Forbes INDIA

Banking on AI and ML to vanquish security challenges

By Ms Aparana Gupta and Professor U Dinesh Kumar| Jul 27, 2020

Banks and financial institutions gear up to wield the potential of AI and ML in their thrust to forfend from the argus-eyed fraudsters

---

Image: Shutterstock[br]

As COVID-19 rages unchecked and continues to spiral up its global footprint exponentially, profound uncertainty and extreme volatility has upturned businesses worldwide resulting in precipitous macroeconomic constraints, sparking off inflation of worrisome magnitude enveloping almost every sphere. Evident meltdown of global economy and Dow Jones exhibiting the single day plunge of nearly 3000 points on March 16th 2020[1] – the worst since the Stock Market Crash of October 19th, 1987 “Black Monday” when the US markets fell more than 20% in a single day – is a cogent testimony of this fact.

As human beings oscillate between prioritizing lives and livelihoods, the ongoing paralytic effects of this contagion has spelt radical changes in consumer behavior as they accelerate towards digital modus operandi for onboarding, trading and payment. Recent survey carried out by 451 Research, part of S&P Global Market Intelligence, proclaimed 52% of US traders envisaging a significant surge in their online sales attributable to the ongoing pandemic, thus necessitating intrinsic digital adoption and transformation at warp-speed across a broad swathes of industries.

_RSS_Being the cornerstone of online trades and payment systems, the Digital Payment Systems are poised to witness a resounding growth, however the entwined challenges of increased fraud risk stemming from the prevailing security vulnerabilities would prove to be too expensive to be overlooked. For Fraudsters, vulnerabilities spell wealth of exploitation opportunities. Being hawkeyed, they have been on the prowl preying emotionally and financially vulnerable in this dire strait. The figures relayed by the Federal Trade Commission state that Americans have been obliterated of a whopping 13.4 million dollars owing to the coronavirus-related fraud.

The enormous impact caused due to vast contour of fraud – Digital Identity theft, Credit Card fraud, money laundering – exhorts the Banks and Financial institutions (Fintech) to effectuate synergized ameliorative measures towards establishing a preemptive, fraud-resilient and robust security framework. A crisp anatomy of the prevailing security framework at these financial institutions reveal it's hackneyed, intricate and frail structure underscoring the need for a total overhaul and rejuvenating the security processes by strategically harnessing the potential of trailblazing Artificial Intelligence (AI) and Machine Learning (ML) techniques.

Starting from customer/bank-personnel identification and authentication to authorization and accounting – the integrant germane to the overarching security process at these Fintech institutions is the Digital Identity (ID). It is the compilation of electronically captured, derived and developed attributes that when synthesized can uniquely identify and authenticate a person. Ranging from something as elementary as one's photograph and government issued ID documents to modalities unique to one's biology, 'Biometric' such as Facial Recognition, Retinal Scanning, Voiceprint, Palm and Fingerprint Recognition – a Digital Identity (also known as Personal Identifiable Information PII) is the convergence of all stored in an encrypted binary format. Con men employ multitude of ploys and confidence tricks – identity theft, cyber stalking, privacy and data breach, cyber extortion and highly sophisticated phishing scams – to steal these digital identities as their gateway to financial gain. Consumer Sentinel Network reported 650572 cases of Identity Theft and 647K imposter scams in 2019. Once stolen, these IDs are a currency for fraudsters to be traded

on an unindexed, encrypted and difficult to access web layer – 'The Dark Net', to be used further for creating synthetic IDs, spoofing and impersonation. The information enriched in these IDs, its shelf life and the severity of the cascading impact that it can potentially cause for the victim, acts as the determining factor of its price which ranges roughly anywhere between $12-$1500.

It's not just the disjoint and brittle nature of run-of-the-mill security and authentication mechanism, but also the static fabric of these IDs that makes it intrusive and enticing to the fraudsters to be used for spoofing and impersonation during remote digital authentication. Asking a user to smile, blink their eyes and nod their head can all be replicated using pre-captured photos, animation effects, video playbacks, 3D masks and sophisticated AI models. Deepfakes – a portmanteau of Deep Learning (a subset of ML in AI comprises, multi-layered neural networks capable of unsupervised learning from unstructured and unlabeled data) and Fake are the latest entrant to the convoluted landscape of fraud. It harnesses Generative Adversarial Networks (GANs), a machine learning algorithm that uses two neural networks, pitting one against the other (thus the name 'adversarial') – where the generator algorithm creates counterfeits until the discriminator can't discriminate between the fake and the real – to create digital synthetic and fabricated representation of one's biometric identity.

As these techniques gain ground while also registering growth year on year, the ability and extremity of the employed multi-layer authentication mechanism needs to be positively correlated with the context and risk-profile of the user and the respective request being made. Multitude of factors such as – wealth possessed by the customer, age and cognizance level about cybersecurity trends, frequency, type, initiating and terminating geo-locations of the transactions need to be taken into account while creating risk-profile of the customer. Once baselined, these risk-profiles can be dynamically evolved using Recurrent Neural Network (RNN) thus accrediting the sequential pattern exhibited by data and further using these patterns to forecast the succeeding plausible scenarios.

Augmenting the above created risk-profile with real-time, immersive and passive 3D Liveness Detection of a user/customer using Deep Learning techniques - Convolutional Neural Network (CNN) and Multi-task cascaded convolutional neural networks (MTCNN) or HaaR Cascade – would be the crucial differentiator and key driver towards propelling a frictionless and seamless authentication system. Integrating it further with the user's ubiquitous 'Behavioral Biometrics' attestation techniques – stemming from Keystroke Dynamics (the rhythm, cadence and timing of the keys pressed while user types) , Gait Analysis, Voiceprint ID, Mouse use characteristic, Signature Analysis and Cognitive Biometrics – would provide non-overlapping addition to this multi-layered authentication

system to thwart fraud and identity theft, while also offering frictionless and secure context aware authentication to the customer.

While AI proactively stands guard to keep the fraudsters at bay by red-flagging them during access management and digital onboarding at Fintech institutions, the intensity of damage is prodigiously perturbing if the skilled tricksters confidence trick the above stated process to successfully aboard the Fintech institutions. Either by exploiting data-breach or by using stolen IDs and relevant financial information of individuals with sound credit score, these external con artist either in cahoots with or without an expedient timeserving internal staff create illegal Bank Accounts known as ‘Bank Drops’ – to hold stolen funds towards enabling Money-Laundering, thus reintroducing and homogenizing laundered funds into the legitimate economy.

In their efforts to foil this, Banks and Financial Institutions need to wield the prowess of Risk Management Knowledge Graphs (KG) that entails the prowess of ML and Graph Analytics. Intertwining AI with KG, equips it to detect data anomalies about the direction and coordinates of a specific fraud event. The data nodes of these knowledge graphs need to be enriched with the granular level data and metadata while also being observed and tuned for concept-drift. The resultant Fraud Threat Map is a complete visualization framework that discovers intra and inter-cluster relationships between the transacting parties and renders assistance to Anti-Money Laundering and Fraud Detection teams to visualize and traverse through the distribution and acuteness of specific actors or fraud instances, crucial to thwart Money-laundering. It also facilitates Dynamic Clustering towards executing prompt and preemptive alleviation steps. This data predicated on user-behavior and related transactions is warehoused over a period of time to create customer profiles.

The mélange of supervised and unsupervised ML techniques can be employed to determine normal user behavior and manifesting anomalies contributing to fraud. Moreover, the customer and event-profile data is utilized to compute the probability of co-occurrence – propensity of two events occurring simultaneously or sequentially – and to identify if it’s statistically significant according to the distribution of the events. Using reinforcement machine learning techniques this data is input into the Knowledge Graph for further impact analysis to know and proactively inform the impacted parties in the event of fraud or potential money laundering.

AI and ML induced adaptive User Entity Behavior Analytics (UEBA) can be fused with rule-based Security information and event management (SIEM) to create a robust shield against these hoodwinked machinations like Insider-Theft. While SIEM offers rule-based solutions, UEBA uses risk scoring techniques and advanced algorithms to create baseline of normal behavior of users on interconnected complex systems, allowing it to detect

anomalies and susceptible behavior over time. During dissection of UEBA profile, if the data does not measures up to the created baseline, then based on the deviation or variance, it is classified under the risk category with a Risk score assigned following which the diagnostics is disseminated to the respective fraud detection team for the relevant imperatives. Not only does this solution dynamically creates the cluster of cohorts and entities to scrutinize their collaborative conduct and flag any incongruous and bizarre actions and behavior, it also identifies any oblique movement of fraudsters as they navigate through the network using multitude of machines, IP addresses and credentials, after infiltrating into the system.

In summary, as these banks and financial institutions gear up to wield the potential of AI and ML in their thrust to forfend from the argus-eyed fraudsters, there is no gainsaying that any laxity in the security framework plied to keep vigil on insider-induced theft could augur intense body-blow to the banks and financial institutions. They need to treat this crisis as the darkness before the dawn that accords an all-embracing sustainable opportunity to leverage AI and ML to strengthen, re-vitalize the security & authentication framework and stay ahead of this new scourge. The time to act, lead and thrive is now.

- By Ms Aparana Gupta, Alumnus (Certificate Programme in Business Analytics), IIM Bangalore and

Professor U Dinesh Kumar, Decision Sciences Area, IIM Bangalore