Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Μεταπτυχιακο Προγραμμα Σπουδων Επιστημη Δεδομενων Και Μηχανικη Μαθηση

Εντοπισμός Ανωμαλιών σε Οικονομικά Δίκτυα με Μεθόδους Μηχανικής Μάθησης

Διπλωματικη Εργασια

του

ΧΡΙΣΤΟΓΕΩΡΓΟΥ ΚΩΝΣΤΑΝΤΙΝΟΥ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής

Αθήνα, Ιούνιος 2025

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Μεταπτυχιακο Προγραμμα Σπουδων Επιστημη Δεδομενων Και Μηχανικη Μαθηση

Εντοπισμός Ανωμαλιών σε Οικονομικά Δίκτυα με Μεθόδους Μηχανικής Μάθησης

Διπλωματικη Εργασια

του

ΧΡΙΣΤΟΓΕΩΡΓΟΥ ΚΩΝΣΤΑΝΤΙΝΟΥ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 23η Ιουνίου 2025.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Συμεών Παπαβασιλείου	Γεώργιος Ματσόπουλος	Ελένη Στάη
Καθηγητής	Καθηγητής	Επίκουρη Καθηγήτρια

Αθήνα, Ιούνιος 2025

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Μεταπτυχιακο Προγραμμα Σπουδων Επιστημη Δεδομενων Και Μηχανικη Μαθηση

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

.....
Χριστογεώργος
Κωνσταντίνος

23η Ιουνίου 2025

Περίληψη

Στη σύγχρονη εποχή των ψηφιακών συναλλαγών, η ανίχνευση απάτης σε τραπεζικές συναλλαγές αποτελεί κρίσιμο ζήτημα για τη διατήρηση της εμπιστοσύνης στο χρηματοπιστωτικό σύστημα. Η διπλωματική εργασία επικεντρώνεται στην ανάπτυξη και αξιολόγηση μεθόδων εντοπισμού απάτης σε σύνολα δεδομένων με έντονη ανισορροπία κλάσεων, όπου οι περιπτώσεις απάτης αποτελούν ένα ελάχιστο ποσοστό του συνόλου. Η μελέτη βασίζεται σε πραγματικά δεδομένα συναλλαγών με πιστωτικές κάρτες στην Ευρωπαϊκή Ένωση και αξιοποιεί στατιστικές μεθόδους για την ανάλυση της κατανομής των χαρακτηριστικών μεταξύ κανονικών και ύποπτων συναλλαγών.

Στο πλαίσιο της πειραματικής διαδικασίας, εφαρμόζονται τεχνικές επαναδειγματοληψίας (undersampling και oversampling) σε διαφορετικές αναλογίες, καθώς και τρεις αλγόριθμοι ταξινόμησης: το πολυεπίπεδο νευρωνικό δίκτυο (Multi-Layer Perceptron), ο ταξινομητής Random Forest και ο ταξινομητής Balanced Random Forest. Συνολικά υλοποιούνται 16 πειράματα, προκύπτοντας από διαφορετικούς συνδυασμούς μεθόδων επαναδειγματοληψίας και ταξινομητών. Η αξιολόγηση της απόδοσης των μοντέλων βασίζεται σε μετρικές κατάλληλες για προβλήματα ανισορροπίας, με έμφαση στο recall. Τα αποτελέσματα αναδεικνύουν τη σημασία της σωστής διαχείρισης της ανισορροπίας του χαρακτηριστικού πρόβλεψης και επιτρέπουν την αξιολόγηση της αποτελεσματικότητας των προτεινόμενων πειραμάτων, συμβάλλοντας στην ανάπτυξη πιο αποδοτικών τεχνικών για την ανίχνευση τραπεζικής απάτης.

Λέξεις Κλειδιά

Ανίχνευση Απάτης, Ανισορροπία Δεδομένων, Συναλλαγές Πιστωτικών Καρτών, Τεχνικές Επαναδειγματοληψίας, Μηχανική Μάθηση

Abstract

In the modern era of digital transactions, fraud detection in banking operations is a critical issue for maintaining trust in the financial system. This thesis focuses on the development and evaluation of fraud detection methods in datasets with a strong class imbalance, where fraudulent cases represent a minimal proportion of the total. The study is based on real-world credit card transaction data from the European Union and employs statistical methods to analyze the distribution of features between legitimate and suspicious transactions.

Within the experimental process, resampling techniques (undersampling and oversampling) are applied in different proportions, as well as three classification algorithms: the multi-layer neural network (MLP), the Random Forest classifier and the Balanced Random Forest classifier. A total of 16 experiments are implemented, resulting from different combinations of resampling methods and classifiers. Model performance is assessed using metrics suitable for imbalanced data problems, such as recall. The results emphasize the importance of properly addressing class imbalance and enable the assessment of the effectiveness of the proposed experiments, contributing to the development of more efficient fraud detection techniques in the banking sector.

Keywords

Fraud Detection, Data Imbalance, Credit Card Transactions, Resampling Techniques, Machine Learning

σε αυτούς που αγαπάνε την επιστήμη

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα καθηγητή μου, κ. Συμεών Παπαβασιλείου, για την πολύτιμη καθοδήγηση, την αμέριστη υποστήριξη και το επιστημονικό ενδιαφέρον που έδειξε καθ' όλη τη διάρκεια της διπλωματικής μου εργασίας. Επίσης, θα ήθελα να ευχαριστήσω θερμά τον συνεπιβλέποντα, κ. Βασίλειο Καρυώτη, για τη συνεργασία, την συνεχή υποστήριξη και τη διαρκή διαθεσιμότητά του σε κάθε στάδιο της εργασίας.

Ανάμεσα στους ανθρώπους που οφείλω να ευχαριστήσω, ξεχωριστή θέση έχουν η οικογένεια μου και οι φίλοι μου, που χωρίς την διαρκή στήριξη, υπομονή και αγάπη που μου έδειξαν, η ολοκλήρωση αυτής της προσπάθειας δεν θα ήταν δυνατή.

Αθήνα, Ιούνιος 2025

Χριστογεώργος Κωνσταντίνος

Περιεχόμενα

Περίληψη 1

Abstract 3

Ευχαριστίες 7

1 Εισαγωγή 17
1.1 Περιεχόμενο της Διπλωματικής - Ορισμός Προβλήματος . . . 18
1.2 Οργάνωση της Διπλωματικής Εργασίας . . . 19

2 Θεωρητικό Υπόβαθρο 21
2.1 Fraud και Anomaly Detection . . . 22
2.2 Imbalanced Learning . . . 22
2.2.1 Imbalanced Datasets . . . 23
2.2.2 Imbalanced Classification . . . 23
2.3 Μηχανική Μάθηση . . . 24
2.3.1 MLPs, Gradient descent και Βελτιστοποιητής Adam . . . 24
2.3.2 Random Forest Classifier . . . 26
2.4 Στατιστικές Μέθοδοι . . . 27
2.4.1 Kolmogorov–Smirnov test . . . 28
2.4.2 Kullback–Leibler divergence . . . 29
2.4.3 Jensen–Shannon divergence . . . 30
2.4.4 Kernel Density Estimation . . . 31
2.4.5 Standard Scaling . . . 32
2.5 Μετρικές Αξιολόγησης . . . 33
2.5.1 Accuracy . . . 33
2.5.2 Recall . . . 33
2.5.3 Precision . . . 33
2.5.4 F1-score . . . 33
2.6 Βιβλιογραφική Ανασκόπηση Περιοχής . . . 34
2.6.1 Ορισμός και Κατηγορίες Απάτης σε Τραπεζικές Συναλλαγές . . . 34
2.6.2 Παραδοσιακές Μέθοδοι Εντοπισμού Απάτης . . . 34
2.6.3 Μέθοδοι Εντοπισμού Απάτης με Μηχανική Μάθηση . . . 35
2.6.4 Χρήση Βαθιάς Μάθησης στον Εντοπισμό Απάτης . . . 35
2.6.5 Κύριες Προκλήσεις . . . 36
2.6.6 Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά . . . 36

3 Dataset - Ανάλυση - Προεπεξεργασία και Χρήσιμα Συμπεράσματα **39**
3.1 Χαρακτηριστικά του Dataset . . . 39
3.1.1 Χαρακτηριστικά V1-V28 . . . 40
3.1.2 Χαρακτηριστικά Time και Amount . . . 46
3.1.3 Χαρακτηριστικό Class . . . 48
3.2 Προεπεξεργασία Δεδομένων . . . 49

4 Ανάλυση και Σχεδίαση Πειραματικών Μεθόδων **51**
4.1 Τεχνικές Επαναδειγματοληψίας . . . 51
4.1.1 Random Undersampling . . . 51
4.1.2 Random Oversampling . . . 51
4.2 Επιλεγμένοι Αλγόριθμοι Μηχανικής Μάθησης . . . 52
4.2.1 Πολυεπίπεδο Νευρωνικό Δίκτυο (MLP) . . . 52
4.2.2 Random Forest Classifer . . . 52
4.2.3 Balanced Random Forest Classifier . . . 52
4.2.4 Isolation Forest . . . 52
4.3 Μετρικές Αξιολόγησης . . . 53
4.3.1 Παραλλαγές Μετρικών . . . 54
4.4 Ροή Πειραματικής Διαδικασίας . . . 54

5 Πειραματική Διαδικασία **55**
5.1 Εκπαίδευση και Αξιολόγηση Μοντέλων . . . 55
5.2 Παράμετροι Αλγορίθμων . . . 56
5.3 Προγραμματιστική Υλοποίηση . . . 57
5.4 Παρουσίαση Αποτελεσμάτων . . . 58
5.4.1 Αποτελέσματα Πειραμάτων . . . 58
5.4.2 Ανάλυση και Σχολιασμός ανά Κατηγορία Μεθόδου . . . 59
5.4.3 Σύγκριση και Σχολιασμός Μεταξύ Ταξινομητών . . . 61
5.5 Συμπεράσματα Πειραμάτων . . . 61

6 Συμπεράσματα και Μελλοντικές Επεκτάσεις **63**
6.1 Συμπεράσματα . . . 63
6.2 Μελλοντικές Επεκτάσεις . . . 63

Παραρτήματα **65**

Α΄ Confusion Matrix ανα Πείραμα **67**
Α΄.1 Πείραμα 1 . . . 67
Α΄.2 Πείραμα 2 . . . 68
Α΄.3 Πείραμα 3 . . . 69
Α΄.4 Πείραμα 4 . . . 70
Α΄.5 Πείραμα 5 . . . 71
Α΄.6 Πείραμα 6 . . . 72
Α΄.7 Πείραμα 7 . . . 73

Α΄.8 Πείραμα 8 74
Α΄.9 Πείραμα 9 75
Α΄.10 Πείραμα 10 76
Α΄.11 Πείραμα 11 77
Α΄.12 Πείραμα 12 78
Α΄.13 Πείραμα 13 79
Α΄.14 Πείραμα 14 80
Α΄.15 Πείραμα 15 81
Α΄.16 Πείραμα 16 82

Βιβλιογραφία **90**

Συντομογραφίες - Αρκτικόλεξα - Ακρωνύμια **91**

Απόδοση ξενόγλωσσων όρων **93**

Κατάλογος Σχημάτων

3.1 Κατανομές V1-V8 . . . 41
3.2 Κατανομές V9-V16 . . . 42
3.3 Κατανομές V17-V24 . . . 43
3.4 Κατανομές V25-V28 . . . 44
3.5 Αποτελέσματα Kolmogorov–Smirnov test για τις V1-V28 . . . 45
3.6 Αποτελέσματα Jensen–Shannon divergence για τις V1-V28 . . . 45
3.7 Αποτελέσματα Kullback–Leibler divergence για τις V1-V28 . . . 46
3.8 Ιστόγραμμα για το χαρακτηριστικό Amount για τις απάτες . . . 47
3.9 Ιστόγραμμα για το χαρακτηριστικό Amount για τις μη-απάτες . . . 47
3.10 Ραβδόγραμμα τιμών για το χαρακτηριστικό Class . . . 48

Α΄.1 Confusion Matrix για το πείραμα 1 . . . 67
Α΄.2 Confusion Matrix για το πείραμα 2 . . . 68
Α΄.3 Confusion Matrix για το πείραμα 3 . . . 69
Α΄.4 Confusion Matrix για το πείραμα 4 . . . 70
Α΄.5 Confusion Matrix για το πείραμα 5 . . . 71
Α΄.6 Confusion Matrix για το πείραμα 6 . . . 72
Α΄.7 Confusion Matrix για το πείραμα 7 . . . 73
Α΄.8 Confusion Matrix για το πείραμα 8 . . . 74
Α΄.9 Confusion Matrix για το πείραμα 9 . . . 75
Α΄.10 Confusion Matrix για το πείραμα 10 . . . 76
Α΄.11 Confusion Matrix για το πείραμα 11 . . . 77
Α΄.12 Confusion Matrix για το πείραμα 12 . . . 78
Α΄.13 Confusion Matrix για το πείραμα 13 . . . 79
Α΄.14 Confusion Matrix για το πείραμα 14 . . . 80
Α΄.15 Confusion Matrix για το πείραμα 15 . . . 81
Α΄.16 Confusion Matrix για το πείραμα 16 . . . 82

Κατάλογος Πινάκων

4.1 Πίνακας σύγχυσης για την ταξινόμηση κανονικών συναλλαγών και απατών . 53
4.2 Συνδυασμοί μεθόδου επαναδειγματοληψίας και ταξινομητή ανά πείραμα . . 54

5.1 Παράμετροι εκπαίδευσης των αλγορίθμων 56
5.2 Αποτελέσματα για κάθε συνδυασμό μεθόδου επαναδειγματοληψίας και ταξινομητή (macro average) 58
5.3 Τιμές Recall για τη μειοψηφική κατηγορία (fraud), ανά συνδυασμό μεθόδου επαναδειγματοληψίας και ταξινομητή. 59

Κεφάλαιο 1

Εισαγωγή

Στη σύγχρονη εποχή, η τεχνολογία και η ψηφιακή οικονομία έχουν καταστήσει τις ηλεκτρονικές συναλλαγές αναπόσπαστο κομμάτι της καθημερινότητας. Καθημερινά, εκατομμύρια τραπεζικές συναλλαγές πραγματοποιούνται παγκοσμίως, καλύπτοντας ένα ευρύ φάσμα οικονομικών δραστηριοτήτων, από μικρές αγορές μέχρι μεγάλες επιχειρηματικές μεταφορές κεφαλαίων [1]. Η ταχύτητα, η ευκολία και η προσβασιμότητα που προσφέρουν οι σύγχρονες ηλεκτρονικές τραπεζικές υπηρεσίες έχουν αλλάξει ριζικά τον τρόπο με τον οποίο οι καταναλωτές και οι επιχειρήσεις διαχειρίζονται τα οικονομικά τους [2].

Ωστόσο, αυτή η εκρηκτική αύξηση των συναλλαγών συνοδεύεται από σημαντικές προκλήσεις, με κυριότερη την ασφάλεια και την αξιοπιστία των συστημάτων [3] [4]. Η ανίχνευση και πρόληψη της απάτης σε τραπεζικές συναλλαγές αποτελεί μια κρίσιμη παράμετρο για τη διατήρηση της εμπιστοσύνης των χρηστών στα χρηματοπιστωτικά ιδρύματα και την προστασία των εισοδημάτων τους. Οι απατεώνες εξελίσσουν διαρκώς τις μεθόδους τους [5], εκμεταλλευόμενοι τρωτά σημεία στα συστήματα πληρωμών, γεγονός που καθιστά αναγκαία τη συνεχή ανάπτυξη και βελτίωση αυτοματοποιημένων συστημάτων ανίχνευσης απάτης [6].

Η ανίχνευση απάτης είναι ένα πρόβλημα που χαρακτηρίζεται από έντονη ανισορροπία στα δεδομένα [7], όπου τα περιστατικά απάτης είναι πολύ πιο σπάνια σε σχέση με τις νόμιμες συναλλαγές [8]. Αυτή η ιδιαιτερότητα δημιουργεί προκλήσεις στην ανάπτυξη αξιόπιστων μοντέλων μηχανικής μάθησης, καθώς τα κλασικά κριτήρια εκπαίδευσης τείνουν να αγνοούν ή να υποεκτιμούν τις μειοψηφικές κλάσεις [9]. Για το λόγο αυτό, η χρήση εξειδικευμένων τεχνικών προεπεξεργασίας, επαναδειγματοληψίας και εξελιγμένων αλγορίθμων αποτελεί βασικό εργαλείο για τη βελτιστοποίηση των αποτελεσμάτων [10], [11].

Στην διπλωματική εργασία, αξιοποιούνται ποικίλες μέθοδοι για τη διερεύνηση της καταλληλότητας διαφόρων τεχνικών στη διαχείριση της ανισορροπίας και στην ανίχνευση απάτης. Πιο συγκεκριμένα, χρησιμοποιούνται σύγχρονα μέτρα σύγκρισης κατανομών, όπως το στατιστικό Kolmogorov–Smirnov και οι αποστάσεις Jensen–Shannon και Kullback–Leibler, προκειμένου να πραγματοποιηθεί οπτική και ποσοτική αξιολόγηση των διαφορών μεταξύ των κανονικών συναλλαγών και των απατών. Επιπλέον, εφαρμόζεται η Kernel Density Estimation (KDE) ξεχωριστά σε κάθε κλάση, προκειμένου να αποτυπωθούν οι κατανομές και να βρεθούν χρήσιμα χαρακτηριστικά με ικανότητα διάκρισης μεταξύ των κλάσεων.

Παράλληλα, γίνεται εκτενής πειραματική αξιολόγηση μέσω επαναδειγματοληψίας, με τεχνικές υποδειγματοληψίας (undersampling) και υπερδειγματοληψία (oversampling) σε διαφορετικές αναλογίες, ώστε να βελτιωθεί η ισορροπία του συνόλου εκπαίδευσης. Τα απο-

τελέσματα αξιολογούνται με τη χρήση τριών διαφορετικών αλγορίθμων ταξινόμησης:

- Πολυεπίπεδα νευρωνικά δίκτυα (MLP)
- Random Forest
- Balanced Random Forest

Η μελέτη συνολικά περιλαμβάνει 16 διαφορετικές πειραματικές συνθήκες που προκύπτουν από τους συνδυασμούς των μεθόδων επαναδειγματοληψίας και των αλγορίθμων ταξινόμησης, αξιολογώντας με βάση κατάλληλες μετρικές απόδοσης, ειδικά προσαρμοσμένες για προβλήματα με ανισορροπία κλάσεων.

Η εργασία συμβάλλει στην καλύτερη κατανόηση των τεχνικών που μπορούν να βελτιώσουν την ανίχνευση απάτης σε τραπεζικές συναλλαγές, αναδεικνύοντας τα πλεονεκτήματα και τους περιορισμούς κάθε προσέγγισης. Παράλληλα, προσφέρει μια ολοκληρωμένη διαδικασία που μπορεί να αξιοποιηθεί ως βάση για περαιτέρω έρευνα και πρακτικές εφαρμογές στον τομέα της χρηματοοικονομικής ασφάλειας και της ανίχνευσης απάτης.

1.1 Περιεχόμενο της Διπλωματικής - Ορισμός Προβλήματος

Η διπλωματική εργασία εστιάζει στην ανίχνευση ανωμαλιών και απάτης σε τραπεζικές συναλλαγές με τη χρήση δεδομένων πραγματικών συναλλαγών απο ένα σύνολο δεδομένων που εμπεριέχει συναλλαγές με πιστωτικές κάρτες που πραγματοποιήθηκαν από Ευρωπαίους κατόχους καρτών τον Σεπτέμβριο του 2013, μέσα σε διάστημα δύο ημερών. Περιέχει συνολικά 284.807 συναλλαγές, εκ των οποίων οι **492** είναι απάτες. Η βασική πρόκληση αφορά την αντιμετώπιση της έντονης ανισορροπίας μεταξύ των κλάσεων των κανονικών συναλλαγών και αυτών που είναι περιπτώσεις απάτης. Για το σκοπό αυτό, πραγματοποιείται αρχική προεπεξεργασία των δεδομένων, όπου εφαρμόζονται στατιστικές μέθοδοι σύγκρισης κατανομών, ώστε να διερευνηθούν και να επιβεβαιωθούν οι διαφορές στις κατανομές των χαρακτηριστικών ανά κλάση.

Στη συνέχεια, εφαρμόζονται μέθοδοι επαναδειγματοληψίας, undersampling και oversampling, σε διάφορες αναλογίες, με στόχο την καλύτερη ισορροπία των κλάσεων στο σύνολο εκπαίδευσης και έναν αρχικό διαχωρισμό των διαφόρων πειραμάτων.

Τέλος, η απόδοση αξιολογείται μέσω 16 πειραμάτων που προκύπτουν από τον συνδυασμό τριών αλγορίθμων ταξινόμησης, MLP, Random Forest και Balanced Random Forest, με τις διαφορετικές αναλογίες δειγματοληψίας. Η αξιολόγηση βασίζεται σε μετρικές που ανταποκρίνονται στην ανάγκη ανίχνευσης της μειοψηφικής κλάσης, όπως το recall, προσφέροντας μια ολοκληρωμένη εικόνα της αποδοτικότητας των διαφόρων προσεγγίσεων στην ικανότητα ανίχνευσης απατών.

Το πρόβλημα που αντιμετωπίζεται στη διπλωματική εργασία αφορά την αποτελεσματική ανίχνευση απάτης σε τραπεζικές συναλλαγές, όπου οι περιπτώσεις απάτης αποτελούν πολύ μικρό ποσοστό του συνολικού όγκου δεδομένων. Ο κύριος στόχος είναι η ανάπτυξη και αξιολόγηση μεθόδων που θα βελτιώσουν την ικανότητα εντοπισμού της μειοψηφικής κλάσης, μέσα από κατάλληλη προεπεξεργασία, διαχείριση της ανισορροπίας των δεδομένων και εφαρμογή αποδοτικών αλγορίθμων ταξινόμησης.

1.2 Οργάνωση της Διπλωματικής Εργασίας

Η εργασία αυτή είναι οργανωμένη σε έξι κεφάλαια: Στο Κεφάλαιο 2 δίνεται το θεωρητικό υπόβαθρο των βασικών μαθηματικών εννοιών και αλγορίθμων που σχετίζονται με το αντικείμενο της διπλωματικής. Στο Κεφάλαιο 3 αρχικά περιγράφονται οι λεπτομέρειες του συνόλου δεδομένων και μια εκτενής ανάλυση των χαρακτηριστικών που περιέχει, με γνώμονα την διατήρηση αυτών που έχουν σημαντική διαχωριστική ικανότητα μεταξύ των δυο κλάσεων. Στο Κεφάλαιο 4 παρουσιάζεται η ανάλυση και η σχεδίαση των πειραματικών μεθόδων που χρησιμοποιούνται, δηλαδή η περιγραφή των λεπτομερειών των πειραμάτων και των τεχνικών που εφαρμόστηκαν για την ανάπτυξη και την υλοποίηση τους. Η εκτέλεση των πειραμάτων, η παρουσίαση των αποτελεσμάτων και ο σχολιασμός τους υπό διαφορετικές οπτικές γίνονται στο Κεφάλαιο 5, όπου επίσης συνοψίζονται χρήσιμα συμπεράσματα από τη διεξαγωγή τους. Τέλος, στο Κεφάλαιο 6 αναφέρονται τα συμπεράσματα της διπλωματικής εργασίας μαζί με τις μελλοντικές επεκτάσεις που κρίνονται απαραίτητες για την συνέχιση της έρευνας.

Κεφάλαιο 2

Θεωρητικό Υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζεται το απαραίτητο θεωρητικό υπόβαθρο που υποστηρίζει την εργασία. Περιγράφονται οι βασικές έννοιες και τεχνικές που σχετίζονται με την ανίχνευση απάτης και ανωμαλιών, καθώς και οι μέθοδοι μηχανικής μάθησης και στατιστικής που αξιοποιούνται για την υλοποίηση και αξιολόγηση αντίστοιχων μοντέλων και αλγορίθμων.

Αρχικά, εξετάζονται τα χαρακτηριστικά της ανίχνευσης απάτης (Fraud detection) και της ανίχνευσης ανωμαλιών (Anomaly detection), με στόχο την κατανόηση των ιδιαίτερων απαιτήσεων και δυσκολιών που παρουσιάζουν αυτά τα προβλήματα. Έμφαση δίνεται στην περίπτωση της μη ισορροπημένης μάθησης (Imbalanced learning), η οποία αποτελεί συχνό φαινόμενο σε σενάρια όπου τα δείγματα απάτης είναι πολύ λιγότερα σε σχέση με τα κανονικά. Παρουσιάζονται έννοιες όπως τα Imbalanced datasets και η Imbalanced classification, καθώς και τεχνικές διαχείρισης αυτών των ζητημάτων.

Στη συνέχεια, παρουσιάζονται βασικές έννοιες της μηχανικής μάθησης, με αναφορά σε νευρωνικά δίκτυα τύπου MLP, τον αλγόριθμο Gradient Descent και τον ταξινομητή Random Forest και κάποιες παραλλαγές του, ο οποίος αποτελεί μια αποτελεσματική προσέγγιση για ποικίλα προβλήματα ταξινόμησης.

Ακολουθεί επισκόπηση σημαντικών στατιστικών μεθόδων που χρησιμοποιούνται για την ανάλυση δεδομένων που χρησιμοποιήθηκαν, όπως οι ελεγκτικές μέθοδοι Kolmogorov–Smirnov, Jensen–Shannon divergence, Kullback–Leibler divergence, καθώς και τεχνικές εκτίμησης πυκνότητας όπως η Kernel Density Estimation και η διαδικασία Standard Scaling για την κανονικοποίηση των χαρακτηριστικών.

Έπειτα, περιγράφονται οι βασικές μετρικές αξιολόγησης ταξινομητών, δηλαδή οι Accuracy, Precision, Recall και F1-score, και αναλύεται ο τρόπος με τον οποίο καθεμία από αυτές αποτιμά την απόδοση ενός συστήματος ανίχνευσης απάτης.

Το κεφάλαιο ολοκληρώνεται με μία βιβλιογραφική ανασκόπηση της σχετικής περιοχής, παρουσιάζοντας προηγούμενες εργασίες και προσεγγίσεις που σχετίζονται με το αντικείμενο της εργασίας.

2.1 Fraud και Anomaly Detection

Η ανίχνευση απάτης (Fraud detection) και η ανίχνευση ανωμαλιών (Anomaly detection) αποτελούν δύο στενά συνδεδεμένα πεδία, τα οποία έχουν ως στόχο τον εντοπισμό σπάνιων και ασυνήθιστων συμπεριφορών μέσα σε δεδομένα. Οι τεχνικές που εφαρμόζονται σε αυτά τα πεδία βρίσκουν εφαρμογή σε πληθώρα πραγματικών σεναρίων, όπως η παρακολούθηση χρηματοοικονομικών συναλλαγών, η ασφάλεια δικτύων, η πρόληψη επιθέσεων στον κυβερνοχώρο και η ποιότητα βιομηχανικών διαδικασιών [12].

Η ανίχνευση απάτης εστιάζει στον εντοπισμό περιπτώσεων δόλιας συμπεριφοράς, όπου ένα υποκείμενο επιχειρεί να παραβιάσει κανόνες με σκοπό την απόκτηση παράνομου οφέλους [13]. Σε εφαρμογές όπως τα τραπεζικά συστήματα ή τα ασφαλιστικά προγράμματα, η απάτη συνήθως παρουσιάζεται σπάνια [14], με συνέπεια να παράγει μη ισορροπημένα σύνολα δεδομένων, στα οποία τα δόλια παραδείγματα είναι πολύ λιγότερα από τα κανονικά.

Η ανίχνευση ανωμαλιών, από την άλλη πλευρά, είναι μια ευρύτερη έννοια και αφορά τον εντοπισμό δειγμάτων που αποκλίνουν σημαντικά από την κανονική συμπεριφορά [15]. Οι ανωμαλίες μπορεί να είναι αποτέλεσμα απάτης, αλλά επίσης και σφάλματα, αστοχίες συστημάτων, ή σπάνια συμβάντα [12].

Οι δύο προσεγγίσεις διαφέρουν στη στόχευση, καθώς η ανίχνευση απάτης βασίζεται σε συγκεκριμένα πρότυπα δόλιας συμπεριφοράς, ενώ η ανίχνευση ανωμαλιών συνήθως προϋποθέτει την ύπαρξη μόνο κανονικών δεδομένων και προσπαθεί να εντοπίσει τις εξαιρέσεις [16].

Κοινό χαρακτηριστικό και των δύο περιπτώσεων είναι ότι πρόκειται για προβλήματα δυαδικής ταξινόμησης με σημαντική πρόκληση να είναι το ζήτημα της ανισορροπίας των δεδομένων, αφού απαιτείται η ανάγκη για υψηλή ακρίβεια και ευαισθησία στην πρόβλεψη των δόλιων περιπτώσεων. Επιπλέον, η ερμηνευσιμότητα των μοντέλων είναι συχνά κρίσιμη, καθώς απαιτείται να μπορεί να δικαιολογηθεί γιατί μια συναλλαγή θεωρείται ύποπτη [17].

Η χρήση τεχνικών μηχανικής μάθησης για αυτούς τους σκοπούς έχει αποδειχθεί ιδιαίτερα αποτελεσματική, τόσο σε επιβλεπόμενα όσο και σε μη επιβλεπόμενα σενάρια μάθησης [18]. Ανάλογα με τη διαθεσιμότητα δεδομένων και τη φύση του προβλήματος, επιλέγονται διαφορετικές στρατηγικές, όπως η χρήση ταξινομητών (classifiers), μοντέλων πυκνότητας, ή μεθόδων ανίχνευσης μη κανονικών τιμών (outlier detection).

Η προσέγγιση που θα εξεταστεί στην εργασία είναι η χρήση ταξινομητών, που έχει αποδειχθεί ως η πλέον αποτελεσματικότερη για την ανίχνευση απατών τα τελευταία χρόνια με την τεράστια άνοδο της βαθιάς μάθησης.

2.2 Imbalanced Learning

Η μη ισορροπημένη μάθηση (Imbalanced learning) αναφέρεται σε προβλήματα στα οποία τα δεδομένα κατανέμονται άνισα μεταξύ των κλάσεων που ανήκουν. Σε πολλά πραγματικά σενάρια, όπως η ανίχνευση απάτης, η πρόβλεψη ασθενειών, ή η ανίχνευση ελαττωματικών προϊόντων, τα θετικά δείγματα (δηλαδή οι περιπτώσεις που ενδιαφέρουν πραγματικά) είναι πολύ πιο σπάνια σε σχέση με τα αρνητικά.

Αυτό δημιουργεί σημαντικές δυσκολίες στη διαδικασία εκπαίδευσης μοντέλων, καθώς τα

παραδοσιακά αλγοριθμικά κριτήρια, όπως η ελαχιστοποίηση του συνολικού σφάλματος ή η μεγιστοποίηση της ακρίβειας (accuracy), τείνουν να ευνοούν την κλάση με την πλειοψηφία [19]. Ως αποτέλεσμα, ένα μοντέλο μπορεί να παρουσιάζει υψηλή συνολική απόδοση αλλά να αποτυγχάνει πλήρως στον εντοπισμό της μικρότερης και πιο κρίσιμης κλάσης.

Η μη ισορροπημένη μάθηση αποτελεί κεντρικό πρόβλημα στην εργασία, καθώς τα δεδομένα απάτης που χρησιμοποιούνται είναι ιδιαίτερα σπάνια, και απαιτείται η χρήση εξειδικευμένων τεχνικών τόσο σε επίπεδο δεδομένων όσο και σε επίπεδο μοντελοποίησης.

2.2.1 Imbalanced Datasets

Ένα μη ισορροπημένο σύνολο δεδομένων (imbalanced dataset) είναι ένα σύνολο όπου η κατανομή των κλάσεων δεν είναι ομοιόμορφη. Συχνά, η κυρίαρχη κλάση (όπως για παράδειγμα οι κανονικές συναλλαγές) καταλαμβάνει πάνω από το 99% των παραδειγμάτων, ενώ η κλάση που περιέχει την μειοψηφία (όπως περιπτώσεις απάτης) είναι εξαιρετικά περιορισμένη, συχνά αποτελούμενη με λιγότερο από το 1% των συνολικών παραδειγμάτων.

Αυτού του είδους η ασυμμετρία μπορεί να οδηγήσει σε υπερεκπροσώπηση της κυρίαρχης κλάσης κατά την εκπαίδευση, και κατά συνέπεια σε μοντέλα που αγνοούν εντελώς τη μειοψηφική κλάση [20]. Επιπλέον, μπορεί να επηρεαστεί η διαδικασία δειγματοληψίας, η εκπαίδευση και η αξιολόγηση, εφόσον η πιο κλασσική μετρική, αυτή της ακρίβειας (accuracy) γίνεται παραπλανητική [21].

Για την αντιμετώπιση του προβλήματος, συχνά εφαρμόζονται τεχνικές όπως [21]:

- Υπερδειγματοληψία (oversampling) της μειοψηφικής κλάσης.
- Υποδειγματοληψία (undersampling) της πλειοψηφικής κλάσης.
- Συνθετική δημιουργία δεδομένων, όπως η τεχνική SMOTE (Synthetic Minority Oversampling Technique).
- Κατάλληλες επιλογές μετρικών αξιολόγησης, όπως τα precision, recall και F1-score.

2.2.2 Imbalanced Classification

Η μη ισορροπημένη ταξινόμηση (imbalanced classification) αφορά την εφαρμογή αλγορίθμων μάθησης σε μη ισορροπημένα δεδομένα, με στόχο την αξιόπιστη πρόβλεψη της μειοψηφικής κλάσης. Η πρόκληση εδώ δεν είναι μόνο η έλλειψη των δεδομένων, αλλά και η ανάγκη για ευαίσθητα και ισορροπημένα μοντέλα που να μπορούν να ανιχνεύουν τα σπάνια αλλά κρίσιμα θετικά παραδείγματα.

Για να επιτευχθεί αυτό, χρησιμοποιούνται ειδικές στρατηγικές ταξινόμησης, όπως:

- Σταθμισμένες συναρτήσεις κόστους (cost-sensitive learning), όπου τα λάθη στην μειοψηφική κλάση έχουν μεγαλύτερο κόστος.
- Ειδικά διαμορφωμένοι ταξινομητές (π.χ. Balanced Random Forest, One-Class SVM).
- Επιλογή μετρικών αξιολόγησης που εστιάζουν στη μειοψηφική κλάση, όπως το ROC-AUC ή το F1-score.

Η επιτυχής διαχείριση του προβλήματος της μη ισορροπημένης ταξινόμησης αποτελεί κρίσιμο παράγοντα για την αποτελεσματικότητα συστημάτων ανίχνευσης απάτης, καθώς εξασφαλίζει ότι οι σπάνιες περιπτώσεις δεν παραβλέπονται απο τα μοντέλα.

2.3 Μηχανική Μάθηση

Η μηχανική μάθηση αποτελεί τον κλάδο της τεχνητής νοημοσύνης που επικεντρώνεται στην ανάπτυξη αλγορίθμων και μοντέλων που έχουν την ικανότητα να μαθαίνουν από δεδομένα και να λαμβάνουν αποφάσεις ή προβλέψεις χωρίς να έχουν προγραμματιστεί ρητά για κάθε ενδεχόμενο. Αντί να ακολουθούν ένα σύνολο κανόνων που έχει ορίσει ο άνθρωπος, τα μοντέλα μηχανικής μάθησης ανακαλύπτουν σχέσεις, μοτίβα και κανόνες απευθείας από τα δεδομένα [22]. Η επιλογή κατάλληλων τεχνικών για την προεπεξεργασία, η επιλογή του σωστού τύπου μοντέλου και των υπερπαράμετρών του, καθώς και η κατάλληλη μέθοδος αξιολόγησης, καθορίζουν σε μεγάλο βαθμό την επιτυχία του μοντέλου μηχανικής μάθησης.

Η μηχανική μάθηση διαιρείται σε υποκατηγορίες [23], όπως η εποπτευόμενη μάθηση (supervised learning), η μη-εποπτευόμενη μάθηση (unsupervised learning) και η ενισχυτική μάθηση (reinforcement learning), με την εργασία να επικεντρώνεται κυρίως στην εποπτευόμενη μάθηση, όπου τα δεδομένα είναι επισημασμένα και ο στόχος είναι η εκμάθηση ενός μοντέλου που προβλέπει τη σωστή κλάση για νέα δείγματα.

2.3.1 MLPs, Gradient descent και Βελτιστοποιητής Adam

Τα **Multilayer Perceptrons (MLPs)** είναι τεχνητά νευρωνικά δίκτυα με τουλάχιστον ένα κρυφό στρώμα και χρησιμοποιούνται για την επίλυση προβλημάτων εποπτευόμενης μάθησης [24]. Η βασική μονάδα ενός MLP είναι ο νευρώνας, ο οποίος υπολογίζει μια γραμμική συνάρτηση των εισόδων του και στη συνέχεια εφαρμόζει μία μη γραμμική συνάρτηση ενεργοποίησης.
Για έναν νευρώνα με είσοδο

$$x = [x_1, x_2, \ldots, x_n]^\top$$

και βάρη

$$w = [w_1, w_2, \ldots, w_n]^\top,$$

η έξοδος πριν τη συνάρτηση ενεργοποίησης είναι:

$$z = w^\top x + b$$

όπου b είναι ο όρος προκατάληψης (bias). Η τελική έξοδος του νευρώνα δίνεται από:

$$a = \varphi(z)$$

όπου φ είναι η συνάρτηση ενεργοποίησης, όπως για παράδειγμα:

$$\mathrm{ReLU}(z) = \max(0, z) \quad \text{ή} \quad \sigma(z) = \frac{1}{1 + e^{-z}}.$$

Η εκπαίδευση του MLP αποσκοπεί στην ελαχιστοποίηση μιας συνάρτησης κόστους $\mathcal{L}$. Έστω ότι υπάρχουν m δείγματα, τότε η συνολική συνάρτηση κόστους είναι:

$$\mathcal{L} = \frac{1}{m} \sum_{i=1}^{m} \ell\left(y^{(i)}, \hat{y}^{(i)}\right)$$

όπου $y^{(i)}$ είναι η πραγματική ετικέτα και $\hat{y}^{(i)}$ η πρόβλεψη του δικτύου για το δείγμα i, ενώ $\ell(\cdot, \cdot)$ είναι η επιμέρους συνάρτηση κόστους.

Η ελαχιστοποίηση της $\mathcal{L}$ γίνεται μέσω του αλγορίθμου **(Gradient Descent)**, ο οποίος ενημερώνει τα βάρη και τις μετατοπίσεις σύμφωνα με τους παρακάτω κανόνες:

$$w \leftarrow w - \eta \nabla_w \mathcal{L}$$

$$b \leftarrow b - \eta \frac{\partial \mathcal{L}}{\partial b}$$

όπου η είναι ο ρυθμός μάθησης.

Για τον υπολογισμό των παραγώγων χρησιμοποιείται ο αλγόριθμος οπισθοδιάδοσης (Back-propagation) [25], ο οποίος βασίζεται στον κανόνα της αλυσίδας. Το σφάλμα στο στρώμα l υπολογίζεται ως:

$$\delta^l = \left(W^{l+1} \delta^{l+1}\right) \circ \phi'(z^l)$$

όπου δ^l είναι το σφάλμα στο στρώμα l, ϕ' η παράγωγος της συνάρτησης ενεργοποίησης και το $\circ$ δηλώνει το γινόμενο Hadamard (Hadamard product).

Οι παράγωγοι για την ενημέρωση των βαρών και μετατοπίσεων δίνονται από:

$$\frac{\partial \mathcal{L}}{\partial W^l} = \delta^l (a^{l-1})^\top, \quad \frac{\partial \mathcal{L}}{\partial b^l} = \delta^l.$$

Η διαδικασία αυτή επαναλαμβάνεται για κάθε δείγμα ή για κάθε παρτίδα (batch) δειγμάτων έως ότου το δίκτυο συγκλίνει σε μια λύση με ικανοποιητική απόδοση.

Ο **Adam** [26] είναι ένας από τους πιο διαδεδομένους και αποτελεσματικούς αλγορίθμους βελτιστοποίησης στη μηχανική μάθηση, ειδικά για την εκπαίδευση νευρωνικών δικτύων. Συνδυάζει τις ιδιότητες του Momentum και της Adaptive Learning Rate, διατηρώντας εκτιμήσεις πρώτης και δεύτερης τάξης της στιγμιαίας κλίσης για κάθε παράμετρο.

Έστω θ_t οι παράμετροι του μοντέλου στη χρονική στιγμή t και $g_t = \nabla_\theta \mathcal{L}_t$ η κλίση της συνάρτησης κόστους στο ίδιο βήμα. Ο αλγόριθμος Adam λειτουργεί ως εξής:

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t$$
$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2$$

Όπου:

- m_t: εκτίμηση της 1ης ροπής (mean των κλίσεων),
- v_t: εκτίμηση της 2ης ροπής (μη κεντροποιημένη variance),

- $\beta_1, \beta_2 \in [0, 1)$: υπερπαράμετροι που ελέγχουν την εκθετική απομείωση (decay).

Επειδή οι εκτιμήσεις m_t και v_t ξεκινούν από το μηδέν, εφαρμόζονται διορθώσεις προκατάληψης (bias correction):

$$\hat{m}_t = \frac{m_t}{1 - \beta_1^t}$$
$$\hat{v}_t = \frac{v_t}{1 - \beta_2^t}$$

Η ενημέρωση των παραμέτρων γίνεται ως εξής:

$$\theta_{t+1} = \theta_t - \eta \cdot \frac{\hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon}$$

Όπου:

- η: ρυθμός μάθησης (learning rate, συνήθως μικρότερος από 0.001),
- ϵ: πολύ μικρός αριθμός (π.χ. 10^{-8}) για αποφυγή διαίρεσης με το μηδέν.

Ο Adam έχει αποδειχθεί ιδιαίτερα σταθερός και αποδοτικός για μεγάλα και αραιά δεδομένα, καθώς και για μη σταθερές συναρτήσεις κόστους, γεγονός που τον καθιστά δημοφιλή επιλογή σε πληθώρα εφαρμογών βαθιάς μάθησης.

2.3.2 Random Forest Classifier

Ο ταξινομητής **Random Forest** [27] αποτελεί έναν αλγόριθμο επιβλεπόμενης μάθησης βασισμένο σε σύνολο (ensemble method) από δέντρα απόφασης. Κάθε δέντρο εκπαιδεύεται ανεξάρτητα πάνω σε ένα υποσύνολο των δεδομένων που παράγεται μέσω δειγματοληψίας με επανάθεση (bootstrap sampling). Επιπλέον, σε κάθε κόμβο επιλέγεται τυχαίο υποσύνολο χαρακτηριστικών για την εύρεση του βέλτιστου διαχωρισμού, ενισχύοντας τη διαφοροποίηση μεταξύ των δέντρων.

Το τελικό αποτέλεσμα προκύπτει μέσω πλειοψηφικής ψήφου, η οποία μπορεί να εκφραστεί μαθηματικά ως:

$$\hat{y} = \arg\max_{c \in C} \sum_{b=1}^{B} \mathbb{I}(h_b(x) = c)$$

όπου:

- $h_b(x)$: η πρόβλεψη του b-οστού δέντρου για το δείγμα x,
- B: ο συνολικός αριθμός των δέντρων,
- C: το σύνολο των κλάσεων,
- $\mathbb{I}(\cdot)$: η συνάρτηση δείκτη, που παίρνει τιμή 1 αν η πρόβλεψη του δέντρου ισούται με την κλάση c, και 0 αλλιώς.

Η τελική πρόβλεψη $\hat{y}$ είναι η κλάση που συγκεντρώνει τις περισσότερες ψήφους από τα B δέντρα.

Η βασική ιδέα του ταξινομητή **Balanced Random Forest** [28] είναι η κατασκευή κάθε δέντρου με ένα ισορροπημένο υποσύνολο δεδομένων. Για κάθε δέντρο $b \in \{1, \ldots, B\}$, επιλέγεται τυχαίο δείγμα από τη μειοψηφική κλάση $\mathcal{D}_{\text{min}}$, και ισάριθμο δείγμα από την πλειοψηφική κλάση $\mathcal{D}_{\text{maj}}$ μέσω υποδειγματοληψίας χωρίς επανάθεση:

$$\mathcal{D}^{(b)} = \mathcal{D}^{(b)}_{\text{min}} \cup \mathcal{D}^{(b)}_{\text{maj}}, \quad |\mathcal{D}^{(b)}_{\text{min}}| = |\mathcal{D}^{(b)}_{\text{maj}}|$$

Η χρήση ισορροπημένων συνόλων κατά την εκπαίδευση οδηγεί σε καλύτερη ευαισθησία στην προβλεπόμενη μειοψηφική κλάση, μειώνοντας τη μεροληψία του μοντέλου υπέρ της πλειοψηφίας.

Η μέθοδος του ταξινομητή **Isolation Forest** [29] αποτελεί τεχνική μη επιβλεπόμενης μάθησης για την ανίχνευση ανωμαλιών. Αντί να μοντελοποιεί την κανονικότητα, επιχειρεί να απομονώσει παρατηρήσεις μέσω τυχαίων διαχωρισμών.

Το βασικό μέγεθος είναι το μήκος της διαδρομής $h(x)$ για το δείγμα x, δηλαδή ο αριθμός των εσωτερικών κόμβων που διανύονται μέχρι το δείγμα να φτάσει σε φύλλο. Ο αναμενόμενος αριθμός βημάτων σε ένα τυχαίο δυαδικό δέντρο ύψους n είναι:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n}$$

όπου $H(i)$ είναι ο αρμονικός αριθμός: $H(i) = \sum_{k=1}^{i} \frac{1}{k} \approx \ln(i) + \gamma$, με $\gamma \approx 0.577$ τη σταθερά του Euler-Mascheroni.

Το τελικό Anomaly Score για ένα δείγμα x ορίζεται ως:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$

Όπου:

- $E(h(x))$: ο μέσος όρος των μηκών διαδρομής του x στα δέντρα,
- $c(n)$: το αναμενόμενο βάθος για δείγμα μεγέθους n.

Τιμές του $s(x, n)$ κοντά στο 1 υποδηλώνουν ανωμαλία, ενώ τιμές κοντά στο 0.5 υποδηλώνουν κανονική συμπεριφορά. Η μέθοδος είναι αποδοτική υπολογιστικά και ιδιαίτερα κατάλληλη για μεγάλες διαστάσεις και αραιά δεδομένα.

2.4 Στατιστικές Μέθοδοι

Στο κεφάλαιο αυτό πραγματοποιείται η ανάλυση και η κατανόηση των διαφορών μεταξύ των κλάσεων στο σύνολο δεδομένων, χρησιμοποιούνται διάφορες στατιστικές μέθοδοι και μετρικές. Αυτές οι μέθοδοι επιτρέπουν τη σύγκριση των κατανομών των χαρακτηριστικών ανάμεσα στην κλάση απάτης (fraud) και την κλάση μη απάτης (non-fraud), βοηθώντας στην ανάδειξη χαρακτηριστικών με υψηλή διακριτική ικανότητα.

Συγκεκριμένα, εφαρμόζονται στατιστικοί έλεγχοι και μετρικές απόστασης που ποσοτικοποιούν τις αποκλίσεις μεταξύ κατανομών, καθώς και τεχνικές οπτικοποίησης και κανονικοποίησης της κατανομής των δεδομένων.

Ακολουθούν οι βασικές μέθοδοι που χρησιμοποιήθηκαν στην ανάλυση:

2.4.1 Kolmogorov–Smirnov test

Το Kolmogorov–Smirnov test είναι μία μη παραμετρική στατιστική δοκιμή που χρησιμοποιείται για να συγκρίνει μια εμπειρική κατανομή με μία θεωρητική ή δύο εμπειρικές κατανομές μεταξύ τους [30]. Βασικός του στόχος είναι να εντοπίσει αν υπάρχουν σημαντικές διαφορές μεταξύ των δύο κατανομών.

Ορισμός

Έστω $F_n(x)$ η εμπειρική συνάρτηση κατανομής ενός δείγματος μεγέθους n, και $F(x)$ η θεωρητική κατανομή ή η εμπειρική κατανομή ενός δεύτερου δείγματος. Ο στατιστικός έλεγχος Kolmogorov–Smirnov ορίζεται ως:

$$D_n = \sup_x |F_n(x) - F(x)|$$

όπου:

- $\sup_x$ είναι η μέγιστη τιμή της διαφοράς (δηλαδή το μέγιστο κατακόρυφο διάστημα ανάμεσα στις δύο συναρτήσεις κατανομής),
- $F_n(x)$ είναι η εμπειρική συνάρτηση κατανομής του δείγματος,
- $F(x)$ είναι είτε η θεωρητική συνάρτηση κατανομής είτε η εμπειρική του δεύτερου δείγματος.

Η τιμή D_n μετρά τη μέγιστη απόκλιση μεταξύ των δύο κατανομών.

Υπόθεση ελέγχου

- **Μηδενική υπόθεση** H_0: Οι δύο κατανομές είναι ίδιες.
- **Εναλλακτική υπόθεση** H_1: Οι κατανομές διαφέρουν σε τουλάχιστον ένα σημείο.

Η απόρριψη ή μη της μηδενικής υπόθεσης βασίζεται στην τιμή του D_n και στο αντίστοιχο p-value, το οποίο μπορεί να προσδιοριστεί με βάση την ασυμπτωτική κατανομή του D_n.

Εφαρμογή στη σύγκριση κλάσεων ενός συνόλου δεδομένων

Στο πλαίσιο της εργασίας, ο έλεγχος Kolmogorov–Smirnov εφαρμόζεται για τη σύγκριση της κατανομής τιμών κάθε αριθμητικού χαρακτηριστικού του συνόλου δεδομένων μεταξύ των δύο κλάσεων: της κλάσης fraud (απάτη) και της κλάσης non-fraud (μη απάτη). Συγκεκριμένα:

- Για κάθε χαρακτηριστικό x_i, διαχωρίζονται οι τιμές που αντιστοιχούν στις δύο κλάσεις.

- Υπολογίζονται οι αντίστοιχες εμπειρικές συναρτήσεις κατανομής $F_{1,i}(x)$ και $F_{0,i}(x)$, για τις κλάσεις απάτης και μη απάτης αντίστοιχα.
- Εφαρμόζεται το two-sample Kolmogorov–Smirnov test για να προσδιοριστεί η μέγιστη απόκλιση μεταξύ των δύο κατανομών:

$$D_i = \sup_x |F_{1,i}(x) - F_{0,i}(x)|$$

- Το αντίστοιχο p-value υπολογίζεται ώστε να εκτιμηθεί αν η παρατηρούμενη διαφορά είναι στατιστικά σημαντική.

Ο στόχος αυτής της διαδικασίας είναι η ποσοτική αξιολόγηση της ομοιότητας ή διαφοράς μεταξύ των δύο κλάσεων ως προς κάθε χαρακτηριστικό. Ένα υψηλό D_i υποδεικνύει ότι το χαρακτηριστικό x_i παρουσιάζει σημαντική διαφοροποίηση μεταξύ των δύο ομάδων και άρα μπορεί να είναι χρήσιμο για την ανίχνευση απάτης. Αντίθετα, ένα μικρό D_i σημαίνει ότι οι δύο κατανομές είναι παρόμοιες και το χαρακτηριστικό πιθανώς δεν έχει διακριτική ικανότητα.

2.4.2 Kullback–Leibler divergence

Η Kullback–Leibler (KL) divergence είναι ένα μέτρο που ποσοτικοποιεί το πόσο μία κατανομή πυκνότητας πιθανότητας $Q(x)$ αποκλίνει από μια άλλη κατανομή αναφοράς $P(x)$ [31], [32]. Παρόλο που δεν αποτελεί αυστηρά απόσταση (δεν είναι συμμετρική και δεν ικανοποιεί την τριγωνική ανισότητα), χρησιμοποιείται εκτενώς για τη σύγκριση κατανομών, ειδικά σε προβλήματα στατιστικής, πληροφορίας και μηχανικής μάθησης.

Ορισμός

Έστω $P(x)$ και $Q(x)$ δύο κατανομές πυκνότητας πιθανότητας πάνω στον ίδιο χώρο τιμών. Η Kullback–Leibler divergence από την Q στην P ορίζεται ως:

$$\mathrm{KL}(P \parallel Q) = \sum_x P(x) \log\left(\frac{P(x)}{Q(x)}\right)$$

ή, στην περίπτωση συνεχών κατανομών:

$$\mathrm{KL}(P \parallel Q) = \int_{-\infty}^{\infty} P(x) \log\left(\frac{P(x)}{Q(x)}\right) dx$$

όπου:

- $P(x)$ είναι η πραγματική ή αναμενόμενη κατανομή,
- $Q(x)$ είναι η προσεγγιστική ή εναλλακτική κατανομή,
- Ο λογάριθμος είναι συνήθως φυσικός ($\log_e$), αν και σε κάποιες περιπτώσεις χρησιμοποιείται και η βάση 2.

Η τιμή της $\mathrm{KL}(P \parallel Q)$ είναι πάντα μη αρνητική και είναι ίση με 0 μόνο όταν $P(x) = Q(x)$ για όλα τα x.

Εφαρμογή στη σύγκριση κλάσεων ενός συνόλου δεδομένων

Στην εργασία, η Kullback–Leibler divergence χρησιμοποιείται για να μετρηθεί η απόκλιση ανάμεσα στις κατανομές ενός αριθμητικού χαρακτηριστικού για τις δύο κλάσεις του συνόλου δεδομένων: fraud και non-fraud. Συγκεκριμένα:

- Για κάθε χαρακτηριστικό x_i, εκτιμώνται οι κατανομές πυκνότητας πιθανότητας $P_i(x)$ (για την κλάση fraud) και $Q_i(x)$ (για την κλάση non-fraud), συνήθως μέσω Kernel Density Estimation.
- Υπολογίζεται η KL divergence:

$$\mathrm{KL}_i = \mathrm{KL}(P_i \parallel Q_i)$$

Η τιμή KL_i δείχνει πόσο διαφορετική είναι η κατανομή της τιμής του χαρακτηριστικού x_i στην κλάση απάτης σε σχέση με την κλάση μη απάτης. Μεγαλύτερες τιμές της KL divergence υποδεικνύουν μεγαλύτερη απόκλιση και συνεπώς πιθανή διακριτική ισχύ του χαρακτηριστικού για την ταξινόμηση.

2.4.3 Jensen–Shannon divergence

Η Jensen–Shannon divergence (JSD) είναι ένα συμμετρικό και πεπερασμένο μέτρο απόστασης μεταξύ δύο κατανομών πυκνότητας πιθανότητας [33], [34]. Χρησιμοποιείται ευρέως για τη μέτρηση της ομοιότητας (ή απόκλισης) μεταξύ δύο κατανομών, προσφέροντας ένα σταθερό και αποδοτικό κριτήριο.

Ορισμός

Έστω $P(x)$ και $Q(x)$ δύο κατανομές πυκνότητας πιθανότητας πάνω στον ίδιο χώρο τιμών. Η Jensen–Shannon divergence ορίζεται ως:

$$\mathrm{JSD}(P \parallel Q) = \frac{1}{2}\mathrm{KL}(P \parallel M) + \frac{1}{2}\mathrm{KL}(Q \parallel M)$$

όπου:

- $M(x) = \frac{1}{2}(P(x) + Q(x))$ είναι η μέση κατανομή,
- $\mathrm{KL}(P \parallel M)$ είναι η Kullback–Leibler divergence μεταξύ P και M,
- και η KL divergence δίνεται από τον τύπο:

$$\mathrm{KL}(P \parallel Q) = \sum_x P(x) \log\left(\frac{P(x)}{Q(x)}\right)$$

Η JSD είναι πάντα ορισμένη και παίρνει τιμές στο διάστημα $[0, \log 2]$, με το 0 να δηλώνει ταυτόσημες κατανομές και το $\log 2$ (ή 1 αν χρησιμοποιηθεί βάση 2 στον λογάριθμο) να δηλώνει μέγιστη απόκλιση.

Εφαρμογή στη σύγκριση κλάσεων ενός συνόλου δεδομένων

Στην εργασία, η Jensen–Shannon divergence χρησιμοποιείται για τη σύγκριση της κατανομής κάθε αριθμητικού χαρακτηριστικού μεταξύ των δύο κλάσεων του συνόλου δεδομένων: fraud (απάτη) και non-fraud (μη απάτη). Η διαδικασία είναι η εξής:

- Για κάθε χαρακτηριστικό x_i, υπολογίζονται οι κανονικοποιημένες κατανομές πυκνότητας πιθανότητας (π.χ. μέσω Kernel Density Estimation) για τις δύο κλάσεις: $P_i(x)$ και $Q_i(x)$.
- Υπολογίζεται η Jensen–Shannon divergence μεταξύ των δύο κατανομών:

$$\mathrm{JSD}_i = \mathrm{JSD}(P_i \parallel Q_i)$$

Η τιμή JSD_i παρέχει ένα μέτρο της διακριτικότητας του χαρακτηριστικού x_i ως προς τις δύο κλάσεις. Όσο υψηλότερη είναι η τιμή της JSD, τόσο μεγαλύτερη είναι η διαφορά μεταξύ των κατανομών και επομένως τόσο πιο πιθανό είναι το χαρακτηριστικό να είναι σημαντικό για την ανίχνευση απάτης. Μικρές τιμές υποδεικνύουν παρόμοια συμπεριφορά του χαρακτηριστικού και στις δύο κλάσεις.

2.4.4 Kernel Density Estimation

Η Kernel Density Estimation (KDE) είναι μία μη παραμετρική μέθοδος εκτίμησης της κατανομής πυκνότητας πιθανότητας μιας τυχαίας μεταβλητής [35], [36]. Σε αντίθεση με τα ιστογράμματα, τα οποία εξαρτώνται από το μέγεθος των διαστημάτων (bins), η KDE παρέχει μια ομαλότερη και πιο συνεχή αναπαράσταση της κατανομής.

Ορισμός

Έστω ένα σύνολο παρατηρήσεων $x_1, x_2, \ldots, x_n$. Η KDE της κατανομής πυκνότητας πιθανότητας δίνεται από τον τύπο:

$$\hat{f}_h(x) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{x - x_i}{h}\right)$$

όπου:

- K είναι ο πυρήνας (kernel function), συνήθως μια συμμετρική συνάρτηση όπως η κανονική (Gaussian),
- $h > 0$είναι ο συντελεστής εξομάλυνσης, που καθορίζει τον βαθμό ομαλότητας της εκτιμώμενης κατανομής.
- n το πλήθος των δειγμάτων.

Η επιλογή του πυρήνα K και του συντελεστή h επηρεάζει σημαντικά την ποιότητα της εκτίμησης.

Εφαρμογή για την οπτική σύγκριση κατανομών

Στο πλαίσιο της εργασίας, η Kernel Density Estimation εφαρμόζεται για την οπτική απεικόνιση και σύγκριση των κατανομών κάθε χαρακτηριστικού του συνόλου δεδομένων μεταξύ των δύο κλάσεων: fraud και non-fraud.

Πιο συγκεκριμένα:

- Για κάθε χαρακτηριστικό x_i, δημιουργούνται δύο KDE καμπύλες: μία για τα παραδείγματα της κλάσης απάτης και μία για τις παρατηρήσεις της κλάσης μη απάτης.
- Η KDE συνδυάζεται με το ιστόγραμμα, ώστε να υπάρχει τόσο η διακριτή όσο και η συνεχής οπτική εκτίμηση της κατανομής.
- Αυτό επιτρέπει την οπτική αναγνώριση διαφορών ή επικαλύψεων των κατανομών μεταξύ των δύο κλάσεων, για κάθε χαρακτηριστικό ξεχωριστά.

Η KDE είναι ιδιαίτερα χρήσιμη για την ανάδειξη διακριτικών μοτίβων ανά χαρακτηριστικό, τα οποία ενδέχεται να μην είναι άμεσα εμφανή μέσω απλών στατιστικών μέτρων ή ιστογραμμάτων. Έτσι, διευκολύνεται η ποιοτική αξιολόγηση της διακριτικής ικανότητας κάθε χαρακτηριστικού.

2.4.5 Standard Scaling

Η μέθοδος Standard Scaling είναι μια τεχνική κανονικοποίησης χαρακτηριστικών που μετασχηματίζει τα δεδομένα ώστε να έχουν μέση τιμή μηδέν και τυπική απόκλιση μονάδα [37], [38]. Συγκεκριμένα, κάθε τιμή x ενός χαρακτηριστικού μετασχηματίζεται ως εξής:

$$x' = \frac{x - \mu}{\sigma}$$

όπου:

- μ είναι ο μέσος όρος των τιμών του χαρακτηριστικού,
- σ είναι η τυπική απόκλιση των τιμών του χαρακτηριστικού.

Η χρήση του Standard Scaling είναι ιδιαίτερα σημαντική για αλγορίθμους μηχανικής μάθησης που επηρεάζονται από την κλίμακα των χαρακτηριστικών, όπως τα πολυεπίπεδα νευρωνικά δίκτυα (MLP) αλλά και γενικότερα τα μοντέλα που χρησιμοποιούν τον gradient descent.

2.5 Μετρικές Αξιολόγησης

Για την αξιολόγηση των ταξινομητών χρησιμοποιούνται οι επόμενες μετρικές [39]: **Accuracy**, **Precision**, **Recall** και **F1-score**. Οι μετρικές αυτές υπολογίζονται με βάση τα εξής:

- **True Positives (TP)**: Αληθώς θετικές προβλέψεις
- **True Negatives (TN)**: Αληθώς αρνητικές προβλέψεις
- **False Positives (FP)**: Ψευδώς θετικές προβλέψεις
- **False Negatives (FN)**: Ψευδώς αρνητικές προβλέψεις

2.5.1 Accuracy

Η **ακρίβεια (accuracy)** δείχνει το ποσοστό των σωστών προβλέψεων επί του συνόλου των παραδειγμάτων:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Ωστόσο, στο πρόβλημα της ανίχνευσης απάτης, όπου τα δεδομένα είναι εξαιρετικά μη ισορροπημένα, η ακρίβεια μπορεί να είναι παραπλανητική. Ένα μοντέλο που προβλέπει τα πάντα ως μη απάτη μπορεί να έχει υψηλή ακρίβεια, αλλά να μην είναι χρήσιμο.

2.5.2 Recall

Η **ανάκληση (recall)**, ή **ευαισθησία**, μετράει την ικανότητα του μοντέλου να εντοπίζει σωστά τα πραγματικά θετικά δείγματα (Frauds):

$$\text{Recall} = \frac{TP}{TP + FN}$$

Είναι μια κρίσιμη μετρική στο πρόβλημα της απάτης, καθώς μας ενδιαφέρει να εντοπίζουμε όσο το δυνατόν περισσότερες απάτες, ακόμα και αν αυτό σημαίνει ότι θα έχουμε κάποιες ψευδώς θετικές.

2.5.3 Precision

Η **ακρίβεια θετικών προβλέψεων (precision)** μετράει το ποσοστό των θετικών προβλέψεων που είναι πραγματικά σωστές:

$$\text{Precision} = \frac{TP}{TP + FP}$$

Υψηλό precision σημαίνει ότι, όταν το μοντέλο προβλέπει απάτη, είναι συνήθως σωστό.

2.5.4 F1-score

Το **F1-score** είναι ο αρμονικός μέσος της Precision και Recall:

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Συνδυάζει τις δύο παραπάνω μετρικές σε μία τιμή και είναι χρήσιμο όταν θέλουμε να ισορροπήσουμε μεταξύ του να εντοπίζουμε όσο το δυνατόν περισσότερα θετικά δείγματα (Recall) και να έχουμε λίγες ψευδώς θετικές προβλέψεις (Precision).

2.6 Βιβλιογραφική Ανασκόπηση Περιοχής

2.6.1 Ορισμός και Κατηγορίες Απάτης σε Τραπεζικές Συναλλαγές

Η απάτη σε τραπεζικές συναλλαγές αναφέρεται σε οποιαδήποτε κακόβουλη ή μη εξουσιοδοτημένη ενέργεια που έχει ως στόχο την παράνομη απόκτηση οικονομικού οφέλους μέσω της κατάχρησης χρηματοπιστωτικών συστημάτων [40]. Πρόκειται για ένα πολυσύνθετο φαινόμενο που επηρεάζει ιδρύματα, πελάτες και ρυθμιστικούς φορείς [41], ενώ εντείνεται συνεχώς λόγω της ψηφιοποίησης των χρηματοοικονομικών υπηρεσιών [42] και της μεγάλης αύξησης των καθημερινών συναλλαγών [43].

Η απάτη μπορεί να διακριθεί σε διάφορες κατηγορίες, ανάλογα με τη φύση της συναλλαγής και τη μέθοδο επίθεσης. Μερικές από τις πλέον συχνές μορφές περιλαμβάνουν [44], [45], [46]:

- **Απάτη με Πιστωτικές Κάρτες (Credit Card Fraud):** Περιλαμβάνει τη χρήση κλεμμένων ή παραποιημένων στοιχείων κάρτας για τη διενέργεια μη εξουσιοδοτημένων αγορών ή αναλήψεων.
- **Απάτη Ταυτότητας (Identity Theft):** Ο δράστης αποκτά και χρησιμοποιεί προσωπικά στοιχεία τρίτου (π.χ. ΑΦΜ, αριθμούς λογαριασμών κτλπ) για να αποκτήσει πρόσβαση σε τραπεζικά προϊόντα ή να προβεί σε συναλλαγές.
- **Κατάληψη Λογαριασμού (Account Takeover):** Πρόκειται για τη μη εξουσιοδοτημένη πρόσβαση και χρήση τραπεζικού λογαριασμού από τρίτους, συχνά μέσω τεχνικών κοινωνικής μηχανικής όπως phishing και smishing.
- **Ξέπλυμα Χρήματος (Money Laundering):** Εμπλέκει τη μετακίνηση και απόκρυψη παράνομων κεφαλαίων μέσω τραπεζικών συναλλαγών με σκοπό τη νομιμοποίησή τους.

2.6.2 Παραδοσιακές Μέθοδοι Εντοπισμού Απάτης

Οι παραδοσιακές μέθοδοι εντοπισμού απάτης βασίζονται κυρίως σε κανόνες και στατιστικές τεχνικές [47], οι οποίες εφαρμόζονται προκειμένου να αναγνωρίσουν αποκλίσεις από το φυσιολογικό πρότυπο συναλλαγών. Αυτές οι μέθοδοι ήταν οι πρώτες που χρησιμοποιήθηκαν από χρηματοπιστωτικούς οργανισμούς [48] πριν την ευρεία εφαρμογή τεχνικών μηχανικής μάθησης και τεχνητής νοημοσύνης.

Μία από τις βασικότερες προσεγγίσεις είναι η ανάλυση βασισμένη σε κανόνες, όπου προδιαγεγραμμένοι κανόνες εφαρμόζονται στα δεδομένα των συναλλαγών [49]. Τα συστήματα αυτά είναι εύκολα στην υλοποίηση και ερμηνεία, αλλά περιορίζονται σε γνωστές μορφές απάτης και παρουσιάζουν υψηλό ποσοστό ψευδών θετικών παραδειγμάτων [50].

Μια δεύτερη κατηγορία είναι οι στατιστικές μέθοδοι, οι οποίες περιλαμβάνουν τεχνικές όπως η γραμμική παλινδρόμηση, ο έλεγχος z-score και η ανάλυση κύριων συνιστωσών (PCA)

[51]. Οι τεχνικές αυτές επιτρέπουν την αναγνώριση συναλλαγών που αποκλίνουν σημαντικά από τον μέσο όρο ή το ιστορικό ενός χρήστη. Αν και πιο ευέλικτες από τα μοντέλα βασισμένα σε κανόνες, οι στατιστικές μέθοδοι δυσκολεύονται να διαχειριστούν δυναμικές απειλές ή σύνθετα πρότυπα απάτης [52], [53].

Τέλος, χρησιμοποιούνται και τεχνικές ανίχνευσης ανωμαλιών, οι οποίες θεωρούν ότι η απάτη αποτελεί σπάνιο γεγονός και προσπαθούν να εντοπίσουν ακραίες περιπτώσεις βάσει κατανομής των δεδομένων [54]. Αν και χρήσιμες, συχνά δεν επαρκούν για την ανίχνευση εξελιγμένων τεχνικών απάτης που προσομοιάζουν κανονικές συναλλαγές [55].

Παρά τον ιστορικό ρόλο των παραδοσιακών μεθόδων, η αύξηση της πολυπλοκότητας των επιθέσεων, ο όγκος δεδομένων και οι ταχύτατα μεταβαλλόμενες συνθήκες στο ψηφιακό χρηματοπιστωτικό περιβάλλον στην σύγχρονη εποχή, οδήγησαν στην ανάγκη για περισσότερο ευφυή και προσαρμοστικά συστήματα, όπως αυτά που βασίζονται στη μηχανική και βαθιά μάθηση [56], [57], [58].

2.6.3 Μέθοδοι Εντοπισμού Απάτης με Μηχανική Μάθηση

Η μηχανική μάθηση έχει αναδειχθεί ως μια ιδιαίτερα αποτελεσματική προσέγγιση για την ανίχνευση απάτης σε τραπεζικές συναλλαγές [59], λόγω της ικανότητάς της να εντοπίζει πρότυπα και ανωμαλίες σε μεγάλα και πολυδιάστατα σύνολα δεδομένων [60]. Οι πιο διαδεδομένες τεχνικές περιλαμβάνουν επιβλεπόμενα μοντέλα όπως οι Random Forests, Support Vector Machines, Logistic Regression και Gradient Boosting Machines, τα οποία εκπαιδεύονται με βάση ιστορικά δεδομένα, όπου κάθε συναλλαγή είναι χαρακτηρισμένη ως κανονική ή απάτη [61].

Από την άλλη πλευρά, μη επιβλεπόμενες τεχνικές όπως η Cluster Analysis, οι Autoencoders και το Isolation Forests χρησιμοποιούνται όταν δεν υπάρχουν επαρκή επισημασμένα δεδομένα, επιτρέποντας τον εντοπισμό ασυνήθιστων συναλλαγών με βάση την απόκλισή τους από τα κανονικά πρότυπα [62],[63],[64].

Επιπλέον, υπάρχουν και ημι-επιβλεπόμενες και ενισχυτικές μέθοδοι [65], ενώ τεχνικές όπως η αντιμετώπιση της ανισορροπίας κλάσεων μέσω υπερδειγματοληψίας ή υποδειγματοληψίας είναι κρίσιμες για τη βελτίωση της απόδοσης των μοντέλων [66].

Συνολικά, τα μοντέλα είναι ικανά να μαθαίνουν και να εξελίσσονται, προσφέροντας μεγαλύτερη ακρίβεια, μειωμένα ψευδώς θετικές απάτες και προσαρμοστικότητα σε νέες μορφές απάτης, σε σχέση με τις παραδοσιακές προσεγγίσεις [67].

2.6.4 Χρήση Βαθιάς Μάθησης στον Εντοπισμό Απάτης

Η βαθιά μάθηση αποτελεί μια εξελιγμένη μορφή μηχανικής μάθησης, η οποία βασίζεται σε τεχνητά νευρωνικά δίκτυα πολλών επιπέδων. Χρησιμοποιείται όλο και περισσότερο στον εντοπισμό απάτης [68], κυρίως λόγω της ικανότητάς της να επεξεργάζεται μεγάλα και σύνθετα σύνολα δεδομένων, αποκαλύπτοντας μη προφανή μοτίβα και συσχετίσεις [69].

Συνηθισμένες αρχιτεκτονικές βαθιάς μάθησης [70] περιλαμβάνουν τα Deep Neural Networks (DNNs), τα Convolutional Neural Networks (CNNs) για ανάλυση χρονικών σειρών συναλλαγών και τα Recurrent Neural Networks (RNNs), ειδικά Long Short-Term Memory (LSTM), που είναι κατάλληλα για την αναγνώριση χρονικών εξαρτήσεων και ακολουθιακών

μοτίβων στις συναλλαγές ενός χρήστη. Επίσης, ένα βασικό πλεονέκτημα της βαθιάς μάθησης είναι η δυνατότητα αυτόματης εξαγωγής χαρακτηριστικών (feature extraction) [71], χωρίς την ανάγκη εκτενούς προεπεξεργασίας ή ανθρώπινης παρέμβασης, που έχει χρήση στην εύρεση διαφόρων περιπτώσεων απάτης [72].

Ωστόσο, η βαθιά μάθηση απαιτεί σημαντική υπολογιστική ισχύ και μεγάλες ποσότητες δεδομένων για να επιτύχει υψηλή απόδοση. Παρ' όλα αυτά, προσφέρει μεγάλη ακρίβεια και καλύτερη γενίκευση σε σύγκριση με τα συμβατικά μοντέλα μηχανικής μάθησης, ειδικά σε περιβάλλοντα με συνεχώς εξελισσόμενες απειλές [56], [73].

2.6.5 Κύριες Προκλήσεις

Παρά τις σημαντικές προόδους που έχουν επιτευχθεί μέσω της χρήσης τεχνικών μηχανικής και βαθιάς μάθησης για τον εντοπισμό απάτης, εξακολουθούν να υφίστανται αρκετές προκλήσεις και τεχνικά ζητήματα που περιορίζουν την αποτελεσματικότητα και την ευρεία εφαρμογή αυτών των συστημάτων [58].

Αρχικά, σε τυπικά σύνολα δεδομένων τραπεζικών συναλλαγών, τα περιστατικά απάτης αποτελούν ένα εξαιρετικά μικρό ποσοστό του συνολικού όγκου [74]. Αυτή η ανισορροπία καθιστά δύσκολη την εκπαίδευση ακριβών μοντέλων [75], καθώς πολλά αλγοριθμικά συστήματα τείνουν να υπερεκπροσωπούν την πλειοψηφική κλάση, αγνοώντας τις απάτες.

Ακόμη, η υπερβολική αυστηρότητα ενός μοντέλου μπορεί να οδηγήσει σε μεγάλο αριθμό ψευδώς θετικών ταξινομήσεων [76], προκαλώντας ενόχληση στους πελάτες [77] και αυξημένο λειτουργικό κόστος. Αντιστρόφως, η χαμηλή ευαισθησία οδηγεί σε ψευδώς αρνητικά ταξινομήσεις, δηλαδή σε πραγματικές απάτες που δεν εντοπίζονται έγκαιρα.

Επιπλέον, οι μορφές απάτης εξελίσσονται συνεχώς, με αποτέλεσμα τα στατικά μοντέλα να «ξεθωριάζουν» ως προς την ακρίβειά τους με την πάροδο του χρόνου [78]. Το φαινόμενο του concept drift απαιτεί την περιοδική επανεκπαίδευση ή την υιοθέτηση προσαρμοστικών μεθόδων [79].

Ακόμη ένα ζήτημα είναι πως τα ποιοτικά και επαρκώς επισημασμένα δεδομένα είναι συχνά περιορισμένα λόγω θεμάτων απορρήτου [80], εμπορικού ανταγωνισμού ή κόστους επισημείωσης, γεγονός που επηρεάζει την απόδοση κυρίως των επιβλεπόμενων μεθόδων [81].

Τέλος, τα πολύπλοκα μοντέλα και ιδιαίτερα αυτά της βαθιάς μάθησης, συχνά λειτουργούν ως «μαύρα κουτιά» και στερούνται επεξηγησιμότητας [82]. Αυτό δημιουργεί προβλήματα συμμόρφωσης με κανονιστικά πλαίσια όπως το GDPR [83], που απαιτούν διαφάνεια στις αποφάσεις που επηρεάζουν καταναλωτές [84].

2.6.6 Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Η ανίχνευση απάτης σε τραπεζικές συναλλαγές παραμένει ένα πεδίο εντατικής έρευνας [85], καθώς οι απειλές εξελίσσονται και οι απαιτήσεις για ακρίβεια, ταχύτητα και ερμηνευσιμότητα εντείνονται. Παρόλο που οι τεχνικές μηχανικής και βαθιάς μάθησης έχουν προσφέρει εντυπωσιακά αποτελέσματα, υφίστανται ακόμη σημαντικά ερευνητικά κενά και ανεξερεύνητες περιοχές.

- **Ανίχνευση Μη Επισημασμένων Μορφών Απάτης:** Οι περισσότερες μέθοδοι βασίζονται σε εποπτευόμενη μάθηση και προϋποθέτουν την ύπαρξη επισημασμένων παραδειγμάτων. Ωστόσο, νέες ή άγνωστες τεχνικές απάτης καθιστούν αναγκαία την ανάπτυξη μεθόδων μη εποπτευόμενης ή ημι-εποπτευόμενης μάθησης, που μπορούν να εντοπίζουν ανωμαλίες χωρίς επισημασμένα δεδομένα [86], [87].

- **Διαλειτουργικότητα των Συστημάτων:** Η απάτη μπορεί να εκδηλωθεί σε πολλαπλά επίπεδα (συναλλαγές, συσκευές, λογαριασμοί, γεωγραφικά σημεία). Μελλοντικές προσεγγίσεις οφείλουν να ενοποιούν ετερογενή δεδομένα από διαφορετικές πηγές [88] σε ένα ενιαίο πλαίσιο, αξιοποιώντας τεχνικές από το πεδίο των γραφημάτων (graph-based learning) και πολυτροπικών συστημάτων [89], [90].

- **Προσαρμογή σε Concept Drift σε Πραγματικό Χρόνο:** Αν και έχουν γίνει προσπάθειες για αντιμετώπιση του concept drift [91], [92], απαιτούνται ακόμη πιο ευέλικτα και αυτοπροσαρμοζόμενα μοντέλα που θα μπορούν να ανιχνεύουν και να ανταποκρίνονται σε αλλαγές στα πρότυπα απάτης σε πραγματικό χρόνο, χωρίς πλήρη επανεκπαίδευση.

- **Ανάπτυξη Συστημάτων Πρόβλεψης και Αντίδρασης:** Οι περισσότερες λύσεις επικεντρώνονται αποκλειστικά στην ανίχνευση. Ερευνητικά, αναδεικνύεται η ανάγκη για ανάπτυξη ολιστικών συστημάτων που όχι μόνο εντοπίζουν την απάτη, αλλά προτείνουν ενέργειες απόκρισης [93], [94], [95] (π.χ. μπλοκάρισμα συναλλαγής, ειδοποίηση, στατιστική μοντελοποίηση επιπτώσεων κτλπ.).

Κεφάλαιο 3

Dataset - Ανάλυση - Προεπεξεργασία και Χρήσιμα Συμπεράσματα

Στο κεφάλαιο αυτό αναλύεται το σύνολο δεδομένων που χρησιμοποιήθηκε για την την διπλωματική εργασία. Όπως και σε κάθε σύνολο δεδομένων καθοριστική σημασία διαδραματίζει η επεξεργασία που του γίνεται με σκοπό να έρθει στην κατάσταση που θα επιτρέψει να εξαχθούν χρήσιμα και αξιοποιήσιμα απο τους αλγορίθμους μηχανικής μάθησης. Αρχικά θα αναλυθούν τα χαρακτηρηστικά του και έπειτα θα γίνει μια βασική προεπεξεργασία ενώ παράλληλα θα παρουσιάζονται γραφήματα για τα θεμελιώδη χαρακτηριστικά του dataset, αναδεικνύοντας τα πιο ουσιώδη αποτελέσματα της ανάλυσης.

Το dataset ονομάζεται Credit Card Fraud Detection και ο σύνδεσμος του παρέχεται εδώ.

3.1 Χαρακτηριστικά του Dataset

Το σύνολο δεδομένων περιλαμβάνει συναλλαγές με πιστωτικές κάρτες που πραγματοποιήθηκαν από Ευρωπαίους κατόχους καρτών τον Σεπτέμβριο του 2013, μέσα σε διάστημα δύο ημερών. Περιέχει συνολικά 284.807 συναλλαγές, εκ των οποίων οι 492 είναι απάτες, γεγονός που καθιστά το σύνολο ιδιαίτερα μη ισορροπημένο (το ποσοστό απάτης είναι περίπου **0.172%** των συνολικών παρατηρήσεων.

Όλα τα χαρακτηριστικά του είναι αριθμητικά και έχουν προκύψει μέσω του μετασχηματισμού **PCA** για τα χαρακτηριστικά **V1-V28**, με εξαίρεση τα χαρακτηριστικά 'Time' και 'Amount'. Το 'Time' δηλώνει τα δευτερόλεπτα που έχουν παρέλθει από την πρώτη συναλλαγή, ενώ το 'Amount' αντιστοιχεί στο χρηματικό ποσό κάθε συναλλαγής. Η μεταβλητή-στόχος είναι το χαρακτηριστικό 'Class', το οποίο παίρνει τιμή 1 για συναλλαγή απάτης και 0 διαφορετικά.

Συνολικά, το dataset περιέχει τα επόμενα χαρακτηριστικά ακολουθούμενα απο τον τύπο τους:

- Time, int
- V1, float
- V2, float
- ..., float

- ..., float
- V26, float
- V28, float
- Amount, float
- Class, int

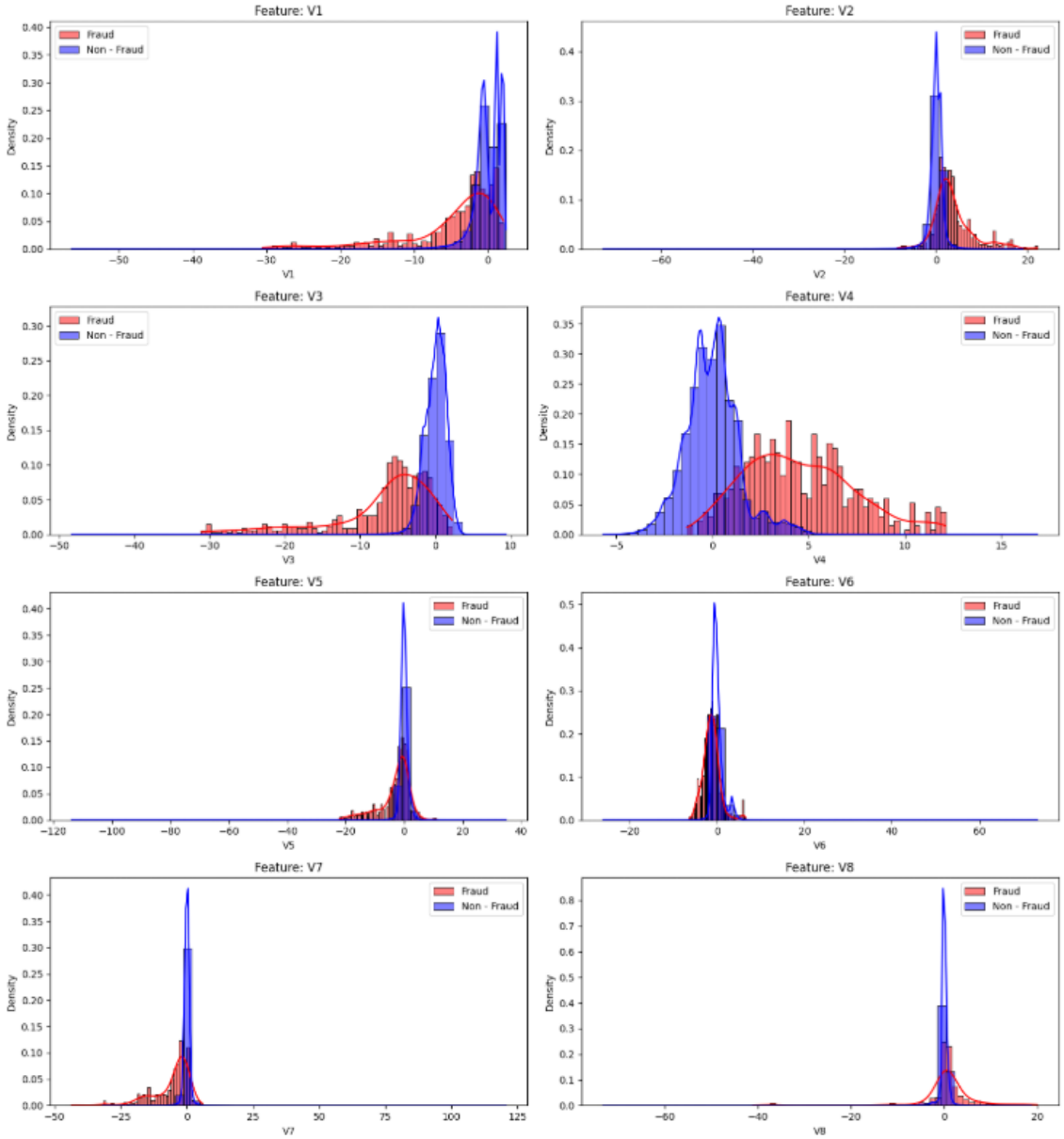
3.1.1 Χαρακτηριστικά V1-V28

Όπως αναφέρθηκε τα συγκεκριμένα χαρακτηριστικά είναι αποτέλεσμα μετασχηματισμού PCA, οπότε το εύρος των τιμών τους είναι πεπερασμένο. Καθώς το πρόβλημα είναι ταξινόμησης και παράλληλα υπάρχει και το πρόβλημα της τεράστιας διαφοράς ανάμεσα στις δυο πιθανές τιμές του χαρακτηριστικού Class, κρίνεται απαραίτητο να εντοπιστούν κατάλληλες οριοθετήσεις στον πολυδιάστατο χώρο των κύριων χαρακτηριστικών, προκειμένου να διευκολυνθεί ο διαχωρισμός των παρατηρήσεων απο τους αλγορίθμους. Κάτι τέτοιο δεν ειναι εύκολο, αφού όπως αναφέρθηκε το ποσοστό των απατών αγγίζει μόλις το **0.172%**.

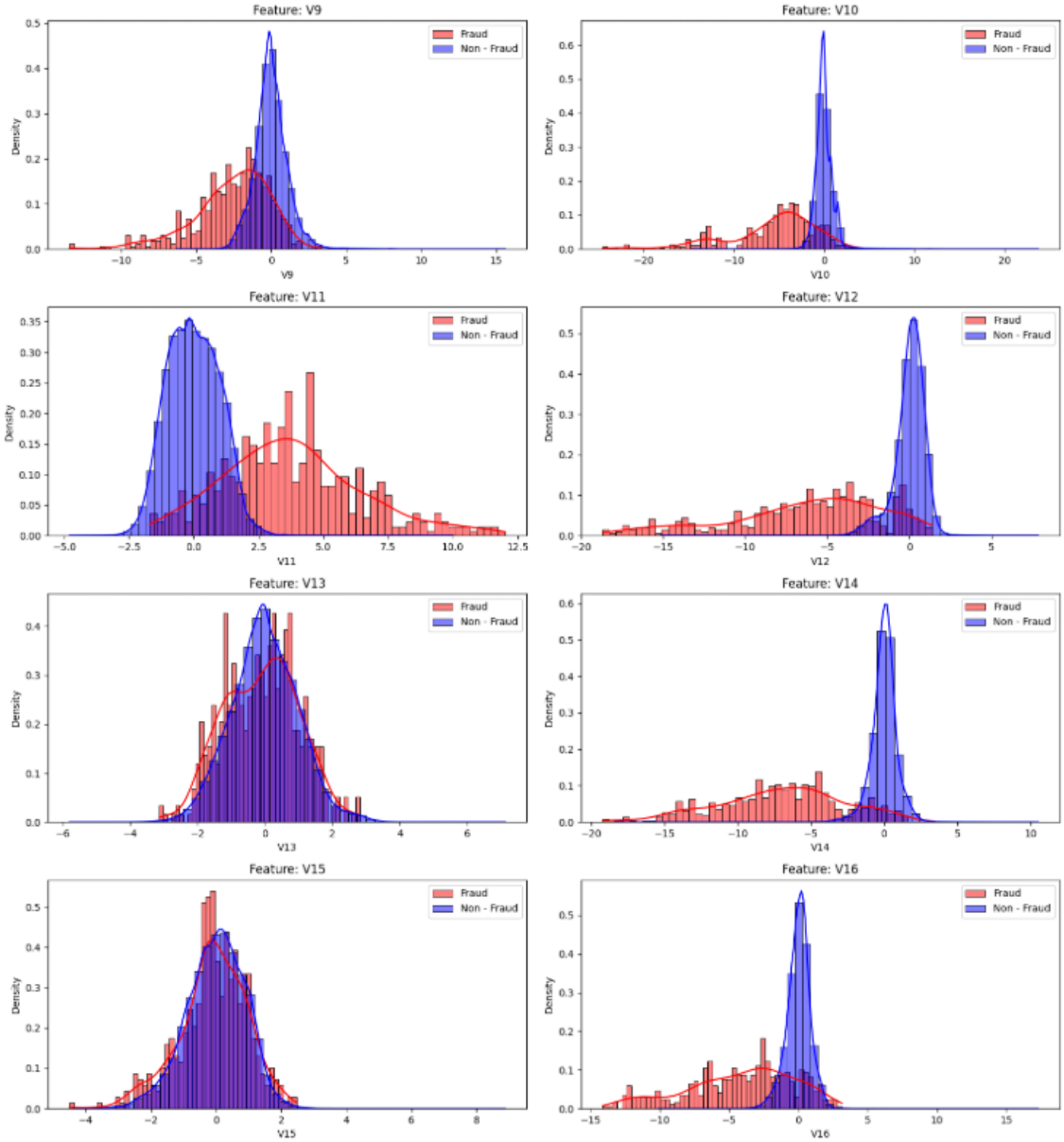
Η μέθοδος **KDE** χρησιμοποιήθηκε για να εκτιμηθεί και να οπτικοποιηθεί η κατανομή των χαρακτηριστικών V1–V28 χωριστά για τις δύο τιμές της μεταβλητής Class (Απάτες και μή απάτες). Λόγω της εξαιρετικά ανισοβαρούς φύσης του dataset, η απλή παρουσίαση αθροιστικών ιστογραμμάτων θα υποβάθμιζε την εμφάνιση των λιγοστών παρατηρήσεων απάτης.

Παρατηρώντας τις αντίστοιχες καμπύλες KDE, εντοπίζονται περιπτώσεις όπου οι δύο κατανομές αποκλίνουν σημαντικά, κάτι που υποδηλώνει την ύπαρξη διαχωριστικής πληροφορίας,που είναι κρίσιμο να χρησιμοποιηθεί για την επιλογή συγκεκριμένων χαρακτηριστικών που θα είναι η είσοδος των αλγορίθμων ταξινόμησης.

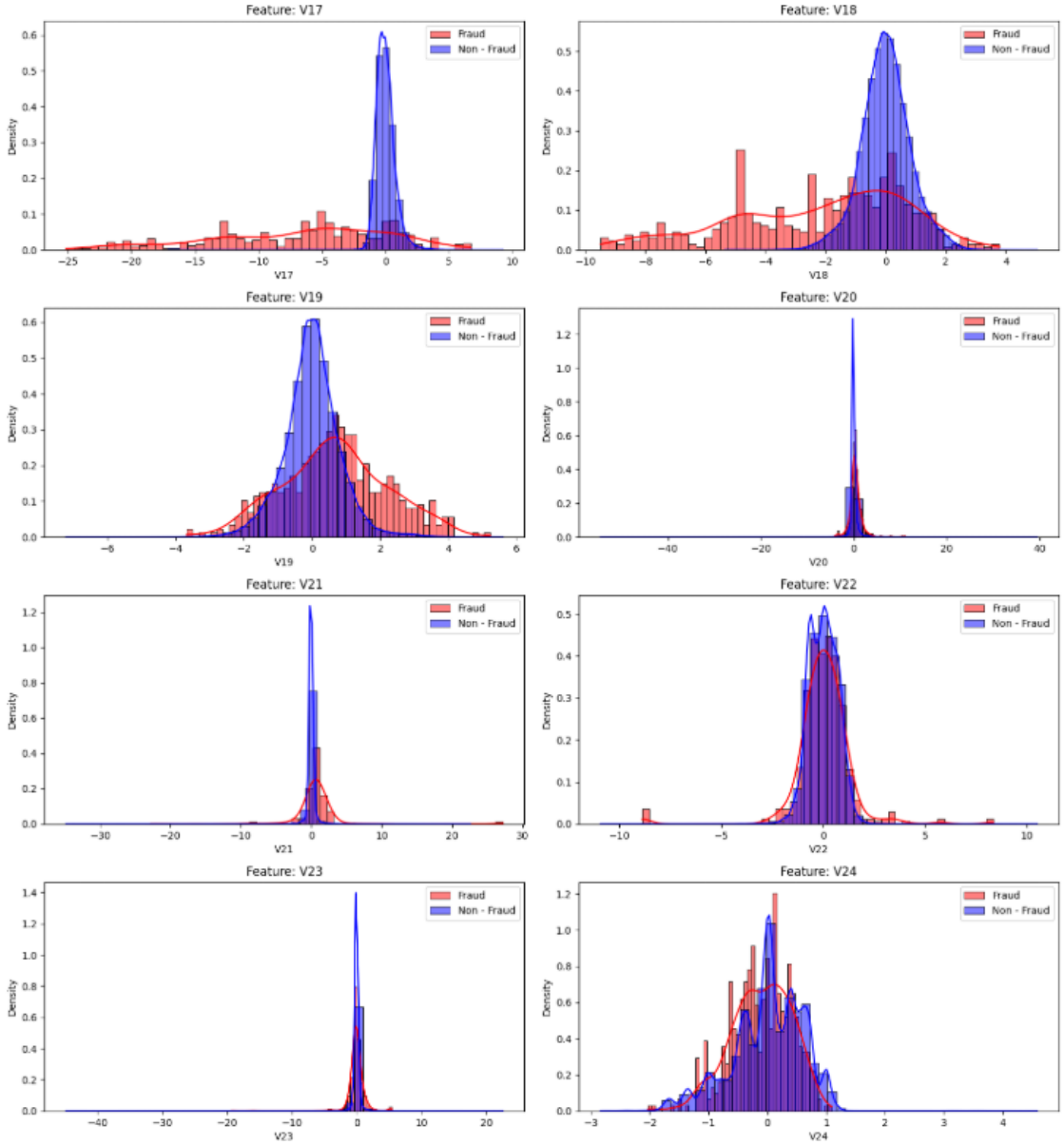
Τα γραφήματα που παρουσιάζονται στα σχήματα 3.1, 3.2, 3.3, 3.4 απεικονίζουν τις κατανομές των χαρακτηριστικών V1-V28, διαχωρίζοντας τις περιπτώσεις απάτης (fraud) και μη απάτης (non-fraud).



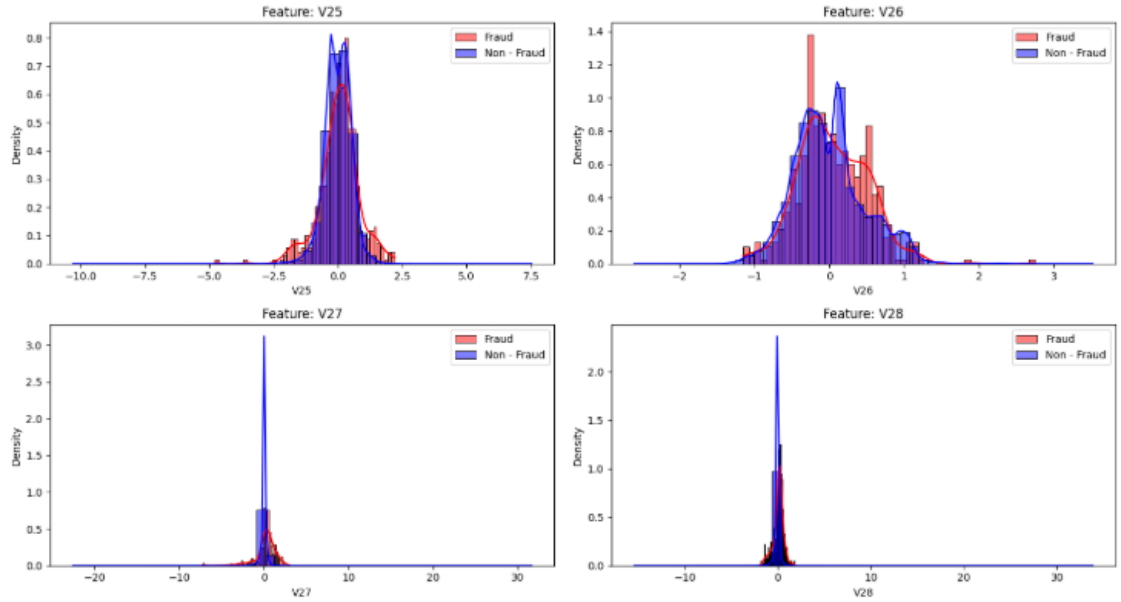
Σχήμα 3.1: *Κατανομές V1-V8*



Σχήμα 3.2: *Κατανομές V9-V16*



Σχήμα 3.3: *Κατανομές V17-V24*



Σχήμα 3.4: *Κατανομές V25-V28*

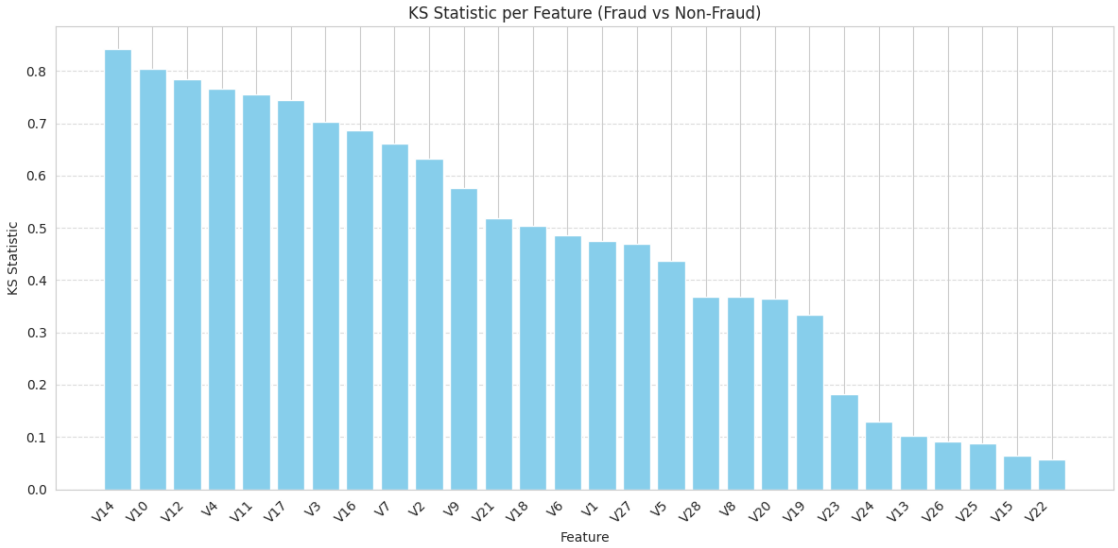
Από τις κατανομές φαίνεται πως για ορισμένα χαρακτηριστικά οι δύο κατανομές διαφέρουν σημαντικά, με λιγότερη επικάλυψη και μίξη μεταξύ τους. Αυτό υποδηλώνει ότι μπορούμε να εξάγουμε χρήσιμα συμπεράσματα και να διακρίνουμε καλύτερα τις δυο κλάσεις του dataset για αυτα τα χαρακτηριστικά.

Οι μέθοδοι Kolmogorov–Smirnov test, Jensen–Shannon divergence και Kullback–Leibler divergence παρέχουν ένα μαθηματικό πλαίσιο για την ποσοτικοποίηση των διαφορών μεταξύ των κατανομών των χαρακτηριστικών στις δύο κλάσεις (fraud και non-fraud). Σε αντίθεση με την οπτική εκτίμηση μέσω των καμπυλών πυκνότητας KDE, οι τεχνικές αυτες μετατρέπουν την ποιοτική αλλά οπτική παρατήρηση σε συγκεκριμένους αριθμητικούς δείκτες, οι οποίοι αντικατοπτρίζουν την απόκλιση ή την αμοιβαία πληροφορία μεταξύ των κατανομών. Συγκεκριμένα, εφαρμόστηκαν οι επόμενες μέθοδοι:

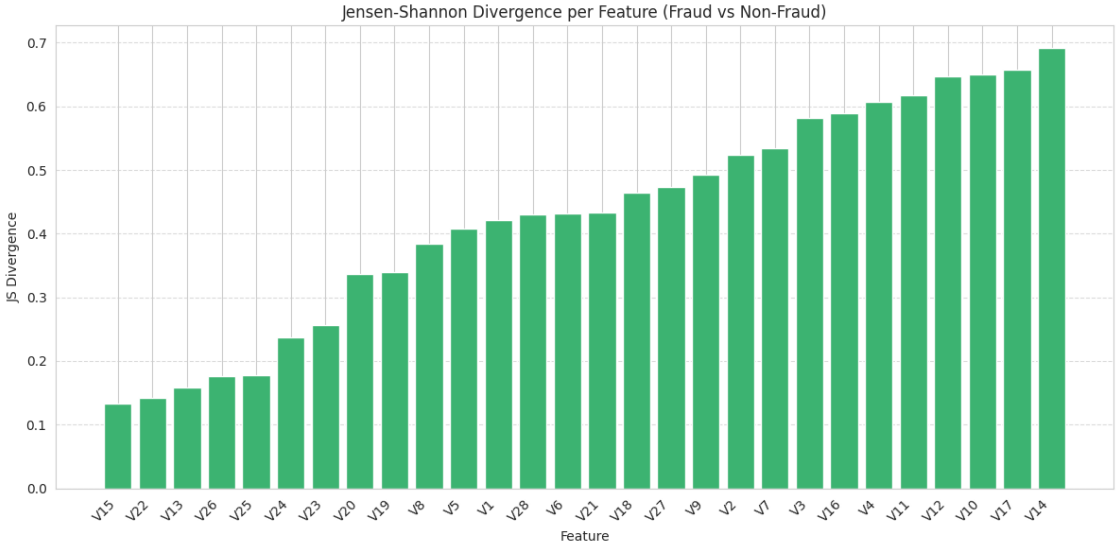
- Το Kolmogorov–Smirnov test για να εξεταστεί η στατιστική απόκλιση μεταξύ των κατανομών των δύο κλάσεων.

- Η Jensen–Shannon divergence και η Kullback–Leibler divergence ως μέτρα πληροφορίας για την ποσοτικοποίηση της διαφοράς μεταξύ των κατανομών των δύο κλάσεων.

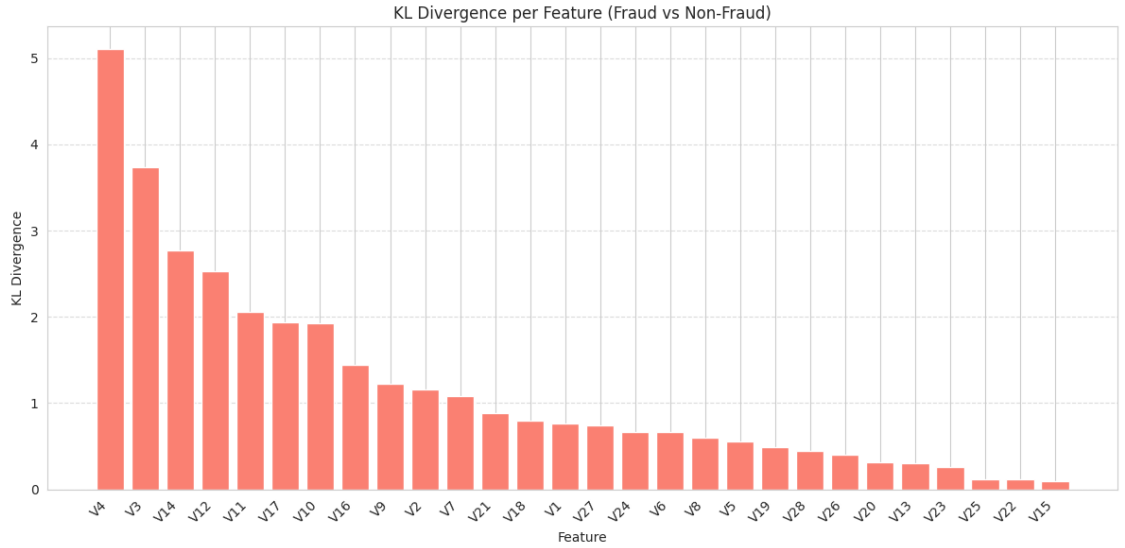
Τα γραφήματα που παρουσιάζονται στα Σχήματα 3.5, 3.6 και 3.7 απεικονίζουν τα αποτελέσματα των μεθόδων Kolmogorov–Smirnov test, Jensen–Shannon divergence και Kullback–Leibler divergence για τα χαρακτηριστικά V1–V28, διαχωρίζοντας τις περιπτώσεις απάτης (fraud) και μη απάτης (non-fraud).



Σχήμα 3.5: *Αποτελέσματα Kolmogorov-Smirnov test για τις V1-V28*



Σχήμα 3.6: *Αποτελέσματα Jensen-Shannon divergence για τις V1-V28*



Σχήμα 3.7: *Αποτελέσματα Kullback-Leibler divergence για τις V1-V28*

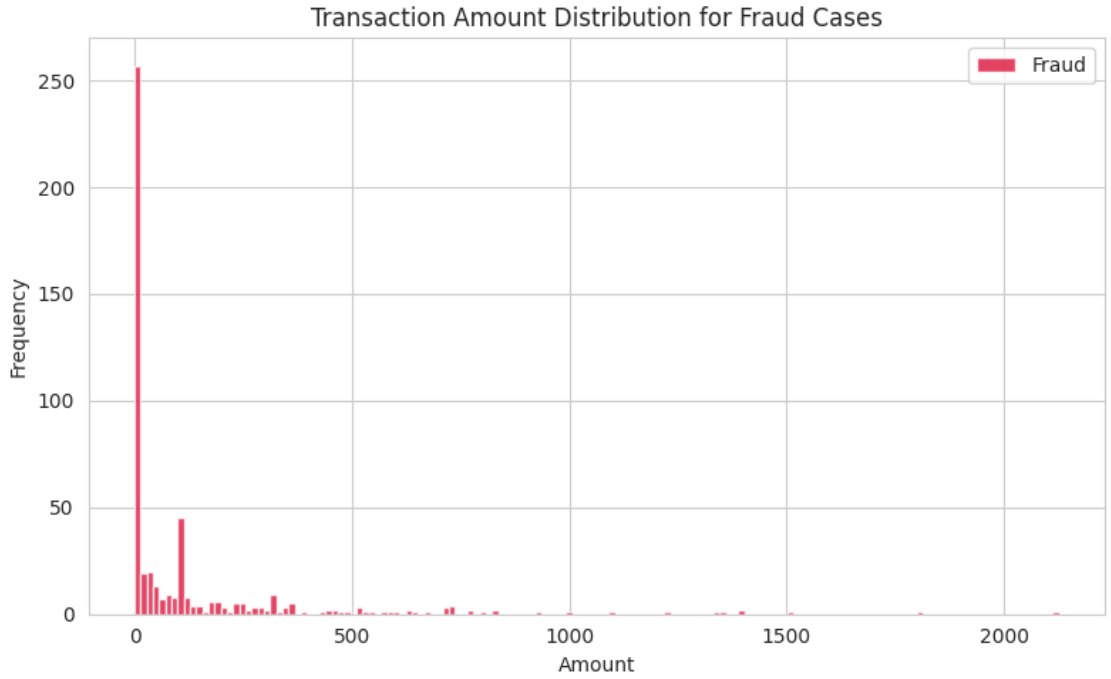
Όσο πιο μεγάλη είναι η τιμή στο Kolmogorov–Smirnov test, τόσο πιο πολύ διαφέρουν οι δυο κατανομές των κλάσεων απάτης και μη-απάτης για το κάθε χαρακτηριστικό. Κατα τον ίδιο τρόπο, στις Jensen–Shannon divergence και Kullback–Leibler divergence, όσο μεγαλύτερη είναι η τιμή, τόσο μεγαλύτερη είναι η απόκλιση μεταξύ των δύο κατανομών, δηλαδή οι κατανομές διαφέρουν περισσότερο. Συνεπώς, υψηλές τιμές στις μετρικές αυτές υποδεικνύουν μεγαλύτερη διαχωριστική ικανότητα του αντίστοιχου χαρακτηριστικού μεταξύ των κλάσεων απάτης και μη-απάτης.

Βάσει της ανάλυσης που προέκυψε από τις τρεις μεθόδους (Kolmogorov–Smirnov test, Jensen–Shannon divergence και Kullback–Leibler divergence) και την αντίστοιχη απεικόνιση των γραφημάτων τους, επιλέχθηκαν προς απόρριψη απο την πειραματική διαδικασία χαρακτηριστικά που παρουσίασαν τη μικρότερη διαχωριστική ικανότητα μεταξύ των κλάσεων. Συγκεκριμένα, τα χαρακτηριστικά **V22, V15, V25, V26, V13, V24 και V23** αφαιρέθηκαν από το σύνολο δεδομένων, καθώς παρέχουν λιγότερη χρήσιμη πληφορορία.

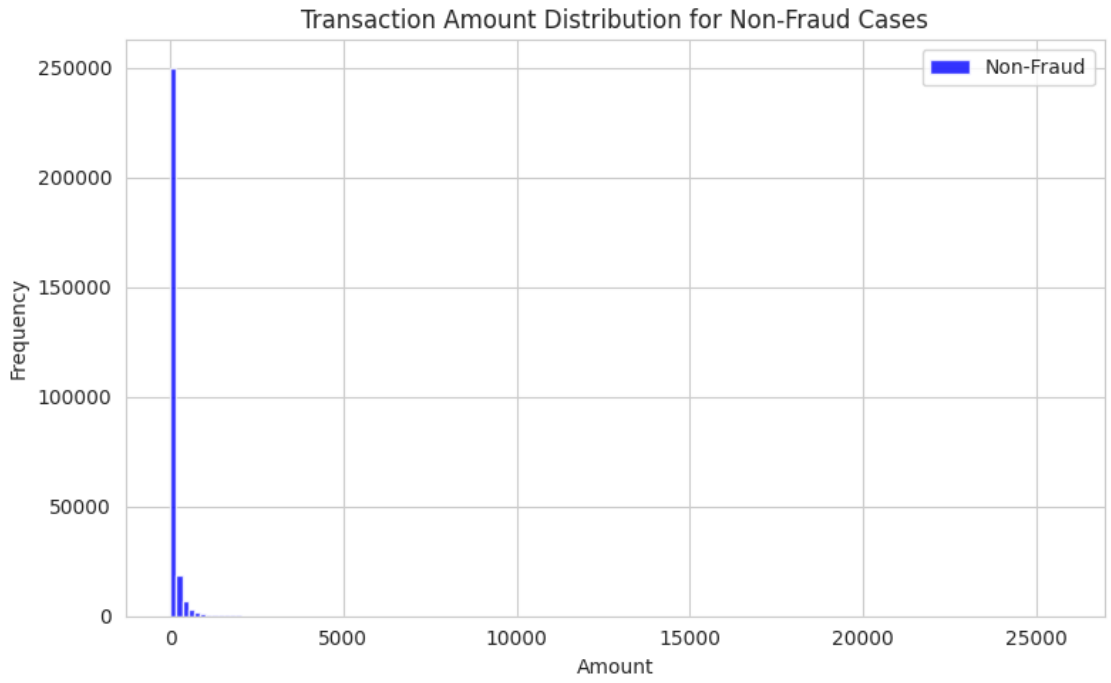
3.1.2 Χαρακτηριστικά Time και Amount

Το χαρακτηριστικό Time είναι ο αύξοντας αριθμός της κάθε συναλλαγής οπότε δεν αποτελεί χρήσιμο μέτρο για την διαχώριση των δυο κλάσεων. Αντίθετα, το χαρακτηριστικό Amount δείχνει το ποσό της κάθε συναλλαγής και είναι ικανό να βοηθήσει τους αλγόριθμους μηχανικής μάθησης.

Στα σχήματα 3.8 και 3.9 απεικονίζονται τα ιστογράμματα των δυο κλάσεων για το χαρακτηριστικό Amount.



Σχήμα 3.8: *Ιστόγραμμα για το χαρακτηριστικό Amount για τις απάτες*

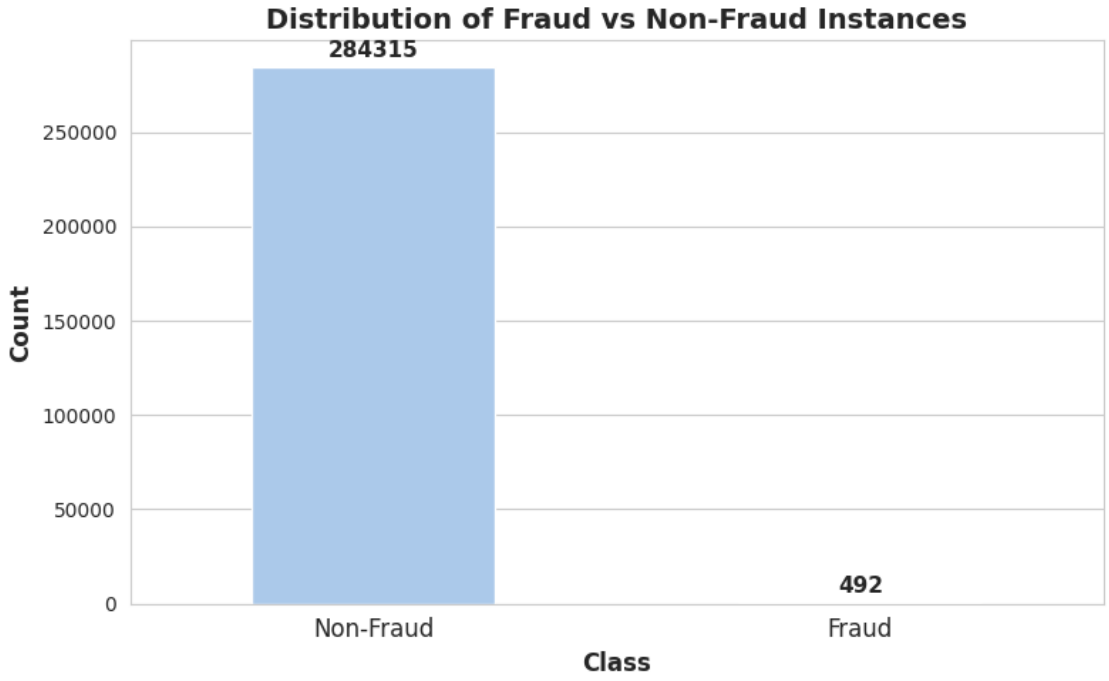


Σχήμα 3.9: *Ιστόγραμμα για το χαρακτηριστικό Amount για τις μη-απάτες*

Από τα δύο σχήματα παρατηρείται ότι το χαρακτηριστικό Amount παρουσιάζει διαφορετική κατανομή ανάμεσα στις δύο κλάσεις. Συγκεκριμένα, στις περιπτώσεις απάτης, οι τιμές του Amount συγκεντρώνονται σε ένα σχετικά στενό εύρος, περίπου μεταξύ $[0, 1500]$. Αντίθετα, στις μη-απάτες, το εύρος του Amount είναι αισθητά μεγαλύτερο, γεγονός που υποδηλώνει διαφορετικά πρότυπα συναλλαγών μεταξύ των δύο κατηγοριών.

3.1.3 Χαρακτηριστικό Class

Το χαρακτηριστικό-στόχος Class είναι δυαδικό και παρουσιάζει έντονη ανισορροπία μεταξύ των δύο κατηγοριών του. Στο Σχήμα 3.10 απεικονίζεται η κατανομή της μεταβλητής μέσω ραβδογράμματος, από το οποίο γίνεται εμφανές ότι η μεγάλη πλειοψηφία των δειγμάτων ανήκει στην κατηγορία μη-απάτης (Class = 0), ενώ οι περιπτώσεις απάτης (Class = 1) είναι εξαιρετικά περιορισμένες. Το σχήμα επιβεβαιώνει την ανισορροπία της κλάσης και καθιστά σαφές ότι απαιτείται η κατάλληλη μεταχείριση του προβλήματος ως μη ισοβαρούς ταξινόμησης.



Σχήμα 3.10: *Ραβδόγραμμα τιμών για το χαρακτηριστικό Class*

3.2 Προεπεξεργασία Δεδομένων

Η προεπεξεργασία του συνόλου δεδομένων αποτελεί κρίσιμο στάδιο, προκειμένου να βελτιωθεί η απόδοση των αλγορίθμων μηχανικής μάθησης και να εξασφαλιστεί η αξιοπιστία των αποτελεσμάτων.

1. **Αφαίρεση χαρακτηριστικών με περιορισμένη διαχωριστική ικανότητα**
   Με βάση την ανάλυση που παρουσιάστηκε στην παράγραφο 3.1.1 και την ποσοτικοποίηση των διαφορών μεταξύ των κατανομών των δύο κλάσεων μέσω των μεθόδων Kolmogorov–Smirnov test, Jensen–Shannon divergence και Kullback–Leibler divergence, επιλέχθηκαν προς απόρριψη τα χαρακτηριστικά **V22, V15, V25, V26, V13, V24 και V23**. Τα εν λόγω χαρακτηριστικά παρουσίασαν ελάχιστη διακριτική ικανότητα, καθιστώντας την αφαίρεσή τους επιβεβλημένη ώστε να περιοριστεί η διάσταση του χώρου χαρακτηριστικών και να μειωθεί ο θόρυβος των δεδομένα.

2. **Αφαίρεση του χαρακτηριστικού Time**
   Το χαρακτηριστικό Time, το οποίο αντιστοιχεί στον χρόνο που έχει παρέλθει από την πρώτη καταγεγραμμένη συναλλαγή, κρίθηκε μη χρήσιμο για την ταξινόμηση καθώς δεν φέρει πληροφορίας σχετικής με την πιθανότητα απάτης. Συνεπώς, εξαιρέθηκε από το τελικό σύνολο χαρακτηριστικών.

3. **Έλεγχος πληρότητας δεδομένων**
   Κατά τον έλεγχο των δεδομένων δεν εντοπίστηκαν ελλιπείς ή μη διαθέσιμες τιμές, επομένως δεν απαιτήθηκε καμία επιπλέον ενέργεια συμπλήρωσης ή διόρθωσης.

4. **Κανονικοποίηση του χαρακτηριστικού Amount και των V1-V28**
   Το χαρακτηριστικα Amount και V1-V28 παρουσιάζουν σημαντική διακύμανση στις τιμές τους, γεγονός που θα μπορούσε να επηρεάσει αρνητικά την εκπαίδευση των αλγορίθμων λόγω διαφοράς της κλίμακας με τα υπόλοιπα χαρακτηριστικά. Για το λόγο αυτό, εφαρμόστηκε μετασχηματισμός κανονικοποίησης με χρήση της μεθόδου StandardScaler, ο οποίος αποσκοπεί στη μετατροπή των τιμών ώστε να έχουν μέση τιμή μηδέν και τυπική απόκλιση μονάδα, καθιστώντας το κάθε χαρακτηριστικό συγκρίσιμο με τα υπόλοιπα.

5. **Διαχωρισμός δεδομένων**
   Για την αξιολόγηση των αλγορίθμων ταξινόμησης, τα δεδομένα χωρίστηκαν σε σύνολα εκπαίδευσης, ελέγχου και επικύρωσης. Συγκεκριμένα, το 80% των δεδομένων χρησιμοποιήθηκε για εκπαίδευση, ενώ το υπόλοιπο 20% διατέθηκε για έλεγχο. Τέλος, το 10% διαχωρίστηκε περαιτέρω ως σύνολο επικύρωσης, το οποίο χρησιμοποιήθηκε για την παραμετροποίηση και την αποφυγή υπερπροσαρμογής των μοντέλων.

Κεφάλαιο 4

Ανάλυση και Σχεδίαση Πειραματικών Μεθόδων

Η πειραματική αξιολόγηση αποτελεί βασικό στάδιο στην ανάπτυξη και τεκμηρίωση μεθόδων ανίχνευσης απάτης, ιδίως όταν τα δεδομένα παρουσιάζουν έντονο πρόβλημα ανισορροπίας μεταξύ των κατηγοριών. Στο κεφάλαιο αυτο περιγράφεται η μεθοδολογική προσέγγιση που ακολουθήθηκε για την προετοιμασία των δεδομένων, την εφαρμογή τεχνικών επαναδειγματοληψίας (sampling) και την επιλογή των διαφορετικών ταξινομητών και των μετρικών αξιολόγησης που επιλέχθηκαν.

4.1 Τεχνικές Επαναδειγματοληψίας

Για την αντιμετώπιση της ανισορροπίας, εφαρμόστηκαν οι εξής τεχνικές:

4.1.1 Random Undersampling

Η τεχνική αυτή αφαιρεί τυχαία δείγματα από την πλειοψηφική κατηγορία (non-fraud), ώστε να μειωθεί το πλήθος της και να προσεγγίσει εκείνο της μειοψηφικής (fraud). Εξετάστηκαν δύο παραλλαγές:

- **Αναλογία 1:10**: η κατηγορία fraud έχει το 10% των δειγμάτων της non-fraud — μειωμένη ανισορροπία, ώστε να βελτιωθεί η εκπαίδευση χωρίς να αλλοιωθεί πολύ η κατανομή.
- **Αναλογία 1:20**: η κατηγορία fraud έχει το 5% των δειγμάτων της non-fraud — διατηρείται πιο έντονη ανισορροπία για περιορισμό υπερπροσαρμογής.

4.1.2 Random Oversampling

Σε αυτήν την περίπτωση, δημιουργούνται συνθετικά αντίγραφα δειγμάτων από την κατηγορία φραυδ, ώστε να αυξηθεί η παρουσία της στο σύνολο εκπαίδευσης. Εξετάστηκαν και εδώ οι ίδιες δύο αναλογίες:

- **Αναλογία 1:10**: η κλάση fraud ενισχύεται ώστε να αποτελεί το 10% της non-fraud — σημαντική αύξηση, χωρίς πλήρη εξισορρόπηση.
- **Αναλογία 1:20**: η κλάση fraud ενισχύεται πιο μετρημένα, στο 5% της non-fraud — διατηρείται η φυσική ανισορροπία με μικρή βελτίωση στην εκπροσώπηση.

Είναι σημαντικό, μετά την επαναδειγματοληψία, η κατανομή των τιμών του χαρακτηριστικού Class να παραμένει αντιπροσωπευτική της επιθυμητής αναλογίας, καθώς οποιαδήποτε αυθαίρετη μεταβολή μπορεί να οδηγήσει σε αλλοίωση της πληροφορίας και να επηρεάσει την αξιοπιστία του μοντέλου. Προφανώς και η αναλογία αλλάζει απο την αρχική κατανομή για να μπορούν οι ταξινομητές να συγκλίνουν, αλλά στόχος είναι οι επιλεγμένες αναλογίες να είναι μια χρυσή τομή μεταξύ των διαθέσιμων επιλογών. Κάθε μέθοδος επαναδειγματοληψίας εφαρμόστηκε ανεξάρτητα και συνδυάστηκε με όλους τους υπό εξέταση αλγορίθμους.

4.2 Επιλεγμένοι Αλγόριθμοι Μηχανικής Μάθησης

Η επιλογή των αλγορίθμων βασίστηκε σε κριτήρια όπως η απόδοσή τους σε προβλήματα ανισόρροπων δεδομένων, η ευκολία εκπαίδευσης και η ερμηνευσιμότητα.

4.2.1 Πολυεπίπεδο Νευρωνικό Δίκτυο (MLP)

Το MLP (Multi-Layer Perceptron) αποτελεί έναν τύπο πλήρως συνδεδεμένου τεχνητού νευρωνικού δικτύου, κατάλληλο για προβλήματα ταξινόμησης. Στην συγκεκριμένη μεθοδολογία, χρησιμοποιήθηκε με τρία κρυφά στρώματα και τη συνάρτηση ενεργοποίησης ReLU, ενω εκπαιδεύτηκε για 6 εποχές με τον βελτιστοποιητή Adam.

4.2.2 Random Forest Classifer

Πρόκειται για έναν ensemble αλγόριθμο βασισμένο σε πολλαπλά δέντρα απόφασης, όπου η τελική απόφαση προκύπτει μέσω πλειοψηφίας. Ο Random Forest είναι ανθεκτικός στο overfit και μπορεί να διαχειριστεί καλά ετερογενή δεδομένα, όμως η απόδοσή του επηρεάζεται σε περιπτώσεις μεγάλης ανισορροπίας. Η υπερπαράμετρος estimators είναι ίση με 100, που δείχνει τον αριθμό των δέντρο μέσα στο δάσος.

4.2.3 Balanced Random Forest Classifier

Αποτελεί μια παραλλαγή του Ρανδομ Φορεστ, η οποία ενσωματώνει τεχνικές υποδειγματοληψίας κατά την εκπαίδευση κάθε δέντρου. Συγκεκριμένα, κάθε δέντρο εκπαιδεύεται με ισορροπημένο υποσύνολο δεδομένων, καθιστώντας τον αλγόριθμο καταλληλότερο για ανισόρροπα σύνολα. Η υπερπαράμετρος estimators είναι ίση με 100 και σε αυτον τον αλγόριθμο.

4.2.4 Isolation Forest

Ο συγκεκριμένος αλγόριθμος είναι unsupervised και βασίζεται στην αρχή ότι οι ανωμαλίες, όπως οι περιπτώσεις απάτης, μπορούν να «απομονωθούν» πιο εύκολα από τις κανονικές παρατηρήσεις. Χρησιμοποιεί δέντρα που τυχαία χωρίζουν το χώρο των χαρακτηριστικών, και η μέση διαδρομή απομόνωσης υποδεικνύει τη «σπανιότητα» ενός δείγματος.

Ο αλγόριθμος ανιχνεύει ανωμαλίες βασισμένος στην ιδέα ότι οι περιπτώσεις απάτης είναι «σπάνιες» και απομονώνονται πιο εύκολα από τα κανονικά δεδομένα. Οι τεχνικές επαναδειγματοληψίας, όπως το undersampling ή το oversampling, αλλάζουν την κατανομή των

κατηγοριών στο dataset, με σκοπό να βοηθήσουν τους εποπτευόμενους αλγορίθμους που χρειάζονται ισορροπημένα δεδομένα. Όμως, επειδή ο αλγόριθμος δεν χρησιμοποιεί τις ετικέτες, οποιαδήποτε τέτοια αλλαγή θα αλλοίωνε τη φυσική κατανομή των δεδομένων και για αυτόν τον λόγο χρησιμοποιείται μόνο στο αρχικό dataset.

4.3 Μετρικές Αξιολόγησης

Η αξιολόγηση των ταξινομητών πραγματοποιήθηκε με βάση συγκεκριμένες μετρικές που ανταποκρίνονται στις ιδιαιτερότητες του προβλήματος ανίχνευσης απάτης. Δεδομένου ότι το σύνολο δεδομένων που χρησιμοποιείται παρουσιάζει ισχυρή ανισορροπία μεταξύ των τάξεων (fraud / non-fraud), η χρήση του ποσοστού ορθής ταξινόμησης (accuracy) ως βασική μετρική αξιολόγησης είναι ανεπαρκής.

Συγκεκριμένα, ένας ταξινομητής που προβλέπει όλες τις συναλλαγές ως **μη απάτες** μπορεί να επιτύχει πολύ υψηλό accuracy, χωρίς όμως να εντοπίζει καθόλου τις περιπτώσεις απάτης, κάτι που καθιστά την εν λόγω μετρική παραπλανητική στο πλαίσιο του προβλήματος.

Για τον λόγο αυτό, δόθηκε έμφαση στη μετρική **Recall** της κατηγορίας fraud, η οποία εκφράζει το ποσοστό των πραγματικών περιπτώσεων απάτης που ανιχνεύτηκαν επιτυχώς από το μοντέλο. Η μετρική αυτή είναι ιδιαίτερα σημαντική καθώς ο κύριος στόχος της διπλωματικής εργασίας είναι η μέγιστη δυνατή ανίχνευση των περιπτώσεων απάτης, ακόμη και με κόστος την αύξηση των περιπτώσεων που μια κανονική συναλλαγή ταξινομείται σαν απάτη. Οπότε, όσο μεγαλύτερη είναι η τιμή του Recall, τόσο λιγότερες απάτες «χάνονται» από το μοντέλο.

Συνοπτικά, οι διαθέσιμες κατηγορίες που μπορούν να ταξινομηθούν τα παραδείγματα που επεξεργάζεται ο κάθε αλγόριθμος είναι οι εξής:

- **TP (True Positives)**: Απάτες που ανιχνεύθηκαν σωστά.
- **TN (True Negatives)**: Κανονικές συναλλαγές που προβλέφθηκαν σωστά.
- **FP (False Positives)**: Κανονικές συναλλαγές που προβλέφθηκαν λανθασμένα ως απάτες.
- **FN (False Negatives)**: Απάτες που δεν ανιχνεύθηκαν από το μοντέλο.

Ο confusion matrix (πίνακας σύγχυσης) είναι ένας πίνακας που χρησιμοποιείται για να αξιολογήσει την απόδοση ενός αλγορίθμου ταξινόμησης. Δείχνει πόσες φορές οι προβλέψεις του μοντέλου ταιριάζουν ή διαφέρουν από τις πραγματικές ετικέτες των παραδειγμάτων.

Δομή του πίνακα:

Πίνακας 4.1: *Πίνακας σύγχυσης για την ταξινόμηση κανονικών συναλλαγών και απατών*

	Προβλεπόμενες Κανονικές	Προβλεπόμενες Απάτες
Πραγματικές Κανονικές	TN	FP
Πραγματικές Απάτες	FN	TP

Για το συγκεκριμένο πρόβλημα, σκοπός είναι η μεγιστοποίηση των True Positive παραδειγμάτων, δηλαδή τον πραγματικών απατών που ταξινομήθηκαν σωστά ως απάτες.

4.3.1 Παραλλαγές Μετρικών

Weighted Average: Υπολογίζει τον μέσο όρο των μετρικών, σταθμισμένο με βάση το πλήθος δειγμάτων κάθε κατηγορίας. Είναι χρήσιμο για να εκτιμηθεί η συνολική απόδοση του μοντέλου, αλλά ευνοεί την κυρίαρχη τάξη.

Macro Average: Υπολογίζει τον απλό μέσο όρο των μετρικών ανά κατηγορία, χωρίς στάθμιση. Είναι ιδιαίτερα χρήσιμο για να αξιολογηθεί η απόδοση σε κάθε κατηγορία εξίσου, ακόμα και σε προβλήματα ανισορροπίας.

Στα πλαίσια της εργασίας, η **macro average** παραλλαγή χρησιμοποιείται κατά τη φάση της βελτιστοποίησης και της επιλογής μοντέλων, προκειμένου να διασφαλιστεί ότι το μοντέλο δεν παραμελεί τη μειοψηφική κατηγορία (απάτη).

4.4 Ροή Πειραματικής Διαδικασίας

Η γενική ροή των πειραμάτων περιλαμβάνει τα εξής στάδια:

- **Στάδιο 1**: Εφαρμογή μεθόδου δειγματοληψίας.
- **Στάδιο 2**: Διαχωρισμός σε δεδομένα εκπαίδευσης/ελέγχου και επικύρωσης.
- **Στάδιο 3**: Εκπαίδευση μοντέλου με έναν από τους ταξινομητές.
- **Στάδιο 4**: Αξιολόγηση των αποτελεσμάτων στο σύνολο ελέγχου.

Ως **σημείο αναφοράς**, εξετάστηκε και η απόδοση κάθε αλγορίθμου στο αρχικό, ανισόρροπο dataset, χωρίς καμία τεχνική επαναδειγματοληψίας. Αυτή η επιλογή επιτρέπει την αντικειμενική σύγκριση των μεθόδων, ώστε να αποτιμηθεί το κατά πόσο και ποιες τεχνικές επαναδειγματοληψίας βελτιώνουν την ικανότητα εντοπισμού των περιπτώσεων απάτης.

Πίνακας 4.2: *Συνδυασμοί μεθόδου επαναδειγματοληψίας και ταξινομητή ανά πείραμα*

Πείραμα	Μέθοδος	Ταξινομητής
1	Χωρίς επαναδειγματοληψία	MLP
2	Χωρίς επαναδειγματοληψία	Random Forest
3	Χωρίς επαναδειγματοληψία	Balanced Random Forest
4	Χωρίς επαναδειγματοληψία	Isolation Forest
5	Random Oversampling 1/10	MLP
6	Random Oversampling 1/10	Random Forest
7	Random Oversampling 1/10	Balanced Random Forest
8	Random Oversampling 1/20	MLP
9	Random Oversampling 1/20	Random Forest
10	Random Oversampling 1/20	Balanced Random Forest
11	Random Undersampling 1/10	MLP
12	Random Undersampling 1/10	Random Forest
13	Random Undersampling 1/10	Balanced Random Forest
14	Random Undersampling 1/20	MLP
15	Random Undersampling 1/20	Random Forest
16	Random Undersampling 1/20	Balanced Random Forest

Κεφάλαιο 5

Πειραματική Διαδικασία

Η πειραματική διαδικασία αποτελεί το βασικότερο στάδιο αξιολόγησης της αποτελεσματικότητας των επιλεγμένων αλγορίθμων και των τεχνικών επεξεργασίας και επαναδειγματοληψίας τους για το συγκεκριμένο σύνολο δεδομένων. Στόχος του κεφαλαίου είναι να παρουσιαστούν αναλυτικά τα αποτελέσματα των πειραμάτων που πραγματοποιήθηκαν, καθώς και να αναδειχθούν οι συνδυασμοί με τις καλύτερες επιδόσεις στο πρόβλημα ανίχνευσης απάτης.

Όπως έχει ήδη αναλυθεί στο προηγούμενο κεφάλαιο, χρησιμοποιήθηκαν τέσσερις αλγόριθμοι μηχανικής μάθησης και δύο βασικές τεχνικές επαναδειγματοληψίας, σε διαφορετικές αναλογίες. Επιπλέον, συμπεριλήφθηκε ένα βασικό σενάριο, στο οποίο δεν εφαρμόστηκε καμία τεχνική εξισορρόπησης, ώστε να υπάρξει αντικειμενικό σημείο σύγκρισης για την αξιολόγηση της επίδρασης των μεθόδων επαναδειγματοληψίας.

Το κεφάλαιο περιγράφει τη διαδικασία εκπαίδευσης και αξιολόγησης των μοντέλων για κάθε πιθανό συνδυασμό επαναδειγματοληψίας–αλγορίθμου, παρουσιάζει τα αποτελέσματα βάσει των μετρικών που αναφέρθηκαν στο 4.3, και καταλήγει σε μία ποιοτική και ποσοτική σύγκριση των διαφορετικών προσεγγίσεων, εστιάζοντας κυρίως στην ικανότητα εντοπισμού των πραγματικών περιπτώσεων απάτης απο κάθε πείραμα.

5.1 Εκπαίδευση και Αξιολόγηση Μοντέλων

Για κάθε συνδυασμό τεχνικής επαναδειγματοληψίας και αλγορίθμου ταξινόμησης, εκπαιδεύτηκαν ξεχωριστά μοντέλα, με χρήση σταθερού συνόλου ελέγχου ώστε να διασφαλιστεί η συγκρισιμότητα των αποτελεσμάτων. Οι πειραματισμοί πραγματοποιήθηκαν στο αρχικό σύνολο δεδομένων, μετά από κατάλληλη προεπεξεργασία και διαχωρισμό σε σύνολο εκπαίδευσης, ελέγχου και επικύρωσης, με τυπική αναλογία 80-20-10.

Οι τεχνικές επαναδειγματοληψίας εφαρμόζονταν μόνο στο σύνολο εκπαίδευσης, ώστε να μην επηρεαστεί η αντικειμενικότητα της τελικής αξιολόγησης. Για κάθε ταξινομητή, εκπαιδεύτηκε μοντέλο τόσο στο αρχικό, μη ισορροπημένο σύνολο, που αποτελεί την βασική απόδοση που μπορεί να επιτευχθεί, όσο και στα επαναδειγματοληπτικά σύνολα, με όλες τις δυνατές παραλλαγές. Ο αλγόριθμος Isolation Forest, λόγω του unsupervised χαρακτήρα του, χρησιμοποιήθηκε αποκλειστικά στο βασικό πείραμα, καθώς η λογική του δεν ευνοεί επεμβάσεις μέσω επαναδειγματοληψίας.

Η αξιολόγηση των μοντέλων βασίστηκε κυρίως στο Recall της κατηγορίας της απάτης,

που αποτελεί κρίσιμο κριτήριο επιτυχίας στα πλαίσια της εργασίας. Συμπληρωματικά, αναλύθηκαν και οι υπόλοιπες μετρικές, Precision, Accuracy και F1-Score, ώστε να επιτευχθεί σφαιρική αποτίμηση της συμπεριφοράς κάθε μοντέλου. Για κάθε πείραμα παρουσιάζεται και το αντίστοιχο confusion matrix του.

5.2 Παράμετροι Αλγορίθμων

Πριν την εφαρμογή των ταξινομητών στο πειραματικό σύνολο δεδομένων, κρίθηκε σκόπιμο να οριστούν οι βασικές υπερπαράμετροι εκπαίδευσης για κάθε αλγόριθμο. Οι περισσότεροι αλγόριθμοι χρησιμοποιήθηκαν με τις προκαθορισμένες τιμές παραμέτρων της βιβλιοθήκης scikit-learn,καθώς μετά απο δοκιμές, η αναζήτηση των βέλτιστων υπερπαραμέτρων δεν έδωσε κάποια αξιοσημείωτη αύξηση στις μετρικές αξιολόγησης. Εξαίρεση αποτελεί το MLP, για το οποίο καθορίστηκαν συγκεκριμένα μεγέθη κρυφών στρωμάτων και αριθμός εποχών, προκειμένου να επιτευχθεί ικανοποιητική σύγκλιση εντός λογικού υπολογιστικού χρόνου.

Πίνακας 5.1: *Παράμετροι εκπαίδευσης των αλγορίθμων*

Αλγόριθμος	**Παράμετρος**	**Τιμή / Περιγραφή**
RandomForestClassifier	n_estimators	100 (αριθμός δέντρων)
	max_depth	None (χωρίς περιορισμό βάθους)
	criterion	gini (κριτήριο διάσπασης)
	class_weight	None (χωρίς αντιστάθμιση)
	random_state	None (τυχαία αρχικοποίηση)
	bootstrap	True (χρήση βοοτστραπ δειγματοληψίας)
BalancedRandomForestClassifier	n_estimators	100
	sampling_strategy	auto (αυτόματη εξισορρόπηση κλάσεων)
	replacement	False (χωρίς επαναληπτική δειγματοληψία)
	random_state	None
	bootstrap	True
IsolationForest	n_estimators	100
	max_samples	auto (χρήση min(256, n_samples))
	contamination	auto (αυτόματη εκτίμηση ποσοστού ανωμαλιών)
	max_features	1.0 (όλα τα χαρακτηριστικά)
	random_state	None
MLPClassifier	hidden_layer_sizes	(128, 64, 32) (τρεις κρυφές στρώσεις)
	activation	ReLU (συνάρτηση ενεργοποίησης)
	optimizer	Adam (αλγόριθμος βελτιστοποίησης)
	learning_rate	constant - 0.01
	max_iter	6 (αριθμός εποχών εκπαίδευσης)
	loss function	categorical crossentropy
	random_state	None

Στον Πίνακα 5.1 παρουσιάζονται συγκεντρωτικά οι τιμές των υπερπαραμέτρων που χρησιμοποιήθηκαν για κάθε μοντέλο κατά την εκπαίδευση.

5.3 Προγραμματιστική Υλοποίηση

Η υλοποίηση της πειραματικής διαδικασίας πραγματοποιήθηκε με τη χρήση του περιβάλλοντος Jupyter Notebook, αξιοποιώντας ένα σύνολο βιβλιοθηκών της Python για την ανάλυση δεδομένων, την εφαρμογή μοντέλων μηχανικής μάθησης και τη στατιστική αξιολόγηση. Παρακάτω παρατίθενται οι κύριες βιβλιοθήκες που χρησιμοποιήθηκαν, καθώς και οι βασικές συναρτήσεις ή μέθοδοι που αξιοποιήθηκαν:

- **NumPy [96]**: Βασική βιβλιοθήκη για αριθμητικούς υπολογισμούς σε dataset. Χρησιμοποιήθηκε για τη διαχείριση δεδομένων και την αριθμητική επεξεργασία τους.
- **Pandas [97]**: Χρησιμοποιήθηκε για την ανάγνωση, επεξεργασία και χειρισμό των δεδομένων σε μορφή DataFrame, διευκολύνοντας την οργάνωση και τον καθαρισμό των δεδομένων.
- **Scikit-learn [98]**: Αποτελεί τη βασική βιβλιοθήκη για την υλοποίηση αλγορίθμων μηχανικής μάθησης. Χρησιμοποιήθηκαν:
  - RandomForestClassifier, BalancedRandomForestClassifier, IsolationForest από το sklearn.ensemble.
  - train_test_split για τον διαχωρισμό των δεδομένων σε σύνολο εκπαίδευσης και ελέγχου.
  - classification_report, confusion_matrix, recall_score, precision_score, f1_score από το sklearn.metrics για την αξιολόγηση των ταξινομητών.
- **Imbalanced-learn [99]**: Βιβλιοθήκη που εξειδικεύεται σε τεχνικές επαναδειγματοληψίας. Χρησιμοποιήθηκαν:
  - RandomOverSampler από το imblearn.over_sampling.
  - RandomUnderSampler από το imblearn.under_sampling.
- **TensorFlow [100]**: Χρησιμοποιήθηκε για την υλοποίηση του MLP μέσω του Keras API. Ορίστηκαν τα πλήρως συνδεδεμένα στρώματα με τη χρήση της Dense, η ReLU ως συνάρτηση ενεργοποίησης, η binary_crossentropy ως συνάρτηση απώλειας και ο Adam ως βελτιστοποιητής.
- **SciPy [101]**: Χρησιμοποιήθηκαν συναρτήσεις από το scipy.stats για την στατιστική σύγκριση των κατανομών χαρακτηριστικών μεταξύ των δύο κατηγοριών:
  - ks_2samp για το Kolmogorov–Smirnov test.
  - entropy για την Kullback–Leibler divergence.
  - jensenshannon για την Jensen–Shannon divergence.
- **Seaborn [102]** και **Matplotlib [103]**: Βιβλιοθήκες για την οπτικοποίηση δεδομένων και αποτελεσμάτων. Χρησιμοποιήθηκαν για τη δημιουργία γραφημάτων, καμπυλών ταξινόμησης και (heatmaps).

5.4 Παρουσίαση Αποτελεσμάτων

Στο κεφάλαιο αυτο παρουσιάζονται τα αποτελέσματα των πειραμάτων που πραγματοποιήθηκαν με στόχο τη σύγκριση διαφορετικών τεχνικών επαναδειγματοληψίας και αλγορίθμων ταξινόμησης. Για κάθε συνδυασμό τεχνικής και αλγορίθμου, υπολογίστηκαν οι βασικές μετρικές απόδοσης: Recall, Precision, F1-score και Accuracy, βασιζόμενες στα δεδομένα που προήλθαν από το σύνολο ελέγχου. Η επιλογή των συγκεκριμένων μετρικών αποσκοπεί στην πληρέστερη αποτίμηση της συμπεριφοράς κάθε μοντέλου, ιδιαίτερα σε περιβάλλοντα σαν αυτο της διπλωματικής, με έντονη ανισορροπία κλάσεων. Τα αποτελέσματα συνοψίζονται στον Πίνακα 5.2 και τον 5.3 ενώ ακολουθεί ποιοτική ανάλυση και ερμηνεία των παρατηρούμενων διαφορών ανά πειραματικό σενάριο.

5.4.1 Αποτελέσματα Πειραμάτων

Στους επόμενους δυο πίνακες παρουσιάζονται τα αποτελέσματα των πειραμάτων μαζί με τις μετρικές αξιολόγησης τους.

Πίνακας 5.2: *Αποτελέσματα για κάθε συνδυασμό μεθόδου επαναδειγματοληψίας και ταξινομητή (macro average)*

Πείραμα	**Μέθοδος**	**Ταξινομητής**	Recall	Precision	F1-score	Accuracy
1	Χωρίς επαναδειγματοληψία	MLP	0.85	0.95	0.90	0.99
2	Χωρίς επαναδειγματοληψία	Random Forest	**0.99**	0.90	**0.94**	0.99
3	Χωρίς επαναδειγματοληψία	Balanced Random Forest	0.94	0.55	0.59	0.99
4	Χωρίς επαναδειγματοληψία	Isolation Forest	0.89	0.51	0.52	0.99
5	Undersampling 1/10	MLP	0.95	0.53	0.56	0.99
6	Undersampling 1/10	Random Forest	0.94	0.82	0.87	0.99
7	Undersampling 1/10	Balanced Random Forest	0.96	0.59	0.65	0.99
8	Undersampling 1/20	MLP	0.96	0.56	0.60	0.99
9	Undersampling 1/20	Random Forest	0.93	0.85	0.88	0.99
10	Undersampling 1/20	Balanced Random Forest	0.96	0.61	0.67	0.99
11	Oversampling 1/10	MLP	0.97	0.52	0.53	0.99
12	Oversampling 1/10	Random Forest	0.90	0.95	0.93	0.99
13	Oversampling 1/10	Balanced Random Forest	0.92	0.92	0.92	0.99
14	Oversampling 1/20	MLP	0.99	0.56	0.60	0.99
15	Oversampling 1/20	Random Forest	0.92	**0.96**	0.93	0.99
16	Oversampling 1/20	Balanced Random Forest	0.95	0.90	0.92	0.99

Πίνακας 5.3: *Τιμές Recall για τη μειοψηφική κατηγορία (fraud), ανά συνδυασμό μεθόδου επαναδειγματοληψίας και ταξινομητή.*

Πείραμα	**Μέθοδος**	**Ταξινομητής**	Recall
1	Χωρίς επαναδειγματοληψία	MLP	0.70
2	Χωρίς επαναδειγματοληψία	Random Forest	0.80
3	Χωρίς επαναδειγματοληψία	Balanced Random Forest	0.90
4	Χωρίς επαναδειγματοληψία	Isolation Forest	0.89
5	Random Undersampling 1/10	MLP	0.93
6	Random Undersampling 1/10	Random Forest	0.88
7	Random Undersampling 1/10	Balanced Random Forest	0.93
8	Random Undersampling 1/20	MLP	0.93
9	Random Undersampling 1/20	Random Forest	0.87
10	Random Undersampling 1/20	Balanced Random Forest	0.92
11	Random Oversampling 1/10	MLP	**0.98**
12	Random Oversampling 1/10	Random Forest	0.81
13	Random Oversampling 1/10	Balanced Random Forest	0.84
14	**Random Oversampling 1/20**	**MLP**	**1.00**
15	Random Oversampling 1/20	Random Forest	0.84
16	Random Oversampling 1/20	Balanced Random Forest	0.90

Στο παράρτημα Α΄ παρουσιάζονται αναλυτικά τα confusion matrix ανα πείραμα.

5.4.2 Ανάλυση και Σχολιασμός ανά Κατηγορία Μεθόδου

Στο κεφάλαιο αυτο πραγματοποιείται η συστηματική ανάλυση των πειραματικών αποτελεσμάτων με βάση την κατηγορία της μεθόδου επαναδειγματοληψίας που εφαρμόστηκε. Σκοπός είναι η διερεύνηση της επίδρασης κάθε μεθόδου (απουσία επαναδειγματοληψίας, υπερδειγματοληψία, υποδειγματοληψία) στην απόδοση των ταξινομητών. Η ανάλυση εστιάζει στην καταγραφή και σύγκριση των μεταβολών των βασικών μετρικών αξιολόγησης, στην αξιολόγηση της σταθερότητας των αποτελεσμάτων, καθώς και στην ανάδειξη πιθανών αδυναμιών ή περιορισμών που προκύπτουν για κάθε κατηγορία. Επιπλέον, αξιολογείται η αποτελεσματικότητα των μεθόδων επαναδειγματοληψίας στη διαχείριση της ανισορροπίας των κλάσεων, και η επίδρασή τους στη βελτίωση ή επιδείνωση της απόδοσης των μοντέλων.

Η ανάλυση βασίζεται στις βασικές macro average μετρικές αξιολόγησης (Recall, Precision, F1-score και Accuracy), καθώς και στην τιμή του Recall για τη μειοψηφική κατηγορία (fraud).

Χωρίς Επαναδειγματοληψία:

Η απουσία επαναδειγματοληψίας (πειράματα 1–4), που αποτελούν καια τα βασικά μοντέλα, οδήγησε, όπως ήταν αναμενόμενο, σε πολύ υψηλές τιμές ακρίβειας (Accuracy = 0.99 σε όλες τις περιπτώσεις). Ωστόσο, η ακρίβεια, ως μετρική, δεν είναι ενδεικτική της συνολικής απόδοσης των μοντέλων, ιδίως στο συγκεκριμένο πρόβλημα, που σκοπός είναι η ικανότητα ανίχνευσης της μειοψηφικής κλάσης.

Εξετάζοντας τις υπόλοιπες μετρικές, διαπιστώνεται ότι ο Random Forest επιτυγχάνει τον υψηλότερο F1-score (0.94), με πολύ καλή ισορροπία Recall (0.99) και Precision (0.90). Α-

ντίθετα, το MLP παρουσιάζει υψηλό Precision (0.95), αλλά σαφώς χαμηλότερο Recall (0.85) και ακόμη χαμηλότερο recall ειδικά για τη μειοψηφική κατηγορία (0.70), γεγονός που καταδεικνύει την αδυναμία του να εντοπίσει αποτελεσματικά περιπτώσεις απάτης χωρίς ενίσχυση του συνόλου δεδομένων.

Ο Balanced Random Forest και το Isolation Forest εμφανίζουν υψηλό Recall για τη μειοψηφία (0.90 και 0.89 αντίστοιχα), ωστόσο συνολικά υπολείπονται σε F1-score (0.59 και 0.52), κυρίως λόγω του χαμηλού Precision (0.55 και 0.51). Συνεπώς, χωρίς επαναδειγματοληψία, η απόδοση ποικίλλει έντονα ανάλογα με τον ταξινομητή, ενώ κανένα μοντέλο δεν επιτυγχάνει ικανοποιητική ισορροπία όλων των μετρικών.

Υποδειγματοληψία (Random Undersampling):

Η εφαρμογή υποδειγματοληψίας με αναλογία 1/10 και 1/20 (πειράματα 5–10) επιφέρει σημαντική ενίσχυση της ικανότητας εντοπισμού της μειοψηφικής κατηγορίας, όπως υποδεικνύεται από την αύξηση του Recall (έως και 0.96 σε macro average, και έως 0.93 ειδικά για τη μειοψηφία στις περιπτώσεις των MLP και Random Forest). Ωστόσο, αυτή η βελτίωση συνοδεύεται από πτώση στην Precision, ιδίως όταν χρησιμοποιείται το MLP (π.χ. Precision = 0.53 στο πείραμα 5).

Η τεχνική αυτή φαίνεται να αποδίδει καλύτερα όταν συνδυάζεται με τον Random Forest και τον Balanced Random Forest, καθώς οι αλγόριθμοι αυτοί διατηρούν ικανοποιητικό Precision (0.82 και 0.59 αντίστοιχα) και παρουσιάζουν σταθερά υψηλό Recall. Η σταθερότητα του F1-score σε αυτά τα σενάρια (έως και 0.88) υποδεικνύει την ικανότητα των δέντρων να προσαρμόζονται στη μειωμένη εκπαιδευτική πληροφορία, που παρέχει η υποδειγματοληψία.

Γενικά, η υποδειγματοληψία προσφέρει μια αποδοτική λύση, ιδιαίτερα σε περιπτώσεις όπου η διατήρηση ενός μικρού, ταχύτερα επεξεργάσιμου συνόλου δεδομένων είναι επιθυμητή. Ωστόσο, η ενδεχόμενη απώλεια πληροφορίας από την πλειοψηφική κατηγορία μπορεί να περιορίσει τη συνολική ακρίβεια των ταξινομητών.

Υπερδειγματοληψία (Random Oversampling):

Η υπερδειγματοληψία (πειράματα 11–16), ιδιαίτερα με αναλογία 1/20, παρουσιάζει τα πλέον εντυπωσιακά αποτελέσματα ως προς το Recall της μειοψηφικής κατηγορίας, φτάνοντας μέχρι και 1.00 με χρήση του MLP (πείραμα 14). Επιπλέον, όταν συνδυάζεται με τους (Random Forest και Balanced RF), παρατηρούνται εξαιρετικές επιδόσεις σε όλες τις μετρικές, με το F1-score να φτάνει έως και 0.93 (πειράματα 12, 13, 15 και 16), και σταθερή διατήρηση υψηλού Precision (έως 0.96).

Ο συγκεκριμένος τύπος επαναδειγματοληψίας επιτυγχάνει ισορροπημένη απόδοση, χωρίς να θυσιάζεται η απόδοση της πλειοψηφικής κατηγορία. Επιπλέον, οι αλγόριθμοι που είναι ανθεκτικοί στο overfitting, καθώς φαίνεται να επωφελούνται περισσότερο από την αύξηση των παραδειγμάτων της μειοψηφικής κλάσης, ενισχύοντας ουσιαστικά τη συνολική απόδοση.

Συμπερασματικά, η υπερδειγματοληψία αναδεικνύεται ως η πλέον αποτελεσματική στρατηγική, υπό την προϋπόθεση ότι συνοδεύεται από κατάλληλο αλγόριθμο ταξινόμησης και

εφαρμογή τεχνικών τακτικής γενίκευσης (regularization) για αποφυγή υπερεκπαίδευσης.

5.4.3 Σύγκριση και Σχολιασμός Μεταξύ Ταξινομητών

Το κεφάλαιο αυτό εστιάζει στη συγκριτική αξιολόγηση των αλγορίθμων ταξινόμησης που χρησιμοποιήθηκαν, ανεξαρτήτως της μεθόδου επαναδειγματοληψίας. Παρουσιάζεται η ανάλυση των διαφορών στην απόδοση των ταξινομητών, με έμφαση στην ικανότητά τους να ανταποκρίνονται στο πρόβλημα της ανισορροπίας των κλάσεων, καθώς και στη συνολική τους αξιοπιστία και αποτελεσματικότητα. Επιπρόσθετα, διερευνώνται τα πλεονεκτήματα και οι περιορισμοί του κάθε αλγορίθμου, λαμβάνοντας υπόψη τόσο το θεωρητικό υπόβαθρο όσο και τις πρακτικές απαιτήσεις του συγκεκριμένου προβλήματος, με στόχο την εξαγωγή τεκμηριωμένων συμπερασμάτων σχετικά με την καταλληλότητά τους.

Ο **Random Forest** παρουσιάζει σταθερά υψηλές επιδόσεις σε όλα τα πειράματα, διατηρώντας ισορροπία μεταξύ του Recall και του Precision. Σε συνθήκες χωρίς επαναδειγματοληψία ή με χρήση oversampling, καταγράφει F1-score έως και 0.94, καθιστώντας τον έναν από τους πλέον αξιόπιστους και προσαρμοστικούς αλγορίθμους.

Ο **Balanced Random Forest**, σχεδιασμένος για προβλήματα με ανισόρροπες κλάσεις, επιτυγχάνει υψηλό Recall, ακόμη και χωρίς επαναδειγματοληψία (0.90). Ωστόσο, υπολείπεται ως προς την Precision (π.χ. 0.55 στο πείραμα 3). Όταν συνδυάζεται με oversampling, παρουσιάζει εξαιρετική ισορροπία (F1-score 0.92), γεγονός που επιβεβαιώνει την αποτελεσματικότητά του όταν συνοδεύεται από κατάλληλη ενίσχυση του συνόλου δεδομένων.

Το **MLP** εμφανίζει έντονη ευαισθησία στην κατανομή των δεδομένων. Χωρίς επαναδειγματοληψία, παρουσιάζει περιορισμένο Recall για τη μειοψηφική κατηγορία (0.70), ενώ με oversampling μπορεί να φτάσει ακόμη και το 1.00 (πείραμα 14), εις βάρος όμως της Precision (0.56). Συνεπώς, απαιτείται ιδιαίτερη προσοχή κατά την επιλογή και ρύθμισή του, καθώς η απόδοσή του επηρεάζεται σημαντικά από τη μέθοδο επαναδειγματοληψίας και ενδεχομένως χρήζει εφαρμογής τεχνικών (regularization) για την αποφυγή του overfitting.

Τέλος, ο **Isolation Forest**, παρότι θεωρητικά ενδείκνυται για anomaly detection, δεν αποδίδει ικανοποιητικά στο συγκεκριμένο σύνολο. Παρουσιάζει χαμηλές τιμές F1-score και Precision, υποδεικνύοντας περιορισμένη ικανότητα ταξινόμησης.

Συμπερασματικά, οι ταξινομητές που βασίζονται στα δέντρα (Random Forest και Balanced Random Forest) επιδεικνύουν σταθερή και ισχυρή απόδοση υπό διαφορετικές συνθήκες, ενώ η χρήση του MLP μπορεί να είναι αποτελεσματική υπό την προϋπόθεση κατάλληλης προεπεξεργασίας και ελέγχου overfitting.

5.5 Συμπεράσματα Πειραμάτων

Τα πειραματικά αποτελέσματα που παρουσιάστηκαν επιβεβαιώνουν τη σημαντική επίδραση των μεθόδων επαναδειγματοληψίας στην απόδοση των ταξινομητών, ειδικά σε προβλήματα με έντονη ανισορροπία κλάσεων, όπως η ανίχνευση απατών σε τραπεζικές συναλλαγές.

Συγκεκριμένα, διαπιστώθηκε ότι η απουσία επαναδειγματοληψίας οδηγεί σε υψηλές τιμές Accuracy, οι οποίες όμως δεν αντικατοπτρίζουν την πραγματική ικανότητα των μοντέλων

να ανιχνεύουν τη μειοψηφική κατηγορία (fraud). Σε αυτές τις περιπτώσεις, τα μοντέλα παρουσιάζουν σημαντικές αδυναμίες στο Recall της μειοψηφικής κλάσης, γεγονός που περιορίζει την πρακτική τους εφαρμογή σε περιβάλλοντα όπου η έγκαιρη και ακριβής ανίχνευση των σπάνιων συμβάντων είναι κρίσιμη, όπως το περιβάλλον της εργασίας.

Η χρήση υποδειγματοληψίας (Random Undersampling) βελτίωσε την ικανότητα ανίχνευσης της μειοψηφικής κατηγορίας, με αύξηση του Recall, ωστόσο συνοδεύτηκε από μείωση του Precision, κυρίως όταν χρησιμοποιήθηκε το MLP. Οι ταξινομητές βασισμένοι σε δέντρα εμφάνισαν μεγαλύτερη ανθεκτικότητα στις μεταβολές αυτές, διατηρώντας καλύτερη ισορροπία μεταξύ των μετρικών.

Αντίθετα, η υπερδειγματοληψία (Random Oversampling) απέδωσε συνολικά τα πιο ισορροπημένα και εντυπωσιακά αποτελέσματα, ιδίως σε συνδυασμό με τον Random Forest. Η μέθοδος αυτή βελτίωσε σημαντικά το Recall της μειοψηφικής κλάσης χωρίς σημαντική θυσία στο Precision, επιτυγχάνοντας υψηλό F1-score, γεγονός που υποδηλώνει τη βελτιστοποίηση της συνολικής απόδοσης των μοντέλων. Ενδεικτικό είναι το γεγονός ότι σε ορισμένες περιπτώσεις το Recall της μειοψηφικής κλάσης έφτασε ακόμα και το 1.00, κάτι ιδιαίτερα σημαντικό για την έγκαιρη ανίχνευση απάτης.

Επιπρόσθετα, η σύγκριση μεταξύ των ταξινομητών ανέδειξε τον Random Forest ως τον πιο ισορροπημένο και αποδοτικό αλγόριθμο, με σταθερή απόδοση και καλή διαχείριση της ανισορροπίας των κλάσεων. Το MLP, αν και σε ορισμένες περιπτώσεις κατέγραψε πολύ υψηλό Recall, παρουσίασε αστάθεια και σημαντική μείωση της Precision, γεγονός που χρήζει περαιτέρω διερεύνησης και προσαρμογής.

Συνοψίζοντας, τα πειράματα καταδεικνύουν ότι η κατάλληλη επιλογή και εφαρμογή της μεθόδου επαναδειγματοληψίας, σε συνδυασμό με τον κατάλληλο αλγόριθμο ταξινόμησης, είναι καθοριστικής σημασίας για την αποτελεσματική αντιμετώπιση προβλημάτων με ανισόρροπα δεδομένα, όπως αυτό της ανίχνευσης απάτης.

Πιο χρήσιμα αποτελέσματα δίνει το **πείραμα 14**, όπου εφαρμόστηκε υπερδειγματοληψία με λόγο 1/20 σε συνδυασμό με τον αλγόριθμο MLP, πέτυχε το μέγιστο Recall (1.00) στη μειοψηφική κατηγορία, εντοπίζοντας σχεδόν όλες τις περιπτώσεις απάτης. Ωστόσο, το σχετικά χαμηλό Precision (0.56) υποδηλώνει αυξημένο αριθμό λανθασμένων θετικών προβλέψεων, γεγονός που μπορεί να επηρεάσει την αξιοπιστία του μοντέλου γενικότερα.

Αντίθετα, ο συνδυασμός υπερδειγματοληψίας με Random Forest (**πειράματα 12 και 15**) παρουσιάζει πιο ισορροπημένη απόδοση, με υψηλά Recall και Precision (έως 0.95), προσφέροντας πιο αξιόπιστη και συνολικά αποτελεσματική ανίχνευση απάτης. Τέλος, για την ανίχνευση συγκριμένα των απατών, τα **πειράματα 7 και 8** πετυχαίνουν Recall 0.93, που είναι αρκετά ικανοποιητικό.

Κεφάλαιο 6

Συμπεράσματα και Μελλοντικές Επεκτάσεις

6.1 Συμπεράσματα

Η διπλωματική εργασία πραγματεύεται το ζήτημα της ανίχνευσης απάτης σε τραπεζικές συναλλαγές, εστιάζοντας στην αντιμετώπιση της έντονης ανισορροπίας των δεδομένων μέσω τεχνικών επαναδειγματοληψίας και την αξιολόγηση της απόδοσης τους απο διάφορους αλγορίθμους ταξινόμησης. Αναδείχθηκε η σπουδαιότητα της κατάλληλης διαχείρισης της ανισορροπίας των δεδομένων στην ανίχνευση απάτης στις τραπεζικές συναλλαγές, όπου μέσα από ένα σύνολο 16 πειραμάτων εξετάστηκαν διαφορετικοί συνδυασμοί τεχνικών επαναδειγματοληψίας και αλγορίθμων ταξινόμησης, με στόχο τη βελτίωση της απόδοσης στο δύσκολο πρόβλημα της ανίχνευσης των απατών.

Τα αποτελέσματα έδειξαν ότι η απουσία επαναδειγματοληψίας οδηγεί σε παραπλανητικά υψηλό accuracy, χωρίς ουσιαστική ικανότητα εντοπισμού των απατών. Η υποδειγματοληψία αύξησε το recall, ιδιαίτερα για τα μοντέλα που είναι βασισμένα σε δενδρικούς αλγορίθμους, αλλά μείωσε το *πρεσισιον*, ειδικά για το MLP. Η υπερδειγματοληψία και ιδιαίτερα σε συνδυασμό με τον αλγόριθμο Random Forest, προσέφερε τις πιο ισορροπημένες και αποδοτικές επιδόσεις, επιτυγχάνοντας υψηλό recall και precision χωρίς ουσιαστικές απώλειες.

Συμπερασματικά, η εργασία υπογραμμίζει ότι η ορθή επιλογή τεχνικής επαναδειγματοληψίας και αλγορίθμου ταξινόμησης είναι καθοριστικής σημασίας για την επιτυχή ανίχνευση σπάνιων συμβάντων όπως η απάτες στις τραπεζικές συναλλαγές. Ειδικότερα, τα πειράματα με υπερδειγματοληψία και Random Forest παρουσίασαν αξιοσημείωτη σταθερότητα και αποτελεσματικότητα, καθιστώντας τα ιδανική επιλογή για πρακτικές εφαρμογές στον χώρο της χρηματοοικονομικής ασφάλειας και της ανίχνευσης απάτης.

6.2 Μελλοντικές Επεκτάσεις

Η εργασία θέτει τις βάσεις για περαιτέρω έρευνα στον τομέα της ανίχνευσης απάτης σε τραπεζικές συναλλαγές και όπως κάθε εργασία, παρουσιάζει περιθώρια βελτίωσης και επέκτασης. Ενδεικτικά, προτείνονται οι εξής μελλοντικές επεκτάσεις:

- Διερεύνηση πιο εξελιγμένων τεχνικών επαναδειγματοληψίας: Η αξιοποίηση μεθόδων όπως τα SMOTE, ADASYN ή συνδυαστικών στρατηγικών (ensemble sampling) ενδέχεται να προσφέρει καλύτερη γενίκευση και ισορροπία μεταξύ των μετρικών.

- Εφαρμογή επιβλεπόμενων και μη επιβλεπόμενων τεχνικών ανίχνευσης ανωμαλιών: Μελέτη μεθόδων όπως οι autoencoders, isolation forests και one-class SVM θα μπορούσε να ενισχύσει την ικανότητα ανίχνευσης απατών χωρίς την ανάγκη πλήρως επισημασμένων δεδομένων.

- Χρήση πιο πρόσφατων και σύνθετων αρχιτεκτονικών νευρωνικών δικτύων: Για παράδειγμα attention-based models (π.χ. LSTM, Transformer) θα μπορούσε να προσφέρει πλεονεκτήματα στην πρόβλεψη της κλάσης των συναλλαγών.

- Αξιοποίηση διαφορετικών συνόλων δεδομένων: Η χρήση νέων δεδομένων ενδέχεται να βελτιώσει την γενικευσιμότητα των μοντέλων και να αποκαλύψει προκλήσεις που δεν εμφανίζεται στο σύνολο δεδομένων της εργασίας.

- Μελέτη σε πραγματικό χρόνο: Η εφαρμογή των μοντέλων σε περιβάλλοντα με ροές δεδομένων και μελέτη της απόδοσης σε συνθήκες πραγματικού χρόνου και περιβάλλοντος αποτελεί κρίσιμο βήμα για την πρακτική αξιοποίηση των μοντέλων που εξετάστηκαν.

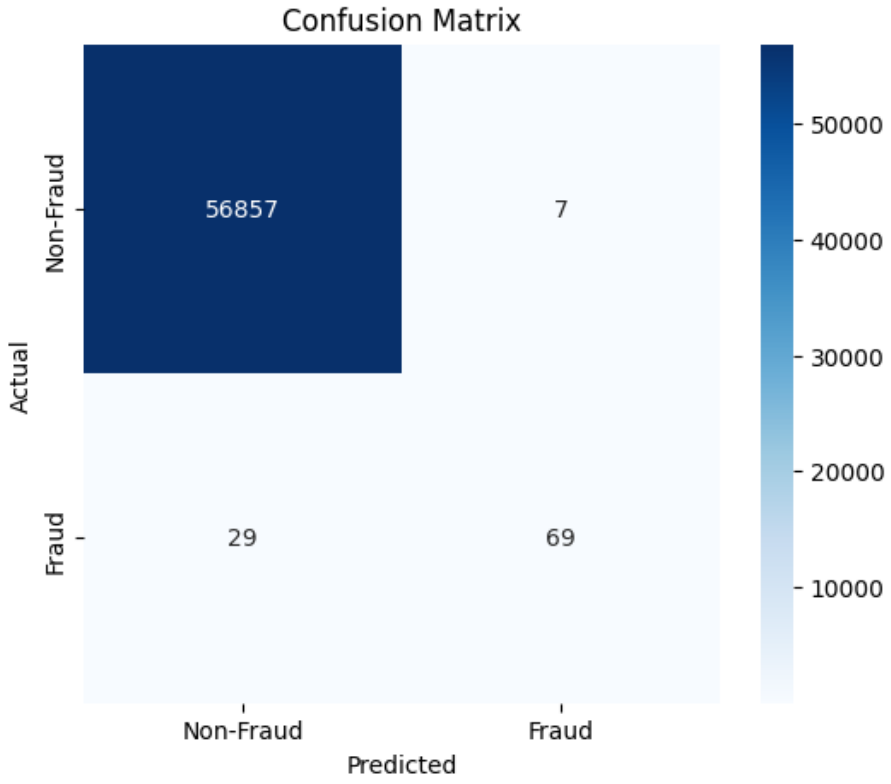
Παραρτήματα

Παράρτημα Α΄

Confusion Matrix ανα Πείραμα

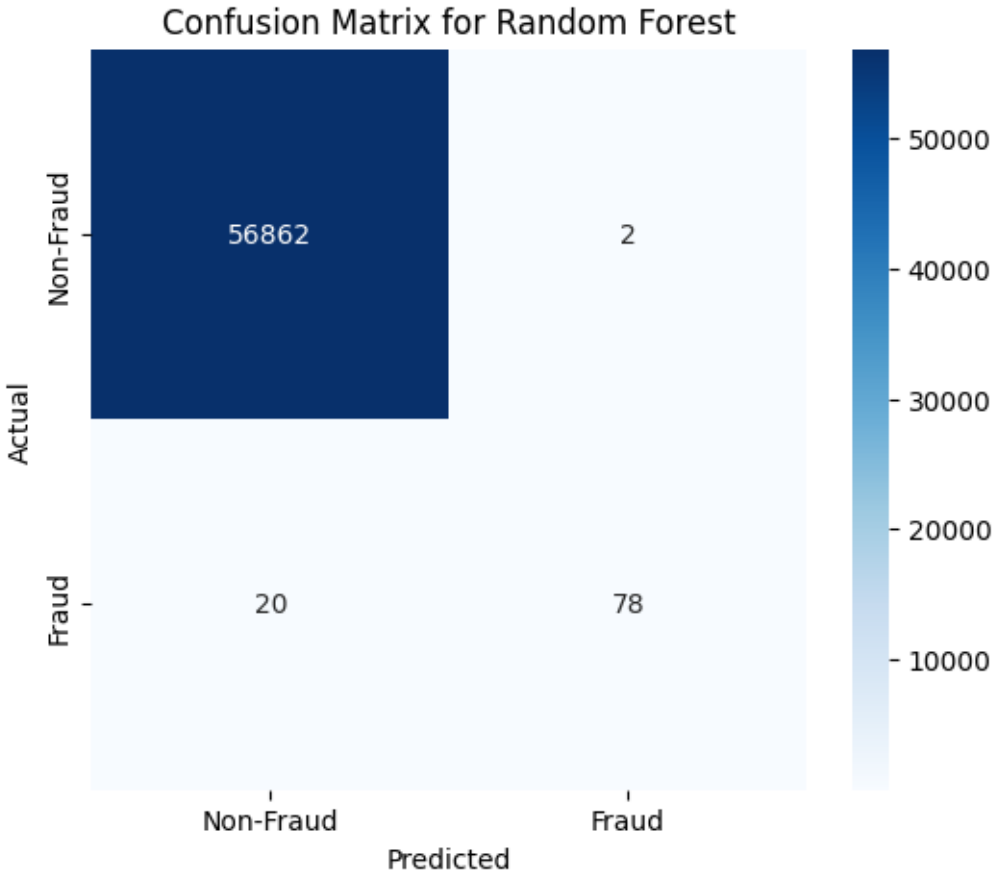
Το confusion matrix είναι ένας πίνακας που συνοψίζει την απόδοση ενός αλγορίθμου ταξινόμησης, παρουσιάζοντας τον αριθμό των σωστών και λανθασμένων προβλέψεων ανά κατηγορία. Αποτελείται από τέσσερις βασικές κατηγορίες: True Positives (TP), True Negatives (TN), False Positives (FP) και False Negatives (FN). Στο πλαίσιο της διπλωματικής εργασίας, όπως αναφέρθηκε και στο κεφάλαιο 4.3, όπου αντιμετωπίζουμε έντονη ανισορροπία μεταξύ των κλάσεων, το confusion matrix βοηθάει να κατανοηθεί πιο λεπτομερώς η συμπεριφορά του μοντέλου.

Α΄.1 Πείραμα 1



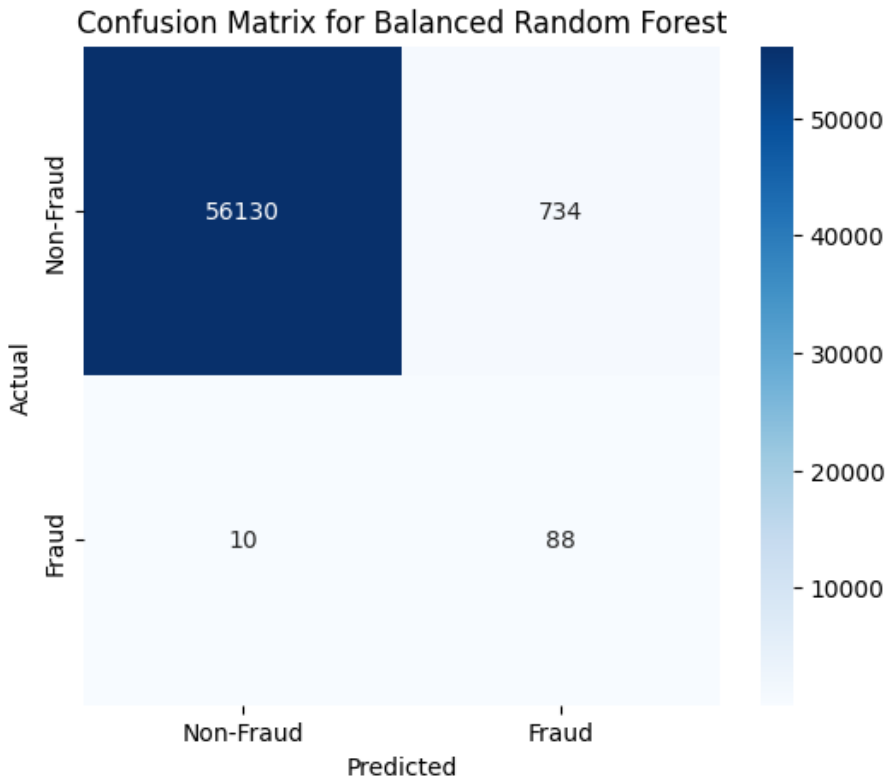
Σχήμα Α΄.1: *Confusion Matrix για το πείραμα 1*

Α΄.2 Πείραμα 2



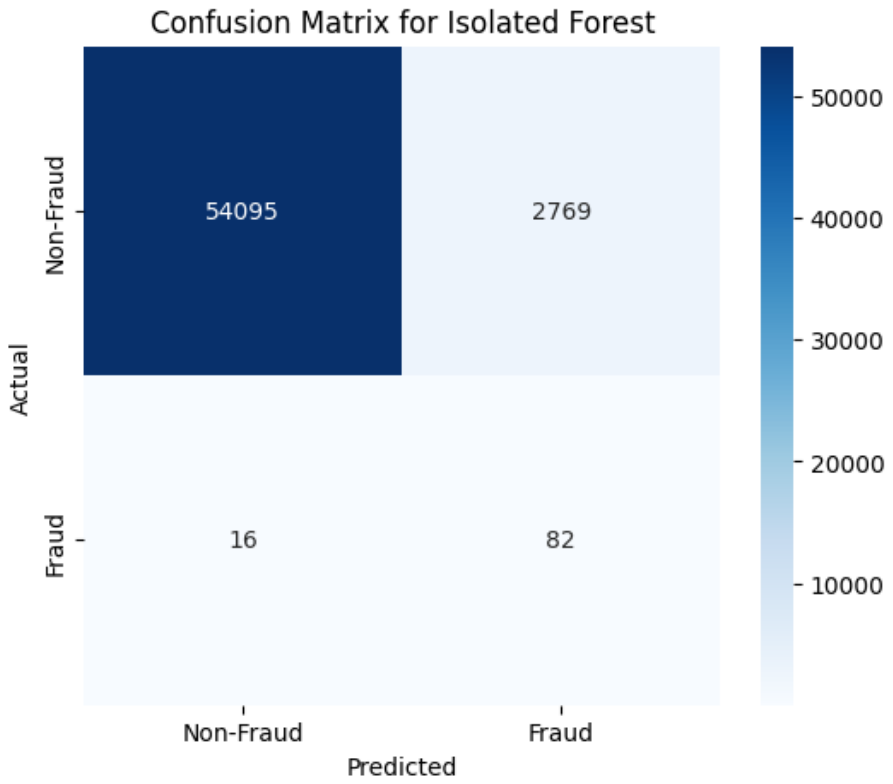
Σχήμα Α΄.2: *Confusion Matrix για το πείραμα 2*

Α΄.3 Πείραμα 3



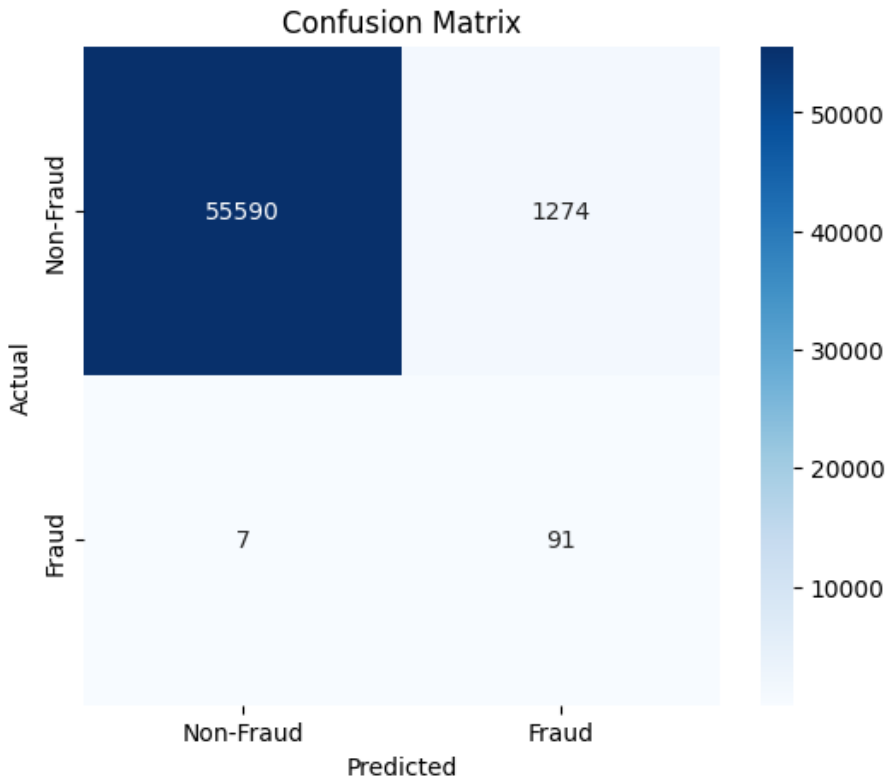
Σχήμα Α΄.3: *Confusion Matrix για το πείραμα 3*

Α΄.4 Πείραμα 4



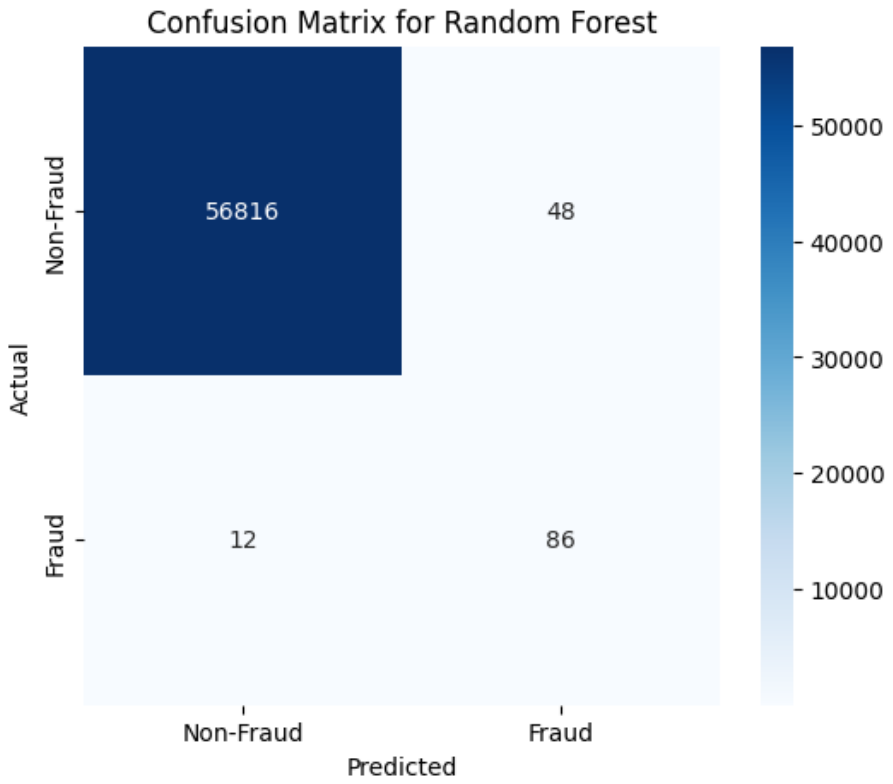
Σχήμα Α΄.4: *Confusion Matrix για το πείραμα 4*

Α΄.5 Πείραμα 5



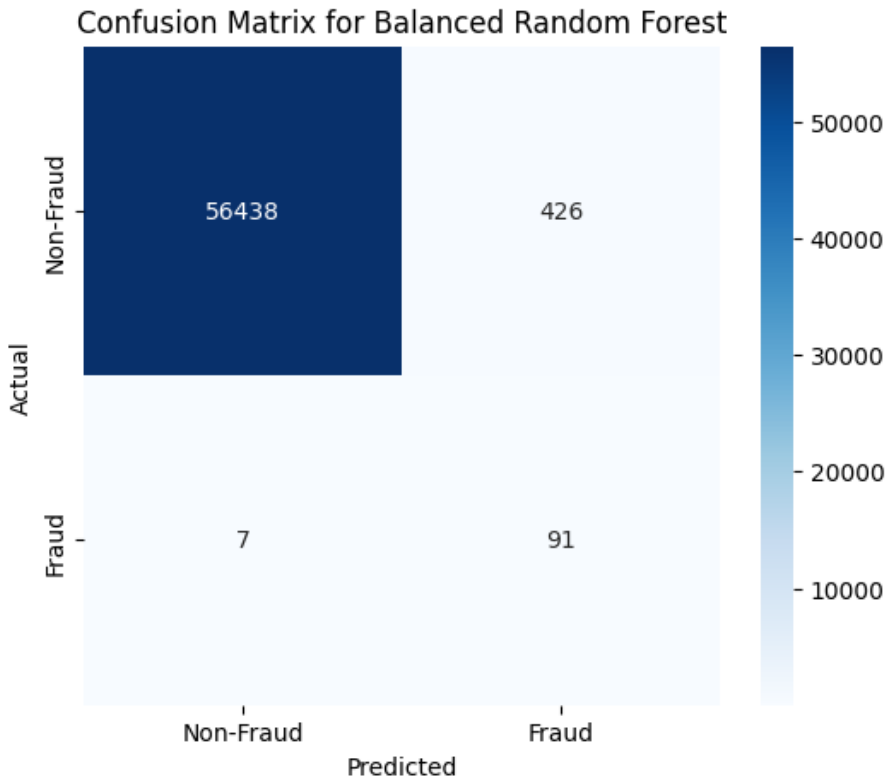
Σχήμα Α΄.5: *Confusion Matrix για το πείραμα 5*

Α΄.6 Πείραμα 6



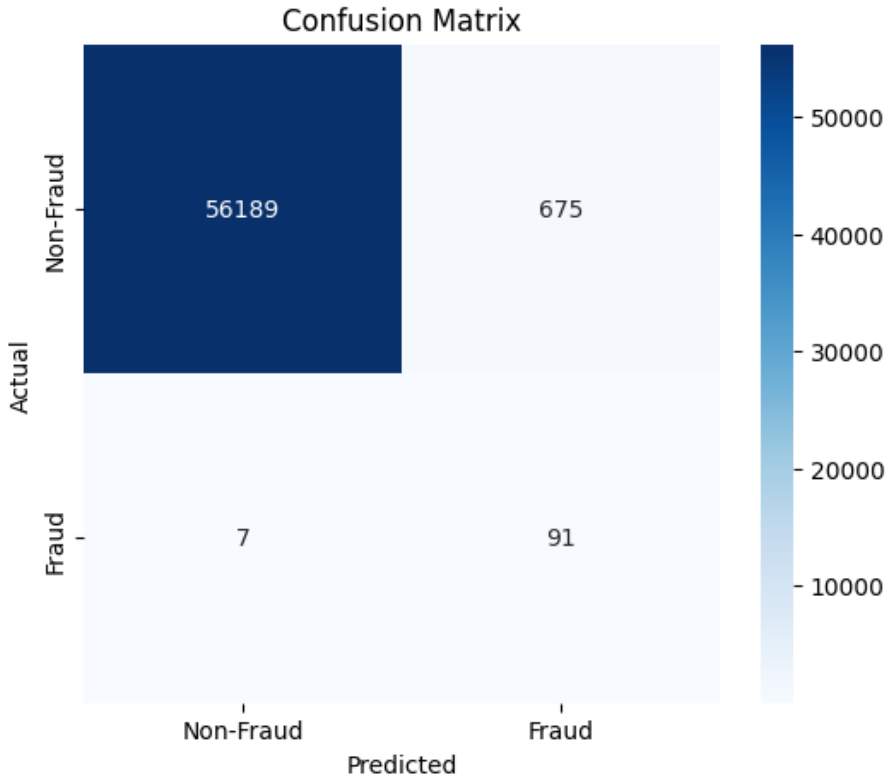
Σχήμα Α΄.6: *Confusion Matrix για το πείραμα 6*

Α΄.7 Πείραμα 7



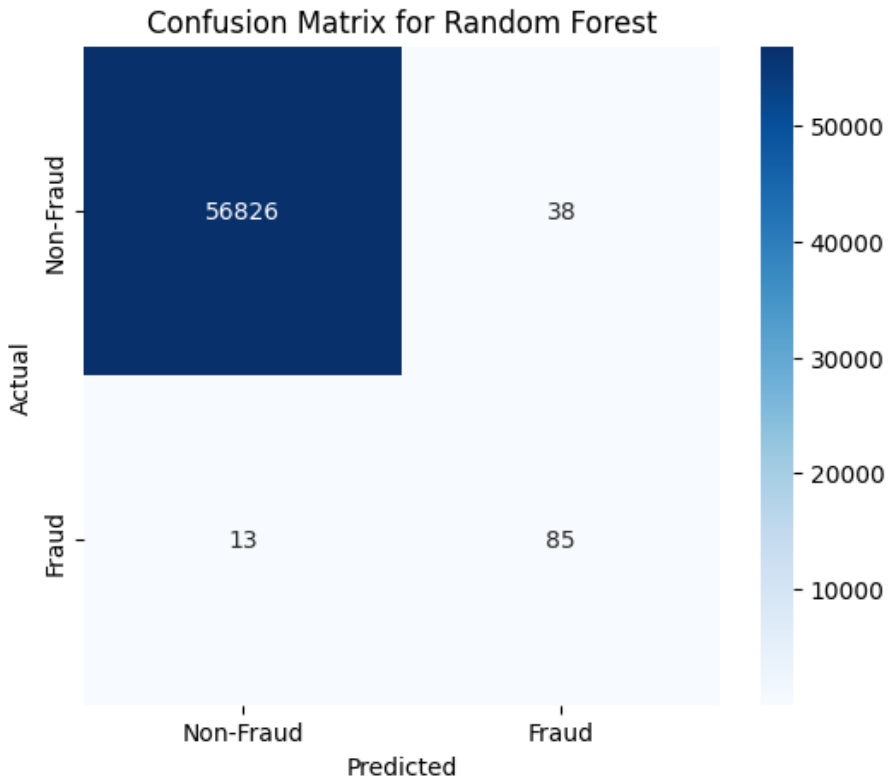
Σχήμα Α΄.7: *Confusion Matrix για το πείραμα 7*

Α'.8 Πείραμα 8



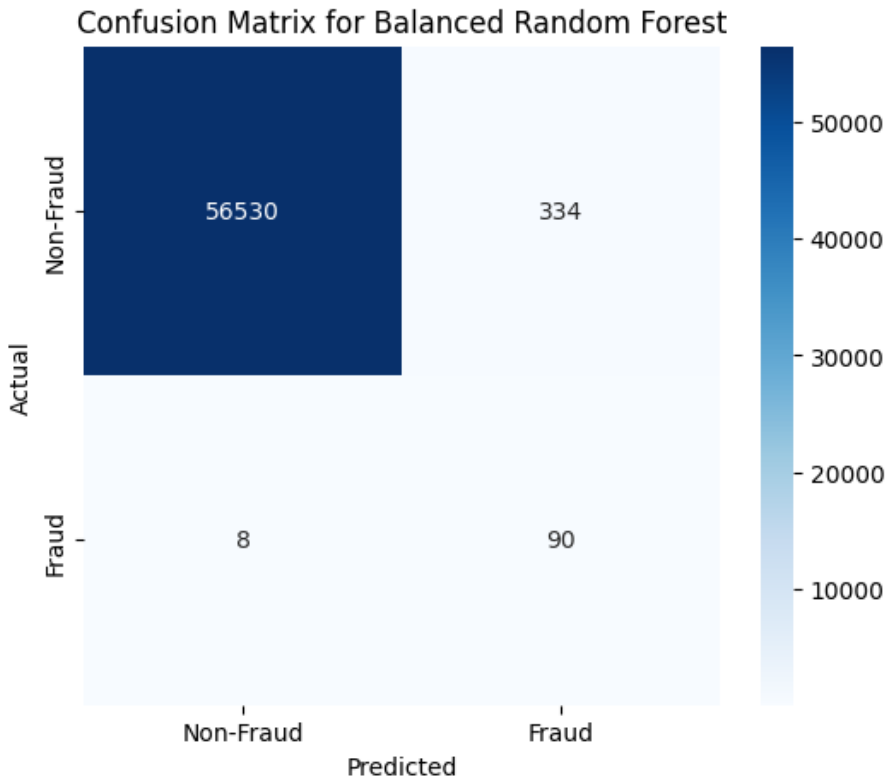
Σχήμα Α'.8: *Confusion Matrix για το πείραμα 8*

Α΄.9 Πείραμα 9



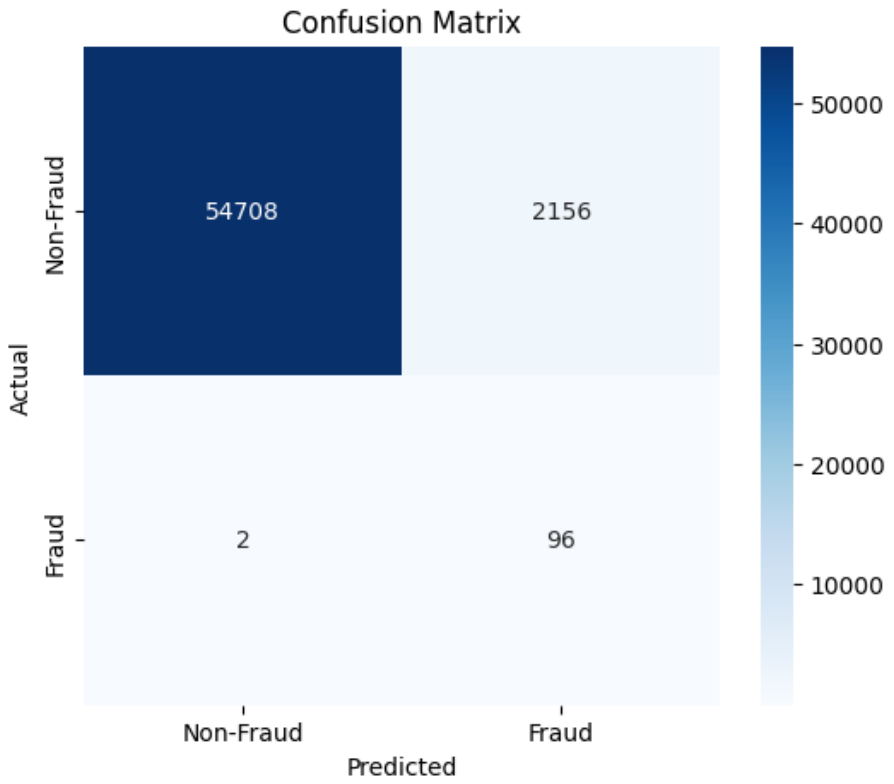
Σχήμα Α΄.9: *Confusion Matrix για το πείραμα 9*

Α΄.10 Πείραμα 10



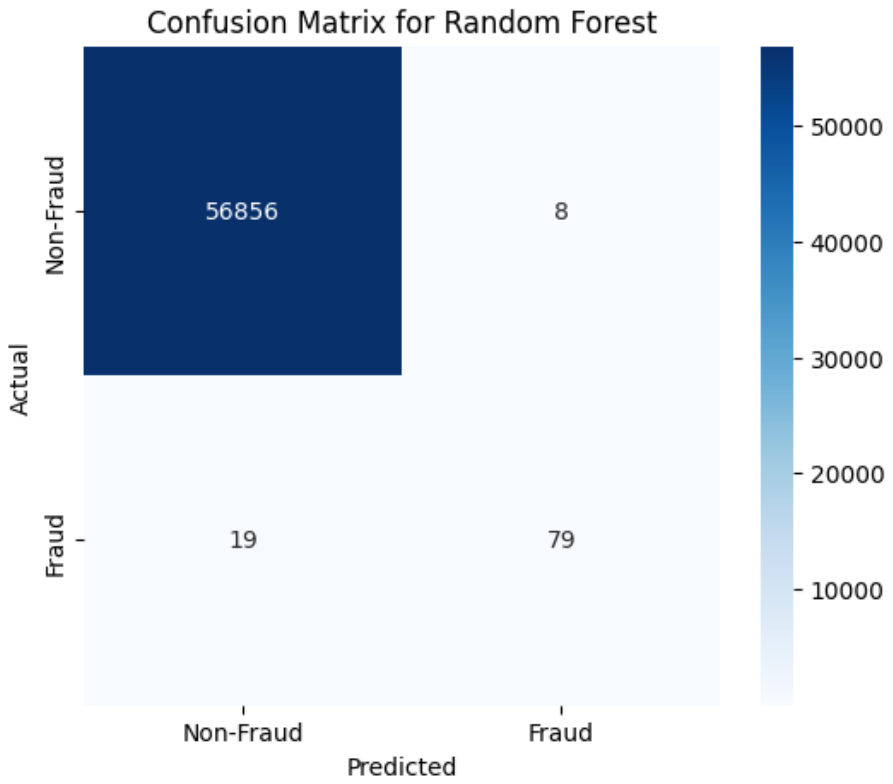
Σχήμα Α΄.10: *Confusion Matrix για το πείραμα 10*

Α΄.11 Πείραμα 11



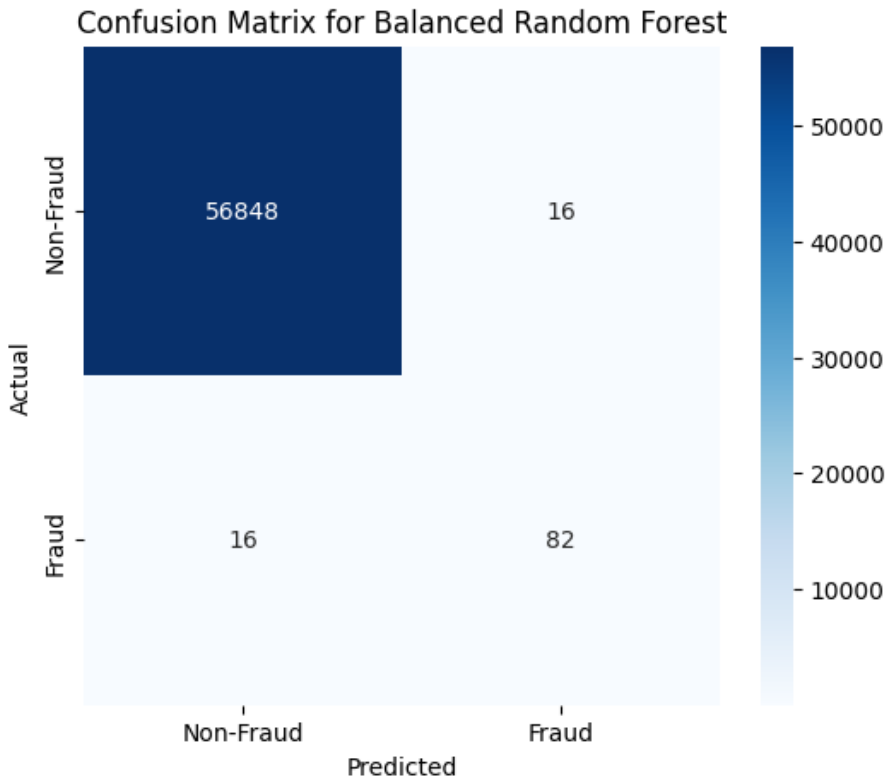
Σχήμα Α΄.11: *Confusion Matrix για το πείραμα 11*

Α΄.12 Πείραμα 12



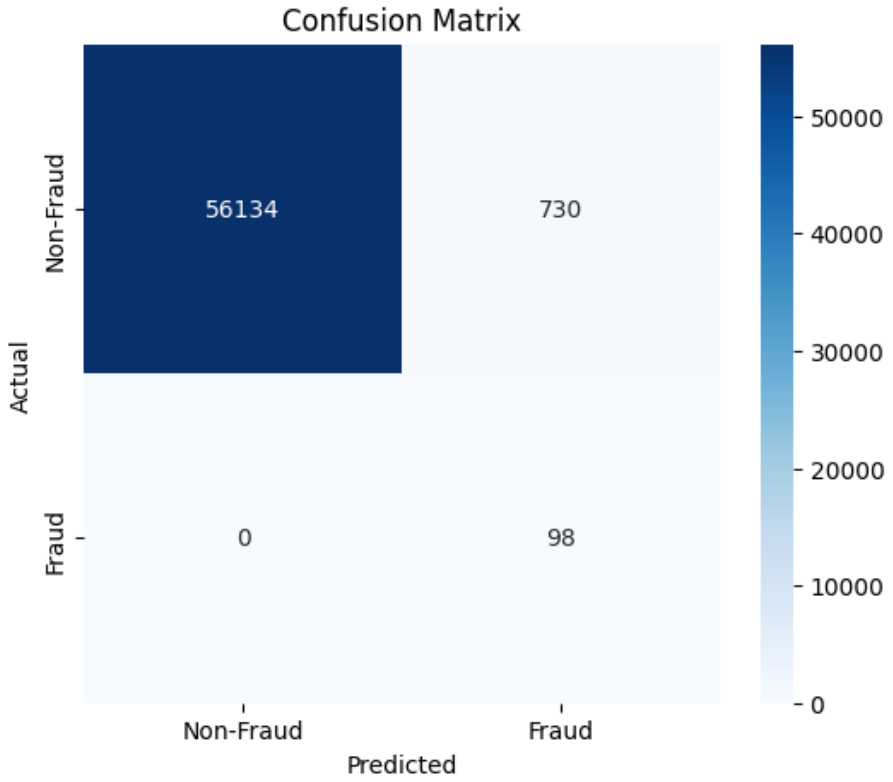
Σχήμα Α΄.12: *Confusion Matrix για το πείραμα 12*

Α΄.13 Πείραμα 13



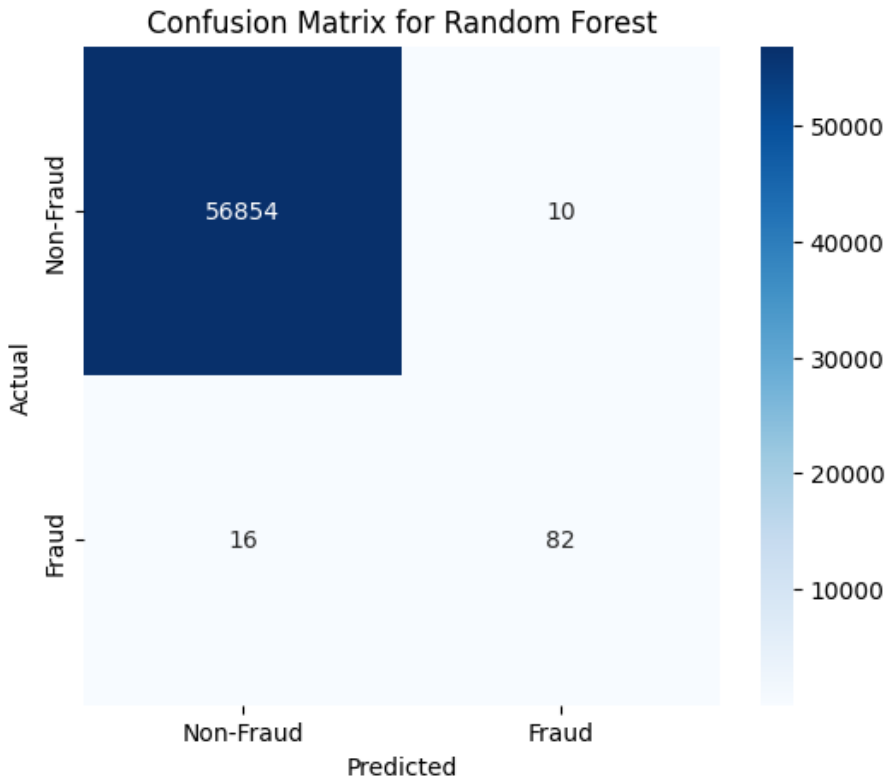
Σχήμα Α΄.13: *Confusion Matrix για το πείραμα 13*

Α΄.14 Πείραμα 14



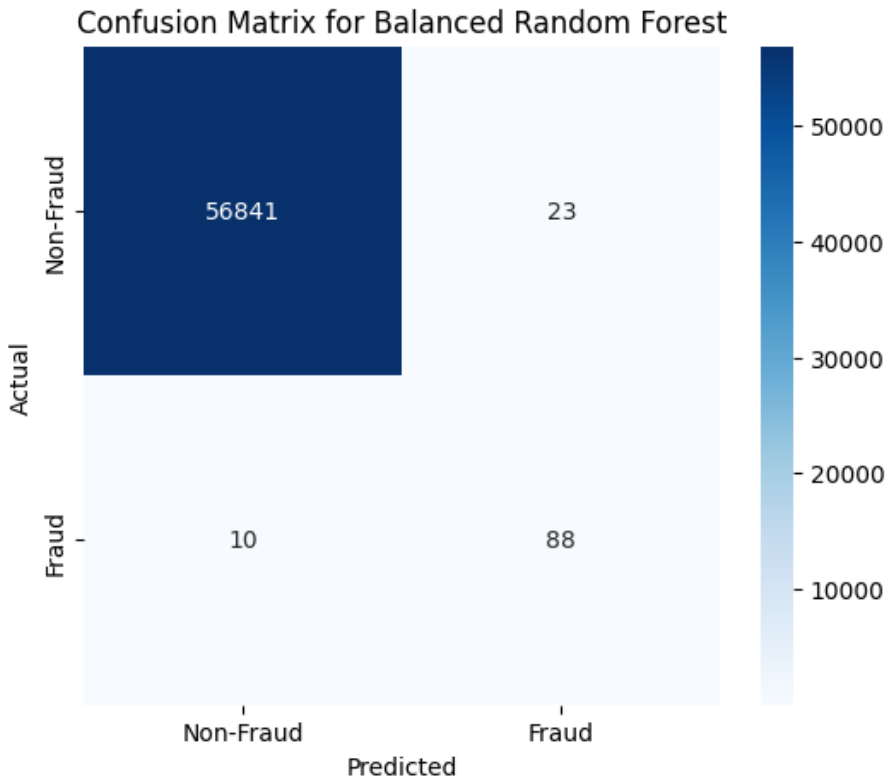
Σχήμα Α΄.14: *Confusion Matrix για το πείραμα 14*

Α΄.15 Πείραμα 15



Σχήμα Α΄.15: *Confusion Matrix για το πείραμα 15*

Α΄.16 Πείραμα 16



Σχήμα Α΄.16: *Confusion Matrix για το πείραμα 16*

Βιβλιογραφία

[1] Abdullah Aldaas. *A study on electronic payments and economic growth: Global evidences*. *Accounting*, 7, 2021.

[2] Chaimaa Belbergui, Najib Elkamoun και Rachid Hilal. *E-banking Overview: Concepts, Challenges and Solutions*. *Wireless Personal Communications*, 117:1059–1078, 2021.

[3] Vasileios Karyotis και Symeon Papavassiliou. *Macroscopic malware propagation dynamics for complex networks with churn*. *IEEE Communications Letters*, 19, 2015.

[4] Ahmed Alsayed και Anwar Bilgrami. *E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities*. *International Journal of Emerging Technology and advanced engineering*, 7(1):109–115, 2017.

[5] Diptiben Ghelani, Tan Kian Hua και Surendra Kumar Reddy Koduru. *Cyber security threats, vulnerabilities, and security solutions models in banking*. *Authorea Preprints*, 2022.

[6] Olawale Olowu, Ademilola Olowofela Adeleye, Abraham Okandeji Omokanye, Akintayo Micheal Ajayi, Adebayo Olabode Adepoju, Olayinka Mary Omole και Ernest C Chianumba. *AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity*. *GSC*, 2024.

[7] Vasilis Chatzigiannakis, Symeon Papavassiliou, Mary Grammatikou και B Maglaris. *Hierarchical anomaly detection in distributed large-scale sensor networks*. *11th IEEE symposium on computers and communications (ISCC'06)*, 2006.

[8] Abdulalem Ali, Shukor Abd Razak, Siti Hajar Othman, Taiseer Abdalla Elfadil Eisa, Arafat Al-Dhaqm, Maged Nasser, Tusneem Elhassan, Hashim Elshafie και Abdu Saif. *Financial fraud detection based on machine learning: a systematic literature review*. *Applied Sciences*, 12, 2022.

[9] Rithin Gopal Goriparthi. *AI-Enhanced Data Mining Techniques for Large-Scale Financial Fraud Detection*. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 14, 2023.

[10] Georgios Androulidakis, Vassilis Chatzigiannakis και Symeon Papavassiliou. *Network anomaly detection and classification via opportunistic sampling*. *IEEE network*, 23, 2009.

[11] Xiaoqian Zhu, Xiang Ao, Zidi Qin, Yanpeng Chang, Yang Liu, Qing He και Jianping Li. *Intelligent financial fraud detection practices in post-pandemic era*. *The Innovation*, 2, 2021.

[12] Vasileios Karyotis. *A Markov random field framework for modeling malware propagation in complex communications networks*. *IEEE Transactions on Dependable and Secure Computing*, 16, 2017.

[13] Constantine Manikopoulos και Symeon Papavassiliou. *Network intrusion and fault detection: a statistical anomaly approach*. *IEEE Communications Magazine*, 40, 2002.

[14] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi και Gianluca Bontempi. *Credit card fraud detection: a realistic modeling and a novel learning strategy*. *IEEE transactions on neural networks and learning systems*, 29, 2017.

[15] Vassilis Chatzigiannakis και Symeon Papavassiliou. *Diagnosing anomalies and identifying faulty nodes in sensor networks*. *IEEE Sensors Journal*, 7, 2007.

[16] Varun Chandola, Arindam Banerjee και Vipin Kumar. *Anomaly detection: A survey*. *ACM computing surveys (CSUR)*, 41, 2009.

[17] Zhong Li, Yuxuan Zhu και Matthijs Van Leeuwen. *A survey on explainable anomaly detection*. *ACM Transactions on Knowledge Discovery from Data*, 18, 2023.

[18] Ali Bou Nassif, Manar Abu Talib, Qassim Nasir και Fatima Mohamad Dakalbab. *Machine learning for anomaly detection: A systematic review*. *Ieee Access*, 9, 2021.

[19] Bartosz Krawczyk. *Learning from imbalanced data: open challenges and future directions*. *Progress in artificial intelligence*, 5, 2016.

[20] Nitesh V Chawla. *Data mining for imbalanced datasets: An overview*. *Data mining and knowledge discovery handbook*, 2010.

[21] Sotiris Kotsiantis, Dimitris Kanellopoulos, Panayiotis Pintelas και others. *Handling imbalanced datasets: A review*. *GESTS international transactions on computer science and engineering*, 30, 2006.

[22] Michael I Jordan και Tom M Mitchell. *Machine learning: Trends, perspectives, and prospects*. *Science*, 349, 2015.

[23] Pedro Domingos. *A few useful things to know about machine learning*. *Communications of the ACM*, 55, 2012.

[24] David E Rumelhart, Geoffrey E Hinton και Ronald J Williams. *Learning representations by back-propagating errors*. *Nature*, 323, 1986.

[25] Ian Goodfellow, Yoshua Bengio και Aaron Courville. *Deep Learning*. MIT press, 2016.

[26] Diederik P Kingma και Jimmy Ba. *Adam: A method for stochastic optimization*. *arXiv preprint arXiv:1412.6980*, 2014.

[27] Leo Breiman. *Random forests*. *Machine learning*, 45, 2001.

[28] Chao Chen, Andy Liaw και Leo Breiman. *Using random forest to learn imbalanced data*. *University of California, Berkeley*, 110, 2004.

[29] Fei Tony Liu, Kai Ming Ting και Zhi Hua Zhou. *Isolation forest*. *2008 Eighth IEEE International Conference on Data Mining*, 2008.

[30] Frank J Massey Jr. *The Kolmogorov-Smirnov test for goodness of fit*. *Journal of the American Statistical Association*, 46, 1951.

[31] Solomon Kullback και Richard A. Leibler. *On information and sufficiency*. *The Annals of Mathematical Statistics*, 22, 1951.

[32] Thomas M. Cover και Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2νδη έκδοση, 2006.

[33] Jianhua Lin. *Divergence measures based on the Shannon entropy*. *IEEE Transactions on Information theory*, 37, 1991.

[34] Bent Fuglede και Flemming Topsoe. *Jensen-Shannon divergence and Hilbert space embedding*. *Proceedings of the IEEE International Symposium on Information Theory*, 2004.

[35] B. W. Silverman. *Density Estimation for Statistics and Data Analysis*. Chapman and Hall, 1986.

[36] David W. Scott. *Multivariate Density Estimation: Theory, Practice, and Visualization*. John Wiley & Sons, 2015.

[37] Gareth James, Daniela Witten, Trevor Hastie και Robert Tibshirani. *An Introduction to Statistical Learning: with Applications in R*. Springer, 2013.

[38] Kevin P. Murphy. *Machine Learning: A Probabilistic Perspective*. MIT press, 2012.

[39] David M. W. Powers. *Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation*, 2020.

[40] Khaled Gubran Al-Hashedi και Pritheega Magalingam. *Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019*. *Computer Science Review*, 40, 2021.

[41] P. Vanini, S. Rossi, E. Zvizdic και T. Domenig. *Online payment fraud: from anomaly detection to risk management*. *Financial Innovation*, 9, 2023.

[42] D. Mangala και L. Soni. *A systematic literature review on frauds in banking sector*. *Journal of Financial Crime*, 30, 2023.

[43] Scott R Baker και Lorenz Kueng. *Household financial transaction data*. *Annual Review of Economics*, 14, 2022.

[44] Maghsoud Amiri και Siavash Hekmat. *Banking fraud: a customer-side overview of categories and frameworks of detection and prevention*. *Journal of Applied Intelligent Systems and Information Sciences*, 2, 2021.

[45] Iftikhar Ahmad, Shahid Iqbal, Shahzad Jamil και Muhammad Kamran. *A systematic literature review of e-banking frauds: current scenario and security techniques*. *Linguistica Antverpiensia*, 2, 2021.

[46] Riyan Pradesyah, Nawir Yuslem και Chuzaimah Batubara. *Fraud In Financial Institutions*. *Journal Of International Conference Proceedings (Jicp)*, τόμος 4, 2021.

[47] Richard J Bolton και David J Hand. *Statistical fraud detection: A review*. *Statistical science*, 17, 2002.

[48] Clifton Phua, Vincent Lee, Kate Smith και Ross Gayler. *A comprehensive survey of data mining-based fraud detection research*. *arXiv preprint arXiv:1009.6119*, 2010.

[49] Nick Duffield, Patrick Haffner, Balachander Krishnamurthy και Haakon Ringberg. *Rule-based anomaly detection on IP flows*. *IEEE INFOCOM 2009*, σελίδες 424–432. IEEE, 2009.

[50] Eric WT Ngai, Yuhau Hu, Yijun H Wong, Yijie Chen και Xin Sun. *The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature*. *Decision support systems*, 50, 2011.

[51] Zahra Zojaji, Reza Ebrahimi Atani, Amir Hassan Monadjemi και others. *A survey of credit card fraud detection techniques: data and technique oriented perspective*. *arXiv preprint arXiv:1611.06439*, 2016.

[52] Peter Rousseeuw, Domenico Perrotta, Marco Riani και Mia Hubert. *Robust Monitoring of Time Series with Application to Fraud Detection*. *Econometrics and Statistics*, 9, 2019.

[53] Gui Yu και Zhenlin Luo. *Financial fraud detection using a hybrid deep belief network and quantum optimization approach*. *Discover Applied Sciences*, 7, 2025.

[54] Xiaodan Xu, Huawen Liu και Minghai Yao. *Recent progress of anomaly detection*. *Complexity*, 2019(1):2686378, 2019.

[55] Amruta D Pawar, Prakash N Kalavadekar και Swapnali N Tambe. *A survey on outlier detection techniques for credit card fraud detection*. *IOSR Journal of Computer Engineering*, 16(2):44–48, 2014.

[56] Ebikella Mienye, Nobert Jere, George Obaido, Ibomoiye Domor Mienye και Kehinde Aruleba. *Deep Learning in Finance: A survey of Applications and techniques*. *AI*, 5, 2024.

[57] Ibrahim Y Hafez, Ahmed Y Hafez, Ahmed Saleh, Amr A Abd El-Mageed και Amr A Abohany. *A systematic review of AI-enhanced techniques in credit card fraud detection*. *Journal of Big Data*, 12, 2025.

[58] Gayan K Kulatilleke. *Challenges and complexities in machine learning based credit card fraud detection*. *arXiv preprint arXiv:2208.10943*, 2022.

[59] John O Awoyemi, Adebayo O Adetunmbi και Samuel A Oluwadare. *Credit card fraud detection using machine learning techniques: A comparative analysis*. *2017 international conference on computing networking and informatics (ICCNI)*. IEEE, 2017.

[60] Pradheepan Raghavan και Neamat El Gayar. *Fraud detection using machine learning and deep learning*. *2019 international conference on computational intelligence and knowledge economy (ICCIKE)*, 2019.

[61] Johan Perols. *Financial statement fraud detection: An analysis of statistical and machine learning algorithms*. *Auditing: A Journal of Practice & Theory*, 30, 2011.

[62] Andrei Sorin Sabau. *Survey of clustering based financial fraud detection research*. *Informatica Economica*, 16, 2012.

[63] MA Al-Shabi. *Credit card fraud detection using autoencoder model in unbalanced datasets*. *Journal of Advances in Mathematics and Computer Science*, 33, 2019.

[64] Hyder John και Sameena Naaz. *Credit card fraud detection using local outlier factor and isolation forest*. *Int. J. Comput. Sci. Eng*, 7, 2019.

[65] Tran Khanh Dang, Thanh Cong Tran, Luc Minh Tuan και Mai Viet Tiep. *Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems*. *Applied Sciences*, 11, 2021.

[66] Maram Alamri και Mourad Ykhlef. *Survey of credit card anomaly and fraud detection using sampling techniques*. *Electronics*, 11, 2022.

[67] Md Kamrul Hasan Chy. *Proactive Fraud Defense: Machine Learning's Evolving Role in Protecting Against Online Fraud*. *arXiv preprint arXiv:2410.20281*, 2024.

[68] Fawaz Khaled Alarfaj, Iqra Malik, Hikmat Ullah Khan, Naif Almusallam, Muhammad Ramzan και Muzamil Ahmed. *Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms*. *Ieee Access*, 10, 2022.

[69] Abhimanyu Roy, Jingyi Sun, Robert Mahoney, Loreto Alonzi, Stephen Adams και Peter Beling. *Deep learning detecting fraud in credit card transactions*. *2018 systems and information engineering design symposium (SIEDS)*, 2018.

[70] Ajay Shrestha και Ausif Mahmood. *Review of deep learning algorithms and architectures*. *IEEE access*, 7, 2019.

[71] Suresh Dara και Priyanka Tumma. *Feature extraction by using deep learning: A survey*. *2018 Second international conference on electronics, communication and aerospace technology (ICECA)*, 2018.

[72] Yu Xie, Guanjun Liu, Ruihao Cao, Zhenchuan Li, Chungang Yan και Changjun Jiang. *A feature extraction method for credit card fraud detection*. *2019 2nd International Conference on Intelligent Autonomous Systems (ICoIAS)*, 2019.

[73] Akash Gandhar, Kapil Gupta, Aman Kumar Pandey και Dharm Raj. *Fraud detection using machine learning and deep learning*. *SN Computer Science*, 5, 2024.

[74] Mary Anne Walauskis και Taghi M Khoshgoftaar. *Unsupervised label generation for severely imbalanced fraud data*. *Journal of Big Data*, 12, 2025.

[75] François De La Bourdonnaye και Fabrice Daniel. *Evaluating resampling methods on a real-life highly imbalanced online credit card payments dataset*. *arXiv preprint arXiv:2206.13152*, 2022.

[76] Roy Wedge, James Max Kanter, Santiago Moral Rubio, Sergio Iglesias Perez και Kalyan Veeramachaneni. *Solving the" false positives" problem in fraud prediction*. *arXiv preprint arXiv:1710.07709*, 2017.

[77] Doaa Hassan. *The impact of false negative cost on the performance of cost sensitive learning based on Bayes minimum risk: a case study in detecting fraudulent transactions*. *International Journal of Intelligent Systems and Applications*, 9, 2017.

[78] Pallavi Kulkarni και Roshani Ade. *Logistic regression learning model for handling concept drift with unbalanced data in credit card fraud detection system*, 2016.

[79] Huiying Mao, Yung wen Liu, Yuting Jia και Jay Nanduri. *Adaptive fraud detection system using dynamic risk features*. *arXiv preprint arXiv:1810.04654*, 2018.

[80] Alexander Goldberg, Giulia Fanti, Nihar Shah και Steven Wu. *Benchmarking Fraud Detectors on Private Graph Data*. 2024.

[81] Robert KL Kennedy, Flavio Villanustre, Taghi M Khoshgoftaar και Zahra Salekshahrezaee. *Synthesizing class labels for highly imbalanced credit card fraud detection data*. *Journal of Big Data*, 11, 2024.

[82] Jabbar Hussain. *Deep learning black box problem*, 2019.

[83] Tamjid Al Rahat, Minjun Long και Yuan Tian. *Is your policy compliant? a deep learning-based empirical study of privacy policies' compliance with gdpr*. *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, 2022.

[84] Giovanni Sartor, Francesca Lagioia και others. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. 2020.

[85] Yisong Chen, Chuqing Zhao, Yixin Xu και Chuanhao Nie. *Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review*, 2025.

[86] Fabrizio Carcillo, Yann Aël Le Borgne, Olivier Caelen, Yacine Kessaci, Frédéric Oblé και Gianluca Bontempi. *Combining unsupervised and supervised learning in credit card fraud detection*. *Information Sciences*, 557, 2021.

[87] Chamal Gomes, Zhuo Jin και Hailiang Yang. *Insurance fraud detection with unsupervised deep learning*. *Journal of Risk and Insurance*, 88, 2021.

[88] Gang Wang, Jingling Ma και Gang Chen. *Attentive statement fraud detection: Distinguishing multimodal financial data with fine-grained attention*. *Decision Support Systems*, 167, 2023.

[89] Zheng Zhang, Xiangyu Su, Ji Wu, Claudio J Tessone και Hao Liao. *Heterogeneous graph representation learning via mutual information estimation for fraud detection*. *Journal of Network and Computer Applications*, 234, 2025.

[90] Nan Jiang, Fuxian Duan, Honglong Chen, Wei Huang και Ximeng Liu. *MAFI: GNN-Based Multiple Aggregators and Feature Interactions Network for Fraud Detection Over Heterogeneous Graph*. *IEEE Transactions on Big Data*, 8, 2022.

[91] Tung Duong Mai, Kien Hoang, Aitolkyn Baigutanova, Gaukhartas Alina και Sundong Kim. *Customs Fraud Detection in the Presence of Concept Drift*, 2021.

[92] Vivek Yelleti. *ROSFD: Robust Online Streaming Fraud Detection with Resilience to Concept Drift in Data Streams*, 2025.

[93] Siddharth Vimal, Kanishka Kayathwal, Hardik Wadhwa και Gaurav Dhama. *Application of deep reinforcement learning to payment fraud*. *arXiv preprint arXiv:2112.04236*, 2021.

[94] ADEYINKA ORELAJA και ADENIKE F ADEYEMI. *Developing Real-Time Fraud Detection and Response Mechanisms for Financial Transactions*. *IRE Journals*, 2024.

[95] Fabrizio Carcillo, Andrea Dal Pozzolo, Yann Aël Le Borgne, Olivier Caelen, Yannis Mazzer και Gianluca Bontempi. *Scarff: a scalable framework for streaming credit card fraud detection with spark*. *Information fusion*, 41, 2018.

[96] *NumPy: the fundamental package for scientific computing with Python*. https://numpy.org/. Προσπελάστηκε τον Ιούνιο 2025.

[97] *Pandas: Python Data Analysis Library*. https://pandas.pydata.org/. Προσπελάστηκε τον Ιούνιο 2025.

[98] *Scikit-learn: Machine Learning in Python*. https://scikit-learn.org/. Προσπελάστηκε τον Ιούνιο 2025.

[99] *Imbalanced-learn*. https://imbalanced-learn.org/stable. Προσπελάστηκε τον Ιούνιο 2025.

[100] *TensorFlow: An end-to-end open source machine learning platform*. https://www.tensorflow.org/. Προσπελάστηκε τον Ιούνιο 2025.

[101] *SciPy: Python-based ecosystem of open-source software for mathematics, science, and engineering*. https://scipy.org/. Προσπελάστηκε τον Ιούνιο 2025.

[102] *Seaborn: statistical data visualization*. https://seaborn.pydata.org/. Προσπελάστηκε τον Ιούνιο 20255.

[103] *Matplotlib: Python plotting — Matplotlib 3.x documentation*. https://matplotlib.org/. Προσπελάστηκε τον Ιούνιο 2025.

Συντομογραφίες - Αρκτικόλεξα - Ακρωνύμια

κτλπ	και τα λοιπά
π.χ.	παραδείγματος χάρη
KDE	Kernel Density Estimation
PCA	Principal Components Analysis
AUC	Area Under the Curve
ROC	Receiver Operating Characteristic
SMOTE	Synthetic Minority Oversampling Technique
MLP	Mutli-Layer Perceptron
LSTM	Long Short-Term Memory
KL	Kullback–Leibler
JSD	Jensen–Shannon Divergence
RF	Random Forest

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος
Ταξινομητής	Classifier
Απάτη	Fraud
Απάτη με Πιστωτικές Κάρτες	Credit Card Fraud
Απάτη Ταυτότητας	Identity Theft
Κατάληψη Λογαριασμού	Account Takeover
Ξέπλυμα Χρήματος	Money Laundering
Μη-Απάτη	Non-Fraud
Ομαλοποίηση	Regularization
Τυποποίηση	Standardization
Υπερπροσαρμογή	Overfit
Επαναδειγματοληψία	Sampling
Υποδειγματοληψία	Undersampling
Υπερδειγματοληψία	Oversampling
Ανίχνευση Ανωμαλιών	Anomaly Detection
Ανίχνευση Απάτης	Fraud Detection
Μάθηση με Ανισόρροπα Δεδομένα	Imbalanced Learning
Σύνολο Δεδομένων με Ανισορροπία Κλάσεων	Imbalanced Dataset
Οπισθοδιάδοση	Back-propagation
Μέθοδος Συνόλου Μοντέλων	Ensemble Method
Ανίχνευση Ακραίων Τιμών	Outlier Detection
Εξαγωγή Χαρακτηριστικών	Feature Extraction
Μάθηση Βασισμένη σε Γράφους	Graph-Based Learning
Μετατόπιση Εννοιας	Concept Drift
Προκατάληψη	Bias
Ρυθμός Μάθησης	Learning rate
Μέγεθος Δείγματος	Batch Size
Διαστήματα	Bins
Ακρίβεια Ταξινόμησης	Accuracy
Ευστοχία	Precision
Ανάκληση	Recall
Πίνακας Σύγχυσης	Confusion Matrix
Σύνολο Εκπαίδευσης	Train Set
Σύνολο Ελέγχου	Test Set
Σύνολο Επικύρωσης	Validation Set