NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 8, Aug. -2021

COGNITIVE ANALYTICS TO MINIMIZE FINANCIAL FRAUD

Vijay Yarabolu
GITAM School of Technology, Hyderabad, India
vyarabol@gitam.in

Srikar Dasharadhi
GITAM School of Technology, Hyderabad, India
sdashara@gitam.in

Under the Guidance of
Prof. Suresh Chittineni
schittin@gitam.edu

Srinivas Tadi
stadi@gitam.edu

ABSTRACT
As the digital technologies are evolving rapidly and gaining more and more maturity, it is becoming difficult to keep the online transactions safe and secure. Because of the rapid Digital transformation, lot of transactions are being done over internet. Organisations are reducing in-person interactions more and more to minimize operational costs. Since the physical verifications are minimized and online or system based transactions gaining traction, it is becoming easy for the attackers to commit more fraud under the carpet. So at this juncture of digital transformation, it is time to focus more on financial fraud to keep the financial lives of customers safe and secure, and to make the transformation seamless.

INTRODUCTION
In this paper we are going to discuss popular financial frauds and how to prevent them using cognitive analytics approach. Also need to note that financial fraud is a broader umbrella term. Some of the aspects of financial considered as customer's digital signature such as session tokens, One Time Authorization Codes or Customer's customer-only-knows Knowledge. Following are the brief introduction of the financial frauds that are considered as in-scope for this paper.

2.1 Account Opening Fraud : In the olden days, when a person wanted to open a bank account, he or she used to visit the banking center where the account is opened after thorough verification of customer's identity and face to face interaction. Since it is manual verification, scope for fraud used to be very less. But in the recent years, to offer simplicity and flexibility to the prospect customers, account opening is offered as self service capability where the identity is verified online which is giving scope for fraudsters to commit account opening fraud using stolen identity. Popular bank relations are – savings account opening, overdraft account opening, loan account opening and post paid(credit card) account opening. Other than savings account opening, remaining all are prone for fraud attacks in which fraudsters can gain financial benefit without depositing the money. Typically after committing the fraud, attackers would withdraw the money or wire transfer the money and disappear. For the financial institutes and law enforcement organizations it is very difficult to trace the fraudsters and recover the money as the fraudsters are mostly remote and may not fall in the same jurisdiction in most cases.
Here in this process System basically verifies the customer details such as Age, Gender, Ethnicity, unique identification details(SSN, UIDAI or so forth), Address, Education Qualification, income source and so forth. Once those details are satisfied, it goes to the next verification which is credit score validation, during this process system fetches data from different credit bureaus based on their unique identification number and does the thorough assessment. Based on the score generated system decides whether the banking services can be offered or declined to the prospect customer. Since all this process is offered through online services, it left a lot of scope for the attackers to open a fraudulent loan account or credit card account with malicious intents.

2.2 Contact Center Fraud : Now a days financial organizations are offering various products and services through their unified contact center platform for simplicity, flexibility and better customer experience. Contact centers also provide opportunity for the financial institutions to record and monitor customer interactions, so that they can improve their products and customer experience. During contact center interactions customers are authorized through Knowledge Based Authentication popularly known as KBA. In Knowledge Based Authentication, customer is validated using his or her knowledge which means customer is asked a series of questions populated in contact center widget, and the authentication based on their answers to the questions asked. If any fraudsters steals the customer's sensitive information such as their personal details it would be easy for him/her to imposter the actual customer, gain access to the customer account and make transactions on get the profile reset to hijack the account altogether. Sensitive information could be either personal in nature such as - Age, Gender, Contact Address, Email Address, Date of Birth and so forth, or financial details such as - Account Number, Card Number, CVV, where last shopped and so forth. Gaining access to the customer's personal information is not so difficult for the fraudsters as most of the applications are capturing these details. If one application compromises security, fraudster can easily get these details. And with the available advanced tech and social engineering techniques, it is not so difficult to get customer's financial information as well. Hence contact center authentication is considered as one of the weakest authentication. So there is a clear need to fortify contact center authentication.

2.3 Account Take over fraud : Account take over could happen in many ways. Few of the popular ways are discussed below -

2.3.1 Session Hijacking : An application session is the most sensitive part in customer authentication. Because a session can overwrite multi-factor authentication. Once the application server receives request with a valid session token, it does not verify any other information which means an attacker who has session token in hand does not need to bother about actual customer's user name, password, biometric, one time authorization codes or any other information. Attacker can simply use session token alone to access or hijack actual customer's account.

This attack can be done using man in middle attacks or network sniffing. By monitoring the network using network traffic interceptors, attacker can analyse the data being transferred between client and server and extract the required session token for attack. Some times attacker also uses persistent session token at the client's device.

Considering the sensitivity of the session tokens, it is important to ensure the legitimate customer is using them. Server should not provide global access to the client, rather there should be a context based session access should be provided.

2.3.2 SIM Cloning and SIM Swapping : In SIM cloning attack, attacker steals the program located in SIM memory or understands the logic behind the SIM Card program and creates a cloned card which would be ultimately used for fraud. Cell Phone Network provider cannot understand the difference between a legitimate card and cloned card, it ends up responding to attacker requests that will compromise second factor authentication of the customer.

In SIM Swapping attack, attacker gets hold of customer's identity information such as customer's driving license, passport or any other unique identification details and approach Cell Network Provider, acts as his or her SIM card is damaged or stolen, blocks the existing SIM and gets a new SIM card which supposed to belong actual customer. Once the SIM card is in hand they start using it to take over the account or hijack the customer profile.

2.3.3 Behaviour Hijacking : Behaviour hijacking is a new kind of attack surfacing with the onset of Artificial Intelligence. Using AI one can mimic anything that humans cannot. Behaviour analysis is the new factor consider during authentication to prevent fraud. In behaviour authentication, how the customer's behaviour analysis is done. It could the way customer interacting with application such as mouse movement and key board strokes, or the facial expressions or the pressure analysis or swipe pattern on the mobile key pad. This characteristics are unique for each customer, so they are treated as unique signature of customer and

considered as one of the biometric aspect that can make the authentication stronger. But if the customer's behaviour pattern is stolen, attacker can easily replicate it using advanced AI techniques. If the behaviour characteristics are compromised, customer cannot reset them like how he or she does for the passwords. Hence it is imperative to prevent behaviour hijacking.

AIM OF THE STUDY

The aim of this study is to how the cognitive techniques can be applied in financial domain to minimize the fraud in various contexts such as Account Opening, Transaction Monitoring, Contact Centers and so forth. We are going to identify various additional factors that can detect fraud, but not analysed by most fraud systems. They are kind of dark features or dark data that can be utilized efficiently by fraud systems.

PROPOSED SOLUTION AND METHODS

In this section we are going to discuss the cognitive analysis approach to minimize major frauds associated to Identity Theft. Before that let us understand what is cognitive computing and how it works.

4.1 What is Cognitive Analysis?

This is an intelligent analytics which consider multiple factor and applies human like logic in taking decision. In simple terms, a cognitive analysis will add additional intelligence to the applications in analysing the context, historical data, request source, location and customer behaviour to identify and prevent fraud. On the technology front Cognitive Analytics utilizes the cutting edge technologies such as algorithms of Artificial Intelligence, Machine Learning techniques, Deep Learning and Semantics to develop additional human like intelligence to the system. When Cognitive Analysis is added, applications become more effective and intelligent so that they can learn things in real-time and analyse the human interactions more efficiently to detect and prevent fraud.
Please note that, since Identity Theft is a broader umbrella term, we would like to limit the scope only to the above discussed fraud areas.

4.2 Key Factors

As part of this paper we are going to discuss the below key factors that would help to assess through cognitive analytics to minimize various frauds discussed in previous section. The additional data could be the following

4.2.1 App Details:

- When the application (request origination point) is installed?
- What is the historical information(logs) available for analysis?
- How many failed or invalid attempts made using the same app?

4.2.2 Device Details:

- What is the device used by customer? Example: Mobile or Desktop, OS Details and User Agent Strings
- What are the other transactions originated from the same device?
- Is there any fraud associated to the user's device?
- What is the device power pattern?

4.2.3 Location Details:

- Where the user is located?
- What is the last known location of the user?
- How risky is the location? In terms of Fraud rate.
- What is the usual customer's transaction perimeter ?

4.2.4 Network Details:

- What is the IP address of the customer?
- Is it a safe IP or block listed by any other institution?

- What is the failure transaction rate of the IP?
- Is there any fraud associated to the IP?

4.2.5 User Interface Data:

- What is the user interaction behaviour with Desktop applications? In terms of, Mouse Moments, Mouse Click speed, Mouse Double Click Speed, Key press rate, failure rate, typing speed and so forth.
- What is the user interaction behaviour with Mobile Applications ? in terms of, Swipe pattern, touch pressure and so forth.

4.2.6 Social Profiling :

- What is the social behaviour of the customer?
- Who is part of user's network?
- What is the social data available for Dynamic Knowledge Based Authentication?

4.2.7 Mood Based Bio-Metric :

- What is the usual response time of the user for a known question?
- What is the usual response time of the user for an unknown question?
- What is the voice intonation of the user when giving a positive answer?
- What is the voice intonation of the user when giving a negative answer?
- What is the voice patterns when user is in different moods?
- What is the overall pattern through out the session? Is it consistent or changing in real time?

4.2.8 Transaction Behaviour :

- What is the usual spending behaviour of the customer ?
- What is the customer's knowledge of his own transactions to generate dynamic knowledge based authentication?
- What are the frequent vendors or merchants customer approach for shopping?
- What are the customer's trusted vendors or merchants or financial organization?

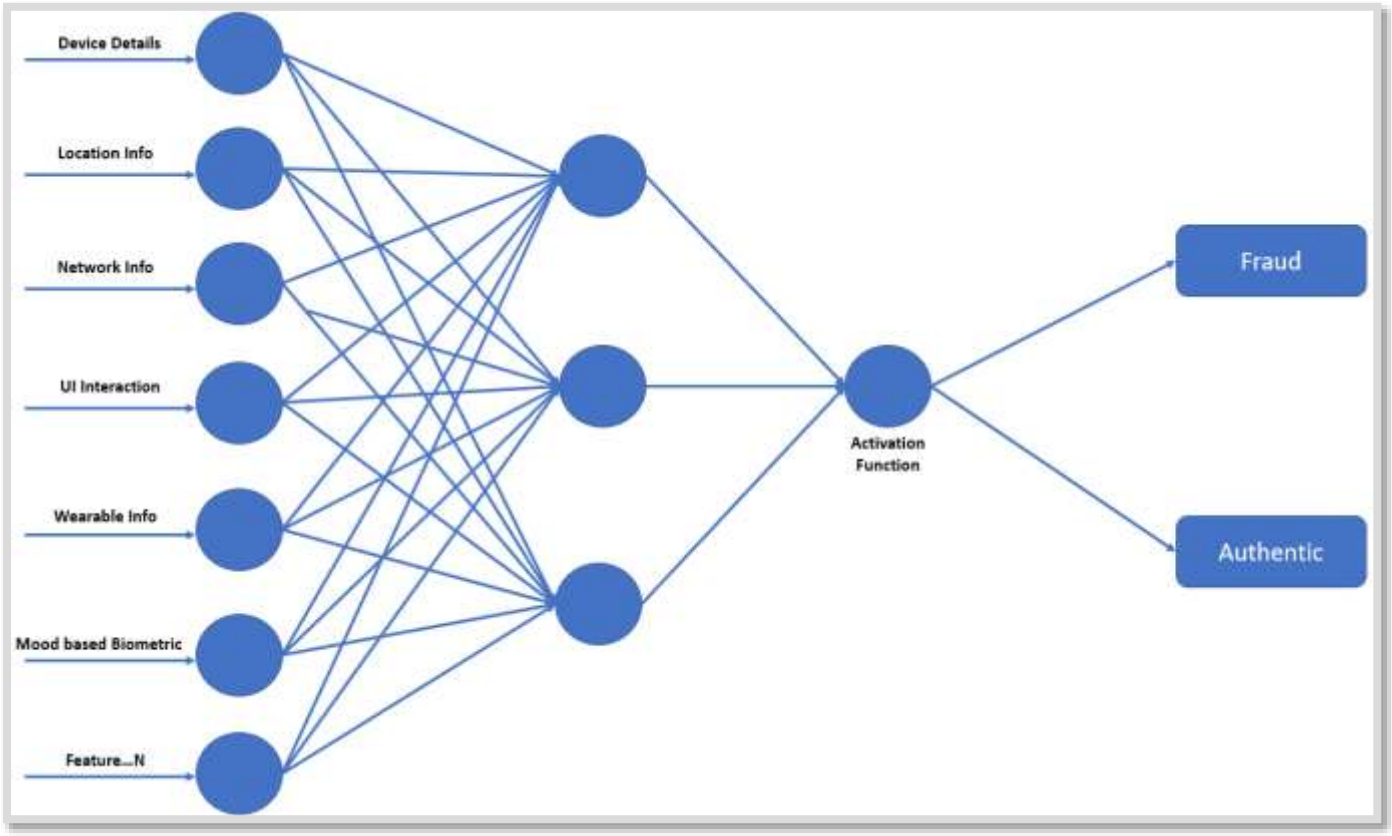
4.2.9 Wearable Data :

- What amount of wearable data available?
- What are the health data of customer?
- Whether customer has healthy life style?
- Wearable data pattern when customer is in different moods?

4.2.10 SIM Characteristics :

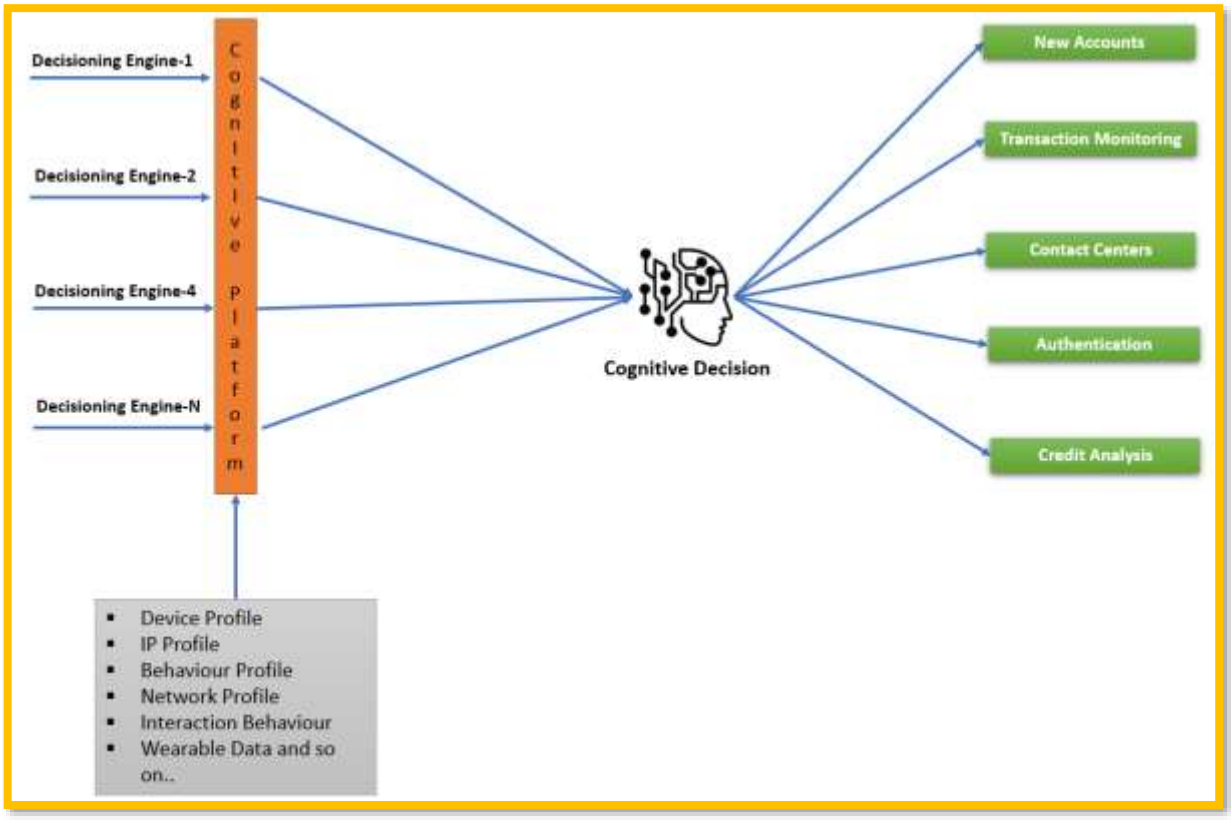
- When user procured the SIM card?
- What are the text messages received to the SIM from different financial and non-financial organizations?
- How many times SIM blocked?
- When is the SIM blocked last time?

Considering the above features, a typical AI based decisioning engine could look like below –



This could be like any other AI based decisioning engine, but the features that we consider for the decisioning makes the difference. Based on the comprehensive or holistic features that we considered for the fraud profiling, the algorithm gains more efficiency such that it builds the intelligence like a human and takes decisions like a human.

A typical cognitive based fraud detection platform could look like the below –



As depicted in above picture each decisioning engine is on boarded to a common decisioning platform. The common decisioning platform considers the additional features like device profiling, IP behaviour, wearable data and so on(features discussed in previous section). They are used for cognitive decisions; a cognitive decision can rule should be able to override the decision of previous non-cognitive decisioning engines. This way a cognitive decisioning engine can work as additional layer of protection to prevent fraud. Cognitive decisioning engine should act as an interface for other applications. Any decisioning by any applications should be taken by the proposed cognitive engine.

IMPLEMENTATION

To elaborate the above process, let us take a contact center example. In a contact center setting, usually a customer call to the contact center agent and request for a service. Then the contact center agent verifies the caller knowledge with various knowledge-based questions such as date of birth, last four digits of the card, unique identification number details and so forth. These questions are basically widget based questions which usually rolled out to the contact center agent screen. Based on the answers given by the customer, a decisioning score is generated. When a decisioning score crosses a threshold limit, agent is given access on the screen to perform requested operations from customer. At this instance, a session cookie is generated that would have access to all customer transactions such as account balance checking, fund transfers, bill payments and so forth. Here at this point, agent is authorized to do anything on customer behalf. Once the access given, there is a scope that an agent can commit fraud if he/she wants to. Because the session token is global in nature and there is no additional monitoring in place to prevent fraud.

Using the above proposed cognitive solution, interaction between customer and agent can be intercepted by an intelligent cognitive platform. This should basically understand what is the need of customer and what is requested by him/her. Based on that system should be able to generate a context restricted session token, that should give access to only to that particular area in the application. For example, if the customer is requesting agent to change the profile address of him/her, the cognitive engine should be able to intercept and understand this conversation and should generate a context restricted session token that can only access to customer profile. Likewise, based on the subsequent requests, the session tokens should be generated dynamically by the cognitive platform and will provide required access to the application features. This way, it will detect and prevent the fraud in an agent assisted customer transactions setting. Because each conversation between customer and agent is monitored and the restricted access is created dynamically, leaving no scope for fraud by agents.

In another example, when a person wants to open a new account with a financial institution, currently customer details such as unique identification number, age, gender, repayment capability, credit score and so forth are evaluated to offer or deny services to the prospect customer. Since the account opening services are made available through online, most of the data capturing and evaluation also being done online which is leaving scope for the attackers to hijack identity of the customer. But using the proposed cognitive engine solution, apart from the regular verifications, a cognitive platform can analyse the additional data too which can prevent the possible fraud. Few examples could be the facial expression data when answering to known questions and unknown questions. Before building this questions, cognitive platform should be able to assess the customer's knowledge based on his previous interactions with other institutes, location data, social profiling and so forth. Let us say if customer has knowledge of football, the one of the dynamic KBA question could be "which countries played in the last football world cup final?". If the user engaged in several discussions on football in his/her social profile, user should be able to answer this question. And the response time and voice intonation should be compared against the usual known answer pattern. Based on that a positive or negative score should be generated. Apart from the dynamic KBA verification, system also can process the text messages of the customer and verify what kind of messages are being received by the customer. Based on that it can get an understanding of customer behaviour, spending pattern which can be used for risk assessment.

Similarly when a transaction is being taken place in a merchant store, system should be able to detect his/her last known location and has to evaluate if it is the customers usual location or is it near to the last transacted location. Based on the distance between last transaction location and the current location, system should find evidence of users travel and means of travel. If the transaction location is too far from the previous location

and there is any evidence of air travel available between these locations, system should be able to authenticate that transaction. This type of intelligence is very much required in modern systems to mitigate fraud.

In other example, during usual application authentication, system authenticates customer only one time during the login. Once the successful authentication, system generates a session token. Subsequent interactions take place only based on session token. But if the session token is hijacked by attackers, in most of the applications there is no mechanism in place to detect and prevent it. But if system can capture and analyse the unique customer interaction signature, it can easily identify if the person interacting with application is legitimate or not. If there is any ambiguity detected, system can enforce the second factor authentication such as authentication code or challenge questions.

Wearable data also an important source to detect the fraud. If a financial organization knows the living style of the user, it can profile the user either risky or non-risky. Or if the algorithm knows what is the vital response of the user when answering a positive question or negative question, that data can be utilized during the dynamic KBA validation. Like validating customer wearable details when asked the customer to answer an unknown question or the response pattern when answering a positive question.

FUTURE RESEARCH AND FOCUS

The additional features discussed in this paper are only few that can contribute to cognitive decisioning and minimize fraud, but these features can vary based on the domain and context. The more and more number of factors considered would minimize the fraud more. In order to evolve this fraud detection and prevention engines, all financial, non-financial organizations, device vendors and key players should come together and share information together. Fraud can be only minimized with collaborative effort among all the organisations. On the other hand organisations should make use of the dark data(unprocessed) as well. The challenge with dark data is, most of the data is unstructured. But with the cutting edge technologies and advanced algorithms, it is much easy to process the data when compared with olden days. With the fraud victim lose his or her money and in many cases they are made liable for the actions that attackers have done. It has both legal and financial aspects. Hence it is imperative to revisit or evaluate the ways periodically and make the protection stronger and stronger to minimize the various financial frauds. Continuously monitor the latest attacking trends and build the detection methods and prevention techniques to gain trust and confidence of customers as they are the backbone for any business in this world.

REFERENCES AND CITATIONS

1) Richard Edward Clark, David Frank Feldon, Kenneth Yates, Jeroen & J. G. Van Merrienboer (2008). Cognitive task analysis.
2) Julie Gore, Adrian P. Banks & Almuth McDowall (2018). Developing cognitive task analysis and the importance of socio-cognitive competence/insight for professional practice.
3) Richard Edward Clark, Editorial board & S. Thill (2021). Cognitive Systems Research.