Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ηλεκτρονική απάτη στον τραπεζικό τομέα** **Fraud Detection in Banking**
Ονοματεπώνυμο Φοιτητή	**Μιχάλης Πάτσης**
Πατρώνυμο	**Απόστολος**
Αριθμός Μητρώου	**ΜΠΚΕΔ 21042**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία παράδοσης **Ιανουάριος 2024**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Δέσποινα Πολέμη Καθηγήτρια	Παναγιώτης Κοτζανικολάου Αναπληρωτής Καθηγητής

Περίληψη

Οι ηλεκτρονικές απάτες στον τραπεζικό τομέα, αποτελούν πλέον ένα κομμάτι μείζονος σημασίας αλλά και άξιο μελέτης. Η ραγδαία εξέλιξη της τεχνολογίας, συνδυαστικά με την ψηφιοποίηση των τραπεζικών υπηρεσιών και συναλλαγών, έχει απότοκη συνέπεια την ανάπτυξη του ηλεκτρονικού εγκλήματος στον κυβερνοχώρο, επηρεάζοντας κατά αυτόν τον τρόπο την οικονομική δραστηριότητα των χρηματοπιστωτικών ιδρυμάτων αλλά και πλήττοντας την φερεγγυότητά τους. Ανάμεσα στον εκτεταμένο όγκο συναλλαγών που πραγματοποιούνται κάθε λεπτό, ο εντοπισμός και η πρόβλεψη των παράνομων κινήσεων έγκαιρα και άμεσα, αποτελεί κομμάτι πρωταρχικής σημασίας, καθώς είναι γεγονός ότι οι ηλεκτρονικές απάτες διενεργούνται με διαρκώς μεταλλασσόμενες και εξελισσόμενες μεθόδους. Αυτό κατ' επέκταση έχει οδηγήσει στην ανάγκη για αποτελεσματικό θωρακισμό των τραπεζικών συστημάτων με χρήση σύγχρονων μεθόδων μηχανικής μάθησης και τεχνικών τεχνητής νοημοσύνης, κάτι που παλαιότερα θα φάνταζε αδύνατο. Τούτων δοθέντων, γίνονται καθημερινές προσπάθειες και δοκιμές για την δημιουργία ενός συστήματος ασφαλείας το οποίο θα είναι σε θέση να παρέχει κάθε δυνατή ασφάλεια απέναντι στην τράπεζα και στο πελατολόγιο της, αλλά και στη δημιουργία υποψιασμένου κοινού από φορείς ενημέρωσης. Το θέμα αυτό αναλύεται στην παρούσα διπλωματική εργασία, ξεκινώντας αρχικά αναλύοντας τα υφιστάμενα περιστατικά απάτης με τα οποία έρχεται αντιμέτωπο ένα σύγχρονο χρηματοπιστωτικό ίδρυμα, τα μοντέλα μηχανικής μάθησης και τις τεχνικές που χρησιμοποιεί σχετικά με την εντοπισμό και την πρόβλεψη τους, αλλά και τις προκλήσεις που προκύπτουν για την σωστή εκτίμηση και διαχείρισή τους. Στη συνέχεια, για το προγραμματιστικό μέρος της εργασίας, έχουμε προχωρήσει σε ανάλυση πραγματικών δεδομένων από καρτικές απάτες, στα οποία εφαρμόσαμε αλγορίθμους μηχανικής μάθησης τους οποίους και στη συνέχεια συγκρίναμε και αξιολογήσαμε. Για την καλύτερη κατανόηση του θέματος, έχουμε επιλέξει για το 2ο μέρος, να σχεδιάσουμε ένα σύστημα ανίχνευσης απάτης από την αρχή, εμπνευσμένο από πραγματικά σενάρια και προκλήσεις και το οποίο θα είναι σε θέση να κατηγοριοποιεί και να εντοπίζει τις απατηλές κινήσεις μέσα σε ένα χρηματοπιστωτικό ίδρυμα.

Το προγραμματιστικό μέρος και η επεξεργασία των δεδομένων έγιναν με χρήση της γλώσσας προγραμματισμού Python, και τα συμπεράσματα που προέκυψαν και από τα δύο μέρη της εργασίας έδειξαν την ακρίβεια πρόβλεψης που είχαν οι αλγόριθμοι, αλλά ταυτοχρόνως μας παρείχαν σημαντικές πληροφορίες σχετικά με τις προκλήσεις αλλά και τις ευπάθειες που υπάρχουν σε ένα σύστημα πρόβλεψης και ανίχνευσης απάτης.

Λέξεις κλειδιά: Ηλεκτρονικές απάτες, σύστημα ανίχνευσης απάτης, τεχνικές μηχανικής μάθησης, καρτικές απάτες, τεχνητή νοημοσύνη

Abstract

Financial fraud in the banking sector is now a topic of major importance and worthy of study. The rapid evolution of technology, combined with the digitalization of banking services and transactions, has had the sharp consequence of the growth of cybercrime in cyberspace, thus affecting the economic activity of financial institutions and affecting their solvency. Among the extensive volume of transactions that take place every minute, detecting and anticipating illegal movements in a timely and swift manner is a matter of primary importance, as it is a fact that financial fraud is carried out by constantly changing and evolving methods. This has consequently led to the need for effective shielding of banking systems using modern machine learning and artificial intelligence techniques, which would previously have seemed impossible. Daily efforts and tests are being made by the banking sector, to create a security system which will be able to provide all possible security to the bank and its clientele, and to create a leery public by information providers. In this thesis we will analyze the existing fraud incidents that a modern financial institution is confronted with, the machine learning models and techniques used to detect and predict them, as well as the challenges that arise for their proper assessment and management. Then, for the programmatic Part 1 of the paper, we analyze real data from credit card fraud cases, to which we apply machine learning algorithms which we then compared and evaluated. For a better understanding of the topic, we have chosen for part 2, to design a fraud detection system from scratch, inspired by real scenarios and challenges, which categorizes and detects fraudulent movements within a financial institution.

The programming part and data processing were done using Python. The conclusions drawn from both parts of the work showed the prediction accuracy of the algorithms, but at the same time provided us with important information about the challenges and vulnerabilities that exist in a fraud prediction and detection system.

Keywords: Financial fraud, fraud detection system, machine learning techniques, credit card fraud, artificial intelligence

Πίνακας Περιεχομένων

1. Εισαγωγή

Η τεχνολογία αποτελεί πλέον ένα αναπόσπαστο μέρος του τραπεζικού συστήματος, το οποίο έχει ολοένα και πιο σημαντικό ρόλο στην καθημερινότητά μας σε διάφορους τομείς, όπως για παράδειγμα στις ηλεκτρονικές πληρωμές λογαριασμών ή υπηρεσιών, στις ηλεκτρονικές αγορές αγαθών και σε διάφορες άλλες οικονομικές δραστηριότητες.

Η θέληση και η ανάγκη για εξέλιξη, σε συνδυασμό με την ανάγκη για ανταπόκριση στις καθημερινά αυξανόμενες απαιτήσεις, έχει φέρει στο προσκήνιο ρηξικέλευθες προτάσεις και εφαρμογές με στόχο την πιο άμεση, σωστή και αποτελεσματική εξυπηρέτηση των πελατών ανάλογα με τις εκάστοτε ανάγκες. Για τον λόγο αυτόν, αναπτύχθηκαν αλγόριθμοι, μέσω των οποίων ο τραπεζικός τομέας εισήλθε σταδιακά στην "ψηφιακή εποχή", η οποία θεωρείται πλέον μονόδρομος για τον κλάδο. Αφορά δηλαδή σε ένα διαρκές παιχνίδι μεταξύ μιας αγοράς που γίνεται ολοένα και πιο ανταγωνιστική και απαιτητική καθώς η τεχνολογία εξελίσσεται, και μιας τεχνολογίας που αλλάζει και εξελίσσεται διαρκώς για να ανταποκρίνεται στις ανάγκες της αγοράς αυτής.

Με την πάροδο των ετών, έχουν καταβληθεί αρκετές προσπάθειες για τη βελτιστοποίηση της σχέσης μεταξύ της ικανοποίησης των πελατών και της ορθής εφαρμογής των διαδικασιών, πάντα με στόχο την ελαχιστοποίηση των κινδύνων στο ψηφιακό περιβάλλον (Michele Carminati, 2018). Ο κοινός παρονομαστής ήταν η δημιουργία ισχυρών λογισμικών τα οποία θα μπορούσαν να διαχειρίζεται εύκολα ο χρήστης αλλά ταυτόχρονα να εκτελούν αποτελεσματικά και γρήγορα όλες τις λειτουργίες που προηγουμένως εκτελούνταν με φυσική παρουσία. Αυτό σχετίζεται με μια τάση που αρχίζει να διαφαίνεται παγκοσμίως, η οποία στοχεύει στην αυτοματοποίηση των λειτουργιών μέσω της ψηφιακής επανάστασης. Παρόλα αυτά, η τάση αυτή έχει φέρει στο προσκήνιο ζητήματα ασφαλείας ως προς την προστασία των δεδομένων των πελατών αλλά και του ίδιου του τραπεζικού συστήματος, τα οποία περισσότερο από ποτέ είναι εκτεθειμένα σε επιθέσεις ασφαλείας με σκοπό την υποκλοπή τους και την δόλια χρήση τους.

Η ασφάλεια είναι ένα θεμελιώδες και ολοένα πιο σημαντικό ζήτημα στη σημερινή τραπεζική βιομηχανία. Τα τελευταία χρόνια ο αριθμός των απατηλών συναλλαγών που διαπράττονται από τρίτους έχει αυξηθεί πάρα πολύ (Banks,2005). Κατά συνέπεια η πρόληψη της απάτης έχει καταστεί κεντρικό μέλημα των τραπεζών, των πελατών και των φορέων χάραξης δημόσιας πολιτικής (Sullivan, 2010). Μια τραπεζική απάτη πλήττει τόσο τις τράπεζες όσο και τους πελάτες της. Οι τράπεζες επιβαρύνονται με σημαντικό λειτουργικό κόστος για την επιστροφή των χρηματικών απωλειών των πελατών, ενώ οι πελάτες, οι οποίοι πρέπει να εντοπίσουν τις δόλιες συναλλαγές, να τις κοινοποιήσουν στην τράπεζά τους, να προχωρήσουν σε ενέργειες μπλοκαρίσματος, επανέκδοσης και επαναλειτουργίας μια κάρτας ή ενός λογαριασμού και αμφισβήτησης των απατηλών συναλλαγών, υφίστανται επίσης σημαντικές χρονικές και οικονομικές απώλειες. Όντας θύμα απάτης μπορεί επίσης να επηρεάσει την αντίληψη των πελατών οτι αισθάνονται ασφαλείς και προστατευμένοι από την τράπεζα τους και κατά συνέπεια να κλονιστεί η σχέση τράπεζας-πελάτη γεγονός που με τη σειρά του μπορεί να επηρεάσει αρνητικά την αφοσίωση των πελατών και να υποκινήσει τη θέληση για αλλαγή και αναζήτηση άλλου χρηματοπιστωτικού ιδρύματος, πλήττοντας έτσι τη φήμη των τραπεζών και παρεμποδίζοντας την προσέλκυση νέου πελατολογίου.

Στη διπλωματική αυτή εργασία, θα αναλύσουμε αρχικά τις διάφορες επιθέσεις ασφαλείας, καθώς και τα διαφορετικά περιστατικά απάτης αναφέροντας για το κάθε είδος και κάποιες περαιτέρω λεπτομέρειες. Θα αναφέρουμε τις πρακτικές που εφαρμόζονται πλέον από τα χρηματοπιστωτικά ιδρύματα για την αντιμετώπιση αυτών των επιθέσεων και πως μεταβλήθηκαν αυτές οι πρακτικές μέσα στα τελευταία χρόνια με την χρήση τεχνικών και αλγορίθμων μηχανικής μάθησης. Τέλος, θα εξετάσουμε την αξιολόγηση των μοντέλων και των τεχνικών που χρησιμοποιούνται για την ανίχνευση της απάτης και θα επισημάνουμε το νομικό πλαίσιο που θεσπίστηκε στην Ελλάδα για την προστασία των καταναλωτών από περιστατικά απάτης και πώς ο τραπεζικός κλάδος καλείται να αντιμετωπίσει το φαινόμενο αυτό.

2. Περιστατικά απάτης

Στο κεφάλαιο αυτό θα αναλύσουμε τα υφιστάμενα περιστατικά απάτης που αντιμετωπίζει ένα σύγχρονο χρηματοπιστωτικό ίδρυμα δίνοντας κάποιες λεπτομέρειες για το κάθε ένα. Έχουμε χωρίσει τα περιστατικά απάτης σε τρεις κατηγορίες, περιστατικά απάτης μέσω καρτών, περιστατικά απάτης μέσω ηλεκτρονικής τραπεζικής, απάτες εις βάρος των εμπόρων της τράπεζας και απάτες εις βάρος της τράπεζας.

2.1. Μέθοδοι απάτης με κάρτες

Στη σύγχρονη πραγματικότητα, οι συναλλαγές με κάρτες, με φυσική παρουσία των πελατών ή με ηλεκτρονική μορφή (από εδώ και στο εξής για συντομία CP: Card Present, CNP: Card Not Present αντίστοιχα) αποτελούν το κύριο μέσο πληρωμής και εξυπηρέτησής μας. Οι αυξημένοι ρυθμοί και οι σημερινές ανάγκες έχουν εκτοξεύσει των αριθμό των συναλλαγών που γίνονται με αυτές, κυρίως στο ηλεκτρονικό κομμάτι, στα ύψη, με αποτέλεσμα να αποτελούν βορά για την αντίστοιχη αύξηση των απατηλών συναλλαγών καθώς και των αυξανόμενων απωλειών για τα χρηματοπιστωτικά ιδρύματα. Το γεγονός αυτό έχει ως αντίκτυπο την συνεχή αναζήτηση νέων τεχνικών, μεθόδων και καινοτομιών για την ανίχνευση, την πρόληψη καθώς και την διαχείριση τέτοιων περιστατικών απάτης. Στην ενότητα αυτή θα αναλύσουμε τις απάτες με καρτικά προϊόντα, θα κάνουμε μια επισκόπηση των διάφορων περιστατικών που υπάρχουν δίνοντας περαιτέρω λεπτομέρειες για το καθένα, θα περιγράψουμε τους τρόπους που χρησιμοποιούν οι απατεώνες προκειμένου να αποκτήσουν πρόσβαση σε οικονομικές και προσωπικές πληροφορίες και θα δούμε και κάποιες τεχνικές πρόληψης και ανίχνευσης.

Οι απάτες από συναλλαγές με κάρτες αποτελούν ένα από τα μεγαλύτερα φαινόμενα απάτης καθώς προκαλούν ολοένα και αυξανόμενες απώλειες για τα χρηματοπιστωτικά ιδρύματα. Καθώς η καταναλωτική συμπεριφορά των πελατών εξελίσσεται, η παγκόσμια αγορά των καρτών έχει αυξηθεί σημαντικά τα τελευταία χρόνια. Οι κάρτες είναι σίγουρα ένα χρήσιμο και βολικό προϊόν για τους καταναλωτές καθώς αποτελούν ένα ευρέως αποδεκτό και αποτελεσματικό τρόπο πληρωμής από τους εμπόρους και έχουν γίνει επί της ουσίας μια βολική αντικατάσταση των μετρητών καθιστώντας με αυτόν τον τρόπο τις απάτες με κάρτες ένα μείζον ζήτημα για τον κλάδο των πληρωμών. Οι σύγχρονοι απατεώνες είναι οργανωμένοι επαγγελματίες που χρησιμοποιούν περίτεχνους τρόπους για να αποκτήσουν τα στοιχεία του κατόχου μιας κάρτας, και συνεχίζουν να αναπτύσσουν νέες μεθόδους επίθεσης χρησιμοποιώντας εξελιγμένες τεχνικές. Είναι σημαντικό να αναφέρουμε οτι τα εγκληματικά κυκλώματα απάτης χρησιμοποιούν μοντέλα και βάσεις δεδομένων μέσω διαδικτυακών τόπων στα οποία παρέχουν πρόσβαση σε κλεμμένες εμπιστευτικές πληροφορίες για περιορισμένο χρονικό διάστημα έναντι καθορισμένης αμοιβής.

Προτού προχωρήσουμε στην ανάλυση των διάφορων περιστατικών καρτικής απάτης, είναι σημαντικό να προσδιορίσουμε έναν γενικό ορισμό αυτών. Όλα τα επικείμενα περιστατικά που θα αναφέρουμε αφορούν επί της ουσίας κατάχρηση πληροφοριών για οικονομικό κέρδος και συμβαίνει όταν οι παράνομα αποκτηθείσες προσωπικές πληροφορίες χρησιμοποιούνται για να γίνουν πληρωμές, για δημιουργία νέων λογαριασμών και για απόπειρες απόκτησης διάφορων υπηρεσιών. (2011 Identity Fraud Survey Report: Consumer Version. Javelin Strategy & Research).

Υπάρχουν αρκετές μέθοδοι που χρησιμοποιούνται για την απόκτηση των πληροφοριών αυτών, τις οποίες θα αναλύσουμε στην ενότητα αυτή.

Κλοπή Κάρτας: Το συγκεκριμένο είδος απάτης αφορά την κλοπή της τραπεζικής κάρτας κατά την οποία γίνεται παράνομη χρήση της από 3^{ο} άτομο για CP (card present) συναλλαγές. Το συγκεκριμένο περιστατικό απάτης έχει άνοδο ως προς την οικονομική απώλεια τα τελευταία χρόνια στα οποία οι συναλλαγές μπορούν να διενεργηθούν ανέπαφα χωρίς την χρήση του μυστικού κωδικού PIN. Ακόμα σε τέτοιου είδους περιστατικά, οι απατεώνες χρησιμοποιούν τεχνικές παρατήρησης προκειμένου να αποσπάσουν τον αριθμό PIN χωρίς το θύμα να το αντιληφθεί.

Κλοπή αλληλογραφίας: Γνωρίσματα του είδους απάτης αυτού, είναι η υποκλοπή αλληλογραφίας με σκοπό να γνωστοποιηθούν αριθμοί χρεωστικών ή πιστωτικών καρτών, βιβλιάρια επιταγών, τραπεζικές καταστάσεις καθώς και φορολογικά έντυπα. Το συγκεκριμένο είδος απάτης, στοχοποιεί κυρίως εταιρίες και υπηρεσίες, και συγκεκριμένα την εισερχόμενη και εξερχόμενη αλληλογραφία η οποία μπορεί να περιέχει οικονομικά στοιχεία πελατών, λογιστικά έγγραφα, αρχεία πληρωμών αλλά και μισθοδοσιών της επιχείρησης, καθώς και άλλες σημαντικές πληροφορίες.

Παραβίαση δεδομένων: Η διαρροή δεδομένων αποτελεί ένα ολοένα και συχνότερο φαινόμενο απάτης δοθέντων των νέων τεχνολογιών, μέσω των οποίων οι απατεώνες δύναται να αποκτήσουν πρόσβαση σε προσωπικά στοιχεία των καταναλωτών ή και πολλές φορές στα καρτικά τους προϊόντα. Αυτό μπορεί να επιτευχθεί με την παράνομη είσοδο στις βάσεις δεδομένων από εμπόρους, από ηλεκτρονικά καταστήματα, από χρηματοπιστωτικά ιδρύματα, ή ακόμα και από κυβερνητικές υπηρεσίες, με αποτέλεσμα την απόκτηση μεγάλης κλίμακας προσωπικών πληροφοριών. Κάποια τέτοια παραδείγματα είναι η αμερικάνικη εταιρία T.J. Maxx η οποία τον Ιανουάριο του 2004 ανέφερε ότι διέρρευσαν 45,7 εκατομμύρια αριθμοί πιστωτικών και χρεωστικών καρτών καθώς και 455.000 αρχεία από επιστροφές εμπορευμάτων τα οποία περιείχαν αριθμούς αδειών οδήγησης των πελατών της [1]. Ένα πιο πρόσφατο παράδειγμα είναι η εμπορική τράπεζα Flagstar Bank η οποία το 2021 έπεσε θύμα κυβερνοεπίθεσης με αποτέλεσμα να γίνει παραβίαση των δεδομένων σε περισσότερους από 1,5 εκατομμύριο πελάτες της [2]. Η διαρροή των πληροφοριών δεν οφείλεται πάντα σε παραβιάσεις μιας βάσης δεδομένων, καθώς ένα μεγάλο κομμάτι μπορεί να εκτεθεί είτε από κάποιο λάθος. Αυτό καθιστά την ασφάλεια των δεδομένων κατά την αποθήκευση και την μεταφορά τους ένα μείζον θέμα για τις τράπεζες και τις επιχειρήσεις.

Skimming: Το skimming Αφορά την αντιγραφή των δεδομένων της κάρτας, τα οποία χρησιμοποιούνται στη συνέχεια για την πραγματοποίηση αγορών όπου η ίδια η κάρτα δεν είναι παρούσα. Ο πιο συνήθης τρόπος αντιγραφής είναι μέσω της φαλκίδευσης των ATM κατά τον οποίο τα «παγιδεύουν» με συσκευές ανίχνευσης στην υποδοχή εισόδου, έτσι ώστε τα δεδομένα της κάρτας να αντιγραφούν όταν αυτή εισάγεται στο μηχάνημα. Πολλές φορές γίνεται και χρήση μικρής κάμερας πάνω από το πληκτρολόγιο, μέσω της οποίας καταφέρνουν να καταγράψουν και το PIN της κάρτας για χρήση σε δόλιες συναλλαγές. Τα δεδομένα από περιστατικά skimming συλλέγονται συχνά από εκατοντάδες κάρτες και πωλούνται σε εγκληματικές οργανώσεις οι οποίες στη συνέχεια κατασκευάζουν της κλωνοποιημένες κάρτες. Καθώς μιλάμε για περιστατικό απάτης με αντιγραφή κάρτας, οι κινήσεις φαίνονται να γίνονται με φυσική παρουσία της κάρτας και ως αποτέλεσμα είναι πολύ δύσκολο να εντοπιστούν οι δόλιες συναλλαγές τόσο από τους ίδιους τους πελάτες όσο και από τα συστήματα ασφαλείας των τραπεζών.

Phishing: Ίσως το πιο διαδεδομένο και ταχύτερα αναπτυσσόμενο είδος απάτης, είναι το ηλεκτρονικό «ψάρεμα», μέσω του οποίου υποκλέβονται προσωπικές και οικονομικές πληροφορίες. Περιλαμβάνει ουσιαστικά την δημιουργία ηλεκτρονικών μηνυμάτων που μοιάζουν αυθεντικά και δολίως εμφανίζουν ως αποστολείς υπάρχουσες νόμιμες υπηρεσίες όπως λόγου χάρη τράπεζες, υπηρεσίες δικτύου, παρόχους υπηρεσιών δικτύου και διαδικτυακούς εμπόρους λιανικής πώλησης. Αυτά τα μηνύματα συχνά περιλαμβάνουν λογότυπα αλλά και άλλες πληροφορίες που εμφανίζονται ως νόμιμες και έγκυρες. Το περιεχόμενο των μηνυμάτων αυτών περιλαμβάνει είτε κάποια υποτιθέμενη απειλή είτε κάποια μορφή επικαιροποίησης και ενημέρωσης λογαριασμού και παραπέμπει τα θύματα μέσω του παρεχόμενου διαδικτυακού συνδέσμου να παράσχουν ευαίσθητες πληροφορίες όπως για παράδειγμα στοιχεία καρτών, στοιχεία λογαριασμού, κωδικούς πρόσβασης κτλ. Με την πάροδο των ετών έχουν δημιουργηθεί νέες εκδοχές του συγκεκριμένου είδους απάτης όπως για παράδειγμα το smishing και το vishing. Το πρώτο αφορά πάλι κακόβουλα μηνύματα που όμως αυτή τη φορά στέλνονται στο κινητό με μορφή sms και όχι ως email, ενώ το δεύτερο αφορά τηλεφωνική απάτη κατά την οποία ο απατεώνας καθοδηγεί το θύμα για γνωστοποίηση των προαναφερθεισών στοιχείων τηλεφωνικά. Τα περιστατικά vishing, δεδομένου ότι μιλάμε για τηλεφωνική

προσέγγιση των θυμάτων συνήθως έχουν ως πρόσχημα κάποια δημόσια υπηρεσία για υποτιθέμενη επιστροφή φόρου, κάποια επενδυτική κίνηση, ή ως υποτιθέμενοι τεχνικοί για κάποιον υποτιθέμενο ίο στον υπολογιστή. Επειδή οι περισσότεροι άνθρωποι εμπιστεύονται περισσότερο τα μήνυμα και την τηλεφωνική επικοινωνία από την ηλεκτρονική αλληλογραφία, το smishing και το vishing παρέχουν στους απατεώνες ένα ακόμα πεδίο επίθεσης.

Transaction Reversal Fraud (TRF): Η συγκεκριμένη μέθοδος χρησιμοποιείται για κλοπή μετρητών από ATM, κατά την οποία αντιστρέφουν την λογική του λογισμικού για αφαίρεση χρημάτων. Αφορά μια εξελιγμένη επίθεση που δημιουργεί κωδικούς σφάλματος στο ATM με αποτέλεσμα να μην χρεώνεται ο λογαριασμός μετά την εκτέλεση πολλαπλών συναλλαγών. Οι απατεώνες με χρήση μηχανημάτων δεν αφήνουν την σύλληψη της κάρτας από το ATM και παρότι δίνεται η εντολή για ανάληψη των χρημάτων, ο κεντρικός υπολογιστής αντιστρέφει την συναλλαγή χωρίς να φανεί η χρέωση στον λογαριασμό. Αφορά μια επίθεση που γίνεται σε αρκετά μικρό χρονικό διάστημα με αλλεπάλληλες συναλλαγές και μεγάλη οικονομική απώλεια εις βάρος της εκάστοτε τράπεζας, και πραγματοποιείται από νέους τραπεζικούς λογαριασμούς που έχουν δημιουργηθεί για αυτόν τον σκοπό με πλαστά συνήθως ονόματα και στοιχεία.

Ιστοσελίδες κοινωνικής δικτύωσης: Τα μέσα κοινωνικής δικτύωσης αποτελούν πλέον ένα σπουδαίο κομμάτι της καθημερινότητάς μας με ολοένα και συχνότερη χρήση τους, φέρνοντας σε επαφή εκατομμύρια ανθρώπους στον κόσμο, δημιουργώντας έτσι νέες και ισχυρές απειλές στον κυβερνοχώρο. Μέσω τον προσωπικών σελίδων, κοινοποιούνται ευαίσθητες πληροφορίες και δεδομένα τα οποία μπορούν να χρησιμοποιηθούν από τρίτους για διάφορες απάτες. Απάτες phishing είναι αρκετά συχνές στο Facebook και μπορούν να εμφανιστούν ως παιχνίδια ή κουίζ. Ένα απλό παράδειγμα είναι το κουίζ «Ποιος σε γνωρίζει καλύτερα» το οποίο στοχοποιεί σε ερωτήσεις όπως λόγου χάρη το μεσαίο όνομα, το αγαπημένο βιβλίο ή τον τόπο γέννησης τα οποία ενδεχομένως να αποτελούν ενδείξεις για τους κωδικούς πρόσβασης ή τις ερωτήσεις ασφαλείας των λογαριασμών. Ένα πολύ συνηθισμένο και επικίνδυνο spam είναι αυτό που παραπλανά τον χρήστη ώστε να κατεβάσει ένα κακόβουλο λογισμικό που καταγράφει τις πληκτρολογήσεις με αποτέλεσμα να δίνεται έτσι η πρόσβαση στους μυστικούς κωδικούς ενός λογαριασμού, και μπορεί να σταλθεί στον απατεώνα ως βίντεο ή ως εικόνα. Όπως αναφέρει ο Tom Clare, επικεφαλής του τμήματος marketing της Blue Coat, μιας εταιρείας ασφάλειας διαδικτύου, «οι απατεώνες καταλαβαίνουν ότι οι περισσότεροι χρήστες χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για τα πάντα» [3] κάτι που καθιστά ιδιαίτερα επικίνδυνο την οποιαδήποτε κοινοποίηση τους, καθώς κάτι φαινομενικά ασήμαντο όπως οι κωδικοί του Facebook, μπορούν να οδηγήσουν τον απατεώνα στους κωδικούς πρόσβασης ενός τραπεζικού λογαριασμού.

2.2. Μέθοδοι απάτης μέσω της ηλεκτρονικής τραπεζικής (e-banking)

Η ταχεία πρόοδος κατά τις τελευταίες δεκαετίες επέτρεψε την ανάπτυξη του ηλεκτρονικού εμπορίου σε παγκόσμιο επίπεδο, επιτρέποντας στις επιχειρήσεις να αλληλοεπιδρούν αποτελεσματικά με τους πελάτες τους αλλά και με άλλες επιχειρήσεις εντός και εκτός της χώρας. Το ηλεκτρονικό εμπόριο βοηθά τις επιχειρήσεις να συνομιλούν μεταξύ τους, να παρακολουθούν τις πληροφορίες και να διασφαλίζουν την ασφάλειά τους. Συμπεριλαμβάνει επίσης τον διαμοιρασμό σημαντικών δεδομένων εύκολα και γρήγορα, με σκοπό την βέλτιστη εξυπηρέτηση των πελατών καθώς και την επίτευξη ενός συγκριτικά ανταγωνιστικού πλεονεκτήματος της επιχείρησης σε σχέση με άλλες. Όπως και άλλες επιχειρήσεις, έτσι και ο τραπεζικός κλάδος, χρησιμοποίησε την τεχνολογία πληροφορίων και επικοινωνιών για να προσφέρει στους πελάτες του ένα ηλεκτρονικό σύστημα το οποίο διευκολύνει την αλληλεπίδρασή τους, μέσω πληθώρας ηλεκτρονικών υπηρεσιών και ενεργειών. Ωστόσο, αυτή η μεταβολή από τις παραδοσιακές τραπεζικές υπηρεσίες στις ηλεκτρονικές έφερε στο προσκήνιο νέες προκλήσεις αλλά και απειλές οι οποίες στοχοποιούν την ασφάλεια των διαδικτυακών συναλλαγών αυτών. Οι δισεκατομμύρια χρηματοοικονομικές συναλλαγές που πραγματοποιούνται καθημερινά, έχουν οδηγήσει σε άνοδο των τραπεζικών εγκλημάτων που απειλούν τα δεδομένα των πελατών καθώς και τις συναλλαγές τους, αναγκάζοντας τις τράπεζες να υιοθετήσουν νέες πρακτικές και συστήματα, προκειμένου να ανταπεξέλθουν στις απειλές αυτές. Στην ενότητα αυτή θα παρουσιάσουμε ζητήματα που αφορούν την ασφάλεια της ηλεκτρονικής τραπεζικής, καθώς και τις απειλές και τις επιθέσεις που υπάρχουν, και πώς αυτές έχουν εξελιχθεί μέσα στα χρόνια, ξεκινώντας αρχικά από μια μικρή ιστορική αναδρομή για την λειτουργία του e-banking.

2.2.1. Ιστορική αναδρομή

Αρχικά είναι σημαντικό να αναφέρουμε ότι το επιχειρηματικό μοντέλο της ηλεκτρονικής τραπεζικής εμφανίστηκε για πρώτη φορά στη Νέα Υόρκη το 1980 όπου προσφερόταν από μεγάλες τράπεζες της πόλης, όπως η Citibank και η Chase Manhattan [4]. Οι πρώτες υπηρεσίες που περιείχε ήταν η προβολή των τραπεζικών καταστάσεων καθώς και η ηλεκτρονική πληρωμή των λογαριασμών. Παρόλο που επρόκειτο για πολύ βασικές λειτουργίες, το συγκεκριμένο σύστημα λειτούργησε ως πρόδρομος των εξελιγμένων υπηρεσιών ηλεκτρονικής τραπεζικής που γνωρίζουμε σήμερα. Μια πιο ολοκληρωμένη υπηρεσία e-banking επιτεύχθηκε από την τράπεζα Stanford Federal Credit Union στα μέσα περίπου της δεκαετίας του ’90, η οποία προσέφερε μια 24ωρη υπηρεσία ηλεκτρονικής τραπεζικής από το οικιακό δίκτυο. Ο δισταγμός και η έλλειψη εμπιστοσύνης από το κοινό για την αξιοποίηση των ηλεκτρονικών αυτών υπηρεσιών οδήγησε σε μια τεράστια προσπάθεια από τον τραπεζικό κλάδο για δημιουργία περισσότερων χαρακτηριστικών ασφαλείας για τις ηλεκτρονικές συναλλαγές και για την προώθησή τους στην αγορά. Έτσι, φτάνουμε στην αρχή της δεκαετίας του 2000, όπου η Τράπεζα της Αμερικής (Bank of America) υιοθέτησε το, αποδεκτό από τους πελάτες της, επιχειρηματικό μοντέλο της «ψηφιακής επιχείρησης» , όπως αυτό είναι γνωστό και σήμερα, δίνοντας περισσότερες και καλύτερες επιλογές μέσω των διαδικτυακών συναλλαγών και υπηρεσιών της.

Η ηλεκτρονική τραπεζική βρίσκεται αρκετό καιρό στο προσκήνιο, ξεκινώντας από τα Αυτοματοποιημένα Ταμειακά Μηχανήματα (ATM) τα οποία προσφέρθηκαν στο κοινό για αναλήψεις χρημάτων αλλά και για διάφορες άλλες τραπεζικές συναλλαγές όπως καταθέσεις χρημάτων, μεταφορές και ερωτήσεις υπολοίπων, τα οποία πραγματοποιούνται με χρήση της κάρτας και ενός μυστικού κωδικού pin. Για πιο περίπλοκα ερωτήματα και για πελάτες που δεν αισθάνονται άνετα ή δεν είναι αρκετά εξοικειωμένοι με τις αυτοματοποιημένες υπηρεσίες, υπάρχει το αντίστοιχο phone banking, μέσω του οποίου μπορούν τηλεφωνικά οι πελάτες να εξυπηρετηθούν με διάφορες συναλλαγές όπως μεταφορές χρημάτων και εμβάσματα ή ακόμα και για λειτουργίες όπως online επανέκδοση κωδικών internet banking και ερωτήσεις υπολοίπου. Αυτό το είδος ηλεκτρονικής τραπεζικής, έγινε λιγότερο διαδεδομένο με την ανάπτυξη της τεχνολογίας και των εφαρμογών λογισμικού, τα οποία έφεραν τη μέθοδο του internet banking στη καθημερινότητά μας. Το internet banking η οποία προσφέρει ένα πλήρες φάσμα προηγμένων τραπεζικών υπηρεσιών με απευθείας πρόσβαση στη ιστοσελίδα της εκάστοτε τράπεζας μέσω του διαδικτύου ή της αντίστοιχης εφαρμογής στο κινητό. Έτσι επιτεύχθηκε μια ψηφιακή υπηρεσία μέσω της οποίας οι πελάτες

μπορούν να απολαμβάνουν 24ωρη εξυπηρέτηση και να προχωράνε σε πραγματοποίηση συναλλαγών αλλά και ελέγχου αυτών, χωρίς να είναι απαραίτητη η επίσκεψή τους σε κατάστημα ή η τηλεφωνική επικοινωνία με την τράπεζα, μειώνοντας με αυτόν τον τρόπο το παραδοσιακό τραπεζικό κόστος, και δίνοντας την δυνατότητα στο πελατολόγιο των τραπεζών για άμεσες και εύκολες ενέργειες και υπηρεσίες.

Ως φυσικό και επόμενο, η ένταξη της ηλεκτρονικής τραπεζικής ως καθιερωμένο μέσο εξυπηρέτησης προκάλεσε άνοδο σε προκλήσεις, οι οποίες είχαν ως στόχο τον εντοπισμό ελαττωμάτων ασφαλείας των ηλεκτρονικών τραπεζικών συναλλαγών με αποτέλεσμα την απώλεια χρημάτων για τους κατόχους λογαριασμών καθώς και για τα χρηματοπιστωτικά ιδρύματα. Οι επιθέσεις ασφαλείας αυτές ποικίλουν και στοχοποιούν ευπάθειες σε λειτουργικά συστήματα, τις οποίες θα αναλύσουμε στο κομμάτι αυτό της εργασίας προσπαθώντας να τις κατηγοριοποιήσουμε.

Phishing – Vishing: Η απάτη του ηλεκτρονικού ψαρέματος έχει γίνει μια από τα πιο διαδεδομένα εγκλήματα τα τελευταία χρόνια. Η πιο συνηθισμένη μέθοδος μιας επίθεσης phishing είναι η αποστολή ψευδών ειδοποιήσεων μέσω ηλεκτρονικού ταχυδρομείου ή μέσω μηνυμάτων, τα οποία δολίως παρουσιάζουν ως αποστολέα την εκάστοτε τράπεζα, επιζητώντας από το εν δυνάμει θύμα, να προβεί σε κάποια άμεση ενέργεια παραπέμποντας σε ένα σύνδεσμο. Στη συνέχεια το θύμα οδηγείται σε έναν δόλιο ιστότοπο ο οποίος μοιάζει με την επίσημη ιστοσελίδα της τράπεζας, και ο χρήστης εσφαλμένα καταχωρεί τις εμπιστευτικές του πληροφορίες όπως το όνομα χρήστη και τον κωδικό πρόσβασης. Μόλις ο χρήστης εισάγει αυτά τα στοιχεία, ο επιτιθέμενος συλλέγει τις πληροφορίες αυτές και μπορεί στη συνέχεια να συνδεθεί στον τραπεζικό λογαριασμό του χρήστη για την διενέργεια δόλιων δραστηριοτήτων. Παραλλαγή του κλασσικού phishing που μόλις αναφέραμε είναι η επίθεση vishing, μέσω της οποίας γίνεται τηλεφωνική προσέγγιση του θύματος και πολλές φορές κοινοποιείται από το θύμα πρόσβαση σε κάποια συσκευή του συνδυάζοντας έτσι την απάτη phishing με απάτες με κακόβουλο λογισμικό τις οποίες θα δούμε στη συνέχεια. Μια ακόμα επίθεση που βασίζεται σε τεχνικές phishing, είναι η επίθεση Man-in-the-Middle, κατά την διάρκεια της οποίας, οι απατεώνες τοποθετούνται μεταξύ των τραπεζών και των πελατών, ενώ οι πελάτες χρησιμοποιούν τους ηλεκτρονικούς τραπεζικούς λογαριασμούς τους. Ως εκ τούτου, τόσο οι τράπεζες όσο και οι τελικοί χρήστες δεν αντιλαμβάνονται ότι οι συναλλαγές διενεργούνται από τους επιτιθέμενους, έως ότου τα χρήματα εξαφανιστούν χωρίς την εξουσιοδότηση του πελάτη.

Malware: Η συγκεκριμένη απάτη κακόβουλου λογισμικού αναφέρεται σε προγράμματα λογισμικού που εγκαθιστούν οι απατεώνες στις συσκευές των θυμάτων τους. Αυτό μπορεί να συμβεί όταν ένας πελάτης επισκέπτεται έναν μη εξουσιοδοτημένο ιστότοπο ή κατεβάζουν κάποια κακόβουλα προγράμματα τα οποία μπορεί να λαμβάνουν μέσω phishing και spam μηνυμάτων. Μια συνηθισμένη τεχνική είναι τα keyloggers, τα οποία είναι προγράμματα που εγκαθιστούνται αυτόματα στους υπολογιστές των χρηστών όταν αυτοί επισκέπτονται κάποια ιστοσελίδα με keyloggers ή κατεβάζουν ένα κομμάτι λογισμικού με keylogger. Αυτό έχεις ως αποτέλεσμα να αποκτήσουν οι απατεώνες πληροφορίες για τα διαπιστευτήρια των τραπεζικών λογαριασμών όπως το όνομα χρήστη και τον κωδικό πρόσβασης. Αφορά ουσιαστικά ένα λογισμικό το οποίο καταγράφει τις πληκτρολογήσεις που κάνει ο χρήστης, το οποίο είναι αρκετά διαδεδομένο καθώς δεν είναι γνώριμο και εύκολα αντιληπτό από το θύμα. Ένα τέτοιο περιστατικό συνέβη το 2006 σε έξι τράπεζες της Βραζιλίας, όπου απατεώνες χρησιμοποιούσαν keyloggers ώστε να συλλέξουν τα τραπεζικά δεδομένα των πελάτων, καταφέρνοντας να υποκλέψουν παραπάνω από 4,5 εκατομμύρια δολάρια [5].

DNS-based phishing: Το γνωστό ως pharming, είναι ένας άλλος τύπος επίθεσης phishing, το οποίο στοχεύει στον διαδικτυακό ιστότοπο μιας τράπεζας. Πιο συγκεκριμένα, αυτή η μορφή επίθεσης ανακατευθύνει τους χρήστες σε ένα ψεύτικο ιστότοπο, παρόλο που οι χρήστες πληκτρολογούν τις σωστές διευθύνσεις URL [6]. Αυτό επιτυγχάνεται με την παραποίηση του πρωτοκόλλου DNS, το οποίο είναι υπεύθυνο για την μετατροπή του host name σε διεύθυνση IP, με αποτέλεσμα ένας υπολογιστής που ακόμα και αν δεν έχει μολυνθεί από κάποιο κακόβουλο λογισμικό να μπορεί να αποτελεί δυνητικά ένα θύμα

επίθεσης. Η επίθεση στον διακομιστή DNS, γνωστή και ως DNS flooding , έχει ως στόχο την υπερφόρτωση του διακομιστή προκειμένου να εμποδίσει τους χρήστες να έχουν πρόσβαση στις υπηρεσίες του ασφαλούς παρόχου αλλά και να αποκρύψουν την προέλευση της επίθεσης και να αυξήσουν την αποτελεσματικότητά της

Sim Swapping: Αφορά μια επίθεση κατά την οποία οι απατεώνες αποκτούν τις προσωπικές πληροφορίες του θύματος και με την μέθοδο της ανταλλαγής sim κάνουν απατηλές κινήσεις μέσω του τραπεζικού τους λογαριασμού. Αρχικά είτε μέσω phishing, είτε τηλεφωνικά, είτε μέσω κοινωνικών δικτύων, αποσπούν από το θύμα τα διαπιστευτήρια του τραπεζικού του λογαριασμού. Στη συνέχεια, επικοινωνώντας με τον εκάστοτε πάροχο κινητής τηλεφωνίας, συνήθως με ψεύτικες εξουσιοδοτήσεις, γίνεται ανταλλαγή της κάρτας SIM αχρηστεύοντας την προηγούμενη, με αποτέλεσμα οι κωδικοί μιας χρήσεως που στέλνονται από την τράπεζα για επιβεβαίωση των κινήσεων να λαμβάνονται πλέον από τον θύτη.

Business compromise email: Αφορά μια μορφή επίθεσης phishing όπου ένας απατεώνας προσπαθεί με δόλιο τρόπο να ξεγελάσει ένα τρίτο άτομο προκειμένου να μεταφέρει χρήματα ή να αποκαλύψει ευαίσθητες πληροφορίες. Αυτό μπορεί να επιτευχθεί με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που μπορούν να ζητούν ασυνήθιστες πληρωμές ή να περιέχουν ιούς ως συνημμένα αρχεία. Συνήθως οι επιθέσεις αυτές στοχοποιούν πελάτες προμηθευτών ή εταιριών. Σε αντίθεση με τα τυπικά μηνύματα phishing που στέλνονται αδιακρίτως σε εκατομμύρια ανθρώπους, η συγκεκριμένη επίθεση απευθύνεται σε συγκεκριμένα άτομα. Αφορά μια απειλή για όλους τους οργανισμούς σε όλους τους τομείς, συμπεριλαμβανομένων και των μη κερδοσκοπικών ή κυβερνητικών οργανισμών.

2.3. Merchant Fraud

Εκτός από τα ηλεκτρονικά εγκλήματα που γίνονται εις βάρος των καταναλωτών είναι σημαντικό να σημειώσουμε τις απάτες των εμπόρων, που αποτελούν μια από τις πιο κοινές και δαπανηρές αιτίες οικονομικών απωλειών.

Αρχικά να αναφέρουμε οτι το τραπεζικό κομμάτι που ασχολείται με τους εμπόρους ονομάζεται Acquiring γνωστό και ως τράπεζα του εμπόρου (Timothy H.Hannan, 2009). Ο τομέας αυτός είναι υπεύθυνος για τον διακανονισμό των συναλλαγών με πιστωτικές και χρεωστικές κάρτες για λογαριασμό των εμπόρων. Πιο αναλυτικά, το Acquiring επιτρέπει στους εμπόρους να πραγματοποιούν πληρωμές, τους παρέχουν το απαιτούμενο λογισμικό για την αποδοχή των συναλλαγών με κάρτες (pos, epos, ανοικτές πληκτρολογήσεις), και λαμβάνουν ένα ποσοστό επι των διατραπεζικών αυτών συναλλαγών. Οι απάτη των εμπόρων είναι πολύ δύσκολη στην ανίχνευσή της, κυρίως λόγω της πολυπλοκότητας των ψηφιακών πληρωμών, παρόλα αυτά είναι επιτακτική η ανάγκη για αντιμετώπιση και πρόληψη της καθώς εμπεριέχει επιστροφές χρεώσεων, αμφισβητήσεις εις βάρος των εμπόρων με αποτέλεσμα την ζημία του εμπορικού σήματος ή ακόμα και κανονιστικές και νομικές κυρώσεις.

Εικονικές εταιρίες: Στο συγκεκριμένο είδος απάτης, ένας έμπορος υποβάλλει αίτηση για δημιουργία ενός εμπορικού λογαριασμού, χωρίς ωστόσο να προτίθεται να λειτουργήσει πραγματικά μια νόμιμη επιχείρηση. Είναι σύνηθες το φαινόμενο να πλαστογραφηθούν ταυτότητες και έγγραφα με αριθμούς κοινωνικής ασφάλειας ώστε να δημιουργηθούν ψεύτικες ή εικονικές επιχειρήσεις, οι οποίες δυστυχώς δεν καταφέρνουν να εντοπιστούν από τα παραδοσιακά KYC (Know Your Customer) προγράμματα τα οποία δεν μπορούν να παρακολουθούν συνεχώς την κατάσταση ενός υφιστάμενου λογαριασμού. Ο στόχος ενός τέτοιου εμπόρου είναι να πραγματοποιήσει όσο το δυνατόν περισσότερες απατηλές συναλλαγές μέσα σε μικρό χρονικό διάστημα, προτού εντοπιστεί από τα συστήματα ασφαλείας της τράπεζας, και στη συνέχεια απλά να «αδειάσει» και να καταργήσει τον λογαριασμό αυτόν, ο οποίος συνδέεται ήδη με υψηλά ποσοστά χρεώσεων. Όταν αναφέρουμε οτι ένας έμπορος δεν λειτουργεί ως νόμιμη επιχείρηση, εννοούμε οτι πραγματοποιεί τις χρεώσεις στους καταναλωτές χωρίς ωστόσο να παραδίδει το προϊόν ή την υπηρεσία. Επομένως, μόλις αρχίσουν να πληθαίνουν οι επιστροφές των χρεώσεων, αυτοί οι έμποροι συνηθώς έχουν ήδη κλείσει τον λογαριασμό, αφήνοντας πίσω τους μια χρεωμένη από αμφισβητήσεις επιχείρηση, ζημιώνοντας με αυτόν τον τρόπο την εκάστοτε τράπεζα τους. Ένα εγχώριο παράδειγμα συνέβη το 2021 όπου υποτιθέμενη εταιρία με προϊόντα με αρκετά ανταγωνιστικές τιμές, κατάφερε να εξαπατήσει συνολικά 187 πελάτες, στους οποίους δεν παρεδόθη ποτέ το προϊόν, με το ύψος της απάτης να υπολογίζεται σε παραπάνω από 53.000 ευρώ [7]. Μια λίγο διαφορετική περίπτωση, η οποία όμως έγκειται στην ίδια μορφή απάτης, είναι να προσκομιθούν πλαστές ή κλεμμένες ταυτότητες από έναν έμπορο για να δημιουργήσουν μια ψεύτικη βιτρίνα προκειμένου να εξασφαλίσουν έναν εμπορικό λογαριασμό. Συγκεκριμένα άτομα, όπως λόγου χάρη άτομα που περιλαμβάνονται στους καταλόγους παρακολούθησης AML/ATF (Anti Money Laundering / anti-terrorist financing), άτομα με κατασχετήρια από δημόσια αρχή, έμποροι από χώρες στις οποίες έχουν επιβληθεί οικονομικές ή νομικές κυρώσεις κ.α., απαγορεύεται να ανοίξουν εμπορικούς λογαριασμούς. Με αυτόν τον τρόπο, καταφέρνουν να δημιουργήσουν με πλαστά έγγραφα μια καθ' όλα νόμιμη επιχείρηση, η οποία μπορεί να οδηγήσει σε υψηλά πρόστιμα και σοβαρή ζημιά για την τράπεζα τους.

Ξέπλυμα χρήματος (AML): Το φαινόμενο του AML, το οποίο είναι ένα σημαντικό ποσοστό των οικονομικών απωλειών, συμβαίνει όταν μια άγνωστη επιχείρηση χρησιμοποιεί τα διαπιστευτήρια πληρωμών ενός εγκεκριμένου εμπόρου για να διεκπεραιώσει πληρωμές για προϊόντα και υπηρεσίες τις οποίες η τράπεζα του εμπόρου δεν γνωρίζει [8]. Έτσι, χωρίς την γνώση των εμπόρων (ή και με την άδειά τους σε αρκετά περιστατικά) καταφέρνουν και πραγματοποιούν παράνομες και άγνωστες συναλλαγές, οι οποίες μπορεί να απαγορεύονται από την τράπεζά τους, όπως για παράδειγμα πώληση αγαθών ή υπηρεσιών υψηλού κινδύνου ή συναλλαγές που δεν συμβαδίζουν με την κατηγορία του εμπόρου (Merchant Category Codes) όπως αυτή συμφωνήθηκε κατά την έναρξη της εμπορικής τους σχέσης.

2.4. Απάτες εις βάρος της τράπεζας

Όλες οι επιθέσεις που έχουμε ήδη προαναφέρει, αποτελούν μια απειλή στον κυβερνοχώρο κατά των χρηματοπιστωτικών ιδρυμάτων, οι οποίες με την αύξηση της ψηφιοποίησης έχουν οδηγήσει όχι μόνο στην αύξηση και στην έντασή τους, αλλά και στο επίπεδο της πολυπλοκότητάς τους. Ο σκοπός των επιθέσεων αυτών ωστόσο, δεν είναι μόνο η κλοπή των προσωπικών δεδομένων ή των κεφαλαίων των πελατών, αλλά και η βλάβη των τραπεζών και ως εκ τούτου και ολόκληρης της οικονομίας. Όπως αναφέρθηκε και στο Συμβούλιο Χρηματοπιστωτικής Σταθερότητας το 2020 από την πρόεδρο Κριστίν Λαγκάρντ, «μια κυβερνοεπίθεση εάν δεν περιοριστεί κατάλληλα θα μπορούσε να διαταράξει τα χρηματοπιστωτικά συστήματα οδηγώντας σε ευρύτερη χρηματοπιστωτική αστάθεια» [9], πράγμα που τονίζει την ανάγκη για πρόληψη και άμεση διαχείριση τέτοιων περιστατικών, καθώς οι επιπτώσεις τους μπορεί να χειραγωγήσουν ολόκληρη την οικονομία. Στο κομμάτι αυτό της εργασίας, θα δούμε τα είδη των επιθέσεων που σε αντίθεση με τα προαναφερθέντα, στοχοποιούν απευθείας τα τραπεζικά ιδρύματα καθώς και το δυναμικό τους.

Phishing: Το στοχευμένο phishing απευθύνεται σε εργαζόμενους με σκοπό την απόσπαση ευαίσθητων πληροφοριών και προσβάσεων, προκειμένου να αποκτήσουν πρόσβαση σε τραπεζικά δεδομένα. Τα συγκεκριμένα μηνύματα phishing μπορεί να περιέχουν ιούς και μολυσμένα αρχεία ή ακόμα και keyloggers τα οποία μπορεί να αποκαλύψουν πληροφορίες που δεν πρέπει. Ειδικά μετά την πανδημία και με το ξεκίνημα της εξ αποστάσεως απασχόλησης, αλλά και του αυξημένου φόρτου εργασίας που προέκυψε μέσω αυτής, το συγκεκριμένο είδος απάτης είχε τεράστια άνοδο, με αρκετές διαρροές διατραπεζικών δεδομένων.

Επιθέσεις Λυτρισμικού (Ransomware): Αρχικά πρέπει να αναφέρουμε οτι το λυτρισμικό είναι μια μορφή κακόβουλου λογισμικού, το οποίο εφόσον εγκατασταθεί σε έναν υπολογιστή ή μια βάση δεδομένων, κρυπτογραφεί σημαντικά αρχεία του θύματος, ζητώντας λύτρα για την αποκατάσταση της πρόσβασης. Τέτοιες επιθέσεις, μπορεί να χρησιμοποιούν διαφορετικά εργαλεία και μεθόδους για να παραβιάσουν συστήματα, τα οποία λαμβάνουν χώρα σε διάστημα αρκετών μηνών ή σε λίγο μόνο λεπτά. Η γνώση του τρόπου ανίχνευσης αλλά και η άμεση αντίδραση και η εφαρμογή αποτελεσματικών ελέγχων, είναι επιτακτικής σημασίας, ιδίως πριν από το βήμα της κρυπτογράφησης των δεδομένων. Σύμφωνα με την έκθεση της Verizon το 2021, οι απατεώνες εγκατέστησαν απευθείας το 30% του κακόβουλου λογισμικού το οποίο προσήλθε στα θύματα με ποσοστά 23% και 20% από email και από εφαρμογή αντιστοίχως. Ο αριθμός των επιθέσεων ransomware έχει αυξηθεί το τελευταίο έτος σε παγκόσμια κλίμακα, καθιστώντας το συγκεκριμένο είδος απάτης από τις πιο συχνές κυβερνοεπιθέσεις [10].

DLT attacks: Εκτός από τις απειλές που αντιμετωπίζουν τα παραδοσιακά τραπεζικά συστήματα, είναι σημαντικό να υπογραμμίσουμε οτι οι κυβερνοεπιθέσεις απευθύνονται και σε Fintech εταιρίες, οι οποίες αποτελούν δυνητικά μια νέα πραγματικότητα στον τραπεζικό τομέα. Με τον όρο DLT (Distributed ledger technology), εννοούμε ένα ψηφιακό σύστημα καταγραφής των συναλλαγών με ένα από τα πιο γνωστά παραδείγματα να είναι το Blockchain, το οποίο παρέχει την τεχνική υποδομή για τα κρυπτονομίσματα Bitcoin. Η αυξανόμενη κυβερνοαπειλή επηρέασε δραστικά και αυτόν τον τομέα. Ένα τέτοιο παράδειγμα αποκαλύφθηκε τον Φεβρουάριο του 2022, 6 χρόνια μετά την δράση του, όπου κατάφεραν μέσω κακόβουλου λογισμικού να διεισδύσουν στην Bitfinex και να κλέψουν μονάδες Bitcoins που πλέον αντιστοιχούν στο ποσό της τάξεως των 4,5 δις. ευρώ. Παρά την πολύ ισχυρή multiple-signature ασφάλεια, κατάφεραν να αποκρυπτογραφήσουν το κλειδί το οποίο χρησιμοποιούσαν στα blockchain, πραγματοποιώντας 2000 μεταφορές οι οποίες εγκρίθηκαν από τους παραβιασμένους λογαριασμούς των χρηστών [11]. Παρόλα αυτά, είναι σημαντικό να τονίσουμε ότι το μεγαλύτερο μέρος από τα κλεμμένα κρυπτονομίσματα έχουν ήδη εντοπιστεί και ανακτηθεί γεγονός που δείχνει πως τα blockchain μπορούν να βοηθήσουν στον εντοπισμό της ροής των κεφαλαίων και πως μπορούν να συνδράμουν στην καταπολέμηση του ηλεκτρονικού εγκλήματος.

3. Ανίχνευση Απάτης

Η ηλεκτρονική τραπεζική κερδίζει συνεχώς δημοτικότητα μέρα με τη μέρα, καθώς συνδυάζει την ευκολία και την αμεσότητα στις συναλλαγές, όπως για παράδειγμα τις ηλεκτρονικές αγορές, τις ηλεκτρονικές πληρωμές λογαριασμών, τις μισθοδοσίες κτλ, οδηγώντας έτσι στην αύξηση των περιπτώσεων απάτης τα οποία επηρεάζουν σε μεγάλο βαθμό τόσο τους πελάτες όσο και τους οικονομικούς φορείς. Αυτά τα περιστατικά θεωρούνται εγκλήματα στον κυβερνοχώρο, και προτού προχωρήσουμε στους τρόπους με τους οποίους προσπαθούν τα τραπεζικά ιδρύματα να τα καταπολεμήσουν, είναι σημαντικό να αναγάγουμε τα είδη της απάτης σε δυο βασικούς πυλώνες, δηλαδή σε «offline απάτες», όπως για παράδειγμα κλοπή κάρτας, ή κάποιου άλλου σημαντικού εγγράφου όπως είναι η ταυτότητα, το δίπλωμα οδήγησης κ.α., και «online απάτες» όπου αφορά τις διαδικτυακές απάτες, όπως για παράδειγμα ένα phishing μήνυμα που χρησιμοποιείται για να αποσπάσει προσωπικά τραπεζικά δεδομένα που μπορούν να οδηγήσουν σε εκτέλεση απατηλών συναλλαγών εις βάρος του πελάτη. Στη συνέχεια του κεφαλαίου αυτού, θα προσδιορίσουμε κάποιους από τους υφιστάμενους μηχανισμούς ασφαλείας που χρησιμοποιούνται ως μέτρο ανίχνευσης των απατηλών κινήσεων από τα τραπεζικά ιδρύματα, και στοχεύουν στο να τις αποτρέψουν ή τουλάχιστον να τις μειώσουν σημαντικά, τόσο στις απάτες που διενεργούνται μέσω καρτών (καρτικό fraud), όσο και στις απάτες που γίνονται μέσω της ηλεκτρονικής τραπεζικής (e-banking fraud).

Address Verification Service (AVS): Με αυτή τη τεχνική ταυτοποιείται η διεύθυνση χρέωσης του κατόχου της κάρτας με την διεύθυνση αποστολής, και προσδιορίζεται αν ο κάτοχος έχει αγοράσει ξανά προϊόν σε αυτή τη διεύθυνση. Ωστόσο, αυτή η τεχνική παρουσιάζει κάποιες αδυναμίες, καθώς δεν ζητάνε όλες οι ηλεκτρονικές συναλλαγές διεύθυνση παράδοσης, και επίσης είναι αρκετά χρονοβόρα σαν διαδικασία να ελέγχεται όλο το αρχείο του πελάτη σε κάθε συναλλαγή που πραγματοποιεί. Σίγουρα, όταν χρησιμοποιείται μια νέα διεύθυνση αυτό μπορεί να αποτελεί μια ένδειξη για μια δυνητικά απατηλή συναλλαγή αλλά αυτό δεν αποτελεί ικανή και αναγκαία συνθήκη για την απόρριψη μιας τέτοιας κίνησης. Ίσως η συγκεκριμένη τεχνική θα μπορούσε να είχε καλύτερα αποτελέσματα πριν αρκετά χρόνια, που ο όγκος των ηλεκτρονικών συναλλαγών που πραγματοποιούνταν ανά λεπτό δεν ήταν τόσο αυξημένος, χωρίς αυτό να σημαίνει οτι δεν μπορεί να συνδυαστεί αυτή η μέθοδος με άλλες προκειμένου να δώσει ένα αρκετά ακριβές μοτίβο ανίχνευσης των απατών.

Fraud Rates: Αυτή η τεχνολογία ελέγχει για γνωστά μοτίβα που χρησιμοποιούνται από τους απατεώνες για την διάπραξη απάτης. Πολλές φορές, ειδικά όταν μιλάμε για καρτικό fraud, οι απατεώνες «τεστάρουν» τις κάρτες σε συγκεκριμένους εμπόρους προκειμένου να ελέγξουν εάν τα στοιχεία τις κάρτας που έχουν στη διάθεση τους είναι σωστά. Αυτό γίνεται συνήθως σε εμπόρους οι οποίοι δεν έχουν μεγάλη κινητικότητα, και σε εμπόρους που συνήθως δεν συμβαδίζουν με το συναλλακτικό προφίλ των πελατών (για παράδειγμα, ένα πελάτης που κατοικεί στην Ελλάδα είναι σχεδόν απίθανο να χρησιμοποιήσει την κάρτα του σε εφαρμογή φαγητού που δραστηριοποιείται στην Αμερική). Ένα άλλο παράδειγμα αφορά τα μαζικά περιστατικά που γίνονται στο καρτικό fraud. Πιο συγκεκριμένα, η απάτη bin attack, αφορά μια επίθεση που εφαρμόζεται σε κάρτες με το ίδιο bin και την ίδια ημερομηνία λήξεως, και τα υπόλοιπα ψηφία συμπληρώνονται συστημικά με τυχαίο τρόπο. Αυτή η απάτη, δεδομένου οτι προσπαθεί να μαντέψει επι της ουσίας τα στοιχεία μιας υπαρκτής κάρτας, μπορεί να διαρκέσει αρκετό διάστημα, και αποτελεί ένα μοτίβο το οποίο η τράπεζα μπορεί να εντοπίσει και στη συνέχεια να το αποτρέψει από το να προκαλέσει οικονομική απώλεια εις βάρος των πελατών.

Relocation: Αυτή η τεχνολογία ανιχνεύει την γεωγραφική θέση του πελάτη μέσω της διεύθυνσης IP που χρησιμοποιεί. Γενικά, στο διαδίκτυο όποια κίνηση και εάν πραγματοποιείται αφήνει πίσω της ένα ηλεκτρονικό στίγμα, είτε αυτό είναι του απατεώνα είτε του πελάτη του ίδιου. Είναι παρόμοια τεχνική με την AVS που αναφέραμε προηγουμένως, απλά σε μια πιο εξελιγμένη μορφή που συμβαδίζει με την άνοδο των

ηλεκτρονικών συναλλαγών και μπορεί να αξιοποιηθεί πιο εύκολα και σωστά. Πρέπει να σημειωθεί ότι οι διευθύνσεις IP μπορούν πολύ εύκολα να αλλοιωθούν με κάποιο πρόγραμμα virtual private network (vpn) κάτι που τις καθιστά πολύ εύθραυστο κριτήριο για να θεωρηθεί μια κίνηση απατηλή, καθώς ένας πελάτης μπορεί καθημερινώς να αλλάζει την IP την οποία χρησιμοποιεί. Παρόλα αυτά, αξίζει να αναφέρουμε οτι αυτό το ηλεκτρονικό αποτύπωμα, όταν ιδίως αφήνεται από τον απατεώνα είναι πολύ σημαντικό για την εύρεση μοτίβων και την σύνδεση των διευθύνσεων IP με τα αντίστοιχα περιστατικά απάτης, γεγονός που βοηθάει στην πρόληψη τους και στην αντιμετώπισή τους.

Chip & Pin: Το PIN είναι ο μυστικός τετραψήφιος κωδικός που πρέπει να εισάγει ο πελάτης πριν από την εκτέλεση μιας συναλλαγή με κάρτα. Είναι ένας αρκετά εύκολος τρόπος προκειμένου να διαπιστωθεί αν μια συναλλαγή είναι γνήσια η όχι. Σαφώς υπάρχουν περιστατικά απάτης στα οποία ο μυστικός αυτός κωδικός κοινοποιείται σε κάποιο τρίτο άτομο, είτε ακούσια είτε εκούσια, και στη συνέχεια γίνονται απατηλές συναλλαγές τις οποίες ο πελάτης δεν αναγνωρίζει. Βέβαια αυτό έγκειται σε offline fraud το οποίο είναι συγκριτικά πολύ μικρό σε όγκο σε σχέση με το online fraud, και είναι και αρκετά δύσκολο στον εντοπισμό του.

3D-Secure: Αυτή η τεχνολογία λειτουργεί με αυθεντικοποίηση της συναλλαγής προτού αυτή πραγματοποιηθεί, η οποία πρέπει να γίνει από πλευράς του πελάτη μέσω της ηλεκτρονικής τραπεζικής του. Αυτό σημαίνει οτι για να εκτελέσει ένας απατεώνας μια τέτοια συναλλαγή χρειάζεται τον κωδικό της αυθεντικοποίησης, και τα τραπεζικά διαπιστευτήρια του πελάτη. Το 3DS είναι ουσιαστικά ένα εργαλείο που επιτρέπει σε έναν έμπορο να επιτύχει το Strong Customer Authentication (SCA), το οποίο προτάθηκε από τον διεθνή οργανισμό της Visa το 1999, και τέθηκε σε ισχύ στην Ευρώπη τον Σεπτέμβριο του 2019 βάσει των οδηγιών του PSD2 (Payment Services Directive). Είναι ένα μέτρο που είχε ως στόχο την αύξηση στην ασφάλεια των συναλλαγών στο ηλεκτρονικό εμπόριο, συνάμα ωστόσο βοήθησε την διαδικασία της αμφισβήτησης μεταξύ των τραπεζών (chargeback procedure), παρέχοντας έτσι επιπλέον προστασία στους εμπόρους.

Βιομετρικά δεδομένα: Αφορούν σε μοναδικά χαρακτηριστικά κάθε πελάτη, όπως δακτυλικά αποτυπώματα, φωνή, υπογραφή κ.α., τα οποία αποθηκεύονται προκειμένου να διαπιστωθεί εάν το άτομο που πραγματοποίησε την συναλλαγή είναι ο ίδιος ο πελάτης. Το κύριο μειονέκτημα αυτής της μεθόδου, είναι οτι η τεχνολογία πίσω της είναι κοστοβόρα και απαιτεί επιπλέον κόστος σε υλικό. Είναι πολύ σημαντικό από την πλευρά της τράπεζας να μπορεί να εντοπίσει πώς πραγματοποιήθηκε μια συναλλαγή και τον τρόπο με τον οποίο αυτή επιβεβαιώθηκε, καθώς με την άνοδο των περιστατικών απάτης υπάρχει και άνοδος των περιστατικών που ψευδώς δηλώνουν οτι έχουν εξαπατηθεί προκειμένου να αποκομίσουν κέρδος από την αποζημίωση της τράπεζάς τους. Τα περιστατικά απάτης δεν στοχοποιούν μονάχα τους πελάτες ή τους εμπόρους των τραπεζών, πολλές φορές μπορεί να γίνονται με σκοπό να βλάψουν την ίδια την τράπεζα, είτε με σκοπό το οικονομικό όφελος είτε την βλάβη στην δημοτικότητα του ιδρύματος. Φυσικά ο αριθμός αυτών τον περιστατικών είναι ένα πολύ μικρό κομμάτι στο σύνολο των εγκλημάτων στον κυβερνοχώρο. Παρόλα αυτά, χρειάζεται και αυτό την σωστή καταπολέμησή του.

One Time Password (OTP): Αφορά έναν τυχαίο κωδικό μιας χρήσης, που δημιουργείται από τον διακομιστή, και αποστέλλεται στον πελάτη στο κινητό του τηλέφωνο, προκειμένου να διασφαλιστεί οτι ο σωστός χρήστης εκτελεί εκείνη την στιγμή την συναλλαγή. Ο χρήστης πρέπει να εισάγει τον κωδικό αυτόν προκειμένου να λάβει την εξουσιοδότηση από την πλευρά της τράπεζας του για την διεκπεραίωση της συναλλαγής. Η διαφορά με την προηγούμενη τεχνική που αναφέραμε πιο πάνω, είναι οτι το OTP στέλνεται για επιβεβαίωση της συναλλαγής όπου θεωρεί η τράπεζα ότι είναι αναγκαίο, γεγονός που σημαίνει οτι κάποιες φορές η επιβεβαίωση με τα βιομετρικά δεδομένα δεν αρκεί και χρειάζεται και ο επιπλέον κωδικός. Στα περισσότερα περιστατικά απάτης ο μυστικός αυτός κωδικός κοινοποιείται στον απατεώνα είτε

τηλεφωνικά είτε γραπτά, και στη συνέχεια μπορεί και πραγματοποιεί τις απατηλές συναλλαγές. Για αυτόν κιόλας τον λόγο, συνήθως δεν χρησιμοποιείται μόνο ο κωδικός OTP για την επιβεβαίωση μιας συναλλαγής αλλά μαζί με κάποιο βιομετρικό δεδομένο, όπως είναι το quick login ή η τηλεφωνική επιβεβαίωση με τον πελάτη.

Transaction Risk Score Generation Method (TRSGM): Το risk score χρησιμοποιείται για τον υπολογισμό του ρίσκου του κινδύνου μιας συναλλαγής και κατά πόσο αυτή η συναλλαγή έχει πιθανότητες να είναι απατηλή. Πιο αναλυτικά, αυτό το ρίσκο αντιπροσωπεύει την πιθανότητα μια συναλλαγή να θεωρηθεί απατηλή και υπολογίζεται με βάση το συναλλακτικό προφίλ του πελάτη, τις δαπάνες του καθώς και την γεωγραφική του τοποθεσία. Επί της ουσίας, ο βαθμός του ρίσκου υπολογίζεται συγκρίνοντας το ποσό της συναλλαγής με τα ποσά των προγενέστερων κινήσεων του πελάτη, καθώς και την τοποθεσία του σε σχέση με την προηγούμενη και κατά πόσο η διαφορά την γεωγραφικής του θέσης στο χρονικό διάστημα που έχει παρέλθει μεταξύ της προηγούμενης κίνησης με την τωρινή ανταποκρίνεται σε λογικά πλαίσια. Εάν η συναλλαγή θεωρηθεί ως ύποπτη κίνηση που δεν πραγματοποιείται από τον πελάτη, ο μηχανισμός ασφαλείας ενδέχεται να του ζητήσει κάποια επιπρόσθετη επιβεβαίωση της κίνησης όπως για παράδειγμα ένα OTP. Η τελική τιμή του risk score υπολογίζεται με το θεώρημα του Bayes, το οποίο βασίζεται στη μεταγενέστερη πιθανότητα, και αφορά αποκλειστικά τις ηλεκτρονικές συναλλαγές.

3.1. Τεχνητή Νοημοσύνη (ΤΝ)

Οι τεχνολογίες που βασίζονται στην ΤΝ έχουν συμβάλλει στην δημιουργία καινοτομιών, και έπαιξαν κρίσιμο ρόλο στην επέκταση των εξατομικευμένων και δημιουργικών λύσεων σε περιστατικά απάτης. Το φαινόμενο της τεχνητής νοημοσύνης επικεντρώνεται κυρίως στην ενσωμάτωση της φυσικής νοημοσύνης που συνδέεται με τους ανθρώπους, όπως η ικανότητα ανάλυσης, κατανόησης των διάφορων προτύπων και μοτίβων, αξιολόγησης και εξαγωγής συμπερασμάτων, εφαρμόζοντας ολοκληρωμένες προσεγγίσεις. Τα προηγμένα εργαλεία και οι μέθοδοι καταπολέμησης της οικονομικής απάτης, όπως η εξόρυξη δεδομένων και η ψηφιακή έρευνα, δεν εφαρμόζονται με εκτεταμένο τρόπο λόγω των προβλημάτων κόστους. Ωστόσο, οι εξελίξεις στις τεχνολογίες και στις εικονικές πλατφόρμες έχουν οδηγήσει σε μεγάλη άνοδο των εγκλημάτων στον κυβερνοχώρο, με αποτέλεσμα η χρήση της ΤΝ ως μέσο ανίχνευσης και καταπολέμησης τους, να μην αποτελεί πλέον πολυτέλεια, αλλά αναγκαιότητα για τον έλεγχο της οικονομικής απάτης. Υπάρχουν αρκετοί τρόποι και εφαρμογές ΤΝ για τον εντοπισμό απάτης στον κλάδο των χρηματοπιστωτικών υπηρεσιών, όπως η ανάλυση των συναλλαγών καθώς και η ομαδοποίηση των καταναλωτών βάσει των συναλλακτικών τους συνηθειών. Όλες αυτές οι προσεγγίσεις είναι απαραίτητες για την οικοδόμηση μιας ισχυρής στρατηγικής ανίχνευσης απάτης και κάτωθι θα αναλύσουμε τις τεχνικές οι οποίες χρησιμοποιούνται για την υλοποίηση αυτής της στρατηγικής.

Δημιουργία συναλλακτικών προφίλ πελατών: Για την ακριβή ανίχνευση της απάτης, τα χρηματοπιστωτικά ιδρύματα πρέπει πρώτα να κατανοήσουν την κανονική ή συνηθισμένη συμπεριφορά των πελατών. Με τη χρήση της τεχνητής νοημοσύνης, οι τράπεζες μπορούν να δημιουργήσουν και να κατανείμουν τους πελάτες σε διάφορα ξεχωριστά προφίλ. Τα συναλλακτικά προφίλ αυτά είναι αρκετά χρήσιμα καθώς παρέχουν μια ενημερωμένη εικόνα της δραστηριότητας ενός λογαριασμού και βοηθούν σε προβλέψεις για μελλοντική συμπεριφορά. Για παράδειγμα, ένας πελάτης μπορεί να συνηθίζει την πραγματοποίηση συναλλαγών σε ταξιδιωτικά γραφεία ανά τρίμηνο, να εφοδιάζει το αυτοκίνητο του με βενζίνη μετά την δουλειά, ή να παραγγέλνει φαγητό από εστιατόρια τα Σαββατοκύριακα. Επομένως, βάσει των δραστηριοτήτων του πελάτη, μπορεί να δημιουργηθεί ένα αντίστοιχο συναλλακτικό προφίλ, το οποίο θα ενημερώνεται σε πραγματικό χρόνο μετά από κάθε συναλλαγή. Καθώς πραγματοποιούνται οι συναλλαγές, η τεχνητή νοημοσύνη καθορίζει αν ταιριάζουν με το μοτίβο των κινήσεων που αποτελούν το προφίλ του πελάτη, ή αν μπορούν να χαρακτηριστούν ως σημαντικά διαφορετικές από τον κανόνα.

Εκτίμηση απάτης: Σε όλες τις συναλλαγές που πραγματοποιούνται, μπορεί να αποδοθεί μια βαθμολογία που θα εκτιμά το ρίσκο για απάτη, με βάση τις προηγούμενες γνήσιες συναλλαγές, τα γνωστά περιστατικά απάτης και παραμέτρους ασφαλείας που έχει ορίσει το εκάστοτε χρηματοπιστωτικό ίδρυμα. Αυτή η βαθμολογία, η οποία λαμβάνει υπόψιν της μεταβλητές όπως το ποσό της συναλλαγής, το χρόνο, τη συχνότητα, την ηλεκτρονική διεύθυνση IP κ.α., οι οποίες χρησιμοποιούνται για την αυτόματη έγκριση της συναλλαγής, την επισήμανση για επανεξέταση, ή ακόμα και την αυτόματη απόρριψη της. Με τη βοήθεια της μηχανικής μάθησης, η ακρίβεια της εκτίμησης της απάτης βελτιώνεται με την πάροδο του χρόνου.

Fraud investigation: Οι αλγόριθμοι μηχανικής μάθησης, μπορούν να αναλύσουν εκατοντάδες συναλλαγές ανά δευτερόλεπτο. Αυτό είναι ιδιαίτερα σημαντικό ώστε να χειρίζεται με επιτυχία ο ανεξέλεγκτος αριθμός των συναλλαγών και να επισημαίνονται εκείνες οι κινήσεις οι οποίες χρειάζονται περαιτέρω διερεύνηση. Οι εφαρμογές ΤΝ βοήθησαν επομένως ώστε να ελέγχονται με προτεραιότητα οι κινήσεις εκείνες οι οποίες έχουν την μεγαλύτερη πιθανότητα να είναι απατηλές και να διαχειρίζονται πιο άμεσα.

Know your client (KYC): Η τεχνητή νοημοσύνη, μπορεί να αξιοποιηθεί για την επαλήθευση και την επικαιροποίηση ταυτοτήτων και εγγράφων, και είναι μια διαδικασία η οποία πραγματοποιείται καθ' όλη την

διάρκεια της σχέσης με τον πελάτη. Είναι μια διαδικασία ζωτικής σημασίας για την πρόληψη της απάτης, τον έλεγχο των εσόδων από παράνομες δραστηριότητες και άλλων οικονομικών εγκλημάτων. Τα τρία διαφορετικά χαρακτηριστικά που αποτελούν το KYC είναι το πρόγραμμα ταυτοποίησης πελατών (Customer Identification Program), ο υπολογισμός της αξίας του πελάτη (Customer Due Diligence), και η συνεχής παρακολούθηση του (Ongoing Monitoring).

Η τεχνητή νοημοσύνη αποτελεί μια νέα ευκαιρία για τις τράπεζες και τους χρήστες, ώστε να διασφαλίσουν τις αποταμιεύσεις τους και τις καταθέσεις τους. Φυσικά υπάρχουν αρκετοί κίνδυνοι αλλά χωρίς την χρήση των εφαρμογών της ΤΝ η απώλεια των χρημάτων από περιστατικά απάτης θα είναι ακόμα μεγαλύτερη, δοσμένης της αύξησης του αριθμού των δόλιων συναλλαγών στον τραπεζικό τομέα. Τα σύγχρονα συστήματα αντιμετώπισης και ανίχνευσης απάτης συμβάλλουν σημαντικά στην προστασία των χρηστών από τις επιθέσεις, χωρίς αυτό να σημαίνει οτι δεν πρέπει να συνεχιστεί η ενημέρωση στους καταναλωτές για τους νέους τύπους απάτης και πως μπορούν και οι ίδιοι να προστατευτούν. Η χρήση των δυνατοτήτων της τεχνητής νοημοσύνης θα βοηθήσει σημαντικά τα υφιστάμενα αντίμετρα και θα δημιουργήσει ένα ισχυρό συνεργικό αποτέλεσμα στην καταπολέμηση της απάτης στα χρηματοπιστωτικά ιδρύματα.

4. Εξόρυξη δεδομένων

Οι προκλήσεις για τον εντοπισμό της απάτης είναι πολύ μεγάλες δεδομένου οτι καθημερινά πραγματοποιούνται εκατομμύρια συναλλαγές, και η εξαγωγή τόσο μεγάλου όγκου δεδομένων από μια βάση δεδομένων απαιτεί εξαιρετικά αποτελεσματικές τεχνικές. Επιπλέον, οι απάτες γίνονται συνήθως αντιληπτές αφού έχουν ήδη συμβεί καθώς είναι ιδιαίτερα δύσκολο να προβλεφθούν οι συμπεριφορές των χρηστών, οι οποίες αλλάζουν συνεχώς. Για αυτόν τον λόγο, χρησιμοποιείται η εξόρυξη δεδομένων ως τεχνική για την ανίχνευση της οικονομικής απάτης, καθώς μπορεί να εντοπίσει νέες επιθέσεις πριν αυτές οδηγήσουν στην οικονομική απώλεια και προτού αυτές ανιχνευτούν από τον ανθρώπινο παράγοντα. Η εξόρυξη δεδομένων χρησιμοποιεί τεχνικές όπως τεχνητή νοημοσύνη και νευρωνικά δίκτυα για την εξαγωγή και ανάκτηση χρήσιμων πληροφοριών από μια μεγάλη βάση δεδομένων. Κάποιες από τις τεχνικές που χρησιμοποιούνται παρουσιάζονται παρακάτω

- Συσχέτιση (Association): Αφορά τις συσχετίσεις μεταξύ των σχέσεων των διάφορων χαρακτηριστικών των συναλλαγών, που αποκαλύπτουν υπάρχοντα μοτίβα. Οι κανόνες συσχέτισης αφορούν στοιχεία που χαρακτηρίζουν κάθε συναλλαγή, όπως για παράδειγμα το είδος των συναλλαγών που πραγματοποιήθηκαν, την ηλικιακή ομάδα του πελάτη, καθώς κι ότι άλλο προσδιορίζει το άτομο που χρησιμοποιεί αυτή τη μορφή πληρωμής.
- Ταξινόμηση (Classification): Η ταξινόμηση είναι μια τεχνική εξόρυξης δεδομένων που βασίζεται στην μηχανική μάθηση και χρησιμοποιείται προκειμένου να κατηγοριοποιήσει κάθε στοιχείο ενός συνόλου δεδομένων σε ένα από τα προκαθορισμένα σύνολα κλάσεων ή ομάδων. Για να επιτευχθεί αυτό, γίνεται χρήση μαθηματικών τεχνικών όπως τα δέντρα αποφάσεων, τον γραμμικό προγραμματισμό, τα νευρωνικά δίκτυα, την στατιστική κ.α. Ένα παράδειγμα ταξινόμησης είναι δοθέντων των παρελθοντικών αρχείων των δόλιων συναλλαγών, να μπορεί να προβλεφθεί τι πιθανότητα έχει μια συναλλαγή να είναι απατηλή, και τι στοιχεία χαρακτηρίζουν μια τέτοια συναλλαγή. Στη περίπτωση αυτή, η ταξινόμηση διαχωρίζει τις συναλλαγές σε δύο ομάδες, οι οποίες είναι οι γνήσιες συναλλαγές και οι απατηλές συναλλαγές.
- Ομαδοποίηση (Clustering): Μια συστάδα είναι μια συλλογή δεδομένων που είναι παρόμοια μεταξύ τους εντός της ίδια συστάδας, και είναι ανόμοια με τα αντικείμενα σε άλλες συστάδες. Πρόκειται ουσιαστικά για μια συλλογή αντικειμένων και χαρακτηριστικών με βάση την ομοιότητα και τη διαφορετικότητα που έχουν μεταξύ τους. Η ομαδοποίηση αποτελεί βασικό εργαλείο για την ανίχνευση της απάτης, καθώς ακυρώνει μέσα που χρησιμοποιήθηκαν για την διενέργεια μιας απάτης, όπως τραπεζικούς λογαριασμούς, οι οποίοι έχουν προηγουμένως χρησιμοποιηθεί για κάποια απατηλή συναλλαγή
- Πρόβλεψη (Prediction): Η πρόβλεψη είναι μια από τις μεθόδους εξόρυξης δεδομένων που ανακαλύπτουν τη σχέση μεταξύ των ανεξάρτητων μεταβλητών, και τη σχέση μεταξύ των ανεξάρτητων και εξαρτημένων μεταβλητών. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί και στα περιστατικά απάτης στα οικονομικά ιδρύματα, θεωρώντας ως ανεξάρτητη μεταβλητή τα στοιχεία μιας συναλλαγής και ως εξαρτημένη μεταβλητή εάν αυτή η συναλλαγή είναι γνήσια ή απατηλή.

Η ανίχνευση της απάτης βασίζεται πάνω σε τρεις βασικές προσεγγίσεις:

- Supervised Approach: Στην επιβλεπόμενη μάθηση, η απάτη μπορεί να ανιχνευθεί με την ανάλυση των προηγούμενων συναλλαγών του πελάτη συγκρίνοντας τη με την τρέχουσα. Χρησιμοποιείται δηλαδή τεχνική της ταξινόμησης για την ανίχνευση της απάτης
- Semi Supervised Approach: Η προσέγγιση με ημιεπίβλεψη είναι μια μέθοδος η οποία μπορεί να χρησιμοποιηθεί για την πρόβλεψη όλων των ακραίων τιμών, που στη προκειμένη περίπτωση είναι οι δραστηριότητες που παρεκκλίνουν από το συναλλακτικό προφίλ ενός πελάτη, υποδεικνύοντας έτσι τις συναλλαγές που ενδεχομένως να μην πραγματοποιούνται από τον νόμιμο κάτοχο του λογαριασμού.

- Unsupervised Approach: Αυτή η προσέγγιση μη επιβλεπόμενης μάθησης, χρησιμοποιείται για την ανίχνευση ασυνήθιστων κινήσεων όπως για παράδειγμα συναλλαγές, πελάτες ή λογαριασμούς των οποίων η συμπεριφορά μπορεί να είναι διαφορετική από την κανονική.

Για την ανίχνευση της απάτης στα οικονομικά ιδρύματα, συνήθως γίνεται χρήση μη επιβλεπόμενης μάθησης. Οι μέθοδοι χωρίς επίβλεψη δεν χρειάζονται την προηγούμενη γνώση των γνήσιων και των απατηλών συναλλαγών καθώς είναι ικανές να εντοπίζουν τις αλλαγές στη συναλλακτική συμπεριφορά των πελατών αλλά και τις ασυνήθιστες συναλλαγές. Αυτές οι μέθοδοι μοντελοποιούν μια βασική κατανομή που αντιπροσωπεύει την κανονική συναλλακτική συμπεριφορά του πελάτη και στη συνέχεια ανιχνεύουν παρατηρήσεις που παρουσιάζουν μεγαλύτερη απόκλιση από αυτήν. Από την άλλη πλευρά, οι μέθοδοι με επίβλεψη απαιτούν ακριβή γνώση των δόλιων συναλλαγών από την βάση δεδομένων, προκειμένου να μπορούν να κατανέμουν την νέα συναλλαγή στην αντίστοιχα κλάση, και ως αποτέλεσμα μπορούν να εφαρμοστούν σε περιστατικά απάτης τα οποία έχουν πραγματοποιηθεί στο παρελθόν. Ένα πλεονέκτημα της χρήσης μη επιβλεπόμενων προσεγγίσεων είναι οτι μπορούν να αποκαλύψουν νέες μεθόδους απάτης, και να αποκρυπτογραφήσουν καινούργια μοτίβα που χρησιμοποιούν οι απατεώνες τα οποία έπειτα μπορούν να αξιοποιηθούν για την αντιμετώπιση τους.

4.1. Προκλήσεις στην εξόρυξη δεδομένων

Τα συστήματα ανίχνευσης απάτης έρχονται αντιμέτωπα με αρκετές προκλήσεις και ζητήματα τα οποία πρέπει να ξεπεράσουν προκειμένου να πετύχουν καλύτερη απόδοση και μεγαλύτερη αποτελεσματικότητα. Τις δυσκολίες αυτές θα απαριθμήσουμε παρακάτω:

- Imbalanced and Overlapping data: Τα σύνολα δεδομένων που σχετίζονται με τα περιστατικά απάτης είναι από την φύση τους μη ισορροπημένα, καθώς πολύ μικρά ποσοστά των συναλλαγών που εκτελούνται σε καθημερινή βάση είναι απατηλά. Αυτό καθιστά την ανίχνευση των απατηλών συναλλαγών πολύ δύσκολη και ανακριβή, λόγω του μεγάλου όγκου λανθασμένων ειδοποιήσεων, δηλαδή ειδοποιήσεων που θεωρούν μια συναλλαγή δόλια, ενώ στην πραγματικότητα δεν είναι. Κατά την διαδικασία ανίχνευσης απάτης, υπάρχει και η πιθανότητα λανθασμένης ταξινόμησης κάποιας συναλλαγής. Η λανθασμένη ταξινόμηση μιας γνήσιας συναλλαγής ως απάτης δεν είναι τόσο σημαντικό ζήτημα, δεδομένου ότι το λάθος θα εντοπιστεί σε περαιτέρω έρευνες, ωστόσο όταν το σύστημα αποτυγχάνει στον εντοπισμό μιας συναλλαγής ως απατηλής, καταλήγει στο να υπάρξει οικονομική ζημία εις βάρος του πελάτη. Ως εκ τούτου, η επίτευξη χαμηλού ποσοστού false positive και false negative ειδοποιήσεων αποτελεί βασική πρόκληση των συστημάτων ανίχνευσης.
- Έλλειψη προσαρμοστικότητας: Οι αλγόριθμοι ταξινόμησης, αντιμετωπίζουν συνήθως το πρόβλημα της ανίχνευσης νέων τύπων κανονικών ή δόλιων μοτίβων. Πολλές φορές, τα συστήματα ανίχνευσης αδυνατούν να εντοπίσουν τα νέα μοτίβα και τα νέα είδη απάτης που χρησιμοποιούν οι απατεώνες, με αποτέλεσμα αρκετές απατηλές συναλλαγές να μην διαχειρίζονται έγκαιρα και να οδηγούν σε οικονομικές απώλειες.
- Κόστος ανίχνευσης απάτης: Το σύστημα θα πρέπει να λαμβάνει υπόψη τόσο το κόστος της απάτης που ανιχνεύεται όσο και το κόστος της πρόληψής του. Όπως είναι φυσικό, δεν δύναται να απορρίπτονται όλες οι συναλλαγές για υπόνοια απάτης καθώς αυτό θα οδηγήσει στην δυσαρέσκεια του πελατολογίου της τράπεζας, την ταλαιπωρία τους για την μη διεκπεραίωση των κινήσεων τους και ένα κλίμα έλλειψης εμπιστοσύνης των πελατών στην τράπεζα τους. Από την άλλη πλευρά, δεν μπορούν να πραγματοποιούνται συνεχώς δόλιες συναλλαγές εις βάρος των πελάτων χωρίς αυτές να εντοπίζονται από τα συστήματα ασφαλείας και ανίχνευσης. Αυτή είναι μια τεράστια πρόκληση, δηλαδή η εξυπηρέτηση των πελατών άμεσα και εύκολα, αλλά ταυτόχρονα να γίνεται σωστός έλεγχος των κινήσεων, ο οποίος έλεγχος δεν θα επηρεάζει άμεσα τη διαδικασία εκτέλεσης της συναλλαγή από μεριάς του πελάτη.

Οι τεχνικές ανίχνευσης επικεντρώνονται τόσο στην ανάλυση της απάτης και την ταξινόμησή της ως δόλια ή γνήσια, όσο και στην ανάλυση της συμπεριφοράς των χρηστών, που ανάγεται στην ανίχνευση ανωμαλιών στο σύνολο των δεδομένων. Είναι σημαντικό να τονίσουμε τις βασικές διαφορές μεταξύ των δύο παραπάνω προσεγγίσεων. Η ανίχνευση της απάτης χρησιμοποιεί ταξινομητές και αλγορίθμους καθώς και τα ιστορικά δεδομένα που υπάρχουν στη βάση δεδομένων προκειμένου να προβλέψουν εάν μια νέα συναλλαγή αποτελεί απειλή ή όχι. Αυτό σημαίνει οτι σε περιστατικά ήδη γνωστά, το σύστημα έχει απόλυτη αποτελεσματικότητα και ακρίβεια, ωστόσο δεν μπορεί να ανιχνεύσει τις δόλιες κινήσεις από μη γνωστά τεχνάσματα απάτης. Από την άλλη πλευρά, η ανίχνευση ανωμαλιών αφορά το συναλλακτικό προφίλ των πελατών και κρίνει βάσει των παρελθοντικών του δραστηριοτήτων, εάν μια νέα συναλλαγή παρεκκλίνει από την κανονική του συμπεριφορά, εντοπίζοντας έτσι νέα μοτίβα και καινούργια περιστατικά απάτης που έως τότε δεν ήταν γνωστά. Αν και οι προσεγγίσεις ανάλυσης της συμπεριφορά των χρηστών είναι ισχυρές στην ανίχνευση καινοτόμων περιστατικών απάτης, παρουσιάζουν πραγματικά υψηλά ποσοστά false alert. Στη συνέχεια θα παρουσιάσουμε εν συντομία ορισμένες τεχνικές και μοντέλα ανίχνευσης που εφαρμόζονται για τον εντοπισμό και την αποφυγή της απάτης.

4.2. Μοντέλα και αλγόριθμοι

Η απάτη στα χρηματοπιστωτικά ιδρύματα, αποτελεί πλέον αντικείμενο ενδιαφέροντος για πολλούς ερευνητές και αναλυτές προκειμένου να διερευνήσουν τα ζητήματα που σχετίζονται με αυτή καθώς και να αναπτύξουν μεθόδους καταπολέμησης και εκτίμησης του κινδύνου και του ρίσκου αυτής. Έχουν προταθεί διάφοροι μέθοδοι για την ανίχνευση της απάτης, οι οποίες πολλές φορές είναι μη υλοποιήσιμες λόγω της συνεχούς εξέλιξης των τεχνασμάτων που χρησιμοποιούνται από τους απατεώνες αλλά και των νέων τεχνολογιών που εμφανίζονται στο προσκήνιο, όπως για παράδειγμα τα κρυπτονομίσματα. Αυτό επιτυγχάνεται με τεχνικές όπως για παράδειγμα τον ταξινομητή Naïve Bayes, τις μηχανές διανυσμάτων υποστήριξης (support vector machine), την λογιστική παλινδρόμηση (LR) κ.α. [12]. Σε αυτό το κομμάτι της εργασίας θα αναλύσουμε κάποιες από αυτές τις τεχνικές, που ασχολούνται με την οικονομική απάτη και μπορούν να εφαρμοστούν για τον εντοπισμό των ύποπτων συναλλαγών και ανωμαλιών.

Support vector machine (SVM): Οι μηχανές διανυσμάτων υποστήριξης είναι τεχνικές στατιστικής μάθησης που έχουν ιδιαίτερη επιτυχία σε προβλήματα δυαδικής ταξινόμησης όπως είναι η ανίχνευση της απάτης. Αφορά ουσιαστικά γραμμικούς ταξινομητές που δέχονται ως είσοδο χαρακτηριστικά υψηλής διάστασης, χωρίς να ενσωματώνουν καμία πρόσθετη υπολογιστική πολυπλοκότητα. Η ικανότητά τους να διαχειρίζονται υψηλοδιάστατα και μη ισορροπημένα δεδομένα (δηλαδή περιπτώσεις απάτης και γνήσιων κινήσεων) , καθιστούν αυτούς τους ταξινομητές ελκυστικούς για ζητήματα ανίχνευσης απάτης, και μπορούν να εξάγουν ουσιαστικά χαρακτηριστικά που είναι κρίσιμα για την ανίχνευση δόλιων συναλλαγών. Οι εφαρμογές των SVM περιλαμβάνουν τη βιοπληροφορική, τη μηχανική όραση, την κατηγοριοποίηση κειμένου καθώς και την ανάλυση χρονοσειρών. Τα SVM χρησιμοποιούν μια συνάρτηση πυρήνα, που επιτρέπει την εκμάθηση των δεδομένων υψηλών διαστάσεων χωρίς πρόσθετη υπολογιστική πολυπλοκότητα, η οποία μπορεί να εκφραστεί ως γινόμενο των προβολών των σημείων από τα δεδομένα εισόδου. Ένα ακόμα προτέρημα του συγκεκριμένου αλγορίθμου, είναι ότι ελαχιστοποιεί τον κίνδυνο του overfitting των δεδομένων εκπαίδευσης, με αποτέλεσμα να καταλήγει στην καλύτερη συνάρτηση ταξινόμησης. Βάσει των πολλών και εντατικών ερευνών που έχουν γίνει μέσα στα χρόνια, τα SVM υπερτερούν έναντι άλλων αλγορίθμων όπως είναι τα δέντρα αποφάσεων, ωστόσο έχουν γίνει πολλές διαφοροποιήσεις στον αλγόριθμο για την αντιμετώπιση των μειονεκτημάτων των σημερινών συστημάτων, είτε συνδυάζοντας τα SVM με άλλους ταξινομητές όπως λογιστική και γραμμική παλινδρόμηση, είτε χρησιμοποιώντας το hybrid SVM (HSVM) μοντέλο.

Fuzzy Logic (FL): Κάθε πελάτης έχει ένα συγκεκριμένο προφίλ δραστηριότητας και αυτό ακριβώς προσπαθούν να καταγράψουν όλοι οι αλγόριθμοι ανίχνευσης απάτης. Ο αλγόριθμος Fuzzy c-means (FCM) είναι ένας αλγόριθμος ομαδοποίησης που επιτρέπει μεμονωμένα δεδομένα να ανήκουν σε παραπάνω από ένα cluster, υιοθετεί δηλαδή μια ασαφή ομαδοποίηση, προκειμένου να ανιχνεύει αποτελεσματικά τις απάτες και μαθαίνει την αλλαγή στο συναλλακτικό προφίλ του πελάτη δυναμικά και όχι στατικά. Σε συνδυασμό με μία ασαφή τεχνική εκμάθησης, όπως είναι για παράδειγμα τα νευρωνικά δίκτυά, μπορεί να μειωθεί και το ποσοστό της λανθασμένης ταξινόμησης με βάση την συναλλαγή, το ποσό, την κατηγορία του εμπόρου που εκτελείται η συναλλαγή ή ακόμα και με το χρόνο της συναλλαγής. Γενικότερα, και αυτό που μπορούμε να συμπεράνουμε, είναι οτι χρήση ασαφής ομαδοποίησης και εκμάθησης, μπορεί να φέρει πολύ καλά αποτελέσματα όσον αφορά προβλήματα ανίχνευσης, και μπορεί να βελτιωθεί ακόμα περαιτέρω με την ένταξη πρόσθετων χαρακτηριστικών όπως είναι η τοποθεσία της συναλλαγή, η χρονική διαφορά μεταξύ των συναλλαγών κ.α. Η FL βασίζεται στη λογική οτι το αποτέλεσμα θα είναι εκτιμώμενο και όχι ακριβές, όπως δηλαδή και η ανθρώπινη σκέψη, γεγονός που την καθιστά ένα ιδανικό πλαίσιο για την αντιμετώπιση περίπλοκων μοντέλων, όπως είναι και η ανίχνευση της απάτης.

Hidden Markov model (HMM): Η HMM είναι μια διπλή στοχαστική διαδικασία η οποία εφαρμόζεται για την μοντελοποίηση πολλών περίπλοκων διεργασιών σε σύγκριση με το παραδοσιακό μοντέλο Markov. Σε απλούστερα μοντέλα, όπως είναι οι μαρκοβιανές αλυσίδες, οι καταστάσεις του συστήματος είναι συγκεκριμένες ενώ οι παράμετροι είναι οι πιθανότητες μετάβασης, σε αντίθεση με το εν λόγω μοντέλο HMM όπου οι καταστάσεις του συστήματος είναι άγνωστες αλλά οι εξαρτώμενες από αυτές έξοδοι είναι γνωστές. Στη ανίχνευση απάτης, εκπαιδεύεται ένα HMM για τη μοντελοποίηση της κανονικής συμπεριφοράς κάθε χρήστη, και σύμφωνα με το μοντέλο αυτό, μια νέα συναλλαγή θα ταξινομηθεί ως απάτη εάν δεν γίνει αποδεκτή με αρκετά υψηλή πιθανότητα από το μοντέλο. Το συγκεκριμένο μοντέλο μπορεί να διαχειριστεί μεγάλο όγκο δεδομένων αλλά και να χρησιμοποιηθεί σε online συστήματα ανίχνευσης απάτης, λαμβάνοντας λεπτομέρειες της συναλλαγής που πρόκειται να πραγματοποιηθεί και εάν θεωρηθεί δυνητικά απατηλή να απορρίπτεται απευθείας από την εκάστοτε τράπεζα. Δεδομένου οτι το μοντέλο από μόνο του παράγει αρκετά false alerts, με μια τεχνική ομαδοποίησης, όπως για παράδειγμα την K-means, μπορεί να αυξηθεί η ακρίβεια και η αποτελεσματικά του, μειώνοντας τις λανθασμένες ειδοποιήσεις.

Artificial neural network (ANN): Το ANN αποτελεί ένα σύνολο από μη γραμμικές μεθόδους τεχνητής νοημοσύνης, που επεξεργάζονται τα δεδομένα με παρόμοιο τρόπο όπως η ανθρώπινη σκέψη, και παρέχει πολύ καλές επιδόσεις σε μεγάλα σύνολα δεδομένων. Το κύριο χαρακτηριστικό ενός νευρωνικού δικτύου είναι ο νευρώνας ο οποίος είναι δομημένος από πολλά στρώματα υπολογιστικών τμημάτων, και δέχεται πολλές εισόδους, τις αθροίζει εφαρμόζοντας μια συνάρτηση μεταφοράς και παράγει το αποτέλεσμα είτε ως πρόβλεψη του μοντέλου είτε ως είσοδο σε άλλους νευρώνες. Ως μεταβλητές, τα νευρωνικά δίκτυα δέχονται χαρακτηριστικά που αφορούν το συναλλακτικό προφίλ του πελάτη όπως για παράδειγμα τη γεωγραφική τοποθεσία, τις ημέρες ή ώρες που συνήθως πραγματοποιεί συναλλαγές κ.α. τα οποία και αποθηκεύονται σε ένα data mart το οποίο αναπαριστά την δραστηριότητα του πελάτη. Στη συνέχεια, οι μεταβλητές αυτές θα χρησιμοποιηθούν για τη δημιουργία ενός μοντέλου που θα διακρίνει τις δόλιες συναλλαγές, οι οποίες θα παρουσιάζουν σημαντικές αποκλίσεις από το προφίλ του πελάτη, όπως αυτό δομήθηκε στο προηγούμενο βήμα, προβλέποντας εάν η συναλλαγή είναι γνήσια ή απατηλή.

Self-Organizing Maps (SOM): Ο SOM είναι μια τεχνική που είναι βασισμένη στα νευρωνικά δίκτυα, δηλαδή βασίζεται στη μη επιβλεπόμενη μάθηση, και αποτελεί ουσιαστικά έναν χάρτη. Πιο συγκεκριμένα, το ιστορικό των κινήσεων αλλά και του γενικότερου συναλλακτικού προφίλ ενός πελάτη που υπάρχει στη βάση δεδομένων, ταξινομούνται μέσω αυτόματης διαδικασίας σε δύο σύνολα, δηλαδή σε γνήσια και απατηλά. Στη συνέχεια κάθε νέα συναλλαγή προ επεξεργάζεται και τροφοδοτείται στο SOM με βάση το εάν αυτή αποτελεί γνήσια ή απατηλή κίνηση. Αποτελεί επί της ουσίας μια πολύπλευρη και πολυεπίπεδη διαδικασία που αρχικά ελέγχει τα ιστορικά δεδομένα των πελατών και τα ταξινομεί αντιστοίχως, στη συνέχεια βαθμολογεί τον κίνδυνο σε σχέση με την παρελθοντική συμπεριφορά του πελάτη, και τέλος δίνει την τελική απόφαση για το εάν θα επιτρέψει την διεκπεραίωση ή μη της συναλλαγής. Όμοια όπως και σε άλλες μεθόδους, το τελευταίο στρώμα του νευρώνα, που αφορά την απόφαση που θα δώσει το σύστημα, μπορεί να ζητήσει από μεριάς του πελάτη κάποια επιπλέον επιβεβαίωση για την εκτέλεση της συναλλαγή (SCA, OTP) και να μην την απορρίψει απευθείας.

Decision Tree: Τα δέντρα αποφάσεων λειτουργούν με δυαδική απόφαση και κατασκευάζονται με μια αναδρομική διαδικασία από πάνω προς τα κάτω. Ένα δέντρο απόφασης μπορεί να χρησιμοποιηθεί σε ένα πρόβλημα ταξινόμησης και χρησιμοποιείται για την ανίχνευση απάτης στο τραπεζικό τομέα. Για παράδειγμα, το δέντρο απόφασης μπορεί να αναπαριστά την καταναλωτική συμπεριφορά ενός πελάτη που περιλαμβάνει ως κόμβους τις δαπάνες του και ως φύλλα τις υψηλές, τις μεσαίες και τις αντίστοιχες χαμηλές δαπάνες του. Επομένως, μια νέα συναλλαγή μπορεί να χαρακτηριστεί ως απατηλή ή ως γνήσια χρησιμοποιώντας αυτή τη προσέγγιση του Decision Tree.

Outliers detection: Ο όρος outlier είναι γνωστός ως μια ακραία τιμή που υποδηλώνει την ύπαρξη μιας συμπεριφοράς που παρεκκλίνει από την κανονική. Η ανίχνευση ακραίων τιμών είναι ένα κομμάτι του data mining το οποίο αποτελεί μια από τις πιο δημοφιλής μεθόδους που χρησιμοποιείται για τον εντοπισμό των δεδομένων που δεν συμπεριφέρονται όπως αναμένεται σύμφωνα με το μοντέλο δεδομένων. Η ανίχνευση αυτών των ανωμαλιών ανάγεται σε ένα πρόβλημα δυαδικής ταξινόμησης που περιλαμβάνει δυο κατηγορίες, τις ακραίες τιμές και τις κανονικές. Η σημασία της ανίχνευσης αυτών των ανωμαλιών βασίζεται στο γεγονός οτι οι απροσδόκητες συμπεριφορές στα δεδομένα, μεταφράζονται ως σημαντικές πληροφορίες σε πολλούς τομείς και εφαρμογές. Τα προβλήματα εντοπισμού ακραίων τιμών μπορούν να επιλυθούν αρκετά αποτελεσματικά με την συγκεκριμένη μέθοδο. Όμοια, και στον εντοπισμό της απάτης σε μεγάλα όγκο δεδομένων στον τραπεζικό τομέα. Το πρώτο βήμα περιλαμβάνει την προ επεξεργασία δεδομένων που αποτελείται από τον καθαρισμό και την ομαδοποίηση των δεδομένων. Στη συνέχεια, γίνεται η εξαγωγή πληροφοριακών χαρακτηριστικών από το σύνολο δεδομένων όπως για παράδειγμα το είδος των συναλλαγών, τα προφίλ των πελατών ή η συναλλακτική τους συμπεριφορά, προκειμένου να δημιουργηθεί ένα ετερογενές δίκτυο πληροφοριών. Έπειτα, υπολογίζεται ο βαθμός συσχέτισης των διαφορετικών συναλλαγών βάσει του δικτύου πληροφοριών, και δημιουργείται βάσει αυτού ένας κανόνας διάκρισης μεταξύ των γνήσιων και των απατηλών κινήσεων και συναλλαγών. Η τεχνική αυτή είναι αρκετά αποτελεσματική, μειώνει την χρονική πολυπλοκότητα και συνάμα αποδίδει υψηλή ακρίβεια και αυξημένο ποσοστό ανίχνευσης.

Genetic Algorithms: Οι γενετικοί αλγόριθμοι είναι εμπνευσμένοι από την φυσική εξέλιξη. Αναζητούν την βέλτιστη λύση μέσα από ένα σύνολο προτεινόμενων λύσεων που αναπαρίστανται με την μορφή δυαδικών συμβολοσειρών, γνωστών ως χρωμοσωμάτων. Όταν εφαρμόζεται αυτός ο αλγόριθμος σε οποιοδήποτε πρόβλημα, η βασική προϋπόθεση είναι οτι μπορούμε να δημιουργήσουμε ένα αρχικό πληθυσμό ατόμων που αντιπροσωπεύουν πιθανές λύσεις στο πρόβλημα αυτό. Κάθε ένα από αυτά τα άτομα έχει ορισμένα χαρακτηριστικά που το καθιστούν περισσότερο ή λιγότερο κατάλληλα για μέλη του πληθυσμού. Το κατάλληλο μέλος, θα έχει την μεγαλύτερη πιθανότητα να παράγει αποτελεσματική λύση. Αυτή η μέθοδος είναι πολύ αποτελεσματική για την εύρεση της βέλτιστης ή σχεδόν βέλτιστης λύσης. Το συγκεκριμένο μοντέλο, μπορεί να χρησιμοποιηθεί για την ανίχνευση απάτης και να ξεπεράσει το πρόβλημα των παραδοσιακών ταξινομητών στην ανίχνευση αντικειμένων μειονοτικής κατηγορίας στο αρχικό ανισόρροπο σύνολο δεδομένων. Χρησιμοποιώντας τον GA αλγόριθμό σε κάθε συστάδα των ήδη ομαδοποιημένων δεδομένων, προκειμένου να παραχθεί ένα νέο σύνολο δεδομένων εκπαίδευσης, βελτιώνεται η ακρίβεια και το ποσοστό ανίχνευσης της απάτης και μειώνεται ο αριθμός των ψευδών ειδοποιήσεων.

Logistic Regression: Η λογιστική παλινδρόμηση είναι ένα πιθανολογικό στατιστικό μοντέλο ταξινόμησης, που χρησιμοποιείται για την ανάλυση συνόλων δεδομένων με βάση ένα γραμμικό μοντέλο. Είναι γενικά μια μέθοδος που χρησιμοποιείται για την μέτρηση της σχέση μεταξύ των εξαρτημένων και ανεξάρτητων μεταβλητών, με τη χρήση χρηματοοικονομικών αριθμοδεικτών προκειμένου να διαπιστωθεί ποιοι από αυτούς συνδέονται με τις απατηλές συναλλαγές και επομένως να εντοπιστεί ποιοι παράγοντες επηρεάζουν σημαντικά το μοτίβο των απατηλών αυτών κινήσεων. Ο αλγόριθμος της λογιστικής παλινδρόμησης μπορεί να παράγει μοντέλα όταν η τελική απόφαση είναι ένα σύνολο πεδίων με δύο ή περισσότερες πιθανές τιμές.

K-Nearest Neighbor algorithm (KNN): Η τεχνική KNN είναι ένας τύπος μη παραμετρικής μεθόδου, που χρησιμοποιείται για την ταξινόμηση και την παλινδρόμηση. Σκοπός της είναι ο προσδιορισμός της κατηγορίας ενός άγνωστου δεδομένου, με βάση τον πλησιέστερο γείτονα, του οποίου η κατηγορία είναι ήδη γνωστή. Η εύρεση των πλησιέστερων γειτόνων, γίνεται με τον υπολογισμό της απόστασης τους, με αρκετούς τρόπους, με τον πιο γνωστό να είναι η ευκλείδεια απόσταση. Στη συνέχεια, και αφού υπολογιστούν οι k

κλάσεις, κάθε καινούργιο δεδομένο προβλέπεται οτι θα ανήκει σε κάποια από αυτές τις κλάσεις βάσει της ομοιότητας των χαρακτηριστικών του με τα υπόλοιπα σύνολα δεδομένων, και κατηγοριοποιείται αναλόγως στην αντίστοιχη κλάση αυτή. Η μέθοδος αυτή οδηγεί σε πολύ καλή και ακριβή επίδοση, επιτυγχάνοντας μεγάλη αποτελεσματικότητα στην ανίχνευση της απάτης, και επί του παρόντος, αποτελεί μια ευρέως χρησιμοποιούμενη μη παραμετρική διαδικασία λήψης αποφάσεων για την επίλυση προβλημάτων ταξινόμησης. Τα πλεονεκτήματα του k-NN είναι η γρήγορη εκπαίδευση των δεδομένων, η απλή διαδικασία εκμάθησης και η ισχυρή αποδοτικότητα έναντι ενός συνόλου δεδομένων που περιέχει θορυβώδη δεδομένα. Ωστόσο, η μέθοδος αυτή απαιτεί μεγάλο όγκο μνήμης, ειδικά όταν χρησιμοποιείται σε μεγάλο μέγεθος δεδομένων, και τα αποτελέσματα της κατηγοριοποίησης επηρεάζονται σχετικά εύκολα από άσχετα χαρακτηριστικά των δεδομένων.

Chi-Square Automatic Interaction Detection (CHAID): Ο αλγόριθμος CHAID είναι μια από της ευρέως χρησιμοποιούμενες μεθόδους ταξινόμησης χωρίς επίβλεψη που βασίζονται σε αναδρομικό δέντρο κατάτμησης. Ο αλγόριθμος αποτελείται από κυρίως τρία βήματα, ξεκινώντας από την δημιουργία του δέντρου από κάτω προς τα πάνω, η οποία γίνεται με τον υπολογισμό του πίνακα με τις κατηγορίες της πρόβλεψης και τις κατηγορίες της εξαρτημένης μεταβλητές. Στη συνέχεια, ο αλγόριθμος συνεχίζει να δοκιμάζει όλους τους πιθανούς τρόπους διαχωρισμού του δείγματος, έως ότου αποκαλυφθούν οι ισχυρότεροι και καλύτεροι προγνωστικοί παράγοντες. Όσο η τιμή του χ^2- τεστ δεν είναι σημαντική, η διαδικασία της συγχώνευσης επαναλαμβάνεται. Το πλεονέκτημα αυτού του αλγορίθμου είναι οτι είναι αρκετά αποτελεσματικός στην αναζήτηση, αλλά δεν είναι βέβαιο οτι θα επιτρέψει την καλύτερη πρόβλεψη διάσπασης σε συγκεκριμένα βήματα. Παρά την απλότητα του, ο CHAID χρησιμοποιείται σε διάφορους τομείς, όπως είναι η εκπαίδευση, η εγκληματολογία, η ζωική παραγωγή , αλλά και η ανίχνευση της απάτης.

Bayesian Network: Το BN είναι μια μορφή γραφικού μοντέλου που λειτουργεί με τις ανεξάρτητες και τις εξαρτημένες σχέσεις μεταξύ των διάφορων τυχαίων μεταβλητών, και έχει τη μορφή ενός κατευθυνόμενου γράφου. Το υποκείμενο γραφικό μοντέλου, είναι χρήσιμο για την εύρεση άγνωστων πιθανοτήτων, δοθέντων των γνωστών πιθανοτήτων των δεδομένων του συνόλου. Τα Μπεϋζιανά δίκτυα, μπορούν να διαδραματίσουν σημαντικό και αποτελεσματικό ρόλο στη μοντελοποίηση των καταστάσεων, όπου κάποιες βασικές πληροφορίες είναι ήδη γνωστές, αλλά τα εισερχόμενα δεδομένα είναι αβέβαια, ή μερικώς μη διαθέσιμα. Ο στόχος της χρήσης του μοντέλου αυτού είναι συχνά η πρόβλεψη μιας κλάσης, που σχετίζεται με ένα διάνυσμα χαρακτηριστικών, και χρησιμοποιείται σε διάφορους τομείς, όπως για παράδειγμα στο churn prevention, στην δημιουργία διαγνωστικών στην ιατρική, στη διάγνωση σφαλμάτων καθώς και στην ανίχνευση ανωμαλιών και περιστατικών απάτης σε διατραπεζικές συναλλαγές. Προτάθηκαν επομένως δύο προσεγγίσεις για την χρήση του δικτύου Bayes, η πρώτη αφορά την συμπεριφορά του δόλιου χρήστη, και η δεύτερη αφορά την νόμιμη συμπεριφορά του χρήστη. Το δίκτυο της δόλιας συμπεριφοράς κατασκευάζεται από τους εμπειρογνώμονες, ενώ η δεύτερη δημιουργείται με τα διαθέσιμα δεδομένα από τους μη δόλιους χρήστες. Η ταξινόμηση των συναλλαγών γίνονται απλά με την εισαγωγή τους και στα δύο δίκτυα και στη συνέχεια καθορίζεται ο τύπος της συμπεριφορά, δηλαδή γνήσια ή απατηλή, σύμφωνα με τις αντίστοιχες πιθανότητες. Το πλεονέκτημα του κανόνα Bayes, είναι οτι υπολογίζει τις πιθανότητες και για τις νέες συναλλαγές, και απαιτεί πολύ λιγότερο χρόνο εφαρμογής σε σχέση με άλλες δημοφιλής μεθόδους όπως η παλινδρόμηση, οι KNN ταξινομητές κ.α.

Case-based reasoning (CBR): Η προσαρμογή των λύσεων που χρησιμοποιήθηκαν για την επίλυση προηγούμενων προβλημάτων και η χρήση τους για την επίλυση νέων προβλημάτων είναι η βασική ιδέα πίσω από το CBR. Στο CBR, οι περιπτώσεις απάτης εισάγονται ως περιγραφές και αποθηκεύονται σε μια βάση δεδομένων, η οποία χρησιμοποιείται για μεταγενέστερη ανάκτηση, όταν παρουσιαστεί ξανά μια νέα περίπτωση με παρόμοιες παραμέτρους. Οι περιπτώσεις αυτές μπορούν εφαρμόζονται ουσιαστικά ως μέθοδος ταξινόμησης, καθώς ένα σύστημα CBR προσπαθεί να βρει μια αντίστοιχη περίπτωση όταν

αντιμετωπίζει ένα νέο πρόβλημα. Πιο συγκεκριμένα, όταν δίνεται κάποια νέα συναλλαγή, το σύστημα αναζητά σε όλη τη βάση δεδομένων να ανακαλύψει ένα υποσύνολο περιπτώσεων που παρουσιάζουν τις περισσότερες ομοιότητες με τη νέα συναλλαγή και τις χρησιμοποιεί ώστε να προβλέψει το αποτέλεσμα. Ο αλγόριθμος KNN εφαρμόζεται συνήθως με το CBR, αν και υπάρχουν αρκετοί άλλοι αλγόριθμοι που χρησιμοποιούνται με αυτή τη προσέγγιση.

4.3. Αξιολόγηση των μοντέλων

Όπως είδαμε και παραπάνω, υπάρχουν αρκετοί αλγόριθμοι και τεχνικές που χρησιμοποιούνται για την ανίχνευση της απάτης, ωστόσο παρακάτω θα αναλύσουμε πως μπορούμε να τα αξιολογήσουμε με γνώμονα τα χρήματα, την ακρίβεια και τον χρόνο, την αποτελεσματικότητα τους.

Η απόδοση ενός αλγορίθμου ταξινόμησης εξετάζεται συνήθως με την αξιολόγηση της ακρίβειας της ταξινόμησης. Η ακρίβεια ταξινόμησης υπολογίζεται προσδιορίζοντας το ποσοστό των εγγραφών που τοποθετούνται στη σωστή κλάση, τα οποία αξιολογούνται με 4 πιθανά αποτελέσματα: True Positive, True Negative, False Positive και False Negative. Τα TP και TN αντιπροσωπεύουν της σωστές ενέργειες και είναι αυτά που πρέπει να βελτιστοποιηθούν, ενώ τα FP και FN τις λανθασμένες και είναι αυτά που πρέπει να ελαχιστοποιηθούν. Ωστόσο αυτό δεν αποτελεί από μόνο του ικανό κριτήριο ώστε να προσδιοριστεί η αποτελεσματικότητα του μοντέλου, καθώς για παράδειγμα ένα μοντέλο μπορεί να είναι ικανό να προβλέπει το 90% των απατηλών συναλλαγών που πραγματοποιούνται σε μικρά ποσά και να είναι εντελώς λάθος για το 10% που αφορά τις πιο δαπανηρές απάτες. Επομένως, υπάρχει ανάγκη για επιπρόσθετα κριτήρια που θα μας βοηθήσουν στην αξιολόγηση των μοντέλων.

- Θόρυβος στα δεδομένα/ Ελλιπή δεδομένα: Τα σύνολα δεδομένων συχνά περιέχουν θόρυβο, δηλαδή ανακρίβειες και ασυνέπειες ή ακόμα και χαρακτηριστικά που απαιτούνται για την ανάλυση και μπορεί να μην είναι καν διαθέσιμα. Αυτό μπορεί να προκαλέσει πρόβλημα στην φάση της εκπαίδευσης και στη διαδικασία της ταξινόμησης. Ως εκ τούτου, η ικανότητα της κάθε τεχνική να καταπολεμά το εμπόδιο αυτό είναι ένας πολύ σημαντικός παράγοντας.
- Scalability: Συνήθως οι εφαρμογές εξόρυξης δεδομένων χρησιμοποιούν πολύ μεγάλα σύνολα δεδομένων. Αυτά τα σύνολα δεδομένων φορτώνονται στη μνήμη RAM και μπορεί να επιβραδύνουν την επεξεργασία και την εκτέλεση του αλγορίθμου. Επομένως η επεκτασιμότητα των τεχνικών αυτών γίνεται ένα αρκετά σημαντικό ζήτημα.
- Διαφορετικοί τύποι δεδομένων: Οι επιχειρηματικές βάσεις ή τα σύνολα δεδομένων περιέχουν δεδομένα διάφορων τύπων (αριθμητικά, ονομαστικά κτλ). Εάν μια τεχνική εξόρυξης δεδομένων μπορεί να χειριστεί τους διαφορετικούς τύπους αυτούς, θα είναι πιο χρήσιμη για μια επιχείρηση.
- Δυνατότητα ενσωμάτωσης: Η εφαρμογές εξόρυξης δεδομένων συνήθως λειτουργούν με άλλα πληροφορικά συστήματα, όπως DSS ή DBMS, επομένως η ευκολία ενσωμάτωσης τους με αυτά είναι ένα επιθυμητό χαρακτηριστικό του μοντέλου που αναζητούμε.
- Ευκολία λειτουργίας: Μια τεχνική που είναι εύκολα κατανοητή, εύκολη στην κατασκευή και που απαιτεί λιγότερη προεπεξεργασία είναι πιο χρήσιμη για τον τελικό χρήστη.
- Skewed distribution: Συνήθως τα δεδομένα ανίχνευσης απάτης είναι ιδιαίτερα λοξά ή ασύμμετρα. Η λοξή κατανομή των δεδομένων, αποτελεί σημαντικό παράγοντα για την απόδοση του ταξινομητή, επομένως η ικανότητα του μοντέλου να χειρίζεται τέτοιου είδους δεδομένα είναι ένα επιθυμητό χαρακτηριστικό.

5. Νομικοί κανονισμοί για τα περιστατικά απάτης στην Ελλάδα

Τον Ιανουάριο του 2023 τέθηκε σε ισχύ, η νέα διάταξη στο άρθρο 22 του νομοσχεδίου με τίτλο «Ενσωμάτωση της Οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2020 σχετικά με τις αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και για την κατάργηση της οδηγίας 2009/22/ΕΚ, ενίσχυση της προστασίας των καταναλωτών, ρυθμιστικό πλαίσιο για την παλαίωση οίνων και άλλες επείγουσες διατάξεις για την ενίσχυση της ανάπτυξης»[13]. Αφορά μια ευρωπαϊκή οδηγία που ενσωματώθηκε στην ελληνική έννομη τάξη με σκοπό την ενίσχυση του επιπέδου προστασίας των καταναλωτών απέναντι σε περιστατικά απάτης εις βάρος των πελατών των τραπεζών και την δημιουργία ενός ρυθμιστικού πλαισίου για την λήψη μέτρων επανόρθωση και αποκατάστασης της ζημίας που υπέστησαν. Ειδικότερα, η παρούσα οδηγία αφορά την διασφάλιση της προστασίας των πελατών από κακόβουλες και αθέμιτες πρακτικές που μπορούν να πλήξουν τα οικονομικά συμφέροντα τους, περιλαμβάνοντας την λήψη νομικών μέτρων που μπορούν να βοηθήσουν στις παραβάσεις αυτές. Συγκεκριμένα το άρθρο 22 του νομοσχεδίου, προβλέπει οτι ο καταναλωτής ευθύνεται μέχρι του ανώτατου ποσού των 1000 ευρώ όσον αφορά περιστατικά απάτης τα οποία διενεργούνται μέσω της ηλεκτρονικής τραπεζικής τους, και περιστατικά τα οποία οφείλονται σε βαριά αμέλεια από μέρους του, όπως για παράδειγμα οικονομική απώλεια που μπορεί να προκύψει από ένα phishing μήνυμα, ή άλλων πρακτικών εξαπάτησης όπως μια ψεύτικη ιστοσελίδα που δολίως παρουσιάζεται ως ο επίσημος ιστότοπος μιας τράπεζας κ.α. Ωστόσο, ο καταναλωτής ευθύνεται εξ' ολοκλήρου για όλες της ζημιές που οφείλονται σε μη εγκεκριμένες πράξεις πληρωμών που διενεργήθηκαν με δόλο αλλά και με την δόλο αθέτηση των υποχρεώσεων του.

Οι ρυθμίσεις αυτές, όπως είναι φυσικό, έχουν θεσμοθετηθεί ως μοχλός πίεσης προς τις τράπεζες ώστε να αυξήσουν τις ασφαλιστικές δικλίδες τους και να ενισχύουν συνεχώς τα συστήματα ασφαλείας για τις ηλεκτρονικές συναλλαγές, προκειμένου να αποτρέπονται τέτοιου είδους περιστατικά, κάτι που καθιστά την ανίχνευση και τον εντοπισμό της απάτης πλέον, ένα πολύ σημαντικό φαινόμενο το οποίο χρειάζεται ουσιαστικά και αποτελεσματικά μέτρα για την αντιμετώπιση του. Όπως προκύπτει και από την έκθεση χρηματοπιστωτικής σταθερότητας της ΤτΕ, το α' εξάμηνο του 2022 ο δείκτης απάτης κυμαίνεται στο 0,02% που αντιστοιχεί σε οικονομική απώλεια της τάξεως των 6 εκατομμυρίων ευρώ, αριθμός που αποτελεί μείωση 14% από το 2ο εξάμηνο του 2021 από τον αντίστοιχο δείκτη απάτης. Αντίθετα, η αξία των απατηλών συναλλαγών αυξήθηκε κατά το έτος 2022, με άνοδο των περιστατικών απάτης από ATM καθώς και των CNP συναλλαγών. Τον Απρίλιο το 2023, η Ευρωπαϊκή Επιτροπή πρότεινε την δημιουργία μιας «ευρωπαϊκής κυβερνοασπίδας», η οποία θα αποτελείται από εθνικά και διασυνοριακά κέντρα επιχειρήσεων ασφαλείας (Security Operations Centers). Αυτή η πρόταση κανονισμού, έχει ως στόχο την δημιουργία ενός μηχανισμού επανεξέτασης περιστατικών απάτης, καθώς και την ενίσχυση αλλά και την αύξηση της ετοιμότητας για την αντιμετώπιση τέτοιων περιστατικών.

Τα περιστατικά απάτης και οι επιθέσεις εις βάρος των πελατών συνεχίζονται με αμείωτη ένταση, οδηγώντας σε μεγάλες οικονομικές απώλειες, κάτι που καθιστά επιτακτική την ανάγκη για την ορθή διαχείριση αυτών των περιστατικών με την σωστή προστασία των πελατών. Υπάρχουν συνεχείς καμπάνιες ενημέρωσης των καταναλωτών για τα περιστατικά απάτης και πως μπορούν οι ίδιοι να προφυλαχτούν, παρόλα αυτά, όπως προκύπτει και από τα παραπάνω στατιστικά, αυτό δεν αρκεί και χρειάζεται μεγάλη μελέτη από πλευρά των τραπεζών για ενισχυμένα συστήματα ασφαλείας που θα ανιχνεύουν τα περιστατικά αυτά προτού οδηγήσουν σε χρηματικές απώλειες. Σίγουρα η ένταξη της ευρωπαϊκής οδηγίας περί αποζημίωσης των θυμάτων, θα κινητοποιήσει όλον τον τραπεζικό κλάδο για τον πιο άμεσο και αποτελεσματικό εντοπισμό των δόλιων συναλλαγών, κάτι που έχει δημιουργήσει την ανάγκη για ανακάλυψη και αξιοποίηση τεχνικών μηχανικής μάθησης και τεχνητής νοημοσύνης. Η απάτη στα οικονομικά ιδρύματα θα αποτελεί πάντα ένα πολύ σημαντικό φαινόμενο, καθώς όσο υπάρχει εξέλιξη στα συστήματα ασφαλείας και στις μεθόδους που χρησιμοποιούνται για την ανίχνευση της, τόσο θα υπάρχουν νέα τεχνάσματα και τεχνικές από τους απατεώνες για να μπορέσουν να παρακάμψουν τα συστήματα αυτά. Για αυτόν κιόλας τον λόγο είναι πολύ σημαντική η δημιουργία θεσμικών πλαισίων προκειμένου να αυξηθεί η προστασία των καταναλωτών και ως

εκ τούτου η αίσθηση οτι μπορούν με ασφάλεια να χρησιμοποιούν τις τόσες δυνατότητες που πλέον τους παρέχονται μέσω των ηλεκτρονικών συναλλαγών και κινήσεων.

6. Εφαρμογή τεχνικών μηχανικής μάθησης για την πρόβλεψη και την ανίχνευση απάτης

Σκοπός του προγραμματιστικού αυτού μέρους, είναι να κατανοηθεί περαιτέρω η έννοια της ηλεκτρονικής απάτης στον τραπεζικό τομέα, οι προκλήσεις και οι δυσκολίες που υπάρχουν όσον αφορά τον εντοπισμό και την πρόβλεψη της αλλά και πως με την χρήση τεχνικών μηχανικής μάθησης μπορούμε να προσεγγίσουμε το συγκεκριμένο ζήτημα με βέλτιστα αποτελέσματα. Το προγραμματιστικό αυτό μέρος αποτελείται από δύο ενότητες, η πρώτη αφορά την ανάλυση και την επεξεργασία πραγματικών δεδομένων, στα οποία εφαρμόσαμε τεχνικές μηχανικής μάθησης, και η δεύτερη αφορά τον σχεδιασμό ενός συστήματος ανίχνευσης απάτης από την αρχή.

6.1. Ανάλυση σε πραγματικά δεδομένα

Στο συγκεκριμένο κομμάτι, θα αναλύσουμε δεδομένα που αφορούν απάτη μέσω τραπεζικών καρτών και θα χρησιμοποιήσουμε αλγόριθμους μηχανικής μάθησης προκειμένου να δούμε και να συγκρίνουμε τα αποτελέσματα. Το dataset αντλήθηκε από το από το Project DEFEATFRAUD του Πανεπιστήμιου «UNIVERSITE Librebde Bruxelles» (http://mlg.ulb.ac.be), και περιέχει κινήσεις τραπεζικών καρτών από τον Σεπτέμβριο του 2013. Λόγω τραπεζικού απορρήτου, τα δεδομένα που διατίθενται δεν είναι συμπληρωμένα με δείκτες, αλλά ανώνυμα δεδομένα που αποτελούνται από 31 στήλες οι οποίες έχουν προκύψει από επεξεργασία PCA (PRINCIPAL COMPONENT ANALYSIS). Τα μόνα χαρακτηριστικά που έχουν μείνει αναλλοίωτα είναι ο χρόνος της συναλλαγής, το αντίστοιχο ποσό καθώς και η στήλη που μας υποδεικνύει εάν η συναλλαγή είναι γνήσια ή απατηλή.

Πιο αναλυτικά, το dataset εμπεριέχει συνολικά 284.807 κινήσεις που αφορούν συναλλαγές που πραγματοποιήθηκαν εντός δύο ημερών, εκ των οποίων οι 492 είναι απατηλές. Οι στήλη που μας υποδεικνύει την γνησιότητα της συναλλαγής είναι ένα δυαδικό χαρακτηριστικό που λαμβάνει την τιμή 1 για συναλλαγές που είναι απατηλές, και την τιμή 0 για τις γνήσιες συναλλαγές.

6.1.1. Διαδικασία

Προτού εφαρμόσουμε τα μοντέλα μηχανικής μάθησης προκειμένου να αξιολογήσουμε και να συγκρίνουμε την αποδοτικότητά τους, θα πρέπει πρώτα να γνωρίσουμε και να εξοικειωθούμε με τα δεδομένα μας, και να προχωρήσουμε σε όλες τις απαραίτητες ενέργειες ως προς την επεξεργασίας τους.

Ξεκινώντας, εισάγουμε τα δεδομένα μας σε ένα dataframe και ελέγχουμε κάποια βασικά στατιστικά σε σχέση με αυτά:

Εισαγωγή δεδομένων:

```
df = pd.read_csv('data/creditcard.csv')
```

```
df.describe()
```

	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	..
count	284807.000000	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	2.848070e+05	..
mean	94813.859575	1.168375e-15	3.416908e-16	-1.379537e-15	2.074095e-15	9.604066e-16	1.487313e-15	-5.556467e-16	1.213481e-16	-2.406331e-15	..
std	47488.145955	1.958696e+00	1.651309e+00	1.516255e+00	1.415869e+00	1.380247e+00	1.332271e+00	1.237094e+00	1.194353e+00	1.098632e+00	..
min	0.000000	-5.640751e+01	-7.271573e+01	-4.832559e+01	-5.683171e+00	-1.137433e+02	-2.616051e+01	-4.355724e+01	-7.321672e+01	-1.343407e+01	..
25%	54201.500000	-9.203734e-01	-5.985499e-01	-8.903648e-01	-8.486401e-01	-6.915971e-01	-7.682956e-01	-5.540759e-01	-2.086297e-01	-6.430976e-01	..
50%	84692.000000	1.810880e-02	6.548556e-02	1.798463e-01	-1.984653e-02	-5.433583e-02	-2.741871e-01	4.010308e-02	2.235804e-02	-5.142873e-02	..
75%	139320.500000	1.315642e+00	8.037239e-01	1.027196e+00	7.433413e-01	6.119264e-01	3.985649e-01	5.704361e-01	3.273459e-01	5.971390e-01	..
max	172792.000000	2.454930e+00	2.205773e+01	9.382558e+00	1.687534e+01	3.480167e+01	7.330163e+01	1.205895e+02	2.000721e+01	1.559499e+01	..

8 rows × 31 columns

Σχήμα 1: Στατιστικά των δεδομένων

Στη συνέχεια θα ελέγξουμε τον τύπο των δεδομένων που έχουμε στο dataset μας. Βλέπουμε ότι οι στήλες των δεδομένων μας περιέχουν πραγματικούς αριθμούς πέραν της στήλης που αφορά την κλάση της συναλλαγής δηλαδή εάν μια συναλλαγή είναι απατηλή ή όχι, η οποία λαμβάνει τις τιμές 0 και 1.

```
df.dtypes
```

```
Time      float64
V1        float64
V2        float64
V3        float64
V4        float64
V5        float64
V6        float64
V7        float64
V8        float64
V9        float64
V10       float64
V11       float64
V12       float64
V13       float64
V14       float64
V15       float64
V16       float64
V17       float64
V18       float64
V19       float64
V20       float64
V21       float64
V22       float64
V23       float64
V24       float64
V25       float64
V26       float64
V27       float64
V28       float64
Amount    float64
Class       int64
dtype: object
```

Ο επόμενος έλεγχος, αφορά την ύπαρξη ή μη κενών πεδίων, δηλαδή την έλλειψη τιμών από το dataset μας

```
df.isnull().sum()
```

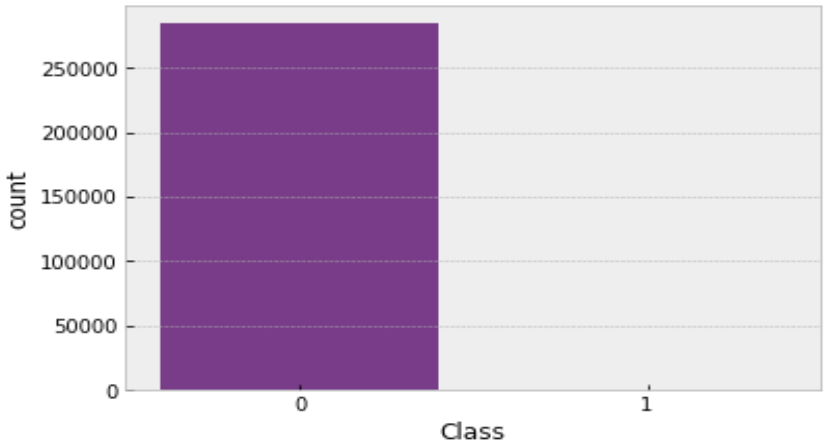
```
Time      0
V1        0
V2        0
V3        0
V4        0
V5        0
V6        0
V7        0
V8        0
V9        0
V10       0
V11       0
V12       0
V13       0
V14       0
V15       0
V16       0
V17       0
V18       0
V19       0
V20       0
V21       0
V22       0
V23       0
V24       0
V25       0
V26       0
V27       0
V28       0
Amount    0
Class     0
dtype: int64
```

Έπειτα, θα ελέγξουμε την κατανομή των γνήσιων και των απατηλών συναλλαγών που υπάρχουν μέσα στο dataset μας. Για τα διαγράμματα θα χρησιμοποιήσουμε την βιβλιοθήκη seaborn της python. Βλέπουμε, οτι το ποσοστό των απατηλών συναλλαγών που εμπεριέχονται στα δεδομένα μας είναι 0,17% κάτι που σημαίνει ότι έχουμε μεγάλη ανισορροπία μεταξύ των δύο κλάσεων την οποία πρέπει να λάβουμε υπόψιν μας προτού προχωρήσουμε σε περαιτέρω εφαρμογή των αλγορίθμων.

```
sns.countplot(x='Class', data=df, palette='CMRmap')
print('Non-fraud transactions:
```

```
{}%'.format(round(df.Class.value_counts()[0]/len(df)*100.0,2)))
print('Fraud transactions:
{}%'.format(round(df.Class.value_counts()[1]/len(df)*100.0,2)))
```

```
Non-fraud transactions: 99.83%
Fraud transactions: 0.17%
```

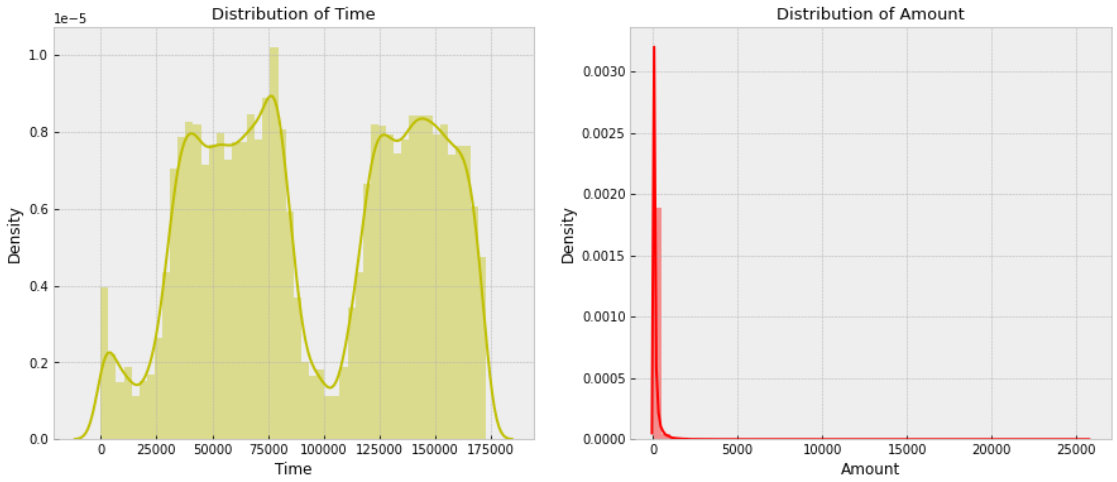


Σχήμα 2: Ποσοστό απατηλών και γνήσιων συναλλαγών

Όλα τα χαρακτηριστικά εκτός από τις στήλες time και amount, έχουν προκύψει από PCA (PRINCIPAL COMPONENT ANALYSIS), οπότε πάμε να ελέγξουμε την κατανομή των δύο αυτών χαρακτηριστικών.

```
f, (ax1, ax2) = plt.subplots(1, 2, figsize=(15, 6))
ax1 = sns.distplot(df['Time'], ax=ax1, color='y')
ax2 = sns.distplot(df['Amount'], ax=ax2, color='r')
ax1.set_title('Distribution of Time', fontsize=13)
ax2.set_title('Distribution of Amount', fontsize=13)
```

```
Text(0.5, 1.0, 'Distribution of Amount')
```



Σχήμα 3: Κατανομή χρόνου και ποσού στα δεδομένα

Από τα παραπάνω διαγράμματα εξάγουμε τις εξής πληροφορίες: Το μεγαλύτερο πλήθος των συναλλαγών πραγματοποιείται απογευματινές ώρες, και κυμαίνεται σε ποσά μικρότερα των 100€. Παρόλα αυτά, εντοπίζουμε αρκετές ακραίες τιμές, που αναπαριστούν συναλλαγές μεγάλων ποσών. Αυτές οι ακραίες τιμές σίγουρα θα επηρεάσουν τα αποτελέσματα των αλγορίθμων που θα εφαρμόσουμε. Μια λύση θα ήταν να τις αφαιρέσουμε από το σύνολο δεδομένων μας. Παρόλα αυτά, ακριβώς επειδή αυτές οι ακραίες τιμές αφορούν συναλλαγές μεγάλων ποσών οι οποίες μπορεί να είναι απατηλές, επιλέγουμε να τις κρατήσουμε καθώς επιζητούμε ένα ιδανικό μοντέλο μηχανικής μάθησης το οποίο θα είναι σε θέση να προβλέψει τα περιστατικά απάτης με μεγάλη οικονομική απώλεια.

Όπως αναφέραμε και προηγουμένως, τα δεδομένα έχουν ήδη κανονικοποιηθεί με PCA τεχνική, πέραν των χαρακτηριστικών του χρόνου και του ποσού. Επομένως, θα προχωρήσουμε σε κανονικοποίηση των δύο αυτών στηλών μέσω του αλγορίθμου Robust Scaler. Η επιλογή του συγκεκριμένου αλγορίθμου έγινε καθώς έχει πολύ καλές αποδόσεις σε σύνολα δεδομένων με ακραίες τιμές, όπως είναι και το δικό μας.

```
from sklearn.preprocessing import RobustScaler
rs = RobustScaler()
df['scaled_amount'] = rs.fit_transform(df['Amount'].values.reshape(-1,1))
df['scaled_time'] = rs.fit_transform(df['Time'].values.reshape(-1,1))
df.drop(['Time', 'Amount'], axis=1, inplace=True)

scaled_amount = df['scaled_amount']
scaled_time = df['scaled_time']
df.drop(['scaled_amount', 'scaled_time'], axis=1, inplace=True)
df.insert(0, 'scaled_amount', scaled_amount)
df.insert(0, 'scaled_time', scaled_time)
```

Όπως αναφέραμε και προηγουμένως και μπορούμε να διακρίνουμε από το Σχήμα 2, έχουμε στη διάθεσή μας μη ισορροπημένα δεδομένα μεταξύ των κλάσεων, γεγονός που θα οδηγήσει στο φαινόμενο της υπερπροσαρμογής (overfitting) σε οποιοδήποτε μοντέλο και αν χρησιμοποιήσουμε. Για τον λόγο αυτόν, επιλέξαμε την τεχνική oversampling SMOTE που σημαίνει Synthetic Minority Over-sampling Technique., η οποία δημιουργεί επιπρόσθετα δεδομένα στην κλάση με την χαμηλότερη κατανομή, για να ισορροπήσουμε τα δεδομένα μας. Προτού όμως γίνει αυτό, θα προχωρήσουμε σε διαχωρισμό του dataset μας σε train και test δεδομένα (cross validation).

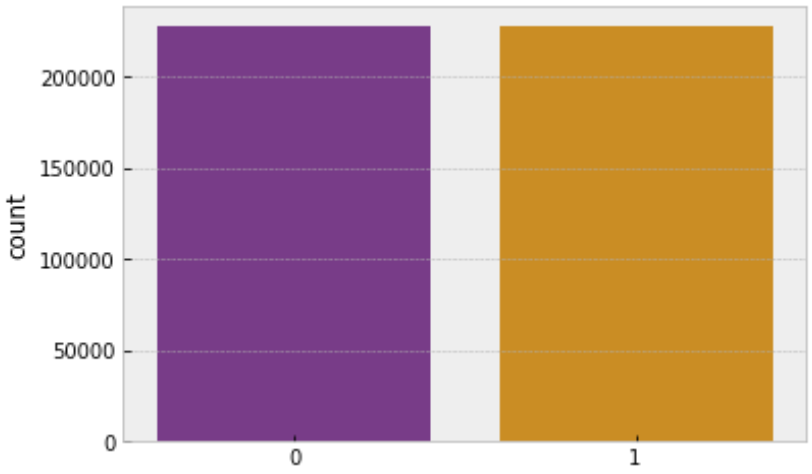
```
from sklearn.model_selection import train_test_split as holdout
x = np.array(df.iloc[:, df.columns != 'Class'])
y = np.array(df.iloc[:, df.columns == 'Class'])
x_train, x_test, y_train, y_test = holdout(x, y, test_size=0.2,
random_state=0)
```

Αφού χωρίσουμε τα δεδομένα μας στη συνέχεια εφαρμόζουμε την τεχνική SMOTE. Ο λόγος που χρησιμοποιήθηκε η τεχνική SMOTE μετά το cross validation, είναι για να αποφύγουμε την διαρροή δεδομένων από το αρχικό set και ως εκ τούτου να αποφευχθεί το φαινόμενο του overfitting.

```
print("Transaction Number x_train dataset: ", x_train.shape)
print("Transaction Number y_train dataset: ", y_train.shape)
print("Transaction Number x_test dataset: ", x_test.shape)
print("Transaction Number y_test dataset: ", y_test.shape)

print("Before OverSampling, counts of label '1':
```

```
{}".format(sum(y_train==1)))
print("Before OverSampling, counts of label '0': {}
\n".format(sum(y_train==0)))

sm = SMOTE(random_state=2)
x_train_s, y_train_s = sm.fit_resample(x_train, y_train.ravel())

print('After OverSampling, the shape of train_x:
{}'.format(x_train_s.shape))
print('After OverSampling, the shape of train_y: {}
\n'.format(y_train_s.shape))

print("After OverSampling, counts of label '1', %:
{}".format(sum(y_train_s==1)/len(y_train_s)*100.0,2))
print("After OverSampling, counts of label '0', %:
{}".format(sum(y_train_s==0)/len(y_train_s)*100.0,2))

sns.countplot(x=y_train_s, data=df, palette='CMRmap')
```

```
Transaction Number x_train dataset:  (227845, 30)
Transaction Number y_train dataset:  (227845, 1)
Transaction Number x_test dataset:  (56962, 30)
Transaction Number y_test dataset:  (56962, 1)
Before OverSampling, counts of label '1': [391]
Before OverSampling, counts of label '0': [227454]

After OverSampling, the shape of train_x: (454908, 30)
After OverSampling, the shape of train_y: (454908,)

After OverSampling, counts of label '1', %: 50.0
After OverSampling, counts of label '0', %: 50.0
```



Σχήμα 4: Κατανομή των κλάσεων μετά από εφαρμογή αλγορίθμου SMOTE

Βλέπουμε πράγματι οτι έχουν ισορροπηθεί η κλάσεις ισόποσα για τις γνήσιες και τις απατηλές συναλλαγές, και οι απατηλές συναλλαγές που προηγουμένως αποτελούσαν το 0,17% του dataset πλέον αποτελούν το 50%.

Μοντέλα μηχανικής μάθησης και αξιολόγηση:

Στη συνέχεια, θα γίνει εκπαίδευση και δοκιμή των ταξινομητών

- Logistic Regression
- Random Forest Classifier
- XGBoost
- Neural Network

καθώς και σύγκριση των αποδόσεών τους. Για την αξιολόγηση των μοντέλων θα χρησιμοποιήσουμε τις μετρικές f1-score, precision/recall score και confusion matrix. Δεν θα βασιστούμε στην μετρική accuracy καθώς σε τόσο μη ισορροπημένα dataset δεν είναι τόσο έγκυρη.

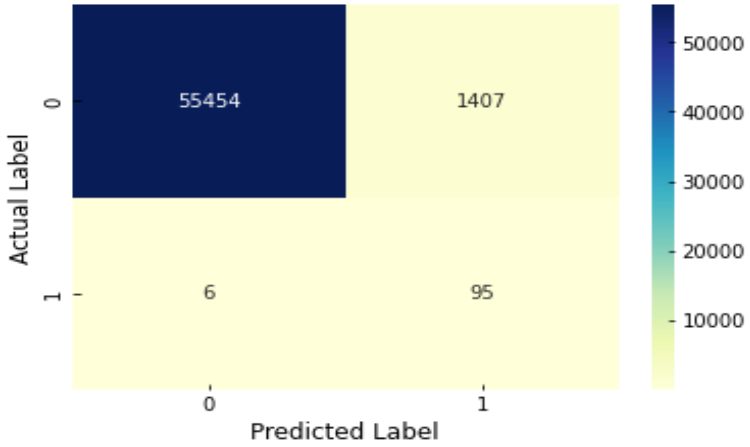
6.1.2. Logistic Regression

Θα ξεκινήσουμε με εφαρμογή της λογιστικής παλινδρόμησης την οποία και θα αξιολογήσουμε μέσω των μετρικών και του πίνακα συσχετίσεων

```
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import confusion_matrix, precision_recall_curve,
classification_report, precision_score, recall_score, accuracy_score


logreg = LogisticRegression()
logreg.fit(x_train_s, y_train_s)
y_pred = logreg.predict(x_test)
cnf_matrix = confusion_matrix(y_test, y_pred)

sns.heatmap(pd.DataFrame(cnf_matrix), annot=True, cmap="YlGnBu", fmt='g')
plt.ylabel('Actual Label')
```

```
plt.xlabel('Predicted Label')

print(classification_report(y_test, y_pred))
```

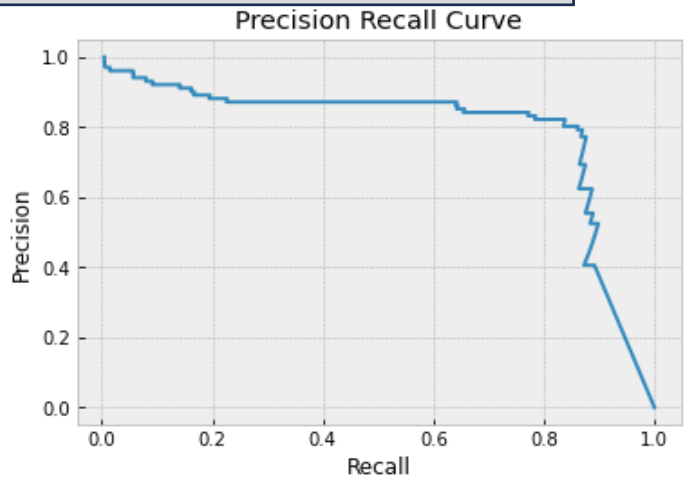
```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99     56861
           1       0.06      0.94      0.12       101

    accuracy                           0.98     56962
   macro avg       0.53      0.96      0.55     56962
weighted avg       1.00      0.98      0.99     56962
```



Σχήμα 5: Confusion Matrix για λογιστική παλινδρόμηση

```
y_pred_prob = logreg.predict_proba(x_test)[:,1]
precision, recall, thresholds = precision_recall_curve(y_test,
y_pred_prob)
plt.plot(precision, recall)
plt.xlabel('Recall')
plt.ylabel('Precision')
```

```
plt.title('Precision Recall Curve')
```



Σχήμα 6: Καμπύλη για Precision και Recall

Το μοντέλο αυτό έδωσε πολύ υψηλή τιμή στην μετρική recall που σημαίνει οτι είναι σε θέση να εντοπίζει τον μεγαλύτερο όγκο απατηλών συναλλαγών. Ωστόσο έχουμε αρκετά χαμηλό precision γεγονός που συνεπάγεται με την κατηγοριοποίηση αρκετών συναλλαγών ως απατηλές χωρίς ωστόσο να είναι. Βλέπουμε μάλιστα από το Σχήμα 6 ότι ο μόνος λόγος που το μοντέλο εντόπισε τον μεγαλύτερο όγκο των απατηλών συναλλαγών είναι λόγω της μείωσης της τιμής precision.

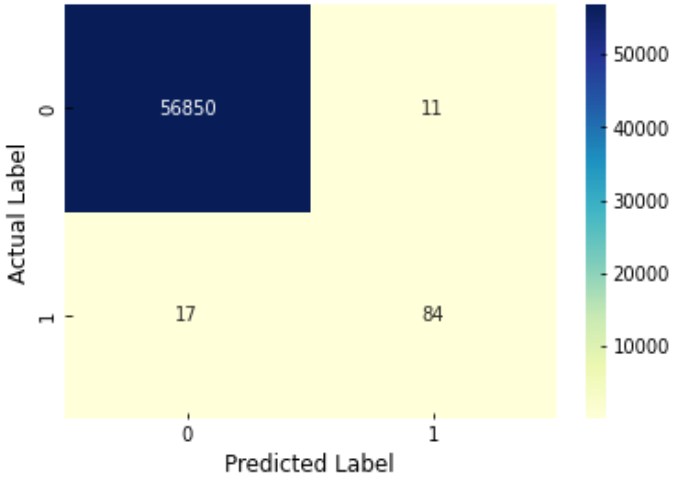
6.1.3. Random Forest Classifier

Θα εφαρμόσουμε τον αλγόριθμο Random Forest τον οποίο και θα αξιολογήσουμε στην συνέχεια

```
from sklearn.ensemble import RandomForestClassifier as rfc
rand_f = rfc(n_estimators=1000, min_samples_split=10, min_samples_leaf=1,
max_features='auto', max_leaf_nodes=None,
oob_score=True, n_jobs=-1, random_state=1)
rand_f.fit(x_train_s, y_train_s)
y_pred = rand_f.predict(x_test)


cnf_matrix = confusion_matrix(y_test, y_pred)
sns.heatmap(pd.DataFrame(cnf_matrix), annot=True, cmap="YlGnBu", fmt='g')
plt.ylabel('Actual Label')
plt.xlabel('Predicted Label')

print(classification_report(y_test, y_pred))
```

```
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     56861
           1       0.88      0.83      0.86       101

    accuracy                           1.00     56962
```

```
   macro avg       0.94      0.92      0.93     56962
weighted avg       1.00      1.00      1.00     56962
```



Σχήμα 7: Confusion Matrix για Random Forest

Ο ταξινομητής Random Forest έχει καλύτερη απόδοση από την λογιστική παλινδρόμηση καθώς έχει πετύχει υψηλές τιμές σε recall και precision. Παρόλο που έχει μειωθεί η τιμή του recall έχουμε καταφέρει να πετύχουμε υψηλό precision γεγονός που σημαίνει οτι γίνονται σωστές κατηγοριοποιήσεις των συναλλαγών στις αντίστοιχες κλάσεις.

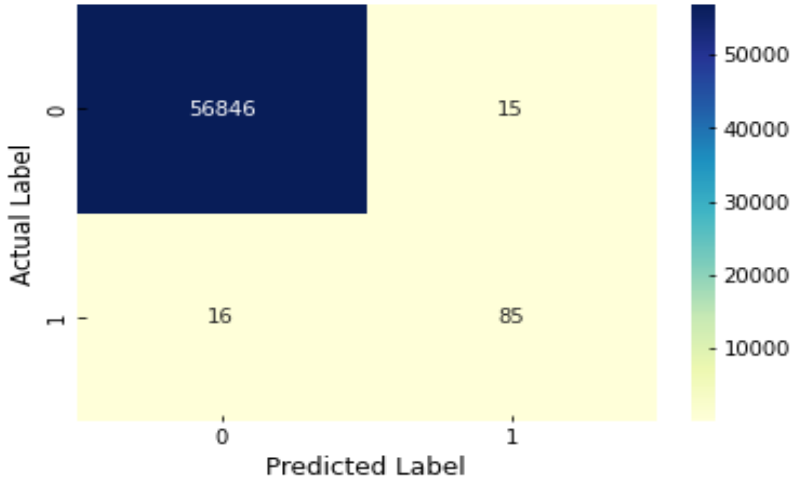
6.1.4. XGBoost

Εδώ θα γίνει χρήση του αλγορίθμου XGBoost

```
import xgboost as xgb
model = xgb.XGBClassifier(n_estimators = 5000, max_depth = 30,
learning_rate = 0.01)
model.fit(x_train_s, y_train_s)
y_pred = model.predict(x_test)

cnf_matrix = confusion_matrix(y_test, y_pred)
sns.heatmap(pd.DataFrame(cnf_matrix), annot=True, cmap="YlGnBu", fmt='g')
plt.ylabel('Actual Label')
plt.xlabel('Predicted Label')

print(classification_report(y_test, y_pred))
```

```
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     56861
           1       0.85      0.84      0.85       101

    accuracy                           1.00     56962
```

```
   macro avg       0.92      0.92      0.92     56962
weighted avg       1.00      1.00      1.00     56962
```



Σχήμα 8: Confusion Matrix για XGBoost

6.1.5. Neural Network

Τέλος θα εφαρμόσουμε τα νευρωνικά δίκτυα

```
from keras.models import Sequential
from keras.layers import Dense, Dropout
model = Sequential([Dense(input_dim=30, units=16, activation='relu'),
                    Dense(units=24, activation='relu'),
                    Dropout(0.5),
                    Dense(units=20, activation='relu'),
                    Dense(units=24, activation='relu'),
                    Dense(units=1, activation='sigmoid')])
model.summary()
```

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 dense (Dense)               (None, 16)                496

 dense_1 (Dense)             (None, 24)                408

 dropout (Dropout)           (None, 24)                0

 dense_2 (Dense)             (None, 20)                500

 dense_3 (Dense)             (None, 24)                504

 dense_4 (Dense)             (None, 1)                 25
```

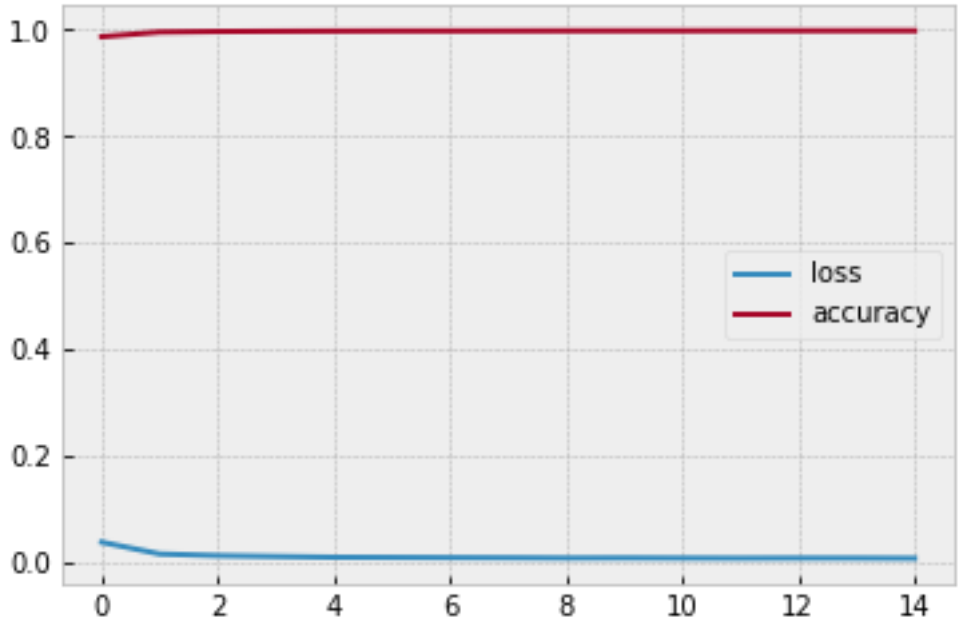
```
=================================================================
Total params: 1,933
Trainable params: 1,933
Non-trainable params: 0
_________________________________________________________________
```

```
model.compile(optimizer='adam', loss='binary_crossentropy',
metrics=['accuracy'])
model.fit(x_train_s, y_train_s, batch_size=15, epochs=15)
```

```
Epoch 1/15
30328/30328 [==============================] - 32s 1ms/step - loss:
0.0365 - accuracy: 0.9874
Epoch 2/15
30328/30328 [==============================] - 31s 1ms/step - loss:
0.0143 - accuracy: 0.9962
Epoch 3/15
30328/30328 [==============================] - 31s 1ms/step - loss:
0.0111 - accuracy: 0.9973
Epoch 4/15
30328/30328 [==============================] - 32s 1ms/step - loss:
0.0095 - accuracy: 0.9978
Epoch 5/15
30328/30328 [==============================] - 32s 1ms/step - loss:
0.0081 - accuracy: 0.9981
Epoch 6/15
30328/30328 [==============================] - 34s 1ms/step - loss:
0.0078 - accuracy: 0.9983
Epoch 7/15
30328/30328 [==============================] - 36s 1ms/step - loss:
0.0074 - accuracy: 0.9983
Epoch 8/15
30328/30328 [==============================] - 32s 1ms/step - loss:
0.0071 - accuracy: 0.9984
Epoch 9/15
30328/30328 [==============================] - 35s 1ms/step - loss:
0.0066 - accuracy: 0.9986
Epoch 10/15
30328/30328 [==============================] - 33s 1ms/step - loss:
0.0068 - accuracy: 0.9986
Epoch 11/15
30328/30328 [==============================] - 46s 2ms/step - loss:
0.0065 - accuracy: 0.9986
Epoch 12/15
30328/30328 [==============================] - 40s 1ms/step - loss:
0.0063 - accuracy: 0.9987
Epoch 13/15
```

```
30328/30328 [==============================] - 33s 1ms/step - loss:
0.0065 - accuracy: 0.9987
Epoch 14/15
30328/30328 [==============================] - 32s 1ms/step - loss:
0.0064 - accuracy: 0.9987
Epoch 15/15
30328/30328 [==============================] - 37s 1ms/step - loss:
0.0060 - accuracy: 0.9988
```

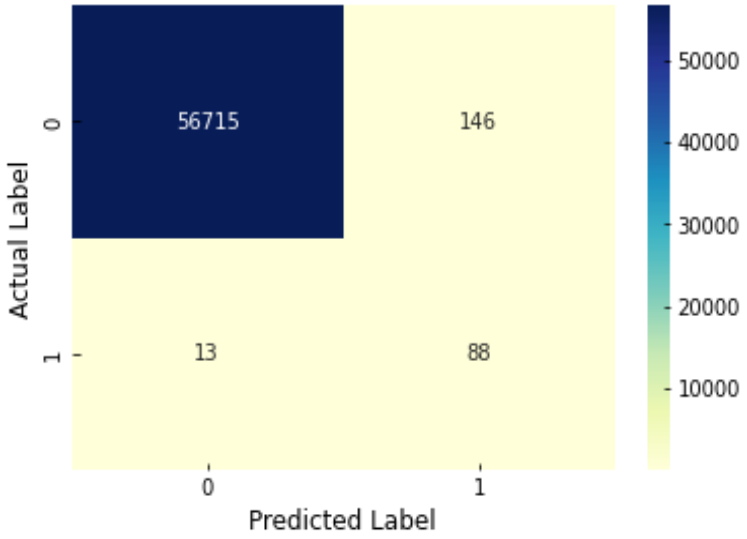
```
model_loss = pd.DataFrame(model.history.history)
model_loss. plot()
```



Σχήμα 9: Καμπύλη για Loss και Accuracy

```
score = model.evaluate(x_test, y_test)
print(score)

1781/1781 [==============================] - 2s 903us/step - loss: 0.0191
- accuracy: 0.9972
[0.019075818359851837, 0.9972086548805237]

y_pred = (model.predict(x_test) > 0.5).astype("int32")

cnf_matrix = confusion_matrix(y_test, y_pred)
sns.heatmap(pd.DataFrame(cnf_matrix), annot=True, cmap="YlGnBu", fmt='g')
plt.ylabel('Actual Label')
plt.xlabel('Predicted Label')

print(classification_report(y_test, y_pred))
```

	precision	recall	f1-score	support
0	1.00	1.00	1.00	56861
1	0.38	0.87	0.53	101
accuracy			1.00	56962
macro avg	0.69	0.93	0.76	56962
weighted avg	1.00	1.00	1.00	56962



Σχήμα 10: Confusion Matrix για Νευρωνικά δίκτυα

Συμπεράσματα:

Στα μοντέλα που εξετάσαμε σαφώς επιθυμούμε υψηλή τιμή στο recall καθώς είναι αυτή η μετρική που μας δείχνει οτι το μοντέλο είναι σε θέση να εντοπίσει τις απατηλές κινήσεις. Παρόλα αυτά, θέλουμε και καλή απόδοση στο precision καθώς μας δείχνει οτι γίνεται σωστή κατηγοριοποίηση των συναλλαγών ως γνήσιες και απατηλές. Οι ταξινομητές Random Forest και XGBoost έδωσαν τα καλύτερα αποτελέσματα καθώς μπόρεσαν να εντοπίσουν παραπάνω από το 80% των απατηλών κινήσεων και ταυτόχρονα δεν κατηγοριοποίησαν τις γνήσιες συναλλαγές ως απατηλές σε αντίθεση με την λογιστική παλινδρόμηση και τα νευρωνικά δίκτυα. Σε ένα τραπεζικό ίδρυμα, είναι πολύ σημαντικός ο εντοπισμός των απατηλών κινήσεων ωστόσο είναι εξίσου σημαντικό να μην υπάρχει μεγάλος όγκος γνήσιων συναλλαγών που το σύστημα τις θεωρεί απατηλές καθώς απαιτεί διαχειριστικό χρόνο από μεριάς της τράπεζας αλλά και στοχοποίηση συναλλαγών και εμπόρων, γεγονός που ενδέχεται να προκαλέσει σύγχυση και φόβο στους πελάτες και αποτροπή από την χρήση των τραπεζικών προϊόντων.

6.2. Σχεδιασμός συστήματος ανίχνευσης απάτης

Στο προηγούμενο μέρος της προγραμματιστικής εργασίας, μελετήσαμε πραγματικά δεδομένα στα οποία εφαρμόσαμε αλγόριθμους μηχανικής μάθησης τους οποίους εν συνεχεία συγκρίναμε και αναλύσαμε. Η ηλεκτρονική απάτη στα τραπεζικά ιδρύματα φέρνει καθημερινά νέες προκλήσεις και απειλές στο προσκήνιο, οι οποίες για να αντιμετωπιστούν σωστά και αποτελεσματικά χρειάζονται περαιτέρω γνώση και ανάλυση,

και η απλή εφαρμογή αλγορίθμων δεν είναι πάντα αρκετή. Ο καλύτερος τρόπος για να αντιληφθούμε τις δυσκολίες αυτές είναι να σχεδιάσουμε από την αρχή ένα σύστημα ανίχνευσης απάτης για καρτικές απάτες, προκειμένου να δούμε και να κατανοήσουμε καλύτερα την έννοια της ηλεκτρονικής απάτης στα τραπεζικά ιδρύματα και πως αυτή διαχειρίζεται σε πραγματικό χρόνο. Στο κομμάτι αυτό της εργασίας, σχεδιάσαμε ένα τέτοιο FDS (Fraud Detection System) εμπνευσμένο από πραγματικά σενάρια και προκλήσεις.

Με την παρακάτω προσομοίωση, πλαισιώνουμε μια προσέγγιση της πραγματικότητας. Έχουμε δημιουργήσει κανόνες για την διαμόρφωση δόλιων συμπεριφορών, που θα βοηθήσουν στην ερμηνεία των μοτίβων που μπορούν να εντοπίσουν οι διάφορες τεχνικές ανίχνευσης απάτης. Τα προσομοιωμένα σύνολα δεδομένων, θα αναδείξουν τα προβλήματα που αντιμετωπίζονται καθημερινά στην ανίχνευση της απάτης. Συγκεκριμένα, θα περιλαμβάνουν ανισορροπία κλάσεων, μείγμα αριθμητικών και κατηγορικών χαρακτηριστικών με μη τετριμμένες σχέσεις μεταξύ τους και σενάρια απάτης τα οποία εξαρτώνται από τον χρόνο.

Θα επικεντρωθούμε στα βασικότερα χαρακτηριστικά μιας συναλλαγής. Πιο συγκεκριμένα, μια συναλλαγή με κάρτα αποτελείται από το ποσό της κίνησης, τον έμπορο στον οποίον πραγματοποιείται η συναλλαγή, τον πελάτη τον οποίον την πραγματοποιεί καθώς και την χρονική στιγμή. Τα βασικά αυτά χαρακτηριστικά συνοψίζονται ως εξής:

- Transaction ID: Ο κωδικός της εκάστοτε συναλλαγής
- Date and time: Η ημερομηνία και η ώρα που πραγματοποιήθηκε η κίνηση
- Customer ID: Ο κωδικός του πελάτη που πραγματοποίησε την κίνηση
- Terminal ID: Ο κωδικός του τερματικού, στο οποίο πραγματοποιήθηκε η συναλλαγή.
- Transaction amount: Το ποσό της συναλλαγής
- Fraud Label: Μια δυαδική μεταβλητή, η οποία θα υποδεικνύει εάν μια κίνηση είναι απατηλή ή όχι (τιμή 1 και 0 αντίστοιχα)

6.2.1. Δημιουργία δεδομένων:

Η διαδικασία που ακολουθήσαμε για τον σχεδιασμό αυτού του συστήματος, ξεκινάει από την δημιουργία του dataset μας, το οποίο θα αποτελείται από πελάτες και πιθανούς εμπόρους (τερματικά). Για την δημιουργία των πελατών, θα προσπαθήσουμε να δημιουργήσουμε ένα συναλλακτικό προφίλ για τον καθένα, το οποίο θα αποτελείται από τις καταναλωτικές του συνήθειες. Πιο αναλυτικά, θα χρησιμοποιήσουμε την γεωγραφική του θέση, την συχνότητα των δαπανών του καθώς και τα αντίστοιχα ποσά. Επιλέξαμε επομένως τα εξής χαρακτηριστικά:

- Customer ID: Ο μοναδικό κωδικός που θα χαρακτηρίζει κάθε πελάτη
- (x_customer,y_customer): Οι συντεταγμένες του πελάτη. Θα θεωρήσουμε οτι οι συντεταγμένες του πελάτη δεν αλλάζουν και παραμένουν σταθερές.
- (mean_amount,std_amount): Η μέση τιμή και η τυπική απόκλιση των ποσών των συναλλαγών που εκτελεί ο πελάτης
- (mean_trx_day): Ο μέσος όρος των συναλλαγών που εκτελεί ο πελάτης την ημέρα

Η δημιουργία των συντεταγμένων των πελατών έγινε από τυχαία κατανομή, που σε πραγματικά δεδομένα λαμβάνονται την ώρα που γίνεται μια συναλλαγή από την ip που χρησιμοποιεί ο πελάτης. Ως μέσο όρο των ποσών από τις συναλλαγές έχουμε επιλέξει από 0€ έως 250€, ενώ θεωρήσαμε ο μέσος όρος των συναλλαγών μέσα σε μια ημέρα να μην ξεπερνάει τις 5 συναλλαγές ανά πελάτη

```
def generate_customer_profiles(n_customers, random_state=0):
    np.random.seed(random_state)
    customer_properties=[]

        for customer_id in range(n_customers):
```

```
        x_customer = np.random.uniform(0,100)
        y_customer = np.random.uniform(0,100)
        mean_amount = np.random.uniform(5,250)
        std_amount = mean_amount/2
        mean_trx_day = np.random.uniform(0,5)
        customer_properties.append([customer_id, x_customer, y_customer,
                                    mean_amount, std_amount,
                                    mean_trx_day])

    customer_profiles = pd.DataFrame(customer_properties,
columns=['customer_id','x_customer', 'y_customer','mean_amount',
'std_amount','mean_trx_day'])

    return customer_profiles
```

Στη συνέχεια, για την δημιουργία τερματικών επιλέξαμε να έχουν τα παρακάτω χαρακτηριστικά:

- terminal_id: Ο μοναδικός κωδικός που θα χαρακτηρίζει το τερματικό
- (x_terminal,y_terminal): Οι συντεταγμένες του εμπόρου
- mcc : Κατηγορία του εμπόρου (Merchant category code)

```
def generate_terminal_table(n_terminals, random_state=0):
    np.random.seed(random_state)
    terminal_properties=[]

    for terminal_id in range(n_terminals):
        x_terminal = np.random.uniform(0,100)
        y_terminal= np.random.uniform(0,100)
        mcc=random.choice(mcc_codes['mcc'])
        terminal_properties.append([terminal_id, x_terminal,
y_terminal,mcc])

    terminal_table = pd.DataFrame(terminal_properties,
columns=['terminal_id','x_terminal', 'y_terminal','mcc'])

    return terminal_table
```

Θα φορτώσουμε ολα τα mcc τα οποια τυχαία θα κατανείμουμε σε κάθε τερματικό

```
mcc_codes=pd.read_csv('mcc_codes.csv')
```

Τα προφίλ των πελατών περιέχουν πλέον όλες τις πληροφορίες που χρειαζόμαστε για την δημιουργία των συναλλαγών. Η δημιουργία των συναλλαγών θα γίνεται από μια συνάρτηση generate_transactions_table, η οποία δέχεται ως είσοδο εάν προφίλ πελάτη, μια ημερομηνία έναρξης και ένα χρονικό διάστημα ημερών για τις οποίες θα δημιουργηθούν συναλλαγές. Έχουμε επιλέξει να κατανείμουμε τον όγκο των συναλλαγών κυρίως τις απογευματινές ώρες καθώς όπως είδαμε και στο προηγούμενο μέρος το βράδυ δεν πραγματοποιείτε το ίδιο πλήθος συναλλαγών. Το dataset μας θεωρούμε οτι ξεκινάει από 01-01-2023 και θα έχει χρονική διάρκεια 120 ημερών

```
def generate_transactions_table(customer_profile,start_date ="2023-01-
01", number_of_days= 120,random_state=0):
    customer_transactions = []
```

```
    for day in range(number_of_days):
        # Τυχαίος αριθμός συναλλαγών για κάθε μέρα,μέσω κατανομής Poisson
        number_trx =int(np.random.poisson(customer_profile.mean_trx_day))

        if number_trx>0:
            for trx in range(number_trx):
                time_trx = int(np.random.normal(86400/2,20000))
                if (time_trx>0) and (time_trx<86400):
                    # Ποσό βάσει κανονικής κατανομής
                    amount =np.random.normal(
customer_profile.mean_amount, customer_profile.std_amount)
                    # Εάν είναι αρνητικός,ακολουθούμε ομοιόμορφη κατανομή
                    if amount<0:
                        amount = np.random.uniform(
0,customer_profile.mean_amount*2)
                    amount=np.round(amount,decimals=2)
                    terminal_id = random.choice(
terminal_table.terminal_id)
                    customer_transactions.append(
[time_trx+day*86400, day,int(customer_profile.customer_id),terminal_id,
amount,time_trx])
    customer_transactions = pd.DataFrame(customer_transactions,
columns=['TRX_TIME_SECONDS', 'TRX_TIME_DAYS', 'CUSTOMER_ID',
'TERMINAL_ID', 'TRX_AMOUNT','TIME_TRX'])

    if len(customer_transactions)>0:
        customer_transactions['TRX_DATETIME'] = pd.to_datetime(
customer_transactions["TRX_TIME_SECONDS"], unit='s', origin=start_date)

customer_transactions=customer_transactions[['TRX_DATETIME','CUSTOMER_ID'
, 'TERMINAL_ID','TRX_AMOUNT','TRX_TIME_SECONDS',
'TRX_TIME_DAYS','TIME_TRX']]

    return customer_transactions
```

Τέλος, δημιουργούμε το τελικό dataset το οποίο θα αποτελείται από :

- 5000 πελάτες
- 10.000 πιθανούς εμπόρους
- διάρκεια 120 ημερών.

```
start_time=time.time()
customer_profiles = generate_customer_profiles(5000, random_state = 0)
print("Time to generate customer profiles table:
{0:.2}s".format(time.time()-start_time))

start_time=time.time()
terminal_table = generate_terminal_table(10000, random_state = 1)
```

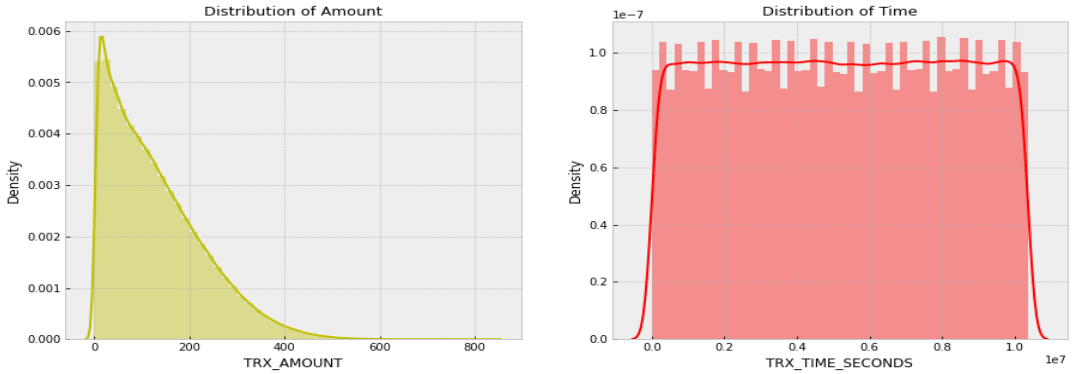
```
print("Time to generate terminal profiles table:
{0:.2}s".format(time.time()-start_time))

start_time=time.time()
transactions_df=customer_profiles.groupby('customer_id').apply(lambda x :
generate_transactions_table(x.iloc[0],
number_of_days=120)).reset_index(drop=True)
print("Time to generate transactions: {0:.2}s".format(time.time()-
start_time))
```

Έχουμε δημιουργήσει ένα πίνακα που αποτελείται από 1437001 συναλλαγές

Αφού έχουμε ετοιμάσει τα δεδομένα μας, προχωράμε σε περαιτέρω ανάλυση. Πλέον γνωρίζουμε τι αφορά κάθε στήλη επομένως έχει νόημα να ελέγξουμε και μερικά διαγράμματα για την καλύτερη κατανόηση τους.

Έλεγχος κατανομής των ποσών και των χρόνων που έγιναν οι συναλλαγές:

```
f, (ax1, ax2) = plt.subplots(1, 2, figsize=(15, 6))
ax1 = sns.distplot(df1['TRX_AMOUNT'], ax=ax1, color='y')
ax2 = sns.distplot(df1['TRX_TIME_SECONDS'], ax=ax2, color='r')
ax1.set_title('Distribution of Amount', fontsize=13)
ax2.set_title('Distribution of Time', fontsize=13)
```



Σχήμα 11: Κατανομή του ποσού και του χρόνου στα δεδομένα μας

Τα ποσά κυμαίνονται κυρίως σε χαμηλές τιμές και ο χρόνος των συναλλαγών είναι μεγαλύτερος το πρωί και το απόγευμα, όπως δηλαδή γίνεται κατά βάση και σε πραγματικά δεδομένα. Για το τελικό dataframe υπολογίζουμε την απόσταση του κάθε πελάτη από τον εκάστοτε έμπορο προκειμένου να έχει την παρακάτω μορφή:

```
dftest=pd.merge(df1,customer_profiles,left_on='CUSTOMER_ID',right_on='cus
tomer_id',how='left')

df2=pd.merge(dftest,terminal_table,left_on='TERMINAL_ID',right_on='termin
al_id',how='left')

df2.drop(['customer_id','mean_amount','std_amount','mean_trx_day','termin
al_id'],axis=1,inplace=True)

df2['dist'] = np.linalg.norm(df2.iloc[:, [8,9]].values - df2.iloc[:,
[10,11]], axis=1)
```

```
df2.drop(['x_customer','y_customer','x_terminal','y_terminal'],axis=1,
inplace=True)
```

df2

	TRANSACTION_ID	TRX_DATETIME	CUSTOMER_ID	TERMINAL_ID	TRX_AMOUNT	TRX_TIME_SECONDS	TRX_TIME_DAYS	TIME_TRX	mcc	dist
0	0	2023-01-01 00:01:01	378	5547	196.61	61	0	61	3779	39.445647
1	1	2023-01-01 00:01:28	2925	9384	40.58	88	0	88	5697	71.405827
2	2	2023-01-01 00:02:00	4746	800	65.32	120	0	120	4784	93.123150
3	3	2023-01-01 00:03:11	2385	2557	58.66	191	0	191	5531	79.447385
4	4	2023-01-01 00:03:48	3118	1505	52.84	228	0	228	3025	106.636814
...	...	...	...	...	...	...	...	...	...	...
1436996	1436996	2023-04-30 23:58:33	2115	8735	166.92	10367913	119	86313	7033	95.079077
1436997	1436997	2023-04-30 23:58:36	2220	1055	469.75	10367916	119	86316	3720	33.045143
1436998	1436998	2023-04-30 23:59:00	3423	4829	53.25	10367940	119	86340	3550	61.241167
1436999	1436999	2023-04-30 23:59:35	3887	4420	102.78	10367975	119	86375	3088	103.907168
1437000	1437000	2023-04-30 23:59:55	4115	2970	16.18	10367995	119	86395	3707	103.844701

1437001 rows × 10 columns

Σχήμα 12: Τελικό dataframe που εμπεριέχει τα δεδομένα μας με τα αντίστοιχα χαρακτηριστικά

Έπειτα, προχωράμε στην δημιουργία fraud σεναρίων, τα οποία θα χαρακτηρίζουν τις συναλλαγές ως απατηλές. Τα σενάρια αυτά είναι εμπνευσμένα από πραγματικά περιστατικά απάτης

- Σενάριο 1: Θεωρούμε οτι εάν ο πελάτης εκτελεί συναλλαγές με χρονική απόσταση μικρότερη των 20 δευτερόλεπτων, τότε η κίνηση είναι απατηλή
- Σενάριο 2: Επιλέγουμε 3 τυχαίους πελάτες κάθε μέρα οι οποίοι θεωρούμε οτι έχουν πέσει θύμα απάτης για τις επόμενες 7 ημέρες, για το 1/3 των συναλλαγών τους πολλαπλασιάζουμε τα ποσά επί 5 και τα θεωρούμε ως απατηλά. Αυτό συμβαίνει και σε πραγματικό χρόνο, όταν δηλαδή ένας πελάτης είναι θύμα απάτης phishing και οι συναλλαγές που πραγματοποιούνται από τον απατεώνα δεν συμβαδίζουν με το συναλλακτικό του προφίλ του πελάτη
- Σενάριο 3: Επιλέγουμε τον κωδικό τερματικού 6051, ο οποίος σχετίζεται με μεταφορές χρημάτων. Χαρακτηρίζουμε όλες τις συναλλαγές που έχουν πραγματοποιηθεί στα τερματικά με τέτοιο mcc ως απατηλές. Το mcc αυτό συνδέετε με τα περισσότερα περιστατικά απάτης που συμβαίνουν καθημερινά
- Σενάριο 4:Θεωρούμε οτι αν η απόσταση ενός πελάτη από έναν έμπορο είναι σε ακτίνα μεγαλύτερη από 120, τότε η συναλλαγή είναι απατηλή

```
def add_frauds(customer_profiles, terminal_table, df2,random_state=0):

    # Θέτουμε όλες τις συναλλαγές ως γνήσιες
    df2['TRX_FRAUD']=0
    df2['TRX_FRAUD_SCENARIO']=0

    # Σενάριο 1
    mask1=df2.groupby('CUSTOMER_ID').TRX_TIME_SECONDS.apply(
```

```
lambda x: x.diff()<20)
    df2.loc[mask1,'TRX_FRAUD']=1
    df2.loc[mask1,'TRX_FRAUD_SCENARIO']=1
    nb_frauds_scenario_1=df2.TRX_FRAUD.sum()
    print("Number of frauds from scenario 2: "+str(nb_frauds_scenario_1))

    # Σενάριο 2
    for day in range(df2.TRX_TIME_DAYS.max()):

        compromised_customers = customer_profiles.customer_id.sample(n=3,
random_state=day).values

        compromised_transactions=df2[(df2.TRX_TIME_DAYS>=day) &
(df2.TRX_TIME_DAYS<day+7) &
(df2.CUSTOMER_ID.isin(compromised_customers))]
        nb_compromised_transactions=len(compromised_transactions)
        random.seed(day)
        index_fauds =
random.sample(list(compromised_transactions.index.values),k=int(
nb_compromised_transactions/3))

df2.loc[index_fauds,'TRX_AMOUNT']=df2.loc[index_fauds,'TRX_AMOUNT']*5
        df2.loc[index_fauds,'TRX_FRAUD']=1
        df2.loc[index_fauds,'TRX_FRAUD_SCENARIO']=2

    nb_frauds_scenario_2=df2.TRX_FRAUD.sum()-nb_frauds_scenario_1
    print("Number of frauds from scenario 2: "+str(nb_frauds_scenario_2))

      # Σενάριο 3
    mask3=df2[(df2['mcc']==6051)]
    df2.loc[mask3.index,'TRX_FRAUD']=1
    df2.loc[mask3.index,'TRX_FRAUD_SCENARIO']=3

    nb_frauds_scenario_3=df2.TRX_FRAUD.sum()-nb_frauds_scenario_2-
nb_frauds_scenario_1
    print("Number of frauds from scenario 3: "+str(nb_frauds_scenario_3))

    #Σενάριο 4
    df2.loc[df2.dist>130, 'TRX_FRAUD']=1
    df2.loc[df2.dist>130, 'TRX_FRAUD_SCENARIO']=4
    nb_frauds_scenario_4=df2.TRX_FRAUD.sum()-nb_frauds_scenario_3-
nb_frauds_scenario_2-nb_frauds_scenario_1
    print("Number of frauds from scenario 4: "+str(nb_frauds_scenario_4))

    return df2
%time df2 = add_frauds(customer_profiles, terminal_table, df2)
```

Έχουμε επομένως 5668 απατηλές συναλλαγές οι οποίες αποτελούν το 0,3% από το σύνολο όλων των συναλλαγών

```
df2.TRX_FRAUD.mean()
```

```
0.0039443257172402805
```

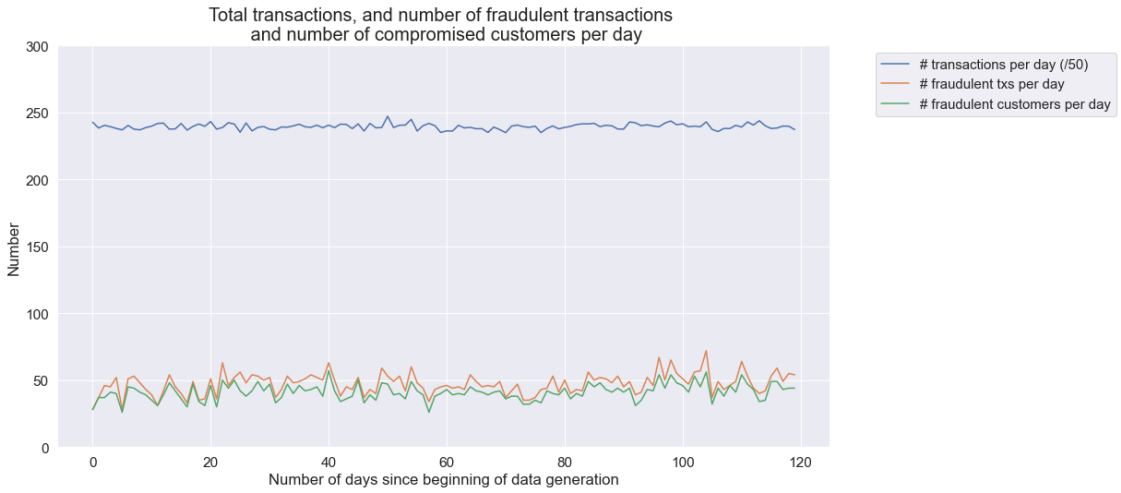
```
df2.TRX_FRAUD.sum()
```

```
5668
```

Έχοντας ολοκληρώσει τον πίνακα των συναλλαγών με την ένδειξη για γνήσια ή μη συναλλαγή πάμε να ελέγξουμε πως μεταβάλλεται ο αριθμός των συναλλαγών, ο αριθμός των απατηλών συναλλαγών αλλά και ο αριθμός των πελατών που έχουν πέσει θύμα απάτης

```
def get_stats(df2):
    #Αριθμός συναλλαγών ανά μέρα
    nb_tx_per_day=df2.groupby(['TRX_TIME_DAYS'])['CUSTOMER_ID'].count()
    #Αριθμός απατηλών συναλλαγών ανά μέρα
    nb_fraud_per_day=df2.groupby(['TRX_TIME_DAYS'])['TRX_FRAUD'].sum()
    #Αριθμός πελατών που έχουν πέσει θύμα απάτης ανά μέρα
    nb_fraudcustomer_per_day=df2[df2['TRX_FRAUD']>0].groupby(
['TRX_TIME_DAYS']).CUSTOMER_ID.nunique()
    return (nb_tx_per_day,nb_fraud_per_day,nb_fraudcustomer_per_day)
(nb_tx_per_day,nb_fraud_per_day,nb_fraudcustomer_per_day)=get_stats(df2)

n_days=len(nb_tx_per_day)
tx_stats=pd.DataFrame({"value":pd.concat([nb_tx_per_day/50,nb_fraud_per_d
ay,nb_fraudcustomer_per_day])})
tx_stats['stat_type']=["nb_tx_per_day"]*n_days+["nb_fraud_per_day"]*n_day
s+["nb_fraudcustomer_per_day"]*n_days
tx_stats=tx_stats.reset_index()
%%capture

sns.set(style='darkgrid')
sns.set(font_scale=1.4)

fraud_and_transactions_stats_fig = plt.gcf()

fraud_and_transactions_stats_fig.set_size_inches(15, 8)

sns_plot = sns.lineplot(x="TRX_TIME_DAYS", y="value", data=tx_stats,
hue="stat_type",
hue_order=["nb_tx_per_day","nb_fraud_per_day","nb_fraudcustomer_per_day"]
, legend=False)

sns_plot.set_title('Total transactions, and number of fraudulent
transactions \n and number of compromised customers per day',
fontsize=20)
sns_plot.set(xlabel = "Number of days since beginning of data
generation", ylabel="Number")
```

```
sns_plot.set_ylim([0,300])

labels_legend = ["# transactions per day (/50)", "# fraudulent txs per
day", "# fraudulent customers per day"]

sns_plot.legend(loc='upper left', labels=labels_legend,bbox_to_anchor=(
1.05, 1), fontsize=15)
fraud_and_transactions_stats_fig
```



Σχήμα 13: Σύνολο συναλλαγών που πραγματοποιούνται κάθε μέρα σε σχέση με τον αριθμό των συναλλαγών που είναι απατηλές και τον αριθμό των πελατών που έχουν πέσει θύμα απάτης

Αυτή η προσομοίωση, παρήγαγε περίπου 12.000 συναλλαγές την ημέρα. Ο αριθμός των απατηλών κινήσεων είναι περίπου 60 την ημέρα, ενώ ο αριθμός των πελατών που είναι θύματα απάτης κυμαίνεται στους 40 την ημέρα. Έχουμε καταφέρει να δημιουργήσουμε ένα σύνολο δεδομένων με μεγάλη ανισορροπία κλάσεων (οι απατηλές συναλλαγές σε σχέση με τις γνήσιες) και συνδυασμό αριθμητικών και κατηγορικών χαρακτηριστικών. Ο τελικός πίνακας ωστόσο διαμορφώθηκε με μόνο το βασικά χαρακτηριστικά μιας συναλλαγής, επομένως θα δημιουργήσουμε επιπρόσθετα χαρακτηριστικά που θα μας βοηθήσουν στην ανάλυση. Τα χαρακτηριστικά αυτά είναι τα εξής:

Εάν η συναλλαγή έχει πραγματοποιηθεί μέσα στο σαββατοκύριακο: Ορίζουμε μια δυαδική μεταβλητή η οποία θα παίρνει την τιμή 1 εάν η συναλλαγή πραγματοποιήθηκε μέσα στο ΣΚ αλλιώς θα παίρνει την τιμή 0

```
def is_weekend(trx_datetime):

    # Μετατροπή της ημερομηνίας σε μέρες της εβδομάδας
    #0 είναι η Δευτέρα, και 6 είναι η Κυριακή
    weekday = trx_datetime.weekday()
    # θα πάρει την τιμή 1 εάν ειναι μέσα στο ΣΚ η συναλλαγή αλλιώς 0
    is_weekend = weekday>=5

    return int(is_weekend)
```

Μέσω της συνάρτησης apply εφαρμόζουμε την συνάρτηση σε όλες τις συναλλαγές.

```
%time df2['TRX_DURING_WEEKEND']=df2.TRX_DATETIME.apply(is_weekend)
```

Εάν η συναλλαγή έχει πραγματοποιηθεί βραδινές ώρες: Όμοια με προηγουμένως, το αποτέλεσμα θα είναι μια δυαδική τιμή με τιμές 1 εάν έχει πραγματοποιηθεί την νύχτα ειδάλλως τιμή 0

```
def is_night(trx_datetime):

    # Μετατροπή σε ώρα
    trx_hour = trx_datetime.hour
    # 1 εάν πραγματοποιήθηκε την νύχτα
    is_night = trx_hour<=8

    return int(is_night)

%time df2['TRX_DURING_NIGHT']=df2.TRX_DATETIME.apply(is_night)
```

Τα χαρακτηριστικά αυτά είναι χρήσιμα καθώς έχει παρατηρηθεί σε σύνολα δεδομένων του πραγματικού κόσμου οτι τα μοτίβα απάτης διαφέρουν μεταξύ καθημερινών και σαββατοκύριακων και μεταξύ ημέρας και νύχτας

Στη συνέχεια για 4 διαφορετικές χρονικές περιόδους 1,7,15,30 ημερών θα υπολογίσουμε 2 χαρακτηριστικά που θα δομούν το συναλλακτικό προφίλ των πελατών. Θα έχουμε επομένως 8 νέα χαρακτηριστικά

Υπολογίζουμε την συχνότητα με την οποία κάνει ένας πελάτης συναλλαγές στο εκάστοτε διάστημα

Ο μέσος όρος των συναλλαγών που εκτελεί ένας πελάτης στο εκάστοτε διάστημα

```
def get_customer_spending_behaviour_features(customer_transactions,
windows_size_in_days=[1,7,15,30]):

    # Ταξινόμηση των συναλλαγών χρονικά
    customer_transactions=customer_transactions.sort_values(
'TRX_DATETIME')
    customer_transactions.index=customer_transactions.TRX_DATETIME

    # Για κάθε χρονική στιγμή
    for window_size in windows_size_in_days:

        # Υπολογισμός του σύνολου των συναλλαγών και των αντίστοιχων ποσό
για το εκάστοτε χρονικό διάστημα

SUM_AMOUNT_TRX_WINDOW=customer_transactions['TRX_AMOUNT'].rolling(str(win
dow_size)+'d').sum()

NUMBER_TRX_WINDOW=customer_transactions['TRX_AMOUNT'].rolling(str(window_
size)+'d').count()

        # Υπολογίζουμε τον μέσο όρο
        AVG_AMOUNT_TRX_WINDOW=SUM_AMOUNT_TRX_WINDOW/NUMBER_TRX_WINDOW

customer_transactions['CUSTOMER_ID_NUMBER_TRX_'+str(window_size)+'DAY_WIN
DOW']=list(NUMBER_TRX_WINDOW)
```

```
customer_transactions['CUSTOMER_ID_AVG_AMOUNT_'+str(window_size)+'DAY_WIN
DOW']=list(AVG_AMOUNT_TRX_WINDOW)

    customer_transactions.index=customer_transactions.TRANSACTION_ID

    return customer_transactions
%time df2=df2.groupby('CUSTOMER_ID').apply(lambda x:
get_customer_spending_behaviour_features(x,
windows_size_in_days=[1,7,15,30]))
df2=df2.sort_values('TRX_DATETIME').reset_index(drop=True)
```

6.2.2. Σχεδιασμός του συστήματος

Ο σχεδιασμός του συστήματος μας θα αποτελείται από τα παρακάτω βασικά βήματα:

- Καθορισμός ενός συνόλου εκπαίδευσης και ενός συνόλου δοκιμής. Το σύνολο εκπαίδευσης είναι το υποσύνολο των συναλλαγών που θα χρησιμοποιηθούν για την εκπαίδευση του μοντέλου. Το σύνολο δοκιμής θα χρησιμοποιηθεί για την αξιολόγηση της απόδοσης του μοντέλου πρόβλεψης.
- Εκπαίδευση του μοντέλου: Θα χρησιμοποιήσουμε το σύνολο εκπαίδευσης για την εύρεση ενός μοντέλου πρόβλεψης που θα είναι σε θέση να προβλέψει αν μια συναλλαγή είναι γνήσια ή απατηλή. Για το βήμα αυτό θα χρησιμοποιήσουμε την βιβλιοθήκη sklearn της Python, η οποία παρέχει εύχρηστες συναρτήσεις για την εκπαίδευση των αλγορίθμων πρόβλεψης.
- Αξιολόγηση της απόδοσης του μοντέλου πρόβλεψης: Η απόδοση του μοντέλου πρόβλεψης αξιολογείται χρησιμοποιώντας το σύνολο δοκιμής.

Επιλέξαμε τα σύνολα δοκιμής και εκπαίδευσης να αποτελούνται από 7 ημέρες το κάθε ένα.

```
def get_train_test_set(dft2,
                       start_date_training,
                       delta_train=7,delta_test=7):

    #training set
    train_df = dft2[(dft2.TRX_DATETIME>=start_date_training) &

(dft2.TRX_DATETIME<start_date_training+datetime.timedelta(days=delta_trai
n))]

    test_df =
dft2[(dft2.TRX_DATETIME>=start_date_training+datetime.timedelta(days=delt
a_train)) &
(dft2.TRX_DATETIME<start_date_training+datetime.timedelta(days=delta_trai
n)+
                                datetime.timedelta(days=delta_test))]
```

```
    # Ταξινόμηση ανά transaction ID
    train_df=train_df.sort_values('TRANSACTION_ID')
    test_df=test_df.sort_values('TRANSACTION_ID')
    test_df.reset_index(drop=True,inplace=True)
    return (train_df, test_df)
(train_df, test_df)=get_train_test_set(dft2,start_date_training,
                                       delta_train=7,delta_test=7)
```

Στο training set υπάρχουν 83810 συναλλαγές εκ των οποίων 267 απατηλές, ενώ test υπάρχουν 83718 συναλλαγές εκ των οποίων 276 απατηλές. Ακόμα, θα προχωρήσουμε σε κανονικοποίηση δεδομένων με RobustScaler λόγω της ύπαρξης ακραίων τιμών.

```
from sklearn.preprocessing import RobustScaler
ss = RobustScaler()

dftest1 = pd.DataFrame(ss.fit_transform(train_df[input_features]),columns
= train_df[input_features].columns)
dftest1.rename(str.lower, axis='columns',inplace=True)
train_df=train_df.merge(dftest1, left_index = True, right_index = True)
train_df.drop(input_features,axis=1,inplace=True)

dftest3=pd.DataFrame(ss.fit_transform(test_df[input_features]),columns =
test_df[input_features].columns)
dftest3.rename(str.lower, axis='columns',inplace=True)
test_df=test_df.merge(dftest3, left_index = True, right_index = True)
test_df.drop(input_features,axis=1,inplace=True)
```

Για την εκπαίδευση του μοντέλου, στόχος είναι να βρεθεί μια συνάρτηση που θα δέχεται ως είσοδο τα χαρακτηριστικά της συναλλαγής και ως έξοδο θα μας υποδεικνύει εάν αυτή η κίνηση είναι απατηλή ή όχι. Το χαρακτηριστικό εξόδου θα είναι η ετικέτα της συναλλαγή TRX_FRAUD, ενώ τα χαρακτηριστικά εισόδου θα είναι όλα τα αυτά που υπολογίστηκαν προηγουμένως και αποτελούν το πλαίσιο μιας συναλλαγής.

```
output_feature="TRX_FRAUD"

input_features=['trx_amount','trx_during_weekend', 'trx_during_night',
'customer_id_number_trx_1day_window',
       'customer_id_avg_amount_1day_window',
'customer_id_number_trx_7day_window',
       'customer_id_avg_amount_7day_window',
'customer_id_number_trx_15day_window',
       'customer_id_avg_amount_15day_window',
'customer_id_number_trx_30day_window',
       'customer_id_avg_amount_30day_window']
```

Θα δημιουργήσουμε την συνάρτηση fit_model_and_get_predictions η οποία θα εκπαιδεύει το μοντέλο και θα επιστρέφει την πρόβλεψη. Πιο συγκεκριμένα, η συνάρτηση αυτή δέχεται ως είσοδο τον εκάστοτε αλγόριθμο μηχανικής μάθησης, τα δεδομένα εκπαίδευσης και δοκιμής, καθώς και τα output_feature και input_features που δημιουργήσαμε προηγουμένως.

```
def fit_model_and_get_predictions(classifier, train_df, test_df,
                                  input_features,
output_feature="TRX_FRAUD"):

    #Εφαρμογή του αντίστοιχου μοντέλου
    start_time=time.time()
    classifier.fit(train_df[input_features], train_df[output_feature])
    training_execution_time=time.time()-start_time
    #Αποθηκεύουμε τις προβλέψεις του μοντέλου για να τις συγκρίνουμε με
τις πραγματικές τιμές
    start_time=time.time()

predictions_test=classifier.predict_proba(test_df[input_features])[:,1]
    prediction_execution_time=time.time()-start_time

predictions_train=classifier.predict_proba(train_df[input_features])[:,1]
    model_and_predictions_dictionary = {'classifier': classifier,
'predictions_test': predictions_test,
'predictions_train': predictions_train,
'training_execution_time': training_execution_time,
'prediction_execution_time': prediction_execution_time}

    return model_and_predictions_dictionary
```

Αξιολόγηση των μοντέλων πρόβλεψης:

Για την αξιολόγηση των μοντέλων μας θα επιλέξουμε τις 3 παρακάτω μετρικές

- Card Precision top-k: Σε ένα πραγματικό FDS σύστημα, παράγονται alert τα οποία διαχειρίζονται από την αντίστοιχη ομάδα, με τις αντίστοιχες ενέργειες(όπως για παράδειγμα επικοινωνία με τον πελάτη για να επιβεβαιωθεί μια κίνηση).Επομένως ο έλεγχος όλων των συναλλαγών είναι κάτι που σε μια μεγάλη τράπεζα είναι ακατόρθωτο. Αυτή η μετρική μας δίνει τις k-συναλλαγές που μπορεί να ελέγξει το σύστημα, και επιλέγει να εμφανίσει τις συναλλαγές αυτές που έχουν μεγαλύτερη πρόβλεψη ώστε να είναι απατηλές. Στο συγκεκριμένο παράδειγμα, επειδή έχουμε μέσο όρο συναλλαγών <250 την ημέρα και μόλις 5000 πελάτες, θα θεωρήσουμε μια αντίστοιχη αναλογία για το πόσες συναλλαγές μπορούν να ελεγχθούν. Θα θεωρήσουμε δηλαδή οτι στο εν λόγω FDS σύστημα μπορούν να ελεγχθούν έως 40 συναλλαγές την ημέρα, βέβαια όσο αυξάνεται το dataset και ο αριθμός των πελατών και των συναλλαγών που εκτελούνται καθημερινά αυξάνεται και ο αριθμός του k. Αυτή η μετρική χρησιμοποιείται και σε πραγματικά FDS συστήματα.
- Average Precision: Είναι η ακρίβεια για τις πιθανές τιμές του k που αναφέραμε παραπάνω

- AUC ROC: Είναι μια εναλλακτική μετρική του Average Precision, η οποία δίνει έμφαση στις συναλλαγές που προκύπτουν για μεγαλύτερες τιμές του αριθμού k. Αφορά ουσιαστικά τις συναλλαγές που έχουν δώσει τα συστήματα λιγότερη πιθανότητα να είναι απάτη. Είναι λιγότερο πρακτικό καθώς οι συναλλαγές για μικρότερο αριθμό k είναι αυτές που το σύστημα κρίνει πιο πιθανές για απάτη, ωστόσο αποτελεί το πιο ευρέως χρησιμοποιούμενο μέτρο απόδοσης για την ανίχνευση απάτης.

Και οι 3 αυτές μετρικές, λαμβάνουν τιμές από 0 έως 1, και όσο μεγαλύτερη η τιμή τόσο καλύτερη απόδοση έχει το μοντέλο

```
def card_precision_top_k_day(df_day,top_k):

    #Επιλέγουμε τις συναλλαγές για κάθε πελάτη που έχουν μέγιστη πρόβλεψη
και που είναι απατηλές
    df_day =
df_day.groupby('CUSTOMER_ID').max().sort_values(by="predictions",
ascending=False).reset_index(drop=False)
    # Και επιλέγουμε τις k συναλλαγές αυτές
    df_day_top_k=df_day.head(top_k)

list_detected_compromised_cards=list(df_day_top_k[df_day_top_k.TRX_FRAUD=
=1].CUSTOMER_ID)
    # Υπολογισμός της ακρίβειας
    card_precision_top_k = len(list_detected_compromised_cards) / top_k

    return list_detected_compromised_cards, card_precision_top_k
def card_precision_top_k(predictions_df, top_k,
remove_detected_compromised_cards=True):
    # Ταξινόμηση των ημερών με αύξουσα σειρά
    list_days=list(predictions_df['TRX_TIME_DAYS'].unique())
    list_days.sort()
    list_detected_compromised_cards = []
    card_precision_top_k_per_day_list = []
    nb_compromised_cards_per_day = []
    # Για κάθε μέρα υπολογίζουμε την ακρίβεια του top-k
    for day in list_days:

        df_day = predictions_df[predictions_df['TRX_TIME_DAYS']==day]
        df_day = df_day[['predictions', 'CUSTOMER_ID', 'TRX_FRAUD']]

        df_day =
df_day[df_day.CUSTOMER_ID.isin(list_detected_compromised_cards)==False]
nb_compromised_cards_per_day.append(len(df_day[df_day.TRX_FRAUD==1].CUSTO
MER_ID.unique()))
        detected_compromised_cards, card_precision_top_k =
card_precision_top_k_day(df_day,top_k)
        card_precision_top_k_per_day_list.append(card_precision_top_k)
        if remove_detected_compromised_cards:
```

```
list_detected_compromised_cards.extend(detected_compromised_cards)
    mean_card_precision_top_k =
np.array(card_precision_top_k_per_day_list).mean()

    return
nb_compromised_cards_per_day,card_precision_top_k_per_day_list,mean_card_
precision_top_k
def performance_assessment(predictions_df, output_feature='TRX_FRAUD',
                           prediction_feature='predictions',
                           top_k_list=[40], rounded=True):
    AUC_ROC = metrics.roc_auc_score(predictions_df[output_feature],
predictions_df[prediction_feature])
    AP = metrics.average_precision_score(predictions_df[output_feature],
predictions_df[prediction_feature])

    performances = pd.DataFrame([[AUC_ROC, AP]],
                           columns=['AUC ROC','Average precision'])

    for top_k in top_k_list:
        mean_card_precision_top_k = card_precision_top_k(
predictions_df, top_k)
        performances['Card Precision@'+str(top_k)]=
mean_card_precision_top_k

    if rounded:
        performances = performances.round(3)

    return performances
```

Τώρα, έχουμε όλα τα δομικά στοιχεία για να εκπαιδεύσουμε και να αξιολογήσουμε τους ταξινομητές μας. Θα επιλέξουμε να εκπαιδεύσουμε τους παρακάτω αλγορίθμους:

- Logistic regression
- Decision tree with depth of two
- Decision tree - unlimited depth
- Random forest
- XGBoost

Αυτά τα μοντέλα είναι τα πιο συνηθισμένα που χρησιμοποιούνται σε περιστατικά ανίχνευσης απάτης.

```
classifiers_dictionary={'Logistic
regression':sklearn.linear_model.LogisticRegression(random_state=0),
                        'Decision tree with depth of
two':sklearn.tree.DecisionTreeClassifier(max_depth=2,random_state=0),
                        'Decision tree - unlimited
```

```
depth':sklearn.tree.DecisionTreeClassifier(random_state=0),
                        'Random
forest':sklearn.ensemble.RandomForestClassifier(random_state=0,n_jobs=-
1),

'XGBoost':xgboost.XGBClassifier(random_state=0,n_jobs=-1)}

fitted_models_and_predictions_dictionary={}

for classifier_name in classifiers_dictionary:

    model_and_predictions =
fit_model_and_get_predictions(classifiers_dictionary[classifier_name],
train_df, test_df,
input_features=input_features, output_feature=output_feature)

fitted_models_and_predictions_dictionary[classifier_name]=model_and_predi
ctions
```

Τέλος, ας αξιολογήσουμε τις επιδόσεις προβλέψεις αυτών των πέντε μοντέλων στο σύνολο δοκιμών και στο σύνολο εκπαίδευσης.

```
def
performance_assessment_model_collection(fitted_models_and_predictions_dic
tionary,dft2,type_set='test',top_k_list=[40]):
    performances=pd.DataFrame()
    for classifier_name, model_and_predictions in
fitted_models_and_predictions_dictionary.items():
        predictions_df=dft2
        predictions_df['predictions']=model_and_predictions[
'predictions_'+type_set]
        performances_model=performance_assessment(predictions_df,
output_feature='TRX_FRAUD',prediction_feature='predictions',
top_k_list=top_k_list)
        performances_model.index=[classifier_name]
        performances=performances.append(performances_model)

    return performances
# performances on test set
df_performances=performance_assessment_model_collection(fitted_models_and
_predictions_dictionary, test_df, type_set='test', top_k_list=[40])
df_performances
```

	AUC ROC	Average precision	Card Precision@40
Logistic regression	0.664	0.191	0.089
Decision tree with depth of two	0.576	0.154	0.071
Decision tree - unlimited depth	0.571	0.006	0.032
Random forest	0.619	0.181	0.096
XGBoost	0.636	0.167	0.107

Σχήμα 14: Απόδοση αλγορίθμων στο σύνολο δοκιμής

```
# performances on training set
df_performances=performance_assessment_model_collection(fitted_models_and
_predictions_dictionary, train_df, type_set='train', top_k_list=[40])
df_performances
```

	AUC ROC	Average precision	Card Precision@40
Logistic regression	0.644	0.114	0.057
Decision tree with depth of two	0.559	0.110	0.046
Decision tree - unlimited depth	1.000	1.000	0.779
Random forest	1.000	1.000	0.779
XGBoost	0.994	0.740	0.525

Σχήμα 15: Απόδοση αλγορίθμων στο σύνολο εκπαίδευσης

Συμπεράσματα:

Όλα τα μοντέλα πρόβλεψης έχουν καταφέρει να εντοπίσουν πολύ χρήσιμες πληροφορίες σχετικά με τα μοτίβα απάτης. Αυτό μπορούμε να το συμπεράνουμε από την τιμή της AUC ROC η οποία για όλους τους ταξινομητές είναι μεγαλύτερη από 0,5 αλλά και από την τιμή του average precision η οποία ξεπερνάει το 0,003 που είναι το αρχικό ποσοστό fraud συναλλαγών που είχαμε στο dataset. Οι ταξινομητές Random Forest και XGBoost έχουν δώσει καλύτερη απόδοση κάτι που το διαπιστώσαμε και στο μέρος 1ο της προγραμματιστικής εργασίας. Αξίζει επίσης να σημειώσουμε οτι οι επιδόσεις ορισμένων ταξινομητών όπως τα Random Forest και Decision Tree με απεριόριστο βάθος, είναι τέλειες στο σύνολο εκπαίδευσης (AUC ROC και μέση ακρίβεια 1), αλλά χαμηλότερες στο σύνολο δοκιμής, γεγονός που σημαίνει οτι έχει γίνει overfitting στο μοντελό.

Με αυτό το προγραμματιστικό μέρος, δείξαμε οτι ο σχεδιασμός ενός βασικού και απλού συστήματος ανίχνευσης απάτης μπορεί να επιτευχθεί με την χρήση απλών στρατηγικών προεπεξεργασίας και εφαρμογής ταξινομητών μηχανικής μάθησης. Συγκεκριμένα, καταφέραμε να επιτύχουμε επιδόσεις ανίχνευσης απάτης που είναι πολύ υψηλότερες από εκείνες ενός τυχαίου ταξινομητή. Ωστόσο, ένας μεγάλος αριθμός πιο προηγμένων τεχνικών μπορεί να χρησιμοποιηθεί για την βελτίωση των επιδόσεων αυτών, οι οποίες μπορούν να βελτιστοποιηθούν και από άποψη ακρίβειας αλλά και από άποψη υπολογιστικών απαιτήσεων όπως η μνήμη που καταναλώνεται αλλά και οι αντίστοιχοι χρόνοι εκτέλεσης. Το τελευταίο είναι στη πράξη το πιο σημαντικό κατά τη διάρκεια της εκπαίδευσης, καθώς τα συστήματα ανίχνευσης απάτης πρέπει να

διαχειρίζονται μεγάλες ποσότητες δεδομένων, πολύ μεγαλύτερες από αυτές που χρησιμοποιήθηκαν σε αυτό το βασικό παράδειγμα.

7. Βιβλιογραφία

[1] Tj maxx company data breach Security Breach: The Case of TJX Companies, Inc,William Xu

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3391&context=cais

[2] Flagstar Bank data breach ,Office of the Maine Attorney General

https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml

[3] Biggest Security Threat: Facebook & You , KATHY KRISTOF , 2011

https://www.cbsnews.com/news/biggest-security-threat-facebook-you/

[4] KEY ISSUES IN E-BANKING STRENGTHS AND WEAKNESSES: THE CASE OF TWO JORDANIAN BANKS, Rifat O. Shannak

[5]Grebennikov J(2007). Keyloggers: how they work and how to detect them (part 1)

https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

[6] https://www.ionos.co.uk/digitalguide/e-mail/e-mail-security/what-is-pharming/

[7] https://www.cnn.gr/ellada/story/309123/thessaloniki-diadiktyaki-apati-me-polisi-proionton-187-ta-thymata-53-000-eyro-i-leia-toy-drasti

[8] Three Types of Merchant Fraud: A Guide For Merchant Acquirers, 2017

https://www.finextra.com/blogposting/14769/three-types-of-merchant-fraud-a-guide-for-merchant-acquirers

[9]Tim Maurer, Arthur Nelson, „The global cyber threat, Finance and Development, IMF," 03 2021. https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

[10]Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup, 2021 Data Breach Investigations Report, Verizon, 2021

[11] Office of Public Affairs, „The United States Department of Justice," 08 02 2022

https://www.justice.gov/opa/pr/twoarrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[12] M. Albashrawi, M. Lowell, Detecting financial fraud using data mining

techniques: A decade review from 2004 to 2015, J. Data Sci. 14 (2016)

[13]αρθρο 22

Υπουργείο ανάπτυξης

http://www.opengov.gr/ypoian/?p=13680

[14] TRF

https://medium.com/@netsentries/transaction-reversal-fraud-trf-dont-be-the-next-target-a948f5a3205

[15]sim swap

Awareness of Sim Swap Attack

Snehal Manohar Awale1, Dr. Praveen Gupta2

YMT College of Management, Navi Mumbai, Maharashtra, India

[16] Business Compromised Email, infographic

https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

[17]SVM

S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland, Data mining for

credit card fraud: A comparative study, Decis. Support Syst. 50 (2011)

602–613.

[18]FL
T.K. Behera, S. Panigrahi, Credit card fraud detection: a hybrid approach
using fuzzy clustering & neural network, in: Advances in Computing
and Communication Engineering (ICACCE), 2015 Second International
Conference on, IEEE, 2015, pp. 494–499.
[19]HMM
Z. Zojaji, R.E. Atani, A.H. Monadjemi, A survey of credit card fraud
detection techniques: data and technique oriented perspective, 2016,
arXiv preprint arXiv:1611.06439
[20] ANN
Y. Sahin, E. Duman, Detecting credit card fraud by ANN and logistic regression, in: Innovations in Intelligent Systems and Applications (INISTA),
2011 International Symposium on, IEEE, 2011, pp. 315–319
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7951441
[21] Fraud Detection by Monitoring Customer Behavior and Activities
Parvinder Singh,Mandeep Singh 2015
https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6d6b11d889cbd132267532a9330b917f8a096524
[22] Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019
Khaled Gubran Al-Hashedi, Pritheega Magalingam
[23] KNN AND CHAD
Y. Heryadi, L.A. Wulandhari, B.S. Abbas, Recognizing debit card fraud
transaction using CHAID and K-nearest neighbor: Indonesian Bank case,
in: Knowledge, Information and Creativity Support Systems (KICSS), 2016
11th International Conference on, IEEE, 2016, pp. 1–5.
[24] TECHNIQUES EVALUATION
Adnan M. Al-Khatib, “Electronic Payment Fraud Detection Techniques”, World of Computer
Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 4, 137-141,
2012.
[25] O’rinov Nodirbek Toxirjonovich, Yuldashev Madaminjon Muxammadqul o‘g‘li, 2023
ARTIFICIAL INTELLIGENCE HOW COUNTERACTION FRAUD AT BANKING SPHERE
[26]ΕΚΘΕΣΗ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΗΣ ΣΤΑΘΕΡΟΤΗΤΑΣ, ΤτΕ 2023
https://www.bankofgreece.gr/Publications/FINANCIAL_STABILITY_REVIEW_MAY_2023_EL.pdf
[27]https://www.newmoney.gr/roh/palmos-oikonomias/trapezes/trapezes-antidroun-gia-ti-diataxi-pou-provlepi-apozimiosi-sta-thimata-ilektronikis-apatis/