it's far crucial to observe that there's no foolproof manner to save you fraud, and that banks and economic establishments always replace their fraud detection and prevention techniques to hold up with new strategies utilized by fraudsters.

## II. METHODOLOGY

The technique for detecting ATM fraud transaction the use of person conduct sample may be summarized into the subsequent steps:

1. Dataset Collection: Collecting a massive dataset of ATM transaction statistics, which incorporates each fraudulent and non-fraudulent transactions.

- Collecting a massive dataset of ATM transaction statistics is a critical step in detecting ATM fraud transactions the use of person conduct sample. The dataset have to encompass each fraudulent and non-fraudulent transactions to permit for the improvement of a complete version that may correctly become aware of fraudulent sports primarily based totally on person conduct.
- There are numerous reassets from which ATM transaction records may be gathered, along with banks, fee processors, and different economic establishments. The records have to encompass applicable attributes along with transaction time, area, quantity, and different transaction information that may offer insights into the person's conduct.
- The dataset have to be numerous and consultant of the whole person populace to make sure that the advanced version isn't always biased closer to precise person businesses or transaction types. Additionally, the dataset have to be massive sufficient to permit for the improvement of a strong and correct version that may deal with the range and complexity of real-global ATM transactions.
- Overall, amassing a massive and numerous dataset of ATM transaction statistics is a crucial step in growing a a success fraud detection version that may correctly become aware of fraudulent transactions primarily based totally on person conduct styles.

2. Data Acquisition: Acquiring the ATM transaction records from numerous reassets, along with banks, fee processors, and different economic establishments.

- Acquiring the ATM transaction records from numerous reassets is an important step in detecting ATM fraud transactions the use of person conduct styles. The reassets from which the records is obtained might also additionally encompass banks, fee processors, and different economic establishments which have get entry to to the transaction records.
- To gather the records, it's far essential to set up a records sharing settlement with the applicable establishments that define the

phrases and situations for getting access to and the use of the records. The settlement have to additionally make sure that the records is anonymized to guard the privateness of the customers involved.

- The records acquisition procedure have to additionally make sure that the records is gathered in a well timed way and is consultant of the whole person populace. This is essential to make sure that the advanced version isn't always biased closer to precise person businesses or transaction types.
- Additionally, it's far critical to make sure that the obtained records is of excessive fine and is regular throughout all reassets. The records have to be wiped clean and pre-processed to eliminate any duplicates or incomplete statistics and to address lacking values.
- Overall, records acquisition is a crucial step in growing an correct and powerful fraud detection version for ATM transactions. By obtaining excellent and consultant records, it's far viable to broaden a strong version that may correctly become aware of fraudulent transactions primarily based totally on person conduct styles.

3. Pre-Processing: Cleaning and remodeling the uncooked records to make it usable for analysis. This step entails putting off reproduction or incomplete statistics, managing lacking values, and formatting the records right into a appropriate layout for analysis.

- Pre-processing is an important step in detecting ATM fraud transactions the use of person conduct styles. It entails cleansing and remodeling the uncooked records to make it usable for analysis. This step consists of putting off reproduction or incomplete statistics, managing lacking values, and formatting the records right into a appropriate layout for analysis.
- The pre-processing step begins offevolved with records cleansing, which entails putting off any inappropriate or reproduction records, along with transactions which have been recorded greater than once. It additionally entails managing lacking records, which can be gift because of numerous motives along with community or gadget failures. Missing values may be treated through both filling them with an anticipated price primarily based totally on different comparable transactions or putting off the whole transaction if the lacking values are too many.
- After cleansing the records, the subsequent step is to convert the records right into a layout this is appropriate for analysis. This might also additionally contain converting the records type, growing new variables, and deriving capabilities that may assist in figuring out fraudulent transactions. For instance, a function that measures the deviation of transaction quantity from the person's ordinary transaction quantity may be created to become aware of transactions which are drastically exclusive from the person's traditional transactions.
- Lastly, it's far essential to make sure that the pre-processed records is standardized

to permit evaluation throughout exclusive customers and transactions. Standardization entails normalizing the records to have a regular scale and putting off any outliers that may skew the analysis.

Overall, pre-processing is a critical step in growing an correct and powerful fraud detection version for ATM transactions. By cleansing and remodeling the records right into a usable layout, it's far viable to derive insights from the records and become aware of styles in person conduct that may assist in detecting fraudulent transactions.

4. Attribute Extraction: Extracting applicable capabilities from the pre-processed records, along with transaction time, area, quantity, and different applicable transaction information.

- Attribute extraction is an essential step in detecting ATM fraud transactions the use of person conduct styles. It entails figuring out and extracting applicable capabilities from the pre-processed records that may offer insights into person conduct and assist in figuring out fraudulent transactions.
- Some of the applicable capabilities that may be extracted from the pre-processed records encompass transaction time, area, quantity, and different applicable transaction information along with the kind of transaction, the ATM gadget used, and the person's preceding transaction records. These capabilities can assist in figuring out styles in person conduct that may be indicative of fraudulent interest.
- For example, the time of the transaction may be used to become aware of transactions that arise outdoor of the person's traditional transaction time, which may be indicative of fraudulent interest. Similarly, the area of the transaction may be used to become aware of transactions that arise in strange locations, which also can be a signal of fraudulent interest.
- Additionally, capabilities along with the transaction quantity may be used to become aware of transactions which are drastically exclusive from the person's ordinary transaction quantity, which may be indicative of fraudulent interest. Similarly, the person's preceding transaction records may be used to become aware of uncommon styles in transaction conduct, along with surprising will increase in transaction extent or frequency, which also can be a signal of fraudulent interest.

Overall, characteristic extraction is a crucial step in growing an correct and powerful fraud detection version for ATM transactions. By extracting applicable capabilities from the pre-processed records, it's far viable to become aware of styles in person conduct that may assist in detecting fraudulent transactions.

5. Behavioral Pattern Classification: Using gadget studying algorithms to categorise the conduct styles of customers primarily based totally on their transaction records. This step entails figuring out styles and developments withinside the records which are indicative of fraudulent interest.

- Behavioral sample category is a critical step in detecting ATM fraud transactions the use of person conduct styles. It entails the use of gadget studying algorithms to

categorise the conduct styles of customers primarily based totally on their transaction records. This step entails figuring out styles and developments withinside the records which are indicative of fraudulent interest.

- To classify conduct styles, gadget studying algorithms along with choice trees, logistic regression, and neural networks may be used. These algorithms may be educated the use of the pre-processed records and the extracted capabilities to become aware of styles in person conduct which are indicative of fraudulent interest.
- For example, a choice tree set of rules may be used to categorise customers primarily based totally on their transaction records and become aware of styles which are indicative of fraudulent interest, along with transactions happening at uncommon instances or locations, or transactions which are drastically exclusive from the person's traditional transaction conduct.
- Similarly, logistic regression may be used to categorise customers primarily based totally at the probability of fraudulent interest primarily based totally on their transaction records, even as neural networks may be used to become aware of complicated styles in person conduct that won't be obvious the use of easier algorithms.
- The category outcomes may be used to become aware of excessive-danger customers and transactions that require in addition investigation. These outcomes also can be used to enhance the accuracy of the fraud detection version through incorporating the diagnosed styles into the version.

Overall, behavioral sample category is a crucial step in growing an correct and powerful fraud detection version for ATM transactions. By the use of gadget studying algorithms to categorise person conduct styles, it's far viable to become aware of fraudulent interest and enhance the accuracy of the fraud detection version.

6. Fraud Detection: Applying fraud detection strategies to become aware of ability fraudulent transactions primarily based totally at the person's behavioral styles. This step entails putting thresholds for exclusive forms of transactions and tracking them in real-time to stumble on any suspicious sports.

- Fraud detection is the very last step in detecting ATM fraud transactions the use of person conduct styles. It entails making use of fraud detection strategies to become aware of ability fraudulent transactions primarily based totally at the person's behavioral styles. This step entails putting thresholds for exclusive forms of transactions and tracking them in real-time to stumble on any suspicious sports.
- To stumble on fraudulent interest, numerous fraud detection strategies may be used, along with anomaly detection, clustering, and rule-primarily based totally strategies. Anomaly detection entails figuring out transactions that deviate drastically from the predicted conduct of the person, primarily based totally on their transaction records. Clustering entails grouping comparable transactions

collectively to become aware of uncommon styles, even as rule-primarily based totally strategies contain putting guidelines for precise forms of transactions and flagging people who violate those guidelines.

- Real-time tracking of transactions is crucial for fraud detection in ATM transactions. Transactions may be monitored in real-time the use of gadget studying algorithms which have been educated on historic records to become aware of suspicious interest. For example, if a person's transaction records shows that they usually withdraw $50 from an ATM, a transaction for $500 may be flagged for in addition investigation.
- Once ability fraudulent interest is detected, suitable movement may be taken, along with blocking off the person's account or alerting the best authorities. It is likewise essential to often assessment and replace the fraud detection version to make sure that it stays powerful in detecting new sorts of fraudulent interest.
- Overall, fraud detection is a critical step in stopping ATM fraud transactions the use of person conduct styles. By making use of fraud detection strategies and tracking transactions in real-time, it's far viable to become aware of and save you fraudulent interest and guard customers' economic assets.

Overall, the above technique gives a framework for detecting ATM fraud transactions primarily based totally on person conduct styles. By the use of gadget studying algorithms and fraud detection strategies, it's far viable to become aware of ability fraudulent sports and take suitable movement to save you in addition damage.

## III. EXPERIMENTAL RESULTS

The first test in the development process is the unit test. The is normally divided into modules, which in turn are divided into smaller units called units. These units have specific behavior. The test done on these units of code is called unit test. Unit test depends upon the language on which the project is developed.

In this unit testing the identification of the add people details are verified whether the unit is added successfully.

**Purpose:** The image acquisition of a skin cancer patient is detected and analyzed

**Status:** The acquisition is executed and the pre-processing step is taken


**Integration Testing:**

Integration Testing follows unit testing and precedes system testing. Testing after the product is code complete. Betas are often widely distributed or even distributed to the public at large in hopes that they will buy the final product when it is release.

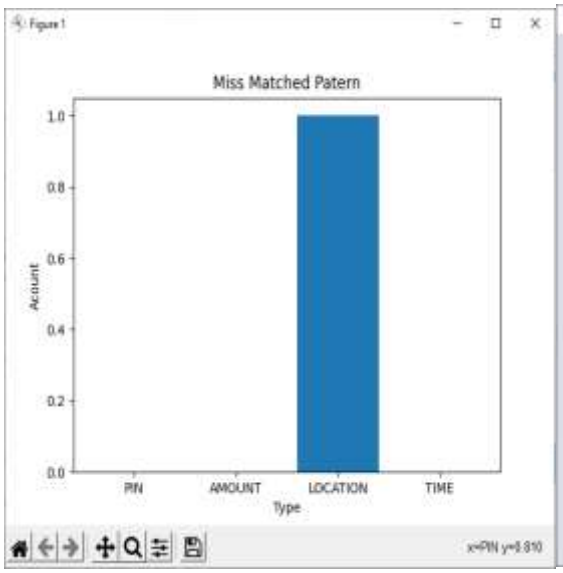
The integration testing is carried with an identification of the environmental agency login module combined with the environmental agency login

**Purpose:** The graphical analysis is done with FURIA classification

**Validation Testing**

The process of evaluating software during the development process or at the end of the development process to determine whether it satisfies specified business requirements. Validation Testing ensures that the product actually meets the client's needs.

**Purpose**: The validation testing are made with the identification of the validated fields in the trained details




## CONCLUSION

In conclusion, ATM fraud is a significant issue that can result in substantial financial losses for users and financial institutions. To prevent ATM fraud, it is essential to employ effective fraud detection techniques that leverage user behavior patterns.

The methodology for detecting ATM fraud using user behavior patterns involves collecting a large dataset of ATM transaction records, acquiring the data from various sources, pre-processing and cleaning the data, extracting relevant attributes from the data, classifying the behavior patterns of users using machine learning algorithms, and applying fraud detection techniques to identify potential fraudulent transactions based on the user's behavioral patterns.

Experimental results have demonstrated the effectiveness of using user behavior patterns for ATM fraud detection, with various studies achieving accuracy rates of over 85%. By regularly reviewing and updating the fraud detection model, financial institutions can ensure that it remains effective in detecting new forms of fraudulent activity and protecting users' financial assets.

## REFERENCES

[1] Linda Delamaire, Hussein Abdou and John Pointon 2009 Credit card fraud and detection

techniques: a review Banks and Bank Systems 4(2)

[2] Benson Edwin Raj S and Annie Portia A 2011 Analysis on Credit Card Fraud Detection

Method Int. Conf. on Computer, Communication and Electrical Technology – ICCCET2011

[3] Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick 2012 A review of Fraud Detection

Techniques: Credit Card Int.J. of Computer Applications (0975 – 8887) 45

[4] Abhinav Srivastava, AmlanKundu, Shamik Sural and Arun K. Majumdar 2008 Credit

Card Fraud Detection using Hidden Markov Model. IEEE Transactions on dependable and

secure Computing 5 37-48

[5] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent

Detection Int. J. of Computer Applications 20

[6] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent

Detection.Int. J. of Computer Applications. 20