ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ»

ΕΙΔΙΚΕΥΣΗ: ΠΡΟΗΓΜΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Ολοκληρωμένο Περιβάλλον Προσομοίωσης Πειραμάτων Ομοσπονδιακής Μηχανικής Μάθησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων Καθηγητής: Δημοσθένης Κυριαζής

Κωνσταντίνος Μαυρογιώργος

Α.Μ.: ΜΕ2144

Email: kostismvg@gmail.com

Πειραιάς, Ιανουάριος 2023

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου προς τον καθηγητή Δημοσθένη Κυριαζή για την καθοδήγησή του καθ’ όλη την διάρκεια της εκπόνησης της παρούσας μεταπτυχιακής διπλωματικής εργασίας. Επίσης, θα ήθελα να ευχαριστήσω την μητέρα μου, τον πατέρα μου και την αδελφή μου που πιστεύουν στις ικανότητές μου και είναι πάντα στο πλευρό μου. Τέλος, θέλω να εκφράσω την ευγνωμοσύνη μου στον άνθρωπό μου που είναι δίπλα μου και με στηρίζει άνευ όρων.

Στην Οικογένειά μου

Πίνακας Περιεχομένων

Πίνακας Ακρωνυμίων 6
Κατάλογος Εικόνων 7
Κατάλογος Πινάκων 9
Περίληψη 10
1. Εισαγωγή 11
1.1. Σκοπός Διπλωματικής Εργασίας 11
1.2. Δομή Διπλωματικής Εργασίας 12
2. Ανασκόπηση Βιβλιογραφίας 13
2.1. Ορισμός Προβλήματος 13
2.2. Ορισμός Ομοσπονδιακής Μάθησης 15
2.3. Ιδιωτικότητα Δεδομένων στην Ομοσπονδιακή Μάθηση 17
2.4. Κατηγορίες Ομοσπονδιακής Μάθησης 20
2.5. Εφαρμογές Ομοσπονδιακής Μάθησης 23
2.6. Μηχανική Μάθηση και Αλγόριθμοι 27
2.6.1. Εποπτευόμενη Μηχανική Μάθηση 27
2.6.2. Μη Εποπτευόμενη Μηχανική Μάθηση 29
2.7. Προκλήσεις Ομοσπονδιακής Μάθησης 30
3. Προτεινόμενη Προσέγγιση 32
3.1. Γενική Αρχιτεκτονική 32
3.2. Χρησιμοποιούμενες Τεχνολογίες 36
3.3. Σύνολα Δεδομένων 38
3.4. Καθαρισμός Δεδομένων 46
3.5. Χρησιμοποιούμενοι Αλγόριθμοι 48
3.6. Οδηγίες Εγκατάστασης και Εκτέλεσης 51
3.6.1. Α’ Τρόπος Εγκατάστασης και Εκτέλεσης 51
3.6.2. Β’ Τρόπος Εγκατάστασης και Εκτέλεσης 52
3.7. Διεπαφή Χρήστη 54
4. Πειραματικά Αποτελέσματα 56
4.1. Πλήρες Ενδεικτικό Σενάριο Χρήσης 56

4.2. Αποτελέσματα Ενδεικτικών Πειραμάτων 65
4.3. Σύγκριση Αποτελεσμάτων Ενδεικτικών Πειραμάτων 70
4.3.1. Ακρίβεια Προβλέψεων 70
4.3.2. Απαιτήσεις σε Πόρους 76
5. Συμπεράσματα 79
Αναφορές 82

Πίνακας Ακρωνυμίων

Ακρωνύμιο	Ορισμός
ΜΕΘ	Μονάδα Εντατικής Θεραπείας
ΟΜ	Ομοσπονδιακή Μάθηση
ΤΝ	Τεχνητή Νοημοσύνη
AdaBoost	Adaptive Boosting
AI	Artificial Intelligence
AJAX	Asynchronous JavaScript And XML
ANN	Artificial Neural Network
CMWK-Means	Constrained Minkowski Weighted K-Means
CNN	Convolutional Neural Network
COP K-Means	Constrained K-means
CSS	Cascading Style Sheets
DNN	Deep Neural Network
DP	Differential Privacy
DT	Decision tree
XGBoost	Extreme Gradient Boosting
FL	Federated Learning
FTL	Federated Transfer Learning
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
GMM	Gaussian Mixture Model
HFL	Horizontal Federated Learning
HTML	HyperText Markup Language
KNN	K-Nearest Neighbors
LDA	Linear Discriminant Analysis
LR	Logistic Regression
ML	Machine Learning
NB	Naive Bayes
PSP	Privacy-aware Ser- vice Placement
RF	Random Forest
SGD	Stochastic Gradient Descent
SMC	Secure Multiparty Computation
SOM	Self-Organizing Map
SVM	Support vector machine
VFL	Vertical Federated Learning

Κατάλογος Εικόνων

Εικόνα 1: Προσέγγιση ομοσπονδιακής μάθησης 16
Εικόνα 2: Οριζόντια ομοσπονδιακή μάθηση 20
Εικόνα 3: Κάθετη ομοσπονδιακή μάθηση 21
Εικόνα 4: Ομοσπονδιακή μάθηση μεταφοράς 22
Εικόνα 5: Αρχιτεκτονική προτεινόμενου μηχανισμού 33
Εικόνα 6: Ενδεικτικό παράδειγμα κανόνα επικύρωσης 46
Εικόνα 7: Ενδεικτικό παράδειγμα σχήματος δεδομένων 46
Εικόνα 8: Παράδειγμα απλού νευρωνικού δικτύου 50
Εικόνα 9: GitHub αποθετήριο εφαρμογής 51
Εικόνα 10: DockerHub αποθετήριο του image της εφαρμογής 52
Εικόνα 11: GitHub αποθετήριο του image της εφαρμογής 53
Εικόνα 12: Αρχική διεπαφή χρήστη μηχανισμού 54
Εικόνα 13: Πραγματοποίηση εκπαίδευσης με συγκεκριμένες παραμέτρους 57
Εικόνα 14: Εμφάνιση αποτελεσμάτων εκπαίδευσης 58
Εικόνα 15: Σύνοψη του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος 59
Εικόνα 16: Πληροφορίες συγκεκριμένου χαρακτηριστικού του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος 60
Εικόνα 17: Προβολή συσχέτισης Pearson χαρακτηριστικών του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος 60
Εικόνα 18: Προβολή ελλιπών τιμών του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος 61
Εικόνα 19: Προβολή σημαντικών ειδοποιήσεων σχετικά με τα χαρακτηριστικά του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος. 61
Εικόνα 20: Διάγραμμα διασποράς των Accuracy και Precision των πειραμάτων, συναρτήσει του Recall, του F1 - Score, του Συνόλου Δεδομένων και του Αλγόριθμου Μηχανικής Μάθησης. 62
Εικόνα 21: Διάγραμμα διασποράς των Accuracy και Precision των Πειραμάτων, συναρτήσει του Recall, του F1 - Score, της Συνάρτησης Βελτιστοποίησης και της Συνάρτησης Ενεργοποίησης. 63
Εικόνα 22: Διάγραμμα διασποράς των Accuracy και Precision των Πειραμάτων, συναρτήσει της Συνάρτησης Ενεργοποίησης, του Συνόλου Δεδομένων, του Αλγόριθμου Μηχανικής Μάθησης και του Πλήθους Περιόδων Εκπαίδευσης. 63
Εικόνα 23: Μέσοι όροι των τιμών των Accuracy, Precision, Recall και F1 – Score ανά Αλγόριθμο Μηχανικής Μάθησης. 64
Εικόνα 24: Διάγραμμα διασποράς της Χρησιμοποιούμενης Μνήμης και του Χρόνου Εκτέλεσης των Πειραμάτων, συναρτήσει του Αλγόριθμου Μηχανικής Μάθησης, του Αριθμού Χρηστών και του Συνόλου Δεδομένων. 64
Εικόνα 25: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του αλγόριθμου μηχανική μάθησης. 70

Εικόνα 26: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει της συνάρτησης ενεργοποίησης. 71
Εικόνα 27: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει της συνάρτησης βελτιστοποίησης..... 72
Εικόνα 28: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του πλήθους χρηστών. 73
Εικόνα 29: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του πλήθους περιόδων..... 74
Εικόνα 30: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του μεγέθους υποσυνόλου δεδομένων εκπαίδευσης..... 75
Εικόνα 31: Σύγκριση πλήθους χρηστών, χρόνου εκτέλεσης και μνήμης, συναρτήσει του αλγόριθμου μηχανική μάθησης. 76
Εικόνα 32: Σύγκριση χρόνου εκτέλεσης και μνήμης, συναρτήσει της συνάρτησης ενεργοποίησης..... 77
Εικόνα 33: Σύγκριση χρόνου εκτέλεσης και μνήμης, συναρτήσει της συνάρτησης βελτιστοποίησης..... 78

Κατάλογος Πινάκων

Πίνακας 1: Εφαρμογές ομοσπονδιακής μάθησης 23
Πίνακας 2: Προκλήσεις ομοσπονδιακής μάθησης 30
Πίνακας 3: Περιγραφή Συνόλου Δεδομένων «Stroke» 38
Πίνακας 4: Περιγραφή Συνόλου Δεδομένων «Covid - 19» 39
Πίνακας 5: Περιγραφή Συνόλου Δεδομένων «Breast Cancer» 40
Πίνακας 6: Περιγραφή Συνόλου Δεδομένων «Kidney Disease» 42
Πίνακας 7: Περιγραφή Συνόλου Δεδομένων «Water Potability» 43
Πίνακας 8: Περιγραφή Συνόλου Δεδομένων «Weather Forecast» 43
Πίνακας 9: Περιγραφή Συνόλου Δεδομένων «Iris» 44
Πίνακας 10: Περιγραφή Συνόλου Δεδομένων «Car Evaluation» 44
Πίνακας 11: Χρησιμοποιούμενοι Αλγόριθμοι 48
Πίνακας 12: Διαθέσιμες Παράμετροι Πειραμάτων 56
Πίνακας 13: Διαθέσιμα Αποτελέσματα Πειραμάτων 58
Πίνακας 14: Αποτελέσματα Πραγματοποιηθέντων Πειραμάτων 65

Περίληψη

Η ραγδαία εξέλιξη του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) έχει οδηγήσει στην εξαιρετικά αυξημένη παραγωγή δεδομένων. Οι ποσότητες των δεδομένων που παράγονται είναι γιγαντιαίες και ο ρυθμός με τον οποίο παράγονται αυξάνεται εκθετικά, οδηγώντας στην εποχή των Μεγάλων Δεδομένων. Πλέον, υπάρχει πληθώρα συσκευών οι οποίες παράγουν τα δικά τους δεδομένα και τα οποία, δυνητικά, μπορούν να αξιοποιηθούν για την εξόρυξη χρήσιμης πληροφορίας και γνώσης. Ωστόσο, ο όγκος των δεδομένων, σε συνδυασμό με άλλους περιορισμούς που πρέπει να λαμβάνονται υπόψη, κυριότερος εξ αυτών είναι η διασφάλιση της ιδιωτικότητας στα δεδομένα, έχουν οδηγήσει στην εύρεση εναλλακτικών μεθόδων για την ανάλυση των δεδομένων και γενικά, για την εφαρμογή τεχνικών Μηχανικής Μάθησης σε αυτά. Η πιο πρόσφατη προσέγγιση που έχει προταθεί για να αντιμετωπίσει τις προαναφερθείσες προκλήσεις είναι η Ομοσπονδιακή Μάθηση. Η Ομοσπονδιακή Μάθηση βασίζεται στην ιδέα της κατανεμημένης επεξεργασίας και ανάλυσης δεδομένων και την δημιουργία μοντέλων Μηχανικής Μάθησης τοπικά στην εκάστοτε συσκευή παραγωγής δεδομένων. Τα προαναφερθέντα επιμέρους μοντέλα, εν συνεχεία, συνδυάζονται σε ένα ενιαίο μοντέλο, χωρίς τη μεταφορά των δεδομένων από τα οποία προέκυψαν τα αντίστοιχα μοντέλα. Με αυτό τον τρόπο η Ομοσπονδιακή Μάθηση διασφαλίζει την ασφάλεια και την αξιοπιστία των δεδομένων, χωρίς να επηρεάζει αρνητικά την αποδοτικότητα και την αποτελεσματικότητα τον αλγορίθμων Μηχανικής Μάθησης, συγκριτικά με αντίστοιχες συμβατικές μεθόδους. Φυσικά, η επιλογή της Ομοσπονδιακής Μάθησης έναντι μιας συμβατικής μεθόδου, θα πρέπει να πραγματοποιείται βάσει διαφορετικών παραγόντων, όπως του εκάστοτε σεναρίου χρήσης και των διαθέσιμων δεδομένων και υπολογιστικών πόρων. Προς αυτή τη κατεύθυνση, η παρούσα διπλωματική εργασία παρέχει, αρχικά, μία αναλυτική ανασκόπηση βιβλιογραφίας αναφορικά με την Ομοσπονδιακή Μάθηση. Εν συνεχεία, προτείνει ένα ολοκληρωμένο περιβάλλον, το οποίο παρέχει στους χρήστες την δυνατότητα εκτέλεσης πειραμάτων με τους αλγορίθμους, τις παραμέτρους και τα σύνολα δεδομένων της αρεσκείας τους και το οποίο οπτικοποιεί τα αποτελέσματα των αντίστοιχων πειραμάτων με κατανοητό τρόπο. Στόχος του συγκεκριμένου περιβάλλοντος είναι, όχι μόνο να λειτουργήσει ως οδηγός για την υιοθέτηση του ομοσπονδιακού τρόπου μάθησης, αλλά και για να συνδράμει στην επιλογή των πιο αποδοτικών αλγορίθμων και των παραμέτρων τους ανάλογα με τα σενάρια χρήσης που ενδιαφέρουν τους εκάστοτε χρήστες.

Θεματική Περιοχή: Ομοσπονδιακή Μάθηση

Λέξεις Κλειδιά: Ομοσπονδιακή Μάθηση, Μηχανική Μάθηση, Αλγόριθμοι, Ανάλυση Δεδομένων

1. Εισαγωγή

1.1. Σκοπός Διπλωματικής Εργασίας

Η Ομοσπονδιακή Μάθηση (ΟΜ) αποτελεί μία από τις πιο σύγχρονες εξελίξεις στο τομέα της Μηχανικής Μάθησης και της Τεχνητής Νοημοσύνης γενικότερα. Η Ομοσπονδιακή Μάθηση αποτελεί την απάντηση στις προκλήσεις που έχουν δημιουργηθεί λόγω των ραγδαίων εξελίξεων στο τομέα του Διαδικτύου των Πραγμάτων και την εκθετική αύξηση του πλήθους των συσκευών που είναι ικανές να παράγουν δεδομένα, αλλά και να τα αναλύουν. Πλέον, τα δεδομένα είναι κατανεμημένα, κάτι το οποίο σημαίνει ότι οι συμβατικές μέθοδοι Μηχανικής Μάθησης ενδεχομένως να μην είναι πλέον τόσο αποδοτικές, ενώ συγχρόνως διεγείρονται ερωτήματα σχετικά με την διασφάλιση της ιδιωτικότητας των αντίστοιχων δεδομένων. Φυσικά, η υιοθέτηση του ομοσπονδιακού τρόπου μάθησης θα πρέπει να γίνεται βάσει του εκάστοτε σεναρίου χρήσης, καθώς, ανάλογα με το είδος των δεδομένων, των συσκευών και των απαιτήσεων των χρηστών που απαρτίζουν ένα σενάριο χρήσης, υπάρχει και ο πιο αποδοτικός και αποτελεσματικός τρόπος εκπαίδευσης μοντέλων Μηχανικής Μάθησης. Ένας τέτοιος τρόπος δύναται να είναι ένας από τους συμβατικούς ή ο ομοσπονδιακός τρόπος μάθησης.

Προς αυτή τη κατεύθυνση, η παρούσα διπλωματική εργασία στοχεύει, αρχικά, να παραθέσει τις βασικές αρχές και τα χαρακτηριστικά της Ομοσπονδιακής Μάθησης, τις εφαρμογές της σε πραγματικά σενάρια χρήσης και τους αλγόριθμους Μηχανικής Μάθησης που έχουν αναπτυχθεί και μπορούν να αξιοποιηθούν και στην επίλυση προβλημάτων με ομοσπονδιακό τρόπο. Εν συνεχεία, η παρούσα διπλωματική εργασία προτείνει ένα ολοκληρωμένο περιβάλλον, δηλαδή μία εφαρμογή, το οποίο επιτρέπει στους χρήστες του να εκπαιδεύσουν υλοποιημένους αλγόριθμους Μηχανικής Μάθησης, επιλέγοντας οι ίδιοι τις παραμέτρους που επιθυμούν, τα σύνολα δεδομένων της αρεσκείας τους και αν επιθυμούν η εκπαίδευση να πραγματοποιηθεί με ομοσπονδιακό τρόπο (δηλαδή με χρήση πολλών χρηστών) ή όχι. Μέσα από τα πειράματά τους οι χρήστες δύναται να πραγματοποιήσουν μία συγκριτική μελέτη των πειραμάτων τους, μέσω κατάλληλων οπτικοποιήσεων, έτσι ώστε να καταλήξουν στην πιο αποδοτική προσέγγιση Μηχανικής Μάθησης και στον πιο αποτελεσματικό αλγόριθμο για τα εκάστοτε σενάρια χρήσης που τους ενδιαφέρουν. Μέσω των ενδεικτικών πειραμάτων που διενεργήθηκαν στα πλαίσια της εργασίας, πραγματοποιείται, επίσης, μία συγκριτική μελέτη μεταξύ των αλγορίθμων που έχουν υλοποιηθεί και των διαφορετικών παραμέτρων που αυτοί δύναται να πάρουν, καταλήγοντας στον αποτελεσματικότερο αλγόριθμο και τις ιδανικότερες παραμέτρους, βάσει της ακρίβειας των αντίστοιχων προβλέψεων και τις απαιτήσεις σε υπολογιστικούς πόρους.

1.2. Δομή Διπλωματικής Εργασίας

Πιο συγκεκριμένα, στην εν λόγω διπλωματική εργασία αρχικά παρατίθεται μία βιβλιογραφική ανασκόπηση, η οποία αφορά τον ορισμό και τα χαρακτηριστικά της Ομοσπονδιακής Μάθησης, τις διαφορετικές ερευνητικές και εμπορικές προσεγγίσεις που την αξιοποιούν και τους αλγόριθμους Μηχανικής Μάθησης που υπάρχουν και μπορούν να συνδράμουν σε αυτή. Στη συνέχεια, προσδιορίζεται και αναλύεται η εφαρμογή που έχει αναπτυχθεί στα πλαίσια της παρούσας διπλωματικής εργασίας, όπου παρατίθεται η αρχιτεκτονική της. Επίσης, αναλύονται οι τεχνολογίες, τα σύνολα δεδομένων και οι αλγόριθμοι που έχουν χρησιμοποιηθεί, ενώ περιγράφεται και ο τρόπος εγκατάστασης και εκτέλεσής της. Τέλος παρατίθενται και σχολιάζονται τα πειραματικά αποτελέσματα της εφαρμογής, παρέχοντας μία ενδελεχή σύγκριση μεταξύ τους.

Ειδικότερα, η παρούσα διπλωματική εργασία οργανώνεται ως εξής:

- Το *Κεφάλαιο 1 (Εισαγωγή)* αποτελεί την εισαγωγή της διπλωματικής εργασίας, καταγράφοντας τον στόχο και την επιμέρους δομή της.
- Το *Κεφάλαιο 2 (Ανασκόπηση Βιβλιογραφίας)* περιλαμβάνει μία πλήρη βιβλιογραφική ανασκόπηση σχετικά με τον ορισμό και τα χαρακτηριστικά της Ομοσπονδιακής Μάθησης, τις διαφορετικές ερευνητικές και εμπορικές προσεγγίσεις που την αξιοποιούν και τους αλγόριθμους Μηχανικής Μάθησης που υπάρχουν και μπορούν να συνδράμουν σε αυτή.
- Το *Κεφάλαιο 3 (Προτεινόμενη Προσέγγιση)* περιλαμβάνει μία αναλυτική περιγραφή της εφαρμογής που αναπτύχθηκε στα πλαίσια της παρούσας διπλωματικής εργασίας, η οποία περιλαμβάνει διάφορους υλοποιημένους αλγόριθμους Μηχανικής Μάθησης με τους οποίους μπορούν να πειραματιστούν οι χρήστες, αξιοποιώντας διάφορα σύνολα δεδομένων, με ή χωρίς τη χρήση του ομοσπονδιακού τρόπου μάθησης.
- Το *Κεφάλαιο 4 (Πειραματικά Αποτελέσματα)* περιλαμβάνει ένα πλήρες ενδεικτικό σενάριο χρήσης της εφαρμογής, ενώ, συγχρόνως, καταγράφει τα αποτελέσματα των ενδεικτικών πειραμάτων που διενεργήθηκαν στα πλαίσια της παρούσας διπλωματικής εργασίας και τα συγκρίνει βάσει της ακρίβειας των αντίστοιχων προβλέψεων και τις απαιτήσεις σε υπολογιστικούς πόρους.
- Το *Κεφάλαιο 5 (Συμπεράσματα)* συνοψίζει τα ευρήματα της παρούσας διπλωματικής εργασίας και καταγράφει τυχών μελλοντικές βελτιώσεις και προεκτάσεις αυτής.

2. Ανασκόπηση Βιβλιογραφίας

2.1. Ορισμός Προβλήματος

Την σημερινή εποχή υπάρχει μία εκθετική αύξηση στη χρήση της Τεχνητής Νοημοσύνης (Artificial Intelligence – AI), προκειμένου να επιλυθούν διάφορα προβλήματα της καθημερινότητας. Οι διάφορες τεχνικές Τεχνητής Νοημοσύνης (ΤΝ) αξιοποιούν δεδομένα που πλέον παράγονται από πληθώρα διαφορετικών πηγών, έτσι ώστε να εξάγουν χρήσιμη γνώση την οποία, εν συνεχεία, θα αξιοποιήσουν για να παρέχουν δυνατότητες που, μέχρι πρότινος δεν ήταν εφικτό να υλοποιηθούν. Με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας , οι υπολογιστικές δυνατότητες των υπολογιστών, είτε πρόκειται για προσωπικούς Η/Υ, είτε για έξυπνες συσκευές, έχουν οδηγήσει σε ραγδαίες εξελίξεις στον τομέα την Τεχνητής Νοημοσύνης και ειδικότερα της Μηχανικής Μάθησης (Machine Learning – ML). Οι προαναφερθείσες υπολογιστικές δυνατότητες έχουν οδηγήσει στην ανάπτυξη νέων αλγορίθμων και προσεγγίσεων που μέχρι πολύ πρόσφατα δεν μπορούσαν να υλοποιηθούν, λόγω περιορισμένων υπολογιστικών δυνατοτήτων. Μία από αυτές τις προσεγγίσεις, η οποία έχει αναπτυχθεί πολύ πρόσφατα, καθότι προτάθηκε από την Google μόλις το 2016, είναι η Ομοσπονδιακή Μάθηση - ΟΜ (Federated Learning – FL).

Η ΟΜ προτάθηκε για να αντιμετωπίσει δύο (2) βασικά προβλήματα τα οποία προέκυψαν λόγω του αυξημένου όγκου δεδομένων που παράγονται και της ανάγκης για διαχείριση και επεξεργασία αυτών με ασφαλή τρόπο, προκειμένου να εξαχθεί χρήσιμη πληροφορία. Το πρώτο πρόβλημα αφορά την συλλογή και επεξεργασία των δεδομένων, καθώς αυτά βρίσκονται σε διαφορετικές «τοποθεσίες», δηλαδή είναι κατανεμημένα. Ο όρος «τοποθεσία» μπορεί να αφορά από κάποιον διακομιστή μέχρι και ολόκληρο οργανισμό. Οι διαφορετικές τοποθεσίες αποτελούν βασικό πρόβλημα καθώς συνεπάγονται μεγάλο κόστος για την «ενοποίηση» των αντίστοιχων δεδομένων, έτσι ώστε αυτά να υποστούν την αντίστοιχη επεξεργασία (π.χ. να εκπαιδευτεί ένα ML μοντέλο). Η παραπάνω «ενοποίηση» μπορεί να είναι αδύνατη, είτε λόγω των διαφορετικών προτύπων που ακολουθούν τα δεδομένα, είτε εξαιτίας του κόστους που συνεπάγεται η συγκεκριμένη ενοποίηση. Το δεύτερο πρόβλημα αφορά την ιδιωτικότητα των δεδομένων. Πλέον, οι διάφορες εταιρίες και οργανισμοί ρίχνουν τεράστιο βάρος στη διασφάλιση της ιδιωτικότητας των δεδομένων και της προστασίας της ταυτότητας των χρηστών, εξαιτίας και των συνεχόμενων επιθέσεων που επιχειρούν να ανακτήσουν δεδομένα χρηστών, χωρίς τη συγκατάθεσή τους, για τη πραγματοποίηση διάφορων παράνομων και κακόβουλων ενεργειών, όπως συνέβη με το Facebook το 2018 [1]. Έχουν θεσπιστεί ολόκληρα νομοθετικά πλαίσια τα οποία επιχειρούν να διασφαλίσουν την ιδιωτικότητα των δεδομένων, όπως είναι για παράδειγμα ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation – GDPR). Ο GDPR νομοθετήθηκε από την Ευρωπαϊκή Ένωση στις 25 Μαΐου του 2018 και απαιτεί από οποιοδήποτε πρόσωπο/οργανισμό διατηρεί δεδομένα χρηστών, να λαμβάνει όλα τα απαραίτητα μέτρα, έτσι ώστε να διασφαλίζεται η προστασία τους και οι αντίστοιχοι χρήστες να έχουν τη δυνατότητα να τα διαχειρίζονται [2].

Μέχρι πρότινος, υπήρχε μία συγκεκριμένη ροή που ακολουθούσαν τα δεδομένα έτσι ώστε να εφαρμοστούν σε αυτά διάφορες ML τεχνικές. Αρχικά, ένας οργανισμός συνέλλεγε και μετέφερε δεδομένα σε έναν άλλο οργανισμό. Ο δεύτερος οργανισμός ήταν υπεύθυνος για τον καθαρισμό των δεδομένων. Εν συνεχεία, ένας τρίτος οργανισμός λάμβανε τα παραπάνω δεδομένα και «έχτιζε» μοντέλα ML έτσι ώστε αυτά να χρησιμοποιηθούν από άλλους οργανισμούς. Ωστόσο, η συγκεκριμένη ροή αντιμετωπίζει αρκετά προβλήματα, καθώς θα πρέπει να ακολουθεί τους κανόνες που έχουν θεσπιστεί αναφορικά με τη προστασία των προσωπικών δεδομένων [3]. Το πρόβλημα που καλείται να επιλύσει η ΟΜ μπορεί να συνοψιστεί στο ακόλουθο ερώτημα:

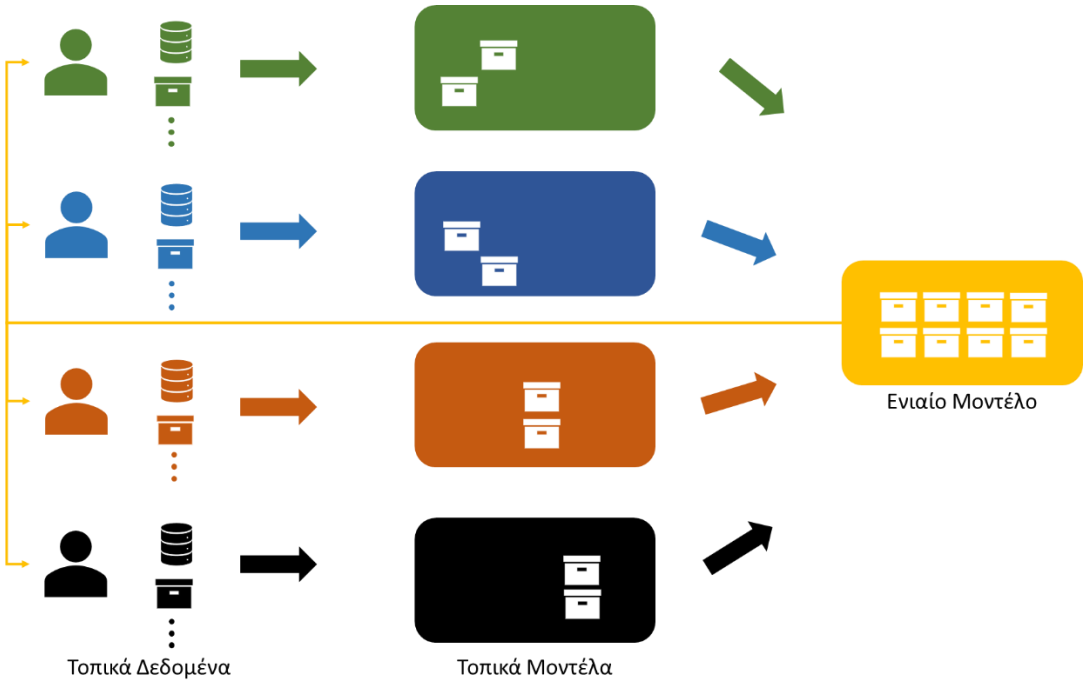
Πώς είναι δυνατή η αποδοτική συλλογή, επεξεργασία και ανάλυση κατανεμημένων δεδομένων με τρόπο που θα διασφαλίζεται η ιδιωτικότητά τους;

2.2. Ορισμός Ομοσπονδιακής Μάθησης

Αναφορικά με την ΟΜ, αποτελεί ένα είδος Μηχανικής Μάθησης. Με άλλα λόγια, αποτελεί έναν διαφορετικό τρόπο έτσι ώστε να εκπαιδευτεί ένας αλγόριθμος πάνω σε κάποια δεδομένα, έτσι ώστε να παρέχει, για παράδειγμα, μία πρόβλεψη. Ωστόσο, υπάρχει μία ειδοποιός διαφορά μεταξύ της ΟΜ και άλλων τεχνικών Μηχανικής Μάθησης, η οποία περιγράφεται παρακάτω.

Έστω ότι υπάρχουν N ιδιοκτήτες δεδομένων $\{I_1, I_2,\ldots, I_N\}$ οι οποίοι επιθυμούν να εκπαιδεύουν έναν αλγόριθμο πάνω στα αντίστοιχα δεδομένα τους $\{\Delta_1, \Delta_2,\ldots, \Delta_N\}$. Σε μία παραδοσιακή μέθοδο εκπαίδευσης, όλα τα δεδομένα «ενοποιούνται» και στη συνέχεια εκπαιδεύεται ο αλγόριθμος. Στην ΟΜ, αυτό που συμβαίνει είναι ότι για τα δεδομένα κάθε χρήστη εκπαιδεύεται ένα μοντέλο, το οποίο εν συνεχεία «ενοποιείται» με τα υπόλοιπα μοντέλα που έχουν αντίστοιχα εκπαιδευτεί και παράγεται ένα συλλογικό μοντέλο, το οποίο έχει αντίστοιχη ακρίβεια με ένα μοντέλο που έχει δημιουργηθεί με τον παραδοσιακό τρόπο εκπαίδευσης. Το συγκεκριμένο μοντέλο, επαναπροωθείται στους χρήστες έτσι ώστε να εφαρμοστεί, να αξιολογηθεί και, αν απαιτηθεί, να ενημερωθεί. Στην περίπτωση της ΟΜ δεν ανταλλάσσονται δεδομένα, αλλά μόνο τα μοντέλα που δημιουργούνται και, συνεπώς, αντιμετωπίζονται στα προβλήματα που αναφέρθηκαν στην προηγούμενη υποενότητα.

Ειδικότερα, και όπως φαίνεται και στην ακόλουθη εικόνα, η ΟΜ αποτελεί μία προσέγγιση κατανεμημένης μάθησης. Η εκπαίδευση/μάθηση πραγματοποιείται σε ένα σύνολο/ομοσπονδία κατανεμημένων χρηστών. Ο στόχος της συγκεκριμένης προσέγγισης είναι να διατηρεί το σύνολο εκπαίδευσης εκεί που παράγεται και να πραγματοποιείται τοπικά η εκπαίδευση του εκάστοτε αλγόριθμου στον αντίστοιχο χρήστη της ομοσπονδίας. Εφόσον έχει δημιουργηθεί τοπικά και για κάθε χρήστη ένα μοντέλο εκπαίδευσης, κάθε χρήστης μεταφέρει τις παραμέτρους του μοντέλου του, αντί των δεδομένων του, σε μία μονάδα συνάθροισης. Η συγκεκριμένη μονάδα συνδυάζει τις παραμέτρους από όλα τα τοπικά μοντέλα έτσι ώστε να δημιουργήσει ένα ενιαίο μοντέλο, το οποίο τελικά αποστέλλεται πίσω στους χρήστες της ομοσπονδίας [4]. Με αυτό τον τρόπο, κάθε χρήστης επωφελείται από το ενιαίο μοντέλο, χωρίς να έχει πρόσβαση σε ευαίσθητα/προσωπικά δεδομένα άλλων χρηστών. Ωστόσο, ενδέχεται και οι παράμετροι ενός μοντέλου να περιέχουν ευαίσθητες πληροφορίες γι’ αυτό και πρέπει να διαφυλάσσεται και η ιδιωτικότητα των παραμέτρων των τοπικών μοντέλων, με χρήση τεχνικών όπως η κρυπτογράφηση [5].



Εικόνα 1: Προσέγγιση ομοσπονδιακής μάθησης

2.3. Ιδιωτικότητα Δεδομένων στην Ομοσπονδιακή Μάθηση

Σύμφωνα με το ερώτημα που διατυπώθηκε στην υποενότητα 1.1, είναι εμφανές ότι στην ΟΜ δίνεται ιδιαίτερη έμφαση στη διασφάλιση της ιδιωτικότητας των δεδομένων βάσει των οποίων εκπαιδεύονται τα μοντέλα μηχανικής μάθησης. Η ιδιωτικότητα των δεδομένων δύναται να διασφαλιστεί με μία πληθώρα τεχνικών και προσεγγίσεων, οι οποίες παρουσιάζονται παρακάτω.

- **Ασφαλής Πολυμερής Υπολογισμός** (Secure Multiparty Computation - SMC). Τα μοντέλα ασφαλείας SMC περιλαμβάνουν πολλαπλούς οργανισμούς / χρήστες και παρέχουν απόδειξη ασφαλείας σε ένα καλά καθορισμένο πλαίσιο προσομοίωσης για να εγγυηθούν πλήρη μηδενική γνώση, δηλαδή, κάθε οργανισμός / χρήστης δεν γνωρίζει τίποτα εκτός από την είσοδο και την έξοδό του. Η μηδενική γνώση είναι ιδιαίτερα επιθυμητή, αλλά αυτή η επιθυμητή ιδιότητα συνήθως απαιτεί περίπλοκα πρωτόκολλα υπολογισμού και μπορεί να μην επιτευχθεί αποτελεσματικά [6].
- **Διαφορικό απόρρητο** (Differential Privacy - DP). Το DP χρησιμοποιεί τις τεχνικές διαφορικής ιδιωτικότητας και k-ανωνυμίας για την προστασία του απορρήτου των δεδομένων. Οι μέθοδοι διαφορικού απορρήτου, k-ανωνυμίας και διαφοροποίησης περιλαμβάνουν την προσθήκη θορύβου στα δεδομένα ή τη χρήση μεθόδων γενίκευσης για την απόκρυψη ορισμένων ευαίσθητων χαρακτηριστικών, έως ότου ο τρίτος οργανισμός / χρήστης δεν μπορεί να διακρίνει το άτομο, καθιστώντας έτσι αδύνατη την επαναφορά των δεδομένων για προστασία απορρήτου χρήστη. Ειδικότερα, οι μέθοδοι διαφορικού απόρρητου αποτελούν ένα μοντέλο στατιστικής ανωνυμίας, προστατεύουν το απόρρητο των δεδομένων προσθέτοντας μια επιθυμητή ποσότητα τυχαιοποιημένων θορύβων χρησιμοποιώντας διάφορους μαθηματικούς αλγόριθμους. Αναφορικά με την k-ανωνυμία, αυτή σημαίνει ότι οποιοδήποτε στοιχείο περιλαμβάνεται σε ένα σύνολο εμφανίζεται με πιθανότητα όχι μεγαλύτερη από 1/k, δηλαδή, για οποιοδήποτε στοιχείο, υπάρχουν τουλάχιστον άλλα k–1 δυσδιάκριτα στοιχεία σε αυτό το σύνολο. Για παράδειγμα, το T(A1, A2, ⋯, An) είναι ένας πίνακας με n χαρακτηριστικά (A1, A2, ⋯, An). Εάν κάθε ακολουθία τιμών σε ένα σύνολο χαρακτηριστικών εμφανίζεται με τουλάχιστον k εμφανίσεις, το T είναι k-ανώνυμο [7]. Ωστόσο, οι προαναφερθείσες μέθοδοι εξακολουθούν να απαιτούν τα δεδομένα να μεταφέρονται αλλού, κάτι που συνήθως περιλαμβάνει μια αντιστάθμιση μεταξύ ακρίβειας και ιδιωτικότητας.
- **Ανάλυση απορρήτου**: Οι προσεγγίσεις που εμπίπτουν σε αυτήν την κατηγορία προτείνονται για την ανάλυση των τρωτών σημείων απορρήτου του ομοσπονδιακού παραδείγματος μάθησης και την εξέταση της αποτελεσματικότητας ορισμένων υφιστάμενων αμυντικών στρατηγικών. Για παράδειγμα, οι συγγραφείς στο [8] διερεύνησαν τη διαρροή ευαίσθητων δεδομένων στην ΟΜ με έμφαση σε μοντέλα λογιστικής παλινδρόμησης. Στην ανάλυση λαμβάνονται υπόψη δύο προσεγγίσεις εκπαίδευσης, δηλαδή η σύγχρονη και η ασύγχρονη. Στη σύγχρονη προσέγγιση, ο πελάτης υπολογίζει τις διαβαθμίσεις με βάση τα δικά του δεδομένα στην τρέχουσα

παρτίδα (batch). Στην ασύγχρονη προσέγγιση, ο πελάτης χρησιμοποιεί πολλές παρτίδες (batches) για να υπολογίσει τις διαβαθμίσεις. Οι συγγραφείς δείχνουν μαθηματικά ότι οι «ειλικρινείς» αλλά «περίεργοι» πελάτες μπορούν εύκολα να συναγάγουν όλα τα δεδομένα εκπαίδευσης άλλων πελατών εάν υιοθετηθεί η σύγχρονη προσέγγιση. Από την άλλη πλευρά, οι συγγραφείς δείχνουν ότι οι «ειλικρινείς» αλλά «περίεργοι» πελάτες δεν μπορούν να συναγάγουν τίποτα εκτός από κάποιους περιορισμούς στα δεδομένα εκπαίδευσης άλλων πελατών εάν υιοθετηθεί η ασύγχρονη προσέγγιση. Οι συγγραφείς του [9] εξετάζουν αρκετές επιθέσεις στο παράδειγμα της ομοσπονδιακής μάθησης. Τα ληφθέντα αποτελέσματα υποδηλώνουν ότι η διαρροή ακούσιων χαρακτηριστικών μέσω της κοινής χρήσης των ενημερώσεων του μοντέλου εκθέτει το ομοσπονδιακό παράδειγμα μάθησης σε σοβαρές ενεργητικές και παθητικές επιθέσεις. Τέτοιες επιθέσεις δίνουν τη δυνατότητα στους κακόβουλους πελάτες να συνάγουν τόσο τη συμμετοχή (δηλαδή την παρουσία ορισμένων σημείων δεδομένων σε δεδομένα εκπαίδευσης άλλων πελατών) όσο και τις ιδιότητες που απεικονίζουν ορισμένα υποσύνολα των δεδομένων εκπαίδευσης (τα οποία είναι ανεξάρτητα από τις ιδιότητες που επιδιώκει να προσδιορίσει το κοινό μοντέλο). Επιπλέον, περαιτέρω πειράματα αναδεικνύουν το γεγονός ότι οι κοινές αμυντικές στρατηγικές, όπως η μείωση διαστάσεων, δεν μπορούν να αποτρέψουν τέτοιες είδους επιθέσεις.

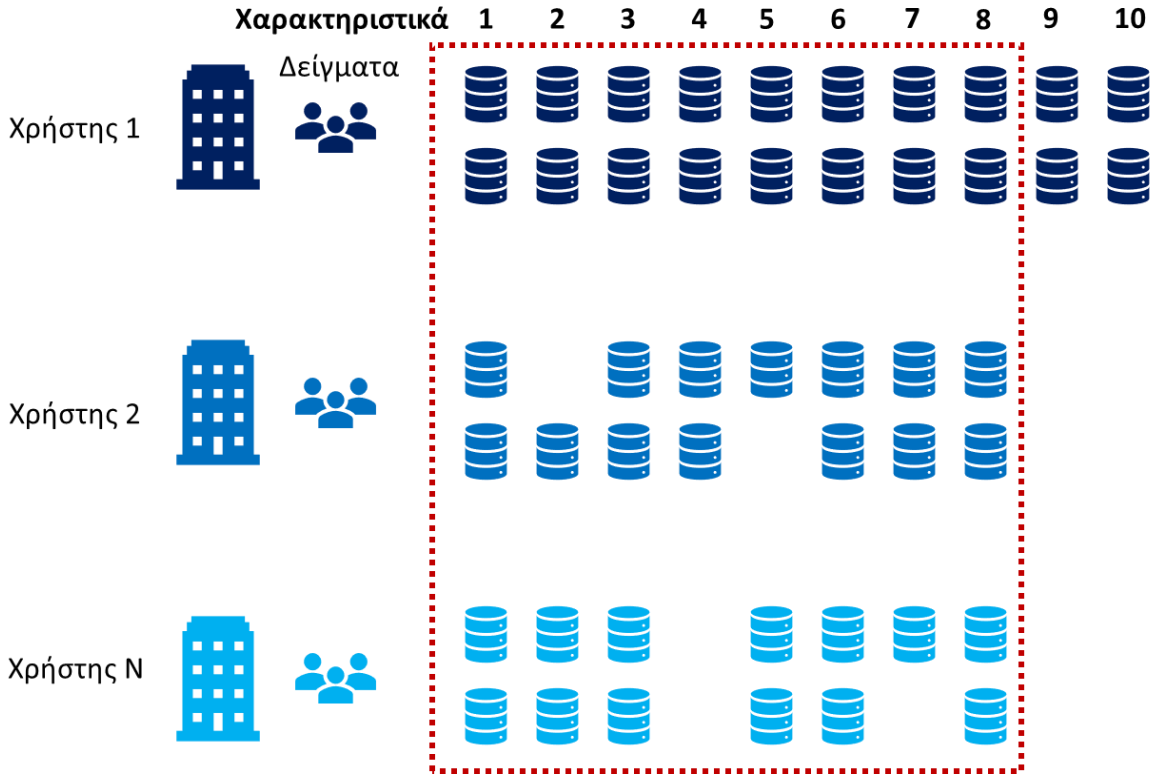
- **Εισαγωγή θορύβου**: Η κύρια ιδέα των προσεγγίσεων εισαγωγής θορύβου είναι να επιτραπεί στους πελάτες να προσθέσουν κάποιο θόρυβο στις ενημερώσεις κλίσης για να εμποδίσουν τον διακομιστή να χρησιμοποιήσει τις πραγματικές κλίσεις για να ανακτήσει ευαίσθητες πληροφορίες από τα δεδομένα εκπαίδευσης. Εμπνευσμένοι από αυτή την ιδέα, οι συγγραφείς του [11] προτείνουν μια προσέγγιση για την αντιμετώπιση διαφορικών επιθέσεων που επιδιώκουν να συναγάγουν τη συμβολή ενός πελάτη στη διαδικασία εκπαίδευσης μέσω της ανάλυσης του κατανεμημένου μοντέλου εκπαίδευσης.
- **Μηχανική μάθηση**: Η μηχανική μάθηση προτείνεται για να παρέχει μια εναλλακτική λύση στις σύνθετες μαθηματικές λύσεις διατήρησης του απορρήτου που συχνά συνεπάγονται υψηλό υπολογιστικό κόστος. Μια ποικιλία λύσεων μηχανικής εκμάθησης, όπως τα GANs (Generative Adversarial Networks) η ομαδοποίηση και η εκμάθηση μεταφοράς έχουν χρησιμοποιηθεί για σκοπούς διατήρησης του απορρήτου. Για παράδειγμα, οι συγγραφείς στο [12] προτείνουν το FedGP, μια προσέγγιση ομοσπονδιακής μάθησης που αξιοποιεί τα GAN για τη βελτίωση του απορρήτου της εκπαιδευτικής διαδικασίας. Η παραπάνω διαδικασία βασίζεται στη δημιουργία ενός GAN στα δεδομένα κάθε πελάτη για τη δημιουργία τεχνητών δεδομένων που μπορούν να αντικαταστήσουν τα αρχικά δεδομένα του πελάτη.
- **Ομομορφική κρυπτογράφηση** (Homomorphic encryption): Η ομομορφική κρυπτογράφηση [12] υιοθετείται επίσης για την προστασία του απορρήτου των δεδομένων χρήστη μέσω της ανταλλαγής παραμέτρων κάτω από τον μηχανισμό κρυπτογράφησης κατά τη διάρκεια εκπαίδευσης μοντέλων μηχανικής μάθησης. Σε

αντίθεση με διαδικασία διαφορικού απόρρητου, τα δεδομένα και το ίδιο το μοντέλο δεν μεταφέρονται, ούτε μπορούν να «μαντέψουν» τα δεδομένα του άλλου πελάτη. Επομένως, υπάρχει μικρή πιθανότητα διαρροής σε επίπεδο πρωτογενών δεδομένων.

2.4. Κατηγορίες Ομοσπονδιακής Μάθησης

Η ΟΜ διαχωρίζεται σε τρεις (3) υποκατηγορίες, η κάθε μία από τις οποίες δύναται να αξιοποιηθεί σε διαφορετικά σενάρια χρήσης. Ειδικότερα, οι υποκατηγορίες είναι οι Οριζόντια Ομοσπονδιακή Μάθηση (Horizontal Federated Learning - HFL), Κάθετη Ομοσπονδιακή Μάθηση (Vertical Federated Learning - VFL) και Ομοσπονδιακή Μάθηση Μεταφοράς (Federated Transfer Learning - FTL).

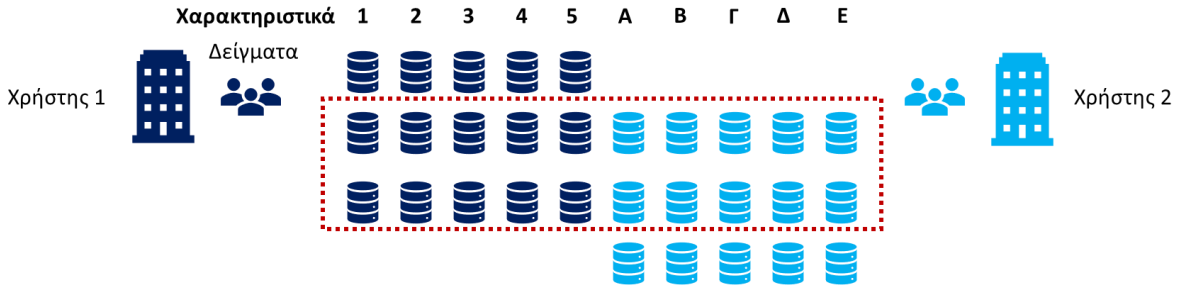
- **Οριζόντια Ομοσπονδιακή Μάθηση**: Η οριζόντια ομοσπονδιακή μάθηση ή ομοσπονδιακή μάθηση βάσει δείγματος, αξιοποιείται στα σενάρια χρήσης στα οποία τα σύνολα δεδομένων μοιράζονται τον ίδιο χώρο χαρακτηριστικών αλλά διαφορετικό χώρο στα δείγματα [13], όπως παρουσιάζεται στην **Εικόνα *2***. Για παράδειγμα, δύο περιφερειακές τράπεζες μπορεί να έχουν πολύ διαφορετικές ομάδες χρηστών από τις αντίστοιχες περιοχές τους και το σύνολο τομής των χρηστών τους είναι πολύ μικρό. Ωστόσο, ο τρόπος λειτουργείας και, κατά συνέπεια, τα δεδομένα που χρησιμοποιούν είναι παρόμοια, επομένως οι χώροι χαρακτηριστικών είναι οι ίδιοι.



Εικόνα 2*: Οριζόντια ομοσπονδιακή μάθηση*

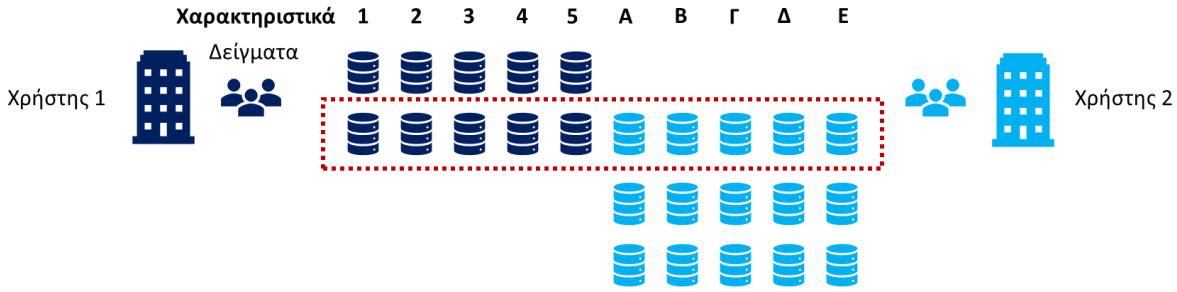
- **Κάθετη Ομοσπονδιακή Μάθηση**: Η κάθετη ομοσπονδιακή μάθηση ή ομοσπονδιακή μάθηση βάσει χαρακτηριστικών εφαρμόζεται στις περιπτώσεις στις οποίες δύο σύνολα δεδομένων μοιράζονται τον ίδιο χώρο αναγνωριστικού δείγματος αλλά διαφέρουν ως προς τον χώρο χαρακτηριστικών [14]. Για παράδειγμα, έστω ότι υπάρχουν δύο

διαφορετικές εταιρείες στην ίδια πόλη: η μία είναι τράπεζα και η άλλη εταιρεία ηλεκτρονικού εμπορίου. Τα σύνολα χρηστών τους είναι πιθανό να περιέχουν τους περισσότερους κατοίκους της περιοχής. Έτσι, η τομή του χώρου χρήστη τους είναι μεγάλη. Ωστόσο, δεδομένου ότι η τράπεζα καταγράφει τη συμπεριφορά εσόδων και δαπανών και την πιστοληπτική ικανότητα του χρήστη και η εταιρεία ηλεκτρονικού εμπορίου διατηρεί το ιστορικό περιήγησης και αγορών του χρήστη, οι χώροι χαρακτηριστικών τους είναι πολύ διαφορετικοί. Επίσης, έστω ότι χρειάζεται και τα δύο μέρη να έχουν ένα μοντέλο πρόβλεψης για αγορές προϊόντων με βάση τις πληροφορίες χρήστη και προϊόντος. Η κάθετα ομοσπονδιακή μάθηση είναι η διαδικασία συγκέντρωσης αυτών των διαφορετικών χαρακτηριστικών και υπολογισμού της απώλειας εκπαίδευσης και των κλίσεων με τρόπο που διατηρεί το απόρρητο για τη δημιουργία ενός μοντέλου με δεδομένα και από τα δύο μέρη από κοινού.



Εικόνα 3: Κάθετη ομοσπονδιακή μάθηση

- **Ομοσπονδιακή Μάθηση Μεταφοράς**: Η ομοσπονδιακή μάθηση μεταφοράς εφαρμόζεται σε σενάρια χρήσης στα οποία δύο σύνολα δεδομένων διαφέρουν όχι μόνο σε δείγματα αλλά και σε χώρο χαρακτηριστικών [15]. Για παράδειγμα, έστω ότι υπάρχουν δύο ιδρύματα: το ένα είναι μια τράπεζα που βρίσκεται στην Κίνα και το άλλο είναι μια εταιρεία ηλεκτρονικού εμπορίου που βρίσκεται στις Ηνωμένες Πολιτείες. Λόγω γεωγραφικών περιορισμών, οι ομάδες χρηστών των δύο ιδρυμάτων έχουν μια μικρή τομή. Από την άλλη πλευρά, λόγω των διαφορετικών επιχειρήσεων, μόνο ένα μικρό μέρος του χώρου χαρακτηριστικών και από τα δύο μέρη επικαλύπτεται. Σε αυτήν την περίπτωση, οι τεχνικές μεταφοράς-μάθησης μπορούν να εφαρμοστούν για την παροχή λύσεων για ολόκληρο το δείγμα και τον χώρο χαρακτηριστικών κάτω από μια ομοσπονδία.



Εικόνα 4: Ομοσπονδιακή μάθηση μεταφοράς

Φυσικά, υπάρχει μία πληθώρα παραγόντων που έχουν οδηγήσει στην ΟΜ και στην ανάπτυξη κατηγοριών που αναφέρθηκαν παραπάνω. Τα κινητά τηλέφωνα, οι φορητές συσκευές και τα αυτόνομα οχήματα είναι μερικά μόνο από τα σύγχρονα κατανεμημένα δίκτυα που παράγουν πληθώρα δεδομένων καθημερινά. Λόγω της αυξανόμενης υπολογιστικής ισχύος αυτών των συσκευών, σε συνδυασμό με τις ανησυχίες σχετικά με τη μετάδοση προσωπικών/ευαίσθητων πληροφοριών, προτείνεται όλο και πιο συχνά η αποθήκευση των δεδομένων να πραγματοποιείται σε τοπικό επίπεδο και να προωθείται ο υπολογισμός του δικτύου στα άκρα (edge computing). Η έννοια του edge computing δεν είναι πρόσφατη. Πράγματι, ο υπολογισμός απλών ερωτημάτων σε κατανεμημένες συσκευές χαμηλής κατανάλωσης είναι ένας τομέας έρευνας δεκαετιών που έχει διερευνηθεί στο πλαίσιο της επεξεργασίας ερωτημάτων σε δίκτυα αισθητήρων, του edge computing και του fog computing [16].

Πρόσφατες έρευνες εξέτασαν επίσης την εκπαίδευση μοντέλων μηχανικής μάθησης κεντρικά, αλλά την εξυπηρέτηση και την αποθήκευσή τους τοπικά. Για παράδειγμα, αυτή είναι μια κοινή προσέγγιση στη μοντελοποίηση και εξατομίκευση της εμπειρίας των χρηστών κινητών . Ωστόσο, καθώς αυξάνονται οι δυνατότητες αποθήκευσης και υπολογισμού των συσκευών σε κατανεμημένα δίκτυα, είναι δυνατό να αξιοποιηθούν βελτιωμένοι τοπικοί πόροι σε κάθε συσκευή. Επιπλέον, οι ανησυχίες αναφορικά με το απόρρητο σχετικά με τη μετάδοση μη επεξεργασμένων δεδομένων απαιτούν τα δεδομένα που δημιουργούνται από τον χρήστη να παραμένουν σε τοπικές συσκευές. Αυτό έχει οδηγήσει σε ένα αυξανόμενο ενδιαφέρον για την ΟΜ, η οποία διερευνά στατιστικά μοντέλα εκπαίδευσης απευθείας σε απομακρυσμένες συσκευές. Η μάθηση σε ένα τέτοιο περιβάλλον διαφέρει σημαντικά από τα παραδοσιακά κατανεμημένα περιβάλλοντα, τα οποία απαιτούν θεμελιώδεις εξελίξεις σε τομείς όπως το απόρρητο, η μεγάλης κλίμακας μηχανική μάθηση και η κατανεμημένη βελτιστοποίηση. Η ομοσπονδιακή μάθηση έχει τη δυνατότητα να ενεργοποιεί λειτουργίες πρόβλεψης σε έξυπνες συσκευές χωρίς να μειώνει την εμπειρία του χρήστη ή να διαρρέονται προσωπικές πληροφορίες [17].

2.5. Εφαρμογές Ομοσπονδιακής Μάθησης

Η ΟΜ δύναται να αξιοποιηθεί σε πληθώρα εφαρμογών και μάλιστα σε διαφορετικά πεδία. Μία σύνοψη των συγκεκριμένων εφαρμογών παρουσιάζονται στον ακόλουθο πίνακα.

Πίνακας 1: Εφαρμογές ομοσπονδιακής μάθησης

Έρευνα	Πεδίο	Εφαρμογή	Περιγραφή	Περιορισμοί
Chen et al. (2019) [18]	Φορητές συσκευές	Πληκτρολόγιο έξυπνου τηλεφώνου	Επέκταση λεξιλογίου πληκτρολογίου βάσει χρησιμοποιούμενων λέξεων, χωρίς την εξαγωγή ευαίσθητης πληροφορίας	Βασίζεται σε μεγάλο βαθμό σε πιθανότητες
Leroy et al. (2019) [19]	Φορητές συσκευές	Έξυπνος βοηθός	Μάθηση και ανίχνευση λέξεων αφύπνισης	Ευαισθησία σε θόρυβο παρασκηνίου
Hard et al. (2018) [20]	Φορητές συσκευές	Πληκτρολόγιο έξυπνου τηλεφώνου	Πρόβλεψη επόμενης λέξης βάσει προτιμήσεων άλλων χρηστών	Υψηλό κόστος επικοινωνίας
Yang et al. (2018) [21]	Φορητές συσκευές	Πληκτρολόγιο έξυπνου τηλεφώνου	Παροχή προτάσεων σχετικά με λέξεις που οι χρήστες θα ήθελαν να χρησιμοποιήσουν	Τα μοντέλα μηχανικής μάθησης δεν μπορούν να περιλαμβάνουν πολλές παραμέτρους
Ramaswamy at al. (2019) [22]	Φορητές συσκευές	Πληκτρολόγιο έξυπνου τηλεφώνου	Πρόβλεψη emoji βάσει κειμένου που πληκτρολογεί ο χρήστης	Αδυναμία αξιολόγησης απόδοσης της προσέγγισης
Wang et al. (2019) [23]	Edge Computing	Εφαρμογή μοντέλων βαθιάς μηχανικής μάθησης	Διαμόρφωση δικτύου για την εκπαίδευση μοντέλων βαθιάς μηχανικής μάθησης	Αδυναμία ορθής κατανομής υπολογιστικού κόστους σε διαφορετικά σενάρια χρήσης
Qian et al. (2019) [24]	Edge Computing	Υπηρεσία διασφάλισης	Σύστημα διαχείρισης υπηρεσιών με	Δεν είναι εφικτό να εφαρμοστεί

		ιδιωτικότητας σε περιβάλλοντα edge	επίγνωση της ιδιωτικής ζωής (Privacy-aware Service Placement - PSP) για την κάλυψη των απαιτήσεων υπηρεσιών των χρηστών	σε έναν αριθμό υπολογιστικών νεφών
Feng et al. (2020) [25]	Φορητές συσκευές	Πρόβλεψη κίνησης χρηστών	Χρήση αισθητήρων κινητών συσκευών και συμπεριφοράς άλλων χρηστών για την πρόβλεψη της σωματικής κίνησης των χρηστών	Χρήση μόνο βασικών μοντέλων κίνησης χρηστών
Sozinov et al. (2018) [26]	Έξυπνες συσκευές	Αναγνώριση δραστηριότητας χρηστών	Χρήση αισθητήρων κινητών συσκευών και συμπεριφοράς άλλων χρηστών για την αναγνώριση της δραστηριότητας των χρηστών	Απόρριψη μοντέλων χρηστών που δεν έχουν ικανοποιητική ακρίβεια
Aïvodji et al. (2019) [27]	Φορητές συσκευές	Έξυπνο σπίτι	Διαχείριση συσκευών που είναι τοποθετημένες σε ένα έξυπνο σπίτι	Περίπλοκη αρχιτεκτονική υλοποίησης
Yu et al. (2020) [28]	Φορητές συσκευές	Έξυπνο σπίτι	Αναγνώριση δραστηριότητας χρηστών για τον εντοπισμό φυσικών εμποδίων	Μη ευέλικτος μηχανισμός για την ευρέα εφαρμογή του
Liu et al. (2020) [29]	Φορητές συσκευές	Δίκτυο Ρομπότ	Βελτίωση διαδικασίας εκπαίδευσης σε δίκτυα ρομπότ	Απαιτείται περαιτέρω μελέτη
Hu et al. (2018) [30]	Βιομηχανία	Προστασία περιβάλλοντος	Παρακολούθηση περιοχών και εκπαίδευση μοντέλων βάσει τοπικών χαρακτηριστικών	Απαιτείται η χρήση πολυδιάστατων δομών

Han et al. (2019) [31]	Βιομηχανία	Ανίχνευση εικόνας	Ανίχνευση σφαλμάτων σε γραμμή παραγωγής	Απαιτείται επέκταση για χρήση σε διαφορετικά σενάρια χρήσης
Liu et al. (2020) [32]	Βιομηχανία	Ανάλυση εικόνας	Βελτιστοποίηση ΟΜ για τη αναγνώριση και κατηγοριοποίηση εικόνων	Αποδοτικό για μικρά σύνολα δεδομένων
Mowla et al. (2019) [33]	Βιομηχανία	Μη επανδρωμένα αεροσκάφη	Αναγνώριση κακόβουλων επιθέσεων σε δίκτυα επικοινωνίας μη επανδρωμένων αεροσκαφών	Μη αξιόπιστο κεντρικό μοντέλο
Saputra et al. (2019) [34]	Βιομηχανία	Ηλεκτρικά οχήματα	Πρόβλεψη κατανάλωσης ενέργειας ηλεκτρικών οχημάτων	Δεν είναι σταθερή και ευέλικτη προσέγγιση
Wang et al. (2020) [35]	Βιομηχανία	Εξόρυξη κειμένου	Φιλτράρισμα ανεπιθύμητων μηνυμάτων και ανάλυση συναισθήματος	Ο θόρυβος που περιέχεται στα δεδομένα επηρεάζει την ακρίβεια των μοντέλων
Brisimi et al. (2018) [36]	Υγεία	Πρόβλεψη εισαγωγών σε νοσοκομείο	Πρόβλεψη εισαγωγών σε νοσοκομείο με χρήση σχετικά μικρού αριθμού χαρακτηριστικών	Απαιτεί αρκετές επαναλήψεις
Silva et al. (2019) [37]	Υγεία	Ανάλυση μαγνητικής τομογραφίας	Ανάλυση μαγνητικών τομογραφιών οι οποίες χαρακτηρίζονται από πολύ υψηλό αριθμό διαστάσεων	Χρήση περιορισμένου συνόλου δεδομένων
Liu et al. (2019) [38]	Υγεία	Συνταγογράφηση	Εξαγωγή κειμένου από συνταγογραφήσεις με χρήση τεχνικών	Μη αξιοποιήσιμο σε

			επεξεργασίας φυσικής γλώσσας (Natural Language Processing – NLP)	συγκεκριμένες υποπεριπτώσεις
Gao et al. (2019) [39]	Υγεία	Ηλεκτρο-εγκεφαλογραφία	Κατηγοριοποίηση ηλεκτρο-εγκεφαλογραφημάτων	Πραγματοποίηση δοκιμών σε περιορισμένο αριθμό συνόλου δεδομένων
Li et al. (2019) [40]	Υγεία	Νοσηλεία	Πρόβλεψη χρόνου αναμονής στο νοσοκομείο και εισαγωγής στις Μονάδες Εντατικής Θεραπείας (ΜΕΘ)	Υψηλό κόστος επικοινωνίας
Pfohl et al. (2019) [41]	Υγεία	Κλινικές προβλέψεις	Πραγματοποίηση κλινικών προβλέψεων, αξιοποιώντας κεντρικοποιημένα και τοπικά μοντέλα μηχανικής μάθησης	Υποβάθμιση κινδύνων ασφαλείας και ιδιωτικότητας
Huang et al. (2018) [42]	Υγεία	Πρόβλεψη θνησιμότητας	Πρόβλεψη θνησιμότητας με βάση την αγωγή που ακολουθείται από τους ασθενείς	Η απόδοση επηρεάζεται από τον τρόπο οργάνωσης των δεδομένων
Lee et al. (2018) [43]	Υγεία	Κατακερματισμός ασθενών	Κατακερματισμός ασθενών με στόχο τη διασφάλιση της ιδιωτικότητας των δεδομένων τους σε περίπτωση κακόβουλης επίθεσης	Υψηλή υπολογιστική πολυπλοκότητα

2.6. Μηχανική Μάθηση και Αλγόριθμοι

Η ΟΜ μπορεί να επιλύσει προβλήματα τα οποία αντιμετωπίζει και η παραδοσιακή μηχανική μάθηση, αλλά με πολύ πιο αποδοτικό τρόπο, δεδομένου ότι ακολουθείται μία διαφορετική κατανεμημένη προσέγγιση. Συνεπώς, οι διαφορετικές τεχνικές και οι αλγόριθμοι που χρησιμοποιούνται στη μηχανική μάθηση, αξιοποιούνται και στην ΟΜ. Ειδικότερα, οι προαναφερθείσες τεχνικές και οι αλγόριθμοι παρουσιάζονται παρακάτω και διαχωρίζονται σε δύο κατηγορίες: Εποπτευόμενη Μηχανική Μάθηση και Μη Εποπτευόμενη Μηχανική Μάθηση [44].

2.6.1. Εποπτευόμενη Μηχανική Μάθηση

Στη κατηγορία της εποπτευόμενης μηχανικής μάθησης (Supervised ML) ανήκουν αλγόριθμοι που πραγματοποιούν κατηγοριοποίηση, κατά τη διάρκεια της οποίας επιχειρείται η πρόβλεψη της κλάσης στην οποία ανήκει κάποια παρατήρηση. Η κατηγοριοποίηση διαχωρίζεται σε επιμέρους κατηγορίες, βάσει των χαρακτηριστικών της κλάσης πρόβλεψης. Αρχικά, υπάρχει η δυαδική κατηγοριοποίηση στην οποία η κλάση πρόβλεψης δύναται να πάρει δύο (2) τιμές όπως «Ναι» και «Όχι» ή «Αληθές» και «Ψευδές» [45]. Επίσης, υπάρχει η πολυταξική κατηγοριοποίηση στην οποία η κλάση πρόβλεψης δύναται να λάβει παραπάνω από δύο (2) τιμές. Τέλος, υπάρχει η κατηγοριοποίηση πολλαπλών ετικετών. Το συγκεκριμένο είδος κατηγοριοποίησης αποτελεί γενίκευση της πολυταξικής κατηγοριοποίησης και αφορά κλάσεις οι οποίες έχουν κάποια ιεραρχία μεταξύ τους, όπως για παράδειγμα μία κλάση που διαθέτει πολλές επιμέρους κλάσεις [46].

Επίσης, εκτός από την κατηγοριοποίηση, υπάρχει και η παλινδρόμηση. Στην παλινδρόμηση είναι δυνατή η πρόβλεψη μιας συνεχούς μεταβλητής βάσει άλλων μεταβλητών. Αρκετοί αλγόριθμοι κατηγοριοποίησης δύνανται να αξιοποιηθούν για την επίλυση προβλημάτων παλινδρόμησης, ενώ υπάρχουν και αλγόριθμοι που σχετίζονται αποκλειστικά με την παλινδρόμηση.

Πληθώρα αλγορίθμων έχουν προταθεί στη βιβλιογραφία για την επίλυση προβλημάτων κατηγοριοποίησης και παλινδρόμησης και οι οποίοι συνήθως ονομάζονται ταξινομητές. Οι ευρέως χρησιμοποιούμενοι ταξινομητές καταγράφονται παρακάτω.

- **Naive Bayes (NB)**: βασίζεται στο θεώρημα του Bayes και υποθέτει ότι οι μεταβλητές είναι ανά δύο ανεξάρτητες. Οι πιο συνήθεις παραλλαγές του είναι η Gaussian, η Bernoulli, η Πολυωνυμική και η Κατηγορική.
- **Γραμμική Διακριτή Ανάλυση (Linear Discriminant Analysis – LDA)**: είναι ένας γραμμικός ταξινομητής ορίων απόφασης που δημιουργείται με την προσαρμογή πυκνοτήτων υπό όρους κατηγορίας στα δεδομένα και την εφαρμογή του κανόνα Bayes.
- **K-Nearest Neighbors (KNN)**: αξιοποιεί κάποιο μέτρο ομοιότητας μεταξύ γειτονικών παρατηρήσεων, όπως είναι για παράδειγμα η Ευκλείδια απόσταση, έτσι ώστε να κατηγοριοποιήσει τα δεδομένα [47].

- **Support vector machine (SVM)**: αξιοποιείται σε δεδομένα με πολλαπλές διαστάσεις και στοχεύει στη δημιουργία υπερεπιπέδου ή συνόλου υπερεπιπέδων. Το υπερεπίπεδο που απέχει τη μεγαλύτερη απόσταση από τις πιο κοντινές παρατηρήσεις επιτυγχάνει τον καλύτερο δυνατό διαχωρισμό. Ωστόσο, ο αλγόριθμος δεν είναι αποδοτικός σε δεδομένα που περιέχουν θόρυβο [48].
- **Decision Tree (DT)**: στηρίζεται στη δημιουργία δέντρων απόφασης στα οποία τα φύλλα αντιπροσωπεύουν τις κλάσεις στις οποίες ανήκουν τα δεδομένα.
- **Random Forest (RF)**: κατασκευάζει παράλληλα πολλαπλά δέντρα απόφασης χρησιμοποιώντας διαφορετικά υποσύνολα από τα αρχικά δεδομένα και στη συνέχεια εξάγει τις τελικές κλάσεις λαμβάνοντας υπόψη το μέσο όρο όλων των δέντρων [49].
- **Adaptive Boosting (AdaBoost)**: συνδυάζει πολλαπλούς μη αποδοτικούς ταξινομητές έτσι ώστε να δημιουργήσει έναν ενιαίο ταξινομητή, ο οποίος επωφελείται από τα λάθη που έχουν πραγματοποιήσει οι επιμέρους ταξινομητές.
- **Extreme Gradient Boosting (XGBoost)**: κατασκευάζει ένα μοντέλο βάσει άλλων επιμέρους μοντέλων και επιχειρεί να ελαχιστοποιήσει τη συνάρτηση κόστους χρησιμοποιώντας τον αλγόριθμο Gradient Descent.
- **Stochastic Gradient Descent (SGD)**: είναι μία επαναληπτική μέθοδος που επιχειρεί να βελτιστοποιήσει μία αντικειμενική συνάρτηση η οποία υπολογίζει τον βαθμό με τον οποίο αλλάζει μία μεταβλητή σε σχέση με μία άλλη μεταβλητή.
- **Απλή Γραμμική Παλινδρόμηση**: αξιοποιεί μία μεταβλητή έτσι ώστε να εντοπίσει την ευθεία που προσαρμόζεται καλύτερα στα δεδομένα (μεταξύ εξαρτημένης και ανεξάρτητης μεταβλητής).
- **Πολλαπλή Γραμμική Παλινδρόμηση**: αξιοποιεί πολλές μεταβλητές έτσι ώστε να εντοπίσει την ευθεία που προσαρμόζεται καλύτερα στα δεδομένα (μεταξύ εξαρτημένης μεταβλητής και ανεξάρτητων μεταβλητών).
- **Πολυωνυμική Παλινδρόμηση**: αξιοποιεί πολλές μεταβλητές έτσι ώστε να εντοπίσει το πολυώνυμο που προσαρμόζεται καλύτερα στα δεδομένα (μεταξύ εξαρτημένης μεταβλητής και ανεξάρτητων μεταβλητών).
- **Λογιστική Παλινδρόμηση (Logistic Regression – LR)**: χρησιμοποιεί μία λογιστική συνάρτηση έτσι ώστε να υπολογιστούν οι αντίστοιχες πιθανότητες. Συχνά αξιοποιεί και τις παλινδρομήσεις L1 & L2, ενώ υποθέτει ότι τα δεδομένα έχουν γραμμική σχέση.
- **Νευρωνικά Δίκτυα:** βασίζεται σε μια συλλογή συνδεδεμένων μονάδων ή κόμβων που ονομάζονται τεχνητοί νευρώνες. Κάθε σύνδεση μπορεί να μεταδώσει ένα σήμα σε άλλους νευρώνες. Ένας τεχνητός νευρώνας λαμβάνει σήματα και στη συνέχεια τα επεξεργάζεται και μπορεί να σηματοδοτήσει τους νευρώνες που συνδέονται με αυτόν. Το "σήμα" σε μια σύνδεση είναι ένας πραγματικός αριθμός και η έξοδος κάθε νευρώνα υπολογίζεται από κάποια μη γραμμική συνάρτηση του αθροίσματος των εισόδων του. [84]

2.6.2. Μη Εποπτευόμενη Μηχανική Μάθηση

Στη κατηγορία της μη εποπτευόμενης μηχανικής μάθησης (Supervised ML) ανήκουν αλγόριθμοι που πραγματοποιούν συσταδοποίηση, κατά τη διάρκεια της οποίας επιχειρείται η ομαδοποίηση των δεδομένων βάσει κάποιου μη προκαθορισμένου κοινού χαρακτηριστικού.

Πληθώρα αλγορίθμων έχουν προταθεί στη βιβλιογραφία για την επίλυση προβλημάτων συσταδοποίησης. Οι ευρέως χρησιμοποιούμενοι αλγόριθμοι καταγράφονται παρακάτω.

- **Μέθοδοι Κατάτμησης**: κατηγοριοποιεί τα δεδομένα σε πολλαπλές ομάδες ή συστάδες με βάση τα χαρακτηριστικά και τις ομοιότητες στα δεδομένα. Οι πιο συνήθεις αλγόριθμοι της συγκεκριμένης κατηγορίας είναι οι K-Means, K-Mediods και CLARA.
- **Μέθοδοι βασισμένες στη Πυκνότητα**: στηρίζονται στην έννοια της πυκνότητας και καθορίζουν τις ομάδες των δεδομένων βάσει αυτής. Τυπικά παραδείγματα τέτοιων αλγορίθμων αποτελούν οι DBSCAN και OPTICS [50].
- **Μέθοδοι βασισμένες στην Ιεραρχία**: κατασκευάζουν ιεραρχία από ομάδες, δηλαδή ένα δέντρο. Ο τρόπος με τον οποίο κατασκευάζεται το δέντρο μπορεί να είναι είτε από κάτω προς τα πάνω, είτε από πάνω προς τα κάτω [51].
- **Μέθοδοι Πλέγματος**: αναπαριστούν ένα σύνολο δεδομένων σε μορφή πλέγματος και εν συνεχεία συνδυάζουν τα κελιά του πλέγματος, έτσι ώστε να σχηματιστούν ομάδες. Τυπικά παραδείγματα αλγορίθμων πλέγματος είναι οι STING [52] και CLIQUE [53].
- **Μέθοδοι Μοντέλων**: αξιοποιούν είτε μεθόδους στατιστικής, είτε νευρωνικά δίκτυα. Τυπικά παραδείγματα αλγορίθμων είναι οι GMM (Gaussian Mixture Model) [54] και SOM (Self-Organizing Map) [55] αντίστοιχα.
- **Μέθοδοι Περιορισμών**: αξιοποιούν κάποιους περιορισμούς που τίθενται από τους χρήστες, έτσι ώστε να πραγματοποιήσουν τη συσταδοποίηση. Τυπικά παραδείγματα αλγόριθμων που ανήκουν σε αυτή τη κατηγορία είναι οι COP K-Means (Constrained K-means) και CMWK-Means (Constrained Minkowski Weighted K-Means).

2.7. Προκλήσεις Ομοσπονδιακής Μάθησης

Η ΟΜ καλείται να αντιμετωπίσει ένα σύνολο προκλήσεων, έτσι ώστε να εδραιωθεί και, εν τέλει, να προτιμηθεί σε σύγκριση με μία συμβατική λύση μηχανικής μάθησης [56]. Οι προαναφερθείσες προκλήσεις συνοψίζονται στον ακόλουθο πίνακα.

Πίνακας 2: Προκλήσεις ομοσπονδιακής μάθησης

Τομέας	Πρόκληση
Ιδιωτικότητα	Στην ΟΜ τα πρωτογενή δεδομένα των χρηστών δεν μεταφέρονται ποτέ από τις συσκευές τους, καθώς η εκπαίδευση κάθε μοντέλου πραγματοποιείται τοπικά. Ωστόσο, η αύξηση του πλήθους των χρηστών συνεπάγεται και την αύξηση του κινδύνου για επιθέσεις που στοχεύουν στη κακόβουλη ανάκτηση ευαίσθητης πληροφορίας από τα δεδομένα εκπαίδευσης των χρηστών.
Επικοινωνία	Στην ΟΜ δεν αποστέλλονται πρωτογενή δεδομένα χρηστών στον διακομιστή και συνεπώς ο όγκος της πληροφορίας που χρειάζεται να αποσταλεί μέσω του δικτύου μειώνεται. Ωστόσο, δεδομένου ότι το μοντέλο εκπαιδεύεται συνεργατικά, απαιτείται αυξημένη επικοινωνία μεταξύ διακομιστή και χρηστών, κάτι το οποίο μπορεί να οδηγήσει σε αυξημένα κόστη επικοινωνίας.
Καθυστέρηση	Στην ΟΜ τα μοντέλα εκπαιδεύονται τοπικά και δεν αποστέλλονται σε κάποιο υπολογιστικό νέφος, κάτι το οποίο οδηγεί σε μικρότερη καθυστέρηση και χρόνους αναμονής.
Στατιστική Ετερογένεια	Το τοπικό μοντέλο κάθε χρήστη, δεδομένου ότι εκπαιδεύεται βάσει των δικών του δεδομένων, δεν αντιπροσωπεύει ολόκληρο τον πληθυσμό των χρηστών.
Μαζική Διανομή	Ο αριθμός των χρηστών που συμμετέχουν στην ΟΜ είναι συνήθως αρκετά μεγαλύτερος από το μέσο αριθμό παρατηρήσεων εκπαίδευσης ανά χρήστη.
Συνδεσιμότητα	Στην ΟΜ, οι συσκευές των χρηστών είναι συχνά εκτός λειτουργίας ή παρουσιάζουν προβλήματα σύνδεσης. Το παραπάνω συνεπάγεται ότι η συνδεσιμότητα στην ΟΜ είναι περιορισμένη και πως η διαδικασία επιλογής χρηστών για να συμμετέχουν σε αυτή μπορεί να είναι υποκειμενική, βάσει συγκεκριμένων κριτηρίων όπως είναι η ζώνη ώρας και η κατάσταση στην οποία βρίσκεται η εκάστοτε συσκευή.

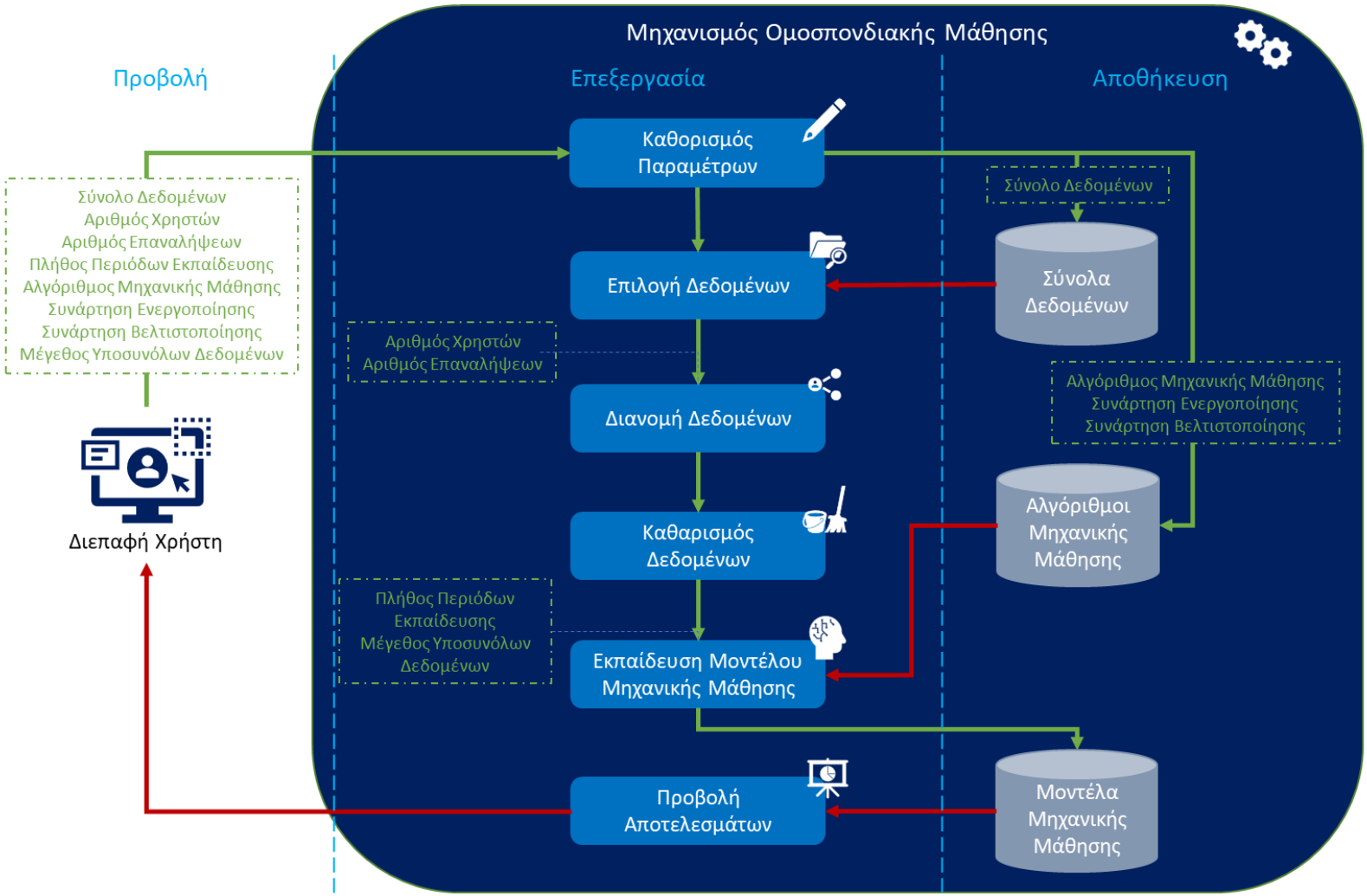
Όπως είναι κατανοητό από όλα τα παραπάνω, η ΟΜ είναι μία πολύ σύγχρονη προσέγγιση στον τομέα της Μηχανικής Μάθησης η οποία δίνει απάντηση στο ερώτημα που διατυπώθηκε στον Ενότητα 1.1. Ωστόσο, η χρήση της συνεπάγεται και την ικανοποίηση κάποιων περιορισμών που σχετίζονται, μεταξύ άλλων, με το υπολογιστικό κόστος, διασφάλιση της ιδιωτικότητας των δεδομένων των χρηστών και φυσικά, στο σενάριο χρήσης που καλείται να εφαρμοστεί. Οι συγκεκριμένοι περιορισμοί θα πρέπει να λαμβάνονται υπόψη, προτού επιλεχθεί η ΟΜ έναντι, για παράδειγμα, ενός συμβατικού τρόπου εκπαίδευσης μοντέλων Μηχανικής Μάθησης. Σε αυτό το πλαίσιο, η συγκεκριμένη εργασία προτείνει ένα περιβάλλον το οποίο πραγματοποιεί εκπαίδευση μοντέλων Μηχανικής Μάθησης με ομοσπονδιακό τρόπο. Το συγκεκριμένο περιβάλλον αφήνει στους χρήστες του πλήρη ελευθερία ως προς τις παραμέτρους, τους αλγόριθμους και τα σύνολα δεδομένων που μπορούν να αξιοποιήσουν. Επιπρόσθετα, παρέχει στους χρήστες πληθώρα μετρήσεων από τα διαφορετικά πειράματα που δύνανται να πραγματοποιήσουν, έτσι ώστε, τελικά, να αξιολογήσουν την ΟΜ και να αποφασίσουν αναφορικά με την αποδοτικότητά και την αποτελεσματικότητά της στα εκάστοτε σενάρια χρήσης.

3. Προτεινόμενη Προσέγγιση

3.1. Γενική Αρχιτεκτονική

Όπως προαναφέρθηκε, ο μηχανισμός που αναπτύχθηκε στα πλαίσια της συγκεκριμένης διπλωματικής εργασίας παρέχει ένα ολοκληρωμένο περιβάλλον εκπαίδευσης μοντέλων μηχανικής μάθησης με ομοσπονδιακό τρόπο. Ο μηχανισμός ονομάζεται «Μηχανισμός Ομοσπονδιακής Μάθησης», εν συντομία «Μηχανισμός ΟΜ» και αποτελείται από επιμέρους κομμάτια που πραγματοποιούν διαφορετικές λειτουργικότητες. Η γενική αρχιτεκτονική του μηχανισμού φαίνεται στην ***Εικόνα 5*** και αναλύεται παρακάτω.

Ο μηχανισμός αποτελείται από τρεις (3) πυλώνες. Ο πρώτος πυλώνας ονομάζεται «Προβολή» και αφορά την προβολή των αποτελεσμάτων. Σε αυτό τον πυλώνα ανήκει η «Διεπαφή Χρήστη». Ο δεύτερος πυλώνας ονομάζεται «Επεξεργασία» και αναφέρεται σε όλες τις διαδικασίες τις οποίες πραγματοποιεί ο μηχανισμός. Ειδικότερα, στο συγκεκριμένο πυλώνα περιλαμβάνονται τα: «Καθορισμός Παραμέτρων», «Επιλογή Δεδομένων», «Διανομή Δεδομένων», «Καθαρισμός Δεδομένων», «Εκπαίδευση Μοντέλου Μηχανικής Μάθησης» και «Προβολή Αποτελεσμάτων». Αναφορικά με τον τρίτο πυλώνα, εκείνος ονομάζεται «Αποθήκευση» και αποτελείται από τα «Σύνολα Δεδομένων» «Αλγόριθμοι Μηχανικής Μάθησης» και «Μοντέλα Μηχανικής Μάθησης». Το εκάστοτε στοιχείο που ανήκει στους προαναφερθέντες πυλώνες πραγματοποιεί μία συγκεκριμένη λειτουργία, ενώ στο σύνολό τους τα στοιχεία αλληλεπιδρούν μεταξύ τους με συγκεκριμένο τρόπο, με στόχο την εκπαίδευση μοντέλων μηχανικής μάθησης.



Εικόνα 5: Αρχιτεκτονική προτεινόμενου μηχανισμού

Όπως παρουσιάζεται και στην εικόνα της αρχιτεκτονικής, αρχικά, η «Διεπαφή Χρήστη» προσφέρει τη δυνατότητα αλληλεπίδρασης των χρηστών με τον υπόλοιπο μηχανισμό, αποκρύπτοντας την πολυπλοκότητά του. Μέσω της διεπαφής, οι χρήστες έχουν τη δυνατότητα να πραγματοποιήσουν την εκπαίδευση μοντέλων μηχανικής μάθησης, καθορίζοντας οι ίδιοι τις παραμέτρους, όπως επίσης και να ανακτήσουν τα αποτελέσματα των πειραμάτων τους, τα οποία οπτικοποιούνται με τη μορφή διαγραμμάτων. Οι παράμετροι τις οποίες μπορεί να ορίσει ο χρήστης είναι οι ακόλουθες:

- **Σύνολο Δεδομένων**: αφορά το σύνολο δεδομένων βάσει του οποίου θα πραγματοποιηθεί η εκπαίδευση. Ο χρήστης δύναται να επιλέξει από μία συλλογή δεδομένων, η οποία είναι διαθέσιμη και η οποία περιλαμβάνει σύνολα δεδομένων από διαφορετικούς τομείς.
- **Αριθμός Χρηστών**: αναφέρεται στον αριθμό πελατών που θα αξιοποιηθούν για την εκπαίδευση του μοντέλου. Αν ο χρήστης ενδιαφέρεται να εκπαιδεύσει το μοντέλο του με τον παραδοσιακό τρόπο, δηλαδή χωρίς τη χρήση κάποιας ομοσπονδίας, τότε θα πρέπει να επιλέξει στον αριθμό 1 (δηλαδή να χρησιμοποιηθεί μόνο ένας πελάτης). Σε διαφορετική περίπτωση το μοντέλο θα εκπαιδευτεί ομοσπονδιακά και ο αριθμός των πελατών που θα χρησιμοποιούν για να λάβει χώρα η συγκεκριμένη εκπαίδευση θα είναι ίσος με τον αριθμό που έχει επιλέξει ο χρήστης.
- **Αριθμός Επαναλήψεων**: καθορίζει τον αριθμό των επαναλήψεων της εκπαίδευσης ενός μοντέλου, ανά πελάτη. Ο συγκεκριμένος αριθμός έχει νόημα καθώς υπάρχουν περιπτώσεις που η απόδοση ενός μοντέλου μπορεί να αυξάνεται ανάλογα με το πλήθος των φορών που επαναλαμβάνεται η εκπαίδευσή του.
- **Πλήθος Περιόδων Εκπαίδευσης**: αναφέρεται στον αριθμό των περιόδων εκπαίδευσης. Μία περίοδος είναι ένα πλήρες πέρασμα του συνόλου δεδομένων εκπαίδευσης μέσα από έναν αλγόριθμο μηχανικής μάθησης.
- **Αλγόριθμος Μηχανικής Μάθησης**: καθορίζει τον αλγόριθμο μηχανικής μάθησης που θα αξιοποιηθεί για την εκπαίδευση του μοντέλου.
- **Συνάρτηση Ενεργοποίησης**: καθορίζει τη συνάρτηση ενεργοποίησης[1] που θα αξιοποιηθεί, σε περιπτώσεις νευρωνικών δικτύων.
- **Συνάρτηση Βελτιστοποίησης**: καθορίζει τη συνάρτηση βελτιστοποίησης[2] που θα αξιοποιηθεί, σε περιπτώσεις νευρωνικών δικτύων.
- **Μέγεθος Υποσυνόλων Δεδομένων**: αφορά το μέγεθος του εκάστοτε υποσυνόλου εκπαίδευσης. Σε κάθε πελάτη, το εκάστοτε σύνολο εκπαίδευσης χωρίζεται σε επιμέρους υποσύνολα, το μέγεθος των οποίων ορίζεται από τον χρήστη.

[1] Μια συνάρτηση ενεργοποίησης αποφασίζει εάν ένας νευρώνας πρέπει να ενεργοποιηθεί ή όχι. Αυτό σημαίνει ότι θα αποφασίσει εάν η είσοδος του νευρώνα είναι σημαντική ή όχι στη διαδικασία πρόβλεψης.

[2] Μία συνάρτηση βελτιστοποίησης τροποποιεί τα χαρακτηριστικά ενός νευρωνικού δικτύου, όπως τα βάρη και τον ρυθμό εκπαίδευσης, συμβάλλοντας στη μείωση της συνολικής απώλειας και στη βελτίωση της ακρίβειας.

Εφόσον οι παράμετροι έχουν επιλεχθεί, εκκινείται το στάδιο της επεξεργασίας. Στο συγκεκριμένο στάδιο και βάσει των παραμέτρων που έχουν επιλεχθεί, πραγματοποιούνται οι ακόλουθες διαδικασίες. Αρχικά, ανακτάται τον σύνολο δεδομένων που έχει επιλεχθεί από το αποθετήριο που περιέχει όλα τα διαθέσιμα σύνολα δεδομένων. Επίσης, επιλέγεται ο αλγόριθμος που θα αξιοποιηθεί για την εκπαίδευση του μοντέλου μηχανικής μάθησης από το σύνολο των υλοποιημένων αλγορίθμων, σε συνδυασμό με τις συναρτήσεις ενεργοποίησης και βελτιστοποίησης. Συγχρόνως, τα δεδομένα διανέμονται στους πελάτες και καθορίζονται οι επαναλήψεις, βάσει των αντίστοιχων παραμέτρων που έχουν δοθεί. Έπειτα, τα δεδομένα καθαρίζονται και τυχών εσφαλμένες τιμές διορθώνονται, έτσι ώστε να μην επηρεαστεί η ακρίβεια των μοντέλων. Εν συνεχεία, πραγματοποιείται ομοσπονδιακά η εκπαίδευση του μοντέλου, βάσει του πλήθους περιόδων εκπαίδευσης και του μεγέθους υποσυνόλων δεδομένων. Το ομοσπονδιακό μοντέλο που προκύπτει από τα επιμέρους μοντέλα, δημιουργείται βάσει του μέσου όρου των παραμέτρων των επιμέρους μοντέλων. Τέλος, το εκπαιδευμένο μοντέλο αποθηκεύεται τοπικά, ενώ τα αποτελέσματα της εκπαίδευσης, μαζί με αυτά που προέκυψαν από προηγούμενα πειράματα οπτικοποιούνται στη διεπαφή του χρήστη, με χρήση κατάλληλων διαγραμμάτων και γραφικών.

3.2. Χρησιμοποιούμενες Τεχνολογίες

Η εφαρμογή που αναπτύχθηκε στα πλαίσια της παρούσας εργασίας είναι web-based και περιλαμβάνει το front-end, το οποίο αποτελείται από τον πυλώνα «Προβολή», και το back-end το οποίο αποτελείται από τους πυλώνες «Επεξεργασία» και «Αποθήκευση». Για το front-end χρησιμοποιήθηκαν οι ακόλουθες τεχνολογίες:

- **HTML5** (HyperText Markup Language) [57]: χρησιμοποιείται για την οργάνωση των επιμέρους τμημάτων από τα οποία αποτελείται η διεπαφή και την προσθήκη κανόνων στις φόρμες υποβολής του χρήστη για διασφάλιση της εγκυρότητας αυτών πριν σταλούν στο back-end.
- **Bootstrap 4** [58]: αξιοποιείται για την μορφοποίηση των παραπάνω τμημάτων ούτος ώστε να είναι ευδιάκριτα και ελκυστικά προς τον χρήστη. Το Bootstrap είναι ένα framework το οποίο αποτελείται από HTML, CSS και JavaScript. Ουσιαστικά, παρέχει στους προγραμματιστές έτοιμες κλάσεις τις οποίες μπορούν να χρησιμοποιήσουν έτσι ώστε να υλοποιήσουν γρήγορα μία πολύ ελκυστική διεπαφή χρήστη.
- **CSS** (Cascading Style Sheets) [59]: χρησιμοποιείται για την μορφοποίηση των παραπάνω τμημάτων ούτος ώστε να είναι ευδιάκριτα και ελκυστικά προς τον χρήστη.
- **JavaScript** [60]: αξιοποιείται για την προσθήκη του στοιχείου της δυναμικότητας στο front-end, διατήρηση cookies και γενικά διαχείριση διάφορων τιμών στο front-end.
- **jQuery** [61]: αποτελεί μία βιβλιοθήκη JavaScript και ουσιαστικά παίρνει πολλές κοινές εργασίες που απαιτούν πολλές γραμμές κώδικα JavaScript για να ολοκληρωθούν και τις «τυλίγει» σε μεθόδους που μπορούν να χρησιμοποιηθούν με μία γραμμή κώδικα. Μέσω της jQuery γίνονται και οι κλήσεις AJAX (Asynchronous JavaScript And XML) μεταξύ των front-end και back-end.

Για το back-end, αξιοποιήθηκε η γλώσσα προγραμματισμού Python (έκδοση 3.9) [62] και ειδικότερα οι ακόλουθες βιβλιοθήκες (modules):

- **Flask** (έκδοση 2.2.2) [63]: χρησιμοποιείται για την ανάπτυξη της εφαρμογής με χρήση υπηρεσιών ιστού, έτσι ώστε αυτές να είναι διαθέσιμες στους χρήστες μέσω της διεπαφής η οποία αναπτύχθηκε με σχετικές web τεχνολογίες.
- **Flask_Cors** (έκδοση 3.0.10) [64]: αξιοποιείται για την αποφυγή εμφάνισης του σφάλματος μη ασφαλούς σύνδεσης (Cross Origin).
- **Keras** (έκδοση 2.10.0) [65]: είναι μια βιβλιοθήκη λογισμικού ανοιχτού κώδικα που παρέχει μια διεπαφή Python για τεχνητά νευρωνικά δίκτυα. Η Keras λειτουργεί και ως διεπαφή για τη βιβλιοθήκη TensorFlow.
- **Matplotlib** (έκδοση 3.5.3) [66]: είναι μια βιβλιοθήκη σχεδίασης διαγραμμάτων από μαθηματικά δεδομένα τα οποία προέρχονται από την βιβλιοθήκη NumPy.
- **NumPy** (έκδοση 1.23.3) [67]: προσθέτει υποστήριξη για μεγάλους, πολυδιάστατους πίνακες, μαζί με μια μεγάλη συλλογή μαθηματικών συναρτήσεων υψηλού επιπέδου για εφαρμογή πάνω σε αυτούς τους πίνακες.

- **Pandas** (έκδοση 1.4.4) [68]: χρησιμοποιείται για την διαχείριση των συνόλων δεδομένων, καθώς και για την επεξεργασία και ανάλυσή τους.
- **Pillow** (έκδοση 9.2.0) [69]: αξιοποιείται για τη διαχείριση πολλών διαφορετικών μορφών αρχείων εικόνας.
- **Plotly** (έκδοση 5.10.0) [70]: είναι μια βιβλιοθήκη σχεδίασης πολύπλοκων διαγραμμάτων.
- **Psutil** (έκδοση 5.9.2) [71]: είναι μια βιβλιοθήκη που χρησιμοποιείται για την ανάκτηση πληροφοριών σχετικά με τις διεργασίες που εκτελούνται και τη χρήση του συστήματος.
- **Scikit_Learn** (έκδοση 1.1.2) [72]: αξιοποιείται για την εκπαίδευση αλγορίθμων μηχανικής μάθησης.
- **TensorFlow** (έκδοση 2.10.0) [73]: είναι μαθηματική βιβλιοθήκη που αξιοποιείται για την επίλυση σύνθετων προβλημάτων μηχανικής μάθησης, αξιοποιώντας νευρωνικά δίκτυα.
- **Pandas Profiling** (έκδοση 3.3.0) [74]: είναι βιβλιοθήκη που αξιοποιείται για τη πραγματοποίηση περιγραφικής ανάλυσης στα δεδομένα.
- **Pandas Schema** (έκδοση 0.3.6) [75]: είναι βιβλιοθήκη που χρησιμοποιείται για την επικύρωση δεδομένων και τον καθαρισμό τους, σύμφωνα με συγκεκριμένους κανόνες επικύρωσης.

3.3. Σύνολα Δεδομένων

Στα πλαίσια της συγκεκριμένης εργασίας επιλέχθηκε μία πληθώρα συνόλων δεδομένων τα οποία προέρχονται από διαφορετικούς τομείς, έτσι ώστε να πραγματοποιηθούν πληθώρα πειραμάτων. Ειδικότερα, αξιοποιήθηκαν οκτώ (8) σύνολα δεδομένων, τα οποία ανακτήθηκαν από το Kaggle, το GitHub και το UCI Machine Learning Repository και τα οποία ανήκουν στους τομείς της υγειονομικής περίθαλψης, του περιβάλλοντος και της βιομηχανίας. Αναφορικά με τον τομέα της υγειονομικής περίθαλψης, τα σύνολα δεδομένων που χρησιμοποιήθηκαν είναι τέσσερα (4) και αφορούν, αντίστοιχα, ασθενείς με εγκεφαλικό (Stroke) [76], Covid-19 [77], καρκίνο του μαστού (Breast Cancer) [78] και νεφρική ανεπάρκεια (Kidney Disease) [79]. Όσον αφορά το τομέα του περιβάλλοντος, χρησιμοποιήθηκαν τρία (3) σύνολα δεδομένων που σχετίζονται με την ποσιμότητα του νερού (Water Potability) [80], την πρόβλεψη καιρού (Weather Forecast) [81] και την κατηγοριοποίηση φυτών Ίρις (Iris) [82]. Τέλος, αξιοποιήθηκε ένα (1) σύνολο δεδομένων από τον τομέα της βιομηχανίας που σχετίζεται με την αξιολόγηση αυτοκινήτων (Car Evaluation) [83]. Τα χαρακτηριστικά που περιλαμβάνει το εκάστοτε σύνολο δεδομένων περιγράφονται στους ακόλουθους πίνακες.

Πίνακας 3: Περιγραφή Συνόλου Δεδομένων «Stroke»

Σύνολο Δεδομένων «Stroke»	
Χαρακτηριστικό	**Περιγραφή**
id	Μοναδικό αναγνωριστικό που αφορά συγκεκριμένη εγγραφή στο σύνολο δεδομένων.
gender	Το βιολογικό φύλο του εκάστοτε ασθενή.
age	Η ηλικία του εκάστοτε ασθενή.
hypertension	Δυαδικό χαρακτηριστικό που υποδεικνύει αν ο εκάστοτε ασθενής έχει υπέρταση ή όχι.
heart_disease	Δυαδικό χαρακτηριστικό που υποδεικνύει αν ο εκάστοτε ασθενής έχει καρδιακή ανεπάρκεια ή όχι.
ever_married	Η οικογενειακή κατάσταση του εκάστοτε ασθενή.
work_type	Το είδος της εργασίας του εκάστοτε ασθενή (π.χ. δημόσιος υπάλληλος, ελεύθερος επαγγελματίας κ.α.).
Residence_type	Ο τύπος της κατοικίας στην οποία διαμένει ο εκάστοτε ασθενής (π.χ. διαμέρισμα σε πόλη, κατοικία στην ύπαιθρο κ.α.)
avg_glucose_level	Το επίπεδο της γλυκόζης στο αίμα του εκάστοτε ασθενή.
bmi	Ο δείκτης μάζας σώματος του εκάστοτε ασθενή.

smoking_status	Χαρακτηριστικό που υποδεικνύει αν ο εκάστοτε ασθενής καπνίζει και, αν ναι, πόσο.
stroke	Δυαδικό χαρακτηριστικό που υποδεικνύει αν ο εκάστοτε ασθενής έπαθε εγκεφαλικό ή όχι.

Πίνακας 4: Περιγραφή Συνόλου Δεδομένων «Covid - 19»

Σύνολο Δεδομένων «Covid - 19»	
Χαρακτηριστικό	**Περιγραφή**
Patient ID	Μοναδικό αναγνωριστικό που αφορά συγκεκριμένη εγγραφή στο σύνολο δεδομένων.
Patient age quantile	Η ηλικία του εκάστοτε ασθενή.
Hematocrit	Η τιμή του αιματοκρίτη.
Hemoglobin	Η τιμή της αιμοσφαιρίνης.
Platelets	Το πλήθος των αιμοπεταλίων.
Red blood Cells	Το πλήθος των ερυθρών αιμοσφαιρίων.
Lymphocytes	Το πλήθος των λεμφοκυττάρων.
Leukocytes	Το πλήθος των λευκοκυττάρων.
Basophils	Το πλήθος των βασεόφιλων.
Eosinophils	Το πλήθος των ηωσινόφιλων.
Monocyte	Το πλήθος των μονοκυττάρων.
Serum Glucose	Η τιμή του ορού γλυκόζης.
Neutrophils	Το πλήθος των ουδετερόφιλων.
Urea	Η τιμή της ουρίας.
Proteina C reativa mg/dL	Η τιμή της πρωτεΐνης C reativa σε mg/dL.
Creatinine	Η ποσότητα της κρεατίνης.
Potassium	Η ποσότητα του καλίου.
Sodium	Η ποσότητα του νατρίου.
Alanine transaminase	Η τιμή της τρανσαμινάσης της αλανίνης.
Aspartate transaminase	Η τιμή της ασπαρτικής τρανσαμινάσης.

Label	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής εισήχθη σε μονάδα εντατικής θεραπείας (ΜΕΘ).

Πίνακας 5: Περιγραφή Συνόλου Δεδομένων «Breast Cancer»

Σύνολο Δεδομένων «Breast Cancer»	
Χαρακτηριστικό	**Περιγραφή**
id	Μοναδικό αναγνωριστικό που αφορά συγκεκριμένη εγγραφή στο σύνολο δεδομένων.
diagnosis	Δυαδικό χαρακτηριστικό που αφορά τη διάγνωση του όγκου αναφορικά με το αν είναι καλοήθης ή κακοήθης.
radius_mean	Ο μέσος όρος των αποστάσεων από το κέντρο σε σημεία της περιμέτρου.
texture_mean	Η τυπική απόκλιση τιμών που βρίσκονται στη κλίμακα του γκρι.
perimeter_mean	Το μέσο μέγεθος του πυρήνα του όγκου.
area_mean	Η περιφέρεια που καταλαμβάνει ο όγκος.
smoothness_mean	Ο μέσος όρος τοπικής διακύμανσης στο μήκος της ακτίνας.
compactness_mean	Ο μέσος όρος της περιμέτρου υψωμένος στο τετράγωνο.
concavity_mean	Ο μέσος όρος της σοβαρότητας των κοίλων τμημάτων του περιγράμματος.
concave points_mean	Ο μέσος όρος του πλήθους των κοίλων τμημάτων του περιγράμματος.
symmetry_mean	Ο μέσος όρος της συμμετρίας.
fractal_dimension_mean	Ο κανονικοποιημένος μέσος όρος για την «προσέγγιση της ακτογραμμής».
radius_se	Το τυπικό σφάλμα για το μέσο όρο των αποστάσεων από το κέντρο σε σημεία της περιμέτρου.
texture_se	Το τυπικό σφάλμα για τη τυπική απόκλιση τιμών που βρίσκονται στη κλίμακα του γκρι.
perimeter_se	Το τυπικό σφάλμα για τη τυπική απόκλιση της περιμέτρου.
area_se	Το τυπικό σφάλμα για τη τυπική απόκλιση της περιοχής.

smoothness_se	Το τυπικό σφάλμα για τη τοπική διακύμανση στα μήκη ακτίνας.
compactness_se	Το τυπικό σφάλμα για την περίμετρο υψωμένη στο τετράγωνο, διαιρούμενη από την περιοχή και μειωμένο κατά ένα.
concavity_se	Το τυπικό σφάλμα για τη σοβαρότητα των κοίλων τμημάτων του περιγράμματος.
concave points_se	Το τυπικό σφάλμα για τον αριθμό των κοίλων τμημάτων του περιγράμματος.
symmetry_se	Το τυπικό σφάλμα για τη συμμετρία.
fractal_dimension_se	Το κανονικοποιημένο τυπικό σφάλμα για την «προσέγγιση της ακτογραμμής».
radius_worst	Η «χειρότερη» ή μεγαλύτερη μέση τιμή για τη μέση απόσταση από το κέντρο σε σημεία της περιμέτρου.
texture_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για τυπική απόκλιση τιμών που βρίσκονται στη κλίμακα του γκρι.
perimeter_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για τη περίμετρο.
area_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για τη περιοχή.
smoothness_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για τοπική διακύμανση στο μήκος της ακτίνας.
compactness_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για την για την περίμετρο υψωμένη στο τετράγωνο, διαιρούμενη από την περιοχή και μειωμένο κατά ένα.
concavity_worst	Η «χειρότερη». ή μεγαλύτερη μέση τιμή για τη σοβαρότητα των κοίλων τμημάτων του περιγράμματος.
concave points_worst	Η «χειρότερη» ή μεγαλύτερη μέση τιμή για τον αριθμό των κοίλων τμημάτων του περιγράμματος.
symmetry_worst	Η «χειρότερη» ή μεγαλύτερη μέση τιμή για τη συμμετρία.
fractal_dimension_worst	Η «χειρότερη» ή μεγαλύτερη μέση τιμή για την «προσέγγιση της ακτογραμμής».

Πίνακας 6: Περιγραφή Συνόλου Δεδομένων «Kidney Disease»

Σύνολο Δεδομένων «Kidney Disease»	
Χαρακτηριστικό	**Περιγραφή**
id	Μοναδικό αναγνωριστικό που αφορά συγκεκριμένη εγγραφή στο σύνολο δεδομένων.
age	Η ηλικία του εκάστοτε ασθενή.
bp	Η τιμή της αρτηριακής πίεσης.
sg	Το ειδικό βάρος.
al	Η τιμή της αλβουμίνης.
su	Η τιμή της ζάχαρης στο αίμα.
rbc	Το πλήθος των ερυθρών αιμοσφαιριών.
pc	Το πλήθος των φαγοκυττάρων.
pcc	Το πλήθος των συστάδων φαγοκυττάρων.
ba	Το πλήθος των βακτηρίων.
bgr	Η ποσότητα της γλυκόζης στο αίμα.
bu	Η τιμή της ουρίας στο αίμα.
sc	Η τιμή της κρεατίνης.
sod	Η τιμή του νατρίου στο αίμα.
pot	Η τιμή του καλίου στο αίμα.
hemo	Η τιμή της αιμοσφαιρίνης στο αίμα.
pcv	Η τιμή του αιματοκρίτη.
wc	Ο αριθμός των λευκών αιμοσφαιρίων στο αίμα.
rc	Ο αριθμός ερυθρών αιμοσφαιρίων στο αίμα.
htn	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής πάσχει από υπέρταση ή όχι.
dm	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής πάσχει από σακχαρώδη διαβήτη ή όχι.
cad	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής πάσχει από στεφανιαία νόσο ή όχι.

appet	Χαρακτηριστικό που σχετίζεται με την όρεξη που έχει ο ασθενής για κατανάλωση φαγητού.
pe	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής πάσχει από οίδημα ή όχι.
ane	Δυαδικό χαρακτηριστικό που υποδηλώνει αν ο ασθενής πάσχει από αναιμία ή όχι.
classification	Δυαδικό χαρακτηριστικό που υποδεικνύει αν ο ασθενής κινδυνεύει να εμφανίσει νεφρική ανεπάρκεια ή όχι.

Πίνακας 7: Περιγραφή Συνόλου Δεδομένων «Water Potability»

Σύνολο Δεδομένων «Water Potability»	
Χαρακτηριστικό	**Περιγραφή**
ph	Το pH του δείγματος (0 έως 14).
Hardness	Η σκληρότητα του νερού, δηλαδή η ικανότητα του νερού να καθιζάνει σαπούνι σε mg/L .
Solids	Τα ολικά διαλυμένα στερεά σε ppm.
Chloramines	Η ποσότητα χλωραμινών σε ppm.
Sulfate	Η ποσότητα θειικών αλάτων διαλυμένη σε mg/L.
Conductivity	Η ηλεκτρική αγωγιμότητα του νερού σε μS/cm.
Organic_carbon	Η ποσότητα οργανικού άνθρακα σε ppm.
Trihalomethanes	Η ποσότητα τριαλομεθανίων σε μg/L.
Turbidity	Η μέτρηση της ιδιότητας εκπομπής φωτός του νερού σε NTU.
Potability	Δυαδικό χαρακτηριστικό που υποδεικνύει εάν το δείγμα νερού είναι ασφαλές για ανθρώπινη κατανάλωση ή όχι.

Πίνακας 8: Περιγραφή Συνόλου Δεδομένων «Weather Forecast»

Σύνολο Δεδομένων «Weather Forecast»	
Χαρακτηριστικό	**Περιγραφή**
date	Η ημερομηνία που λήφθηκαν οι μετρήσεις.

precipitation	Όλες οι μορφές στις οποίες πέφτει νερό στην επιφάνεια της γης και σε ανοιχτά υδάτινα σώματα όπως βροχή, χιονόνερο, χιόνι, χαλάζι ή ψιλόβροχο.
temp_max	Η μέγιστη θερμοκρασία που καταγράφηκε τη συγκεκριμένα ημερομηνία.
temp_min	Η ελάχιστη θερμοκρασία που καταγράφηκε τη συγκεκριμένα ημερομηνία.
wind	Η ταχύτητα του ανέμου.
weather	Ο καιρός που προβλέπεται για την επόμενη μέρα.

Πίνακας 9: Περιγραφή Συνόλου Δεδομένων «Iris»

Σύνολο Δεδομένων «Iris»	
Χαρακτηριστικό	**Περιγραφή**
sepal_length	Το μήκος σέπαλου σε εκατοστά.
sepal_width	Το πλάτος σέπαλου σε εκατοστά.
petal_length	Το μήκος πετάλου σε εκατοστά
petal_width	Το πλάτος πετάλου σε εκατοστά.
class	Η κλάση στην οποία ανήκει το συγκεκριμένο φυτό.

Πίνακας 10: Περιγραφή Συνόλου Δεδομένων «Car Evaluation»

Σύνολο Δεδομένων «Car Evaluation»	
Χαρακτηριστικό	**Περιγραφή**
buying	Η κατηγορία στην οποία ανήκει η τιμή αγοράς του αυτοκινήτου.
maint	Η κατηγορία στην οποία ανήκει το κόστος συντήρησης του αυτοκινήτου.
doors	Το πλήθος των πορτών που έχει το αυτοκίνητο.
persons	Το πλήθος των επιβατών που μπορεί να εξυπηρετήσει το συγκεκριμένο αυτοκίνητο.
lug_boot	Η κατηγορία στην οποία ανήκει ο διαθέσιμος χώρος αποσκευών του αυτοκινήτου.

safety	Η κατηγορία στην οποία ανήκει η ασφάλεια του αυτοκινήτου.
class	Η κατηγορία στην οποία ανήκει το αυτοκίνητο βάσει των διαθέσιμων παραμέτρων και της «άνεσης» που προσφέρει στους ιδιοκτήτες του.

3.4. Καθαρισμός Δεδομένων

Η αξιοπιστία των δεδομένων που χρησιμοποιούνται για την εκπαίδευση ενός αλγόριθμου μηχανικής μάθησης είναι μεγίστης σημασίας, καθώς αυτά επηρεάζουν σε μεγάλο βαθμό την αποτελεσματικότητά του. Κατά τη διαδικασία του καθαρισμού επιδιορθώνονται τυχών σφάλματα στα δεδομένα, ελλιπείς τιμές αντικαθίστανται/προβλέπονται και οι διπλότυπες εγγραφές αφαιρούνται. Στα πλαίσια της συγκεκριμένης υλοποίησης, ο καθαρισμός των δεδομένων λαμβάνει χώρα στον εκάστοτε χρήστη. Για παράδειγμα, αν η εκπαίδευση πραγματοποιείται σε μία ομοσπονδία τεσσάρων (4) χρηστών, τότε τα δεδομένα του εκάστοτε χρήστη καθαρίζονται. Για να καθαριστούν τα δεδομένα των χρηστών, θα πρέπει πρώτα να επικυρωθούν σύμφωνα με συγκεκριμένους κανόνες επικύρωσης, οι οποίοι είναι αποθηκευμένοι σε συγκεκριμένες δομές που ονομάζονται σχήματα. Ένας ενδεικτικός κανόνας επικύρωσης παρουσιάζεται στην ***Εικόνα 6***, ενώ ένα ενδεικτικό παράδειγμα σχήματος φαίνεται στην ***Εικόνα 7***.

```
def check_int(num):
    try:
        int(num)
    except ValueError:
        return False
    return True

int_validation = [CustomElementValidation(lambda i: check_int(i), 'is not integer.')]
```

Εικόνα 6: Ενδεικτικό παράδειγμα κανόνα επικύρωσης

```
iris_schema = pandas_schema.Schema([
    Column('sepal length in cm', null_validation + int_validation),
    Column('sepal width in cm', null_validation + int_validation),
    Column('petal length in cm', null_validation + int_validation),
    Column('petal width in cm', null_validation + int_validation),
    Column('class', null_validation + string_validation)
])
```

Εικόνα 7: Ενδεικτικό παράδειγμα σχήματος δεδομένων

Ειδικότερα, στην ***Εικόνα 6***, παρουσιάζεται ένας κανόνας επικύρωσης που ελέγχει αν μία τιμή είναι ακέραιος αριθμός. Οι κανόνες αποτελούνται από συναρτήσεις που πραγματοποιούν τους αντίστοιχους ελέγχους. Για παράδειγμα, στη συγκεκριμένη περίπτωση η συνάρτηση *check_int* ελέγχει αν μία τιμή είναι ακέραια. Αν δεν είναι ακέραια, τότε ο κανόνας επικύρωσης ενημερώνει ότι η συγκεκριμένη τιμή δεν είναι ακέραιος αριθμός. Για κάθε χαρακτηριστικό σε ένα σύνολο δεδομένων μπορούν να υπάρχουν πολλοί κανόνες επικύρωσης στο αντίστοιχο σχήμα, όπως φαίνεται στην ***Εικόνα 7***. Αναλυτικότερα, στη συγκεκριμένη εικόνα φαίνεται το σχήμα για το σύνολο δεδομένων «Iris», στο οποίο αποθηκεύονται οι κανόνες επικύρωσης ανά χαρακτηριστικό του συνόλου δεδομένων. Στο συγκεκριμένο σύνολο δεδομένων φαίνεται ότι τα

τέσσερα (4) πρώτα χαρακτηριστικά θα πρέπει να μην είναι κενά και, μάλιστα, να είναι ακέραιοι αριθμοί, ενώ το τελευταίο χαρακτηριστικό θα πρέπει να μην είναι κενό, αλλά να είναι κάποιο κείμενο/λεκτικό.

Τα σφάλματα που εντοπίστηκαν στα δεδομένα των πειραμάτων που διεξήχθησαν στα πλαίσια της παρούσας διπλωματικής εργασίας αφορούσαν στην ύπαρξη ελλιπών τιμών σε αριθμητικά χαρακτηριστικά. Για την αντιμετώπιση του συγκεκριμένου σφάλματος, εξετάστηκαν δύο (2) λύσεις. Η πρώτη αφορούσε τη διαγραφή των αντίστοιχων εγγραφών που περιείχαν ελλιπείς τιμές. Ωστόσο, αυτή η προσέγγιση οδηγούσε σε απώλεια πληροφορίας και, προφανώς, επηρέαζε την ακρίβεια των προβλέψεων των αλγορίθμων Μηχανικής Μάθησης. Η δεύτερη προσέγγιση αναφερόταν στην αντικατάσταση των ελλιπών τιμών με τον μέσο όρο των τιμών του αντίστοιχου χαρακτηριστικού στο οποίο ανήκαν οι συγκεκριμένες ελλιπείς τιμές. Η συγκεκριμένη προσέγγιση δεν επηρέασε αρνητικά την ακρίβεια των αλγορίθμων Μηχανικής Μάθησης, γι’ αυτό και τελικά υιοθετήθηκε για τα παρόντα σύνολα δεδομένων.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι οι τεχνικές με τις οποίες διασφαλίζεται η αξιοπιστία των δεδομένων δεν είναι καθολικά οι ίδιες, αλλά διαφέρουν ανά σενάριο χρήσης. Επιλέγονται με βάση τα χαρακτηριστικά του εκάστοτε σεναρίου χρήσης δηλαδή, τις απαιτήσεις σε υπολογιστικούς πόρους και φυσικά, το σύνολο δεδομένων και τα αντίστοιχα χαρακτηριστικά του.

3.5. Χρησιμοποιούμενοι Αλγόριθμοι

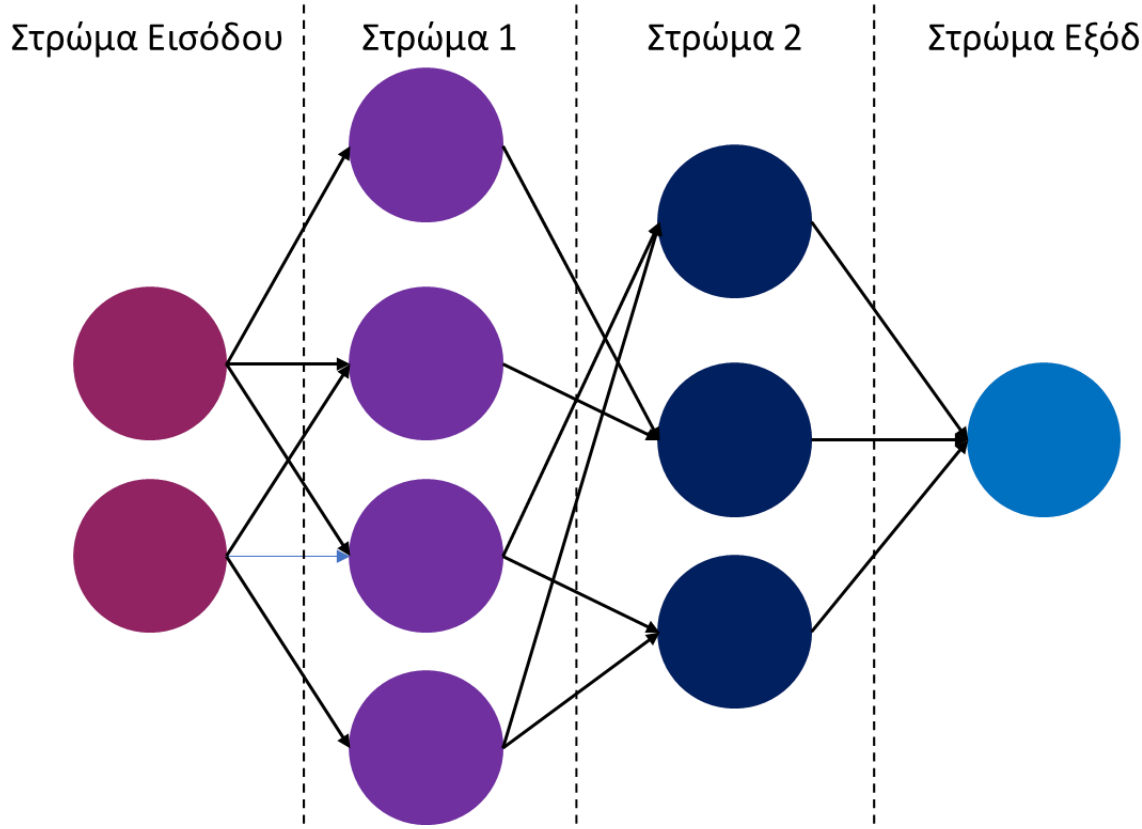
Στα πλαίσια της παρούσας εργασίας και για την εκτέλεση των πειραμάτων, αξιοποιήθηκαν τέσσερις (4) αλγόριθμοι με τη βοήθεια της βιβλιοθήκης Keras. Ειδικότερα, οι αλγόριθμοι παρουσιάζονται συνοπτικά στον ακόλουθο πίνακα.

Πίνακας 11: Χρησιμοποιούμενοι Αλγόριθμοι

Αλγόριθμος	Περιγραφή
Τεχνητό Νευρωνικό Δίκτυο (Artificial Neural Network – ANN)	Βασίζεται σε μια συλλογή συνδεδεμένων μονάδων ή κόμβων που ονομάζονται τεχνητοί νευρώνες. Κάθε σύνδεση μπορεί να μεταδώσει ένα σήμα σε άλλους νευρώνες. Ένας τεχνητός νευρώνας λαμβάνει σήματα και στη συνέχεια τα επεξεργάζεται και μπορεί να σηματοδοτήσει τους νευρώνες που συνδέονται με αυτόν. Το "σήμα" σε μια σύνδεση είναι ένας πραγματικός αριθμός και η έξοδος κάθε νευρώνα υπολογίζεται από κάποια μη γραμμική συνάρτηση του αθροίσματος των εισόδων του. Οι νευρώνες μπορεί να έχουν ένα κατώφλι τέτοιο ώστε ένα σήμα να αποστέλλεται μόνο εάν το αθροιστικό σήμα υπερβαίνει αυτό το κατώφλι [84].
Συνελικτικό Νευρωνικό Δίκτυο (Convolutional Neural Network – CNN)	Είδος ANN που αποτελείται από πλήρως συνδεδεμένα δίκτυα, δηλαδή, κάθε νευρώνας σε ένα στρώμα συνδέεται με όλους τους νευρώνες στο επόμενο στρώμα. Η "πλήρης συνδεσιμότητα" αυτών των δικτύων τα καθιστά επιρρεπή στην υπερπροσαρμογή δεδομένων (overfitting). Συνήθης εφαρμογή τέτοιου είδους νευρωνικών δικτύων πραγματοποιείται σε δεδομένα που προέρχονται από εικόνες [85].
Βαθύ Νευρωνικό Δίκτυο (Deep Neural Network – DNN)	Είδος ANN που εμπεριέχει υψηλή πολυπλοκότητα, καθώς αποτελείται από πολλά στρώματα νευρώνων. Συνήθως ένα νευρωνικό δίκτυο το οποίο αποτελείται από τουλάχιστον δύο (2) επίπεδα, χαρακτηρίζεται ως βαθύ νευρωνικό δίκτυο [86].
Λογιστική Παλινδρόμηση (Logistic Regression – LR)	Προβλέπει τις σχέσεις μεταξύ εξαρτημένων και ανεξάρτητων μεταβλητών. Υπολογίζει την πιθανότητα να συμβεί κάτι ανάλογα με πολλαπλά σύνολα μεταβλητών. Είναι ένας από τους πιο συνήθεις

	αλγόριθμους ταξινόμησης που χρησιμοποιείται στη μηχανική μάθηση [87].

Δεδομένου ότι αξιοποιείται η βιβλιοθήκη Keras για την υλοποίηση των παραπάνω αλγορίθμων και η οποία στηρίζεται σε νευρωνικά δίκτυα, κρίνεται σκόπιμο να παρατεθεί ένα απλό παράδειγμα νευρωνικού δικτύου, το οποίο φαίνεται στην ***Εικόνα 8***.



Εικόνα 8: Παράδειγμα απλού νευρωνικού δικτύου

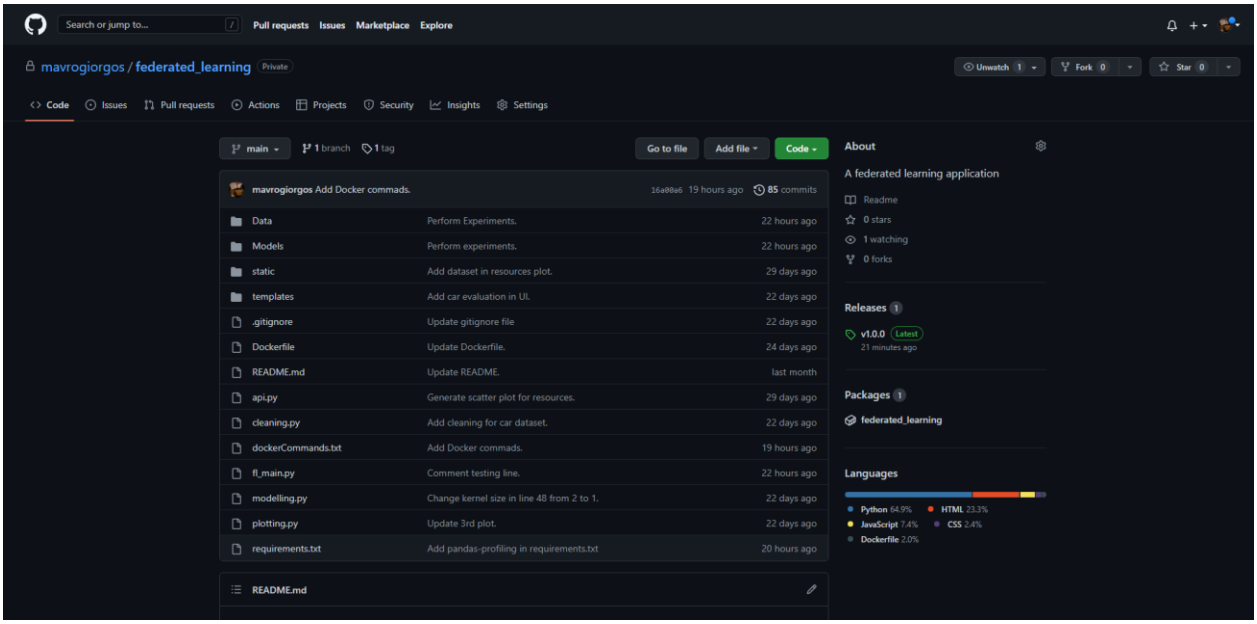
Ειδικότερα, ένα νευρωνικό δίκτυο αποτελείται από τουλάχιστον τρία (3) στρώματα. Το πρώτο στρώμα ονομάζεται στρώμα εισόδου, αποτελείται από τεχνητούς νευρώνες εισόδου και εισάγει τα αρχικά δεδομένα στο δίκτυο για περαιτέρω επεξεργασία από επόμενα στρώματα τεχνητών νευρώνων. Το δεύτερο στρώμα είναι το κρυφό, το οποίο, ανάλογα και με τη πολυπλοκότητα του νευρωνικού δικτύου, μπορεί να αποτελείται από επιμέρους στρώματα. Για παράδειγμα, το νευρωνικό δίκτυο που απεικονίζεται παραπάνω, αποτελείται από δύο (2) κρυφά στρώματα που ονομάζονται «Στρώμα 1» και «Στρώμα 2». Τα κρυφά στρώματα εκτελούν μη γραμμικούς μετασχηματισμούς των δεδομένων που εισάγονται σε αυτά, βάσει κάποιας συνάρτησης ενεργοποίησης. Τέλος, το στρώμα εξόδου είναι το τελικό στρώμα στο νευρωνικό δίκτυο, όπου λαμβάνονται οι επιθυμητές προβλέψεις.

3.6. Οδηγίες Εγκατάστασης και Εκτέλεσης

Προκειμένου να εκτελεστεί τοπικά η αναπτυχθείσα εφαρμογή, θα πρέπει πρώτα να γίνουν κάποιες εγκαταστάσεις, βάσει του τρόπου εγκατάστασης και εκτέλεσης που θα επιλεχθεί. Υπάρχουν δύο (2) διαθέσιμοι τρόποι εγκατάστασης και εκτέλεσης, οι οποίοι περιγράφονται παρακάτω.

3.6.1. Α' Τρόπος Εγκατάστασης και Εκτέλεσης

Αρχικά, η εφαρμογή είναι διαθέσιμη στο αποθετήριο GitHub [88] με ηλεκτρονική διεύθυνση: https://github.com/mavrogiorgos/federated_learning και το οποίο απεικονίζεται στην **Εικόνα *9***.



Εικόνα 9: GitHub αποθετήριο εφαρμογής

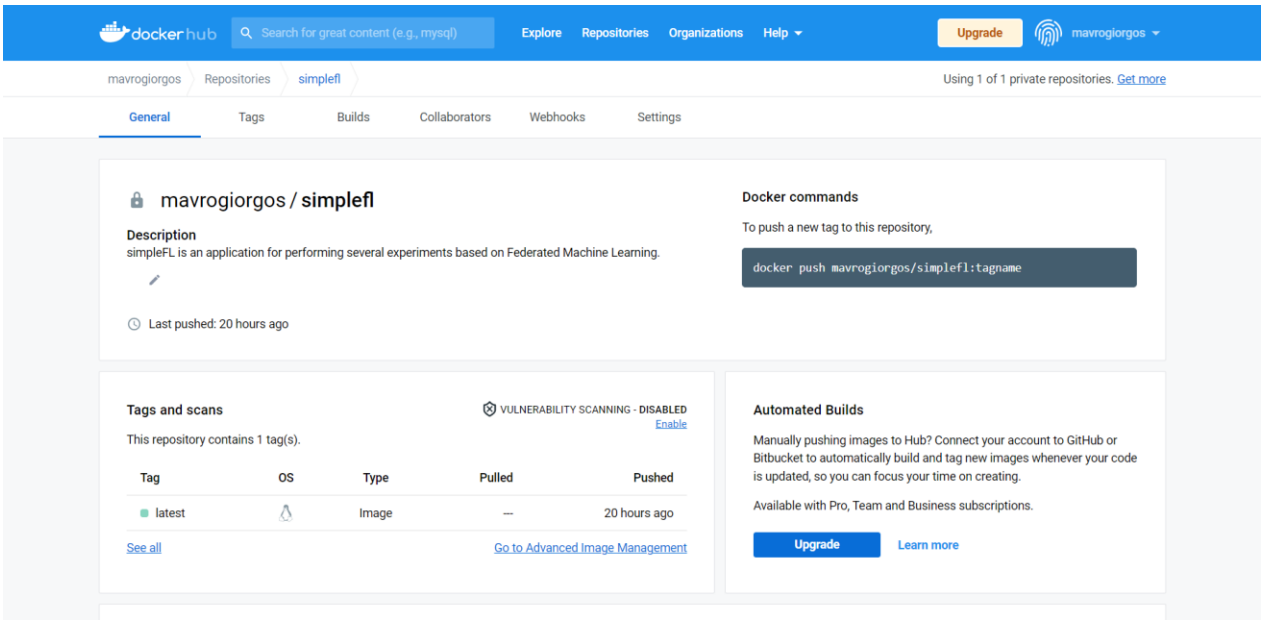
Το συγκεκριμένο αποθετήριο είναι ιδιωτικό, το οποίο σημαίνει ότι για να εξουσιοδοτηθεί η πρόσβαση σε αυτό είναι απαραίτητη η επικοινωνία με το e-mail kostismvg@gmail.com, οποίο ανήκει στον συγγραφέα της παρούσας διπλωματικής εργασίας. Δεδομένου ότι έχει εξασφαλιστεί η πρόσβαση στο προαναφερθέν αποθετήριο, ο ενδιαφερόμενος θα πρέπει να εγκαταστήσει την Python (έκδοση 3.9.10) [89] και τη τελευταία έκδοση του συστήματος ελέγχου εκδόσεων Git [90], φυσικά για το λειτουργικό σύστημα το οποίο έχει στον υπολογιστή του. Εφόσον ο ενδιαφερόμενος έχει πραγματοποιήσει τις παραπάνω εγκαταστάσεις, θα πρέπει να εκτελέσει σειριακά τις ακόλουθες ενέργειες σε ένα τερματικό.

- «Κλωνοποίηση» του αποθετηρίου GitHub με χρήση της εντολής *git clone https://github.com/mavrogiorgos/federated_learning.git.*
- Εγκατάσταση των απαραίτητων βιβλιοθηκών που αναφέρθηκαν στην ενότητα 3.2 με χρήση της εντολής *pip install requirements.txt.*

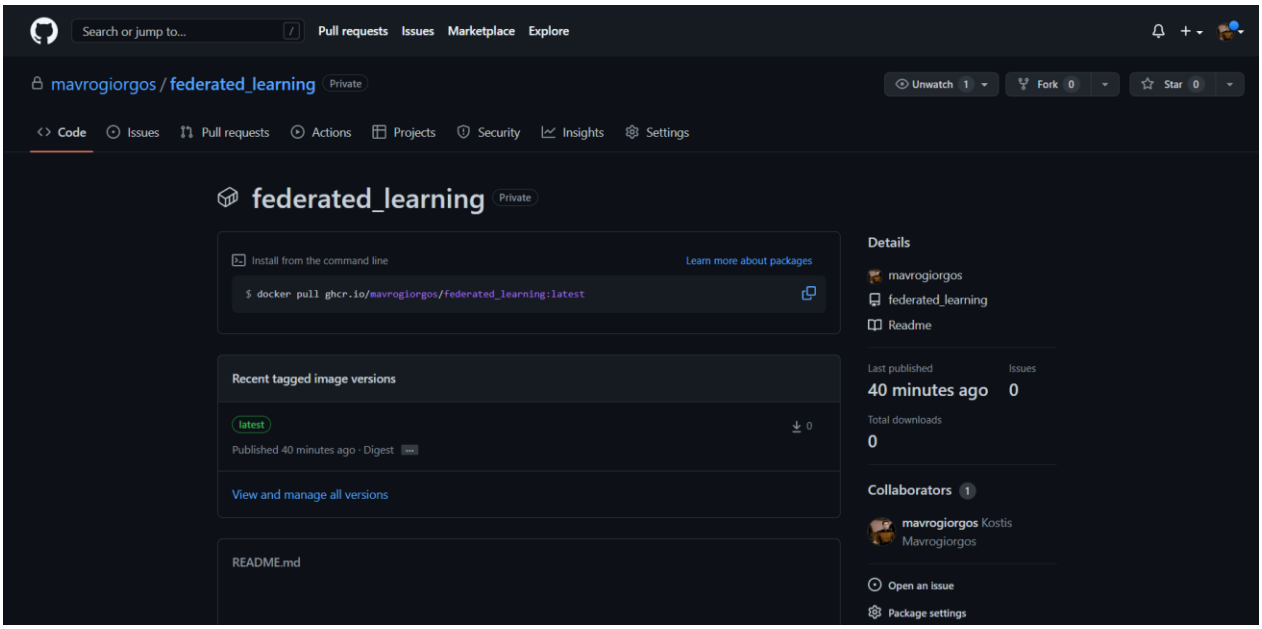
- Εκτέλεση της εφαρμογής με χρήση της εντολής *python3 api.py*.
- Άνοιγμα ενός οποιοδήποτε φυλλομετρητή στη διεύθυνση http://localhost:5000, όπου πλέον «τρέχει» η εφαρμογή.

3.6.2. Β' Τρόπος Εγκατάστασης και Εκτέλεσης

Η εφαρμογή είναι επίσης διαθέσιμη και ως Docker Container [91] στη διεύθυνση https://hub.docker.com/repository/docker/mavrogiorgos/simplefl, αλλά και στη διεύθυνση https://github.com/mavrogiorgos/federated_learning/pkgs/container/federated_learning, όπως παρουσιάζεται στην **Εικόνα *10*** και στην **Εικόνα *11***.



Εικόνα 10: DockerHub αποθετήριο του image της εφαρμογής



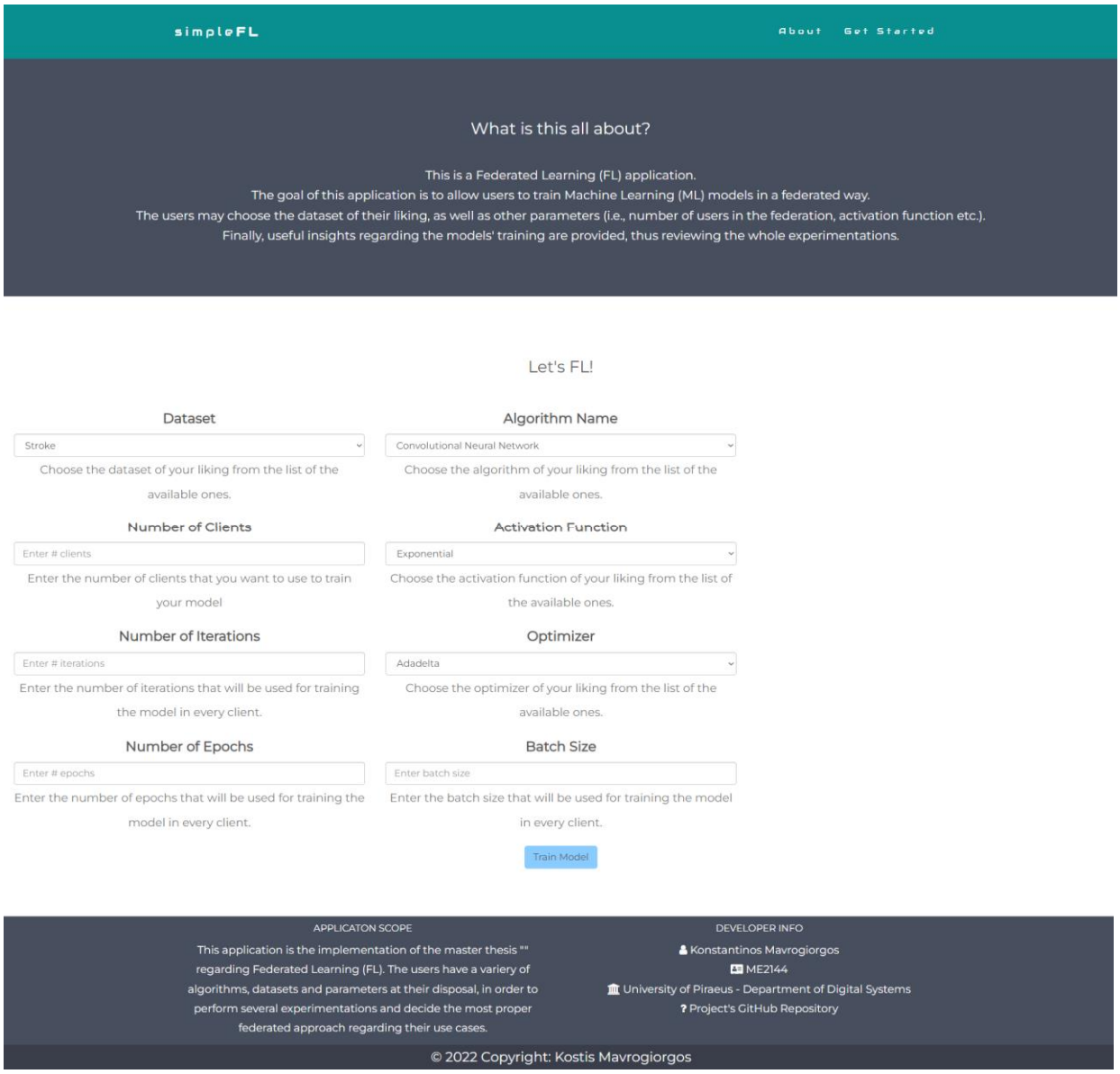
Εικόνα 11: GitHub αποθετήριο του image της εφαρμογής

Σε αυτή τη περίπτωση, ο ενδιαφερόμενος θα πρέπει να έχει εγκαταστήσει την αντίστοιχη έκδοση του Docker βάσει του λειτουργικού συστήματος που διαθέτει ο υπολογιστής του [92]. Εν συνεχεία θα πρέπει να εκτελέσει σειριακά τις ακόλουθες ενέργειες σε ένα τερματικό.

- «Κλωνοποίηση» του Image της εφαρμογής με χρήση της εντολής *docker pull mavrogiorgos/simplefl* ή της εντολής docker pull ghcr.io/mavrogiorgos/federated_learning:latest.
- Εκτέλεση της εφαρμογής με χρήση της εντολής *docker run -p5000:5000 mavrogiorgos/simplefl* ή της εντολής *docker run -p5000:5000* ghcr.io/mavrogiorgos/federated_learning.
- Άνοιγμα ενός οποιοδήποτε φυλλομετρητή στη διεύθυνση http://localhost:5000, όπου πλέον «τρέχει» η εφαρμογή.

3.7. Διεπαφή Χρήστη

Όπως αναφέρθηκε και στην ενότητα 3.1, η διεπαφή χρήστη αποτελεί ένα από τα κύρια στοιχεία του προτεινόμενου μηχανισμού. Αποτελεί την «πύλη» μέσα από την οποία οι χρήστες δύνανται να πραγματοποιήσουν τα πειράματά τους, να τα παραμετροποιήσουν και να οπτικοποιήσουν τα αντίστοιχα αποτελέσματα. Η διεπαφή χρήστη αποτελείται από μία σελίδα, στην οποία είναι διαθέσιμες οι απαραίτητες πληροφορίες και παρέχονται όλες οι διαθέσιμες δυνατότητες. Ειδικότερα, δεδομένου ότι έχει εκκινήσει τοπικά ο μηχανισμός, η διεπαφή χρήστη είναι προσβάσιμη από οποιονδήποτε φυλλομετρητή στη διεύθυνση http://localhost:5000, όπως φαίνεται στην **Εικόνα *12***.



Εικόνα 12: Αρχική διεπαφή χρήστη μηχανισμού

Μέσα από το πλήρες ενδεικτικό σενάριο χρήσης της ενότητας 4.1 αναλύεται περαιτέρω η διεπαφή χρήστη, όπως επίσης και ο τρόπος με τον οποίο τα στοιχεία της μεταβάλλονται κατά τη διάρκεια της αλληλεπίδρασης με τους χρήστες.

4. Πειραματικά Αποτελέσματα

4.1. Πλήρες Ενδεικτικό Σενάριο Χρήσης

Στη συγκεκριμένη υποενότητα παρατίθεται ένα πλήρες παράδειγμα ενδεικτικού σεναρίου χρήσης, το οποίο περιγράφει ολόκληρη τη διαδικασία, από την έναρξη της εφαρμογής και τη συμπλήρωση των πειραματικών παραμέτρων από τους χρήστες, μέχρι και την εκπαίδευση των μοντέλων μηχανικής μάθησης και της προβολής των αντίστοιχων αποτελεσμάτων στη διεπαφή χρήστη.

Αρχικά, οι χρήστες πρέπει να επιλέγουν τις παραμέτρους των πειραμάτων τους, από αυτές που είναι διαθέσιμες και παρουσιάζονται συνοπτικά στον ακόλουθο πίνακα.

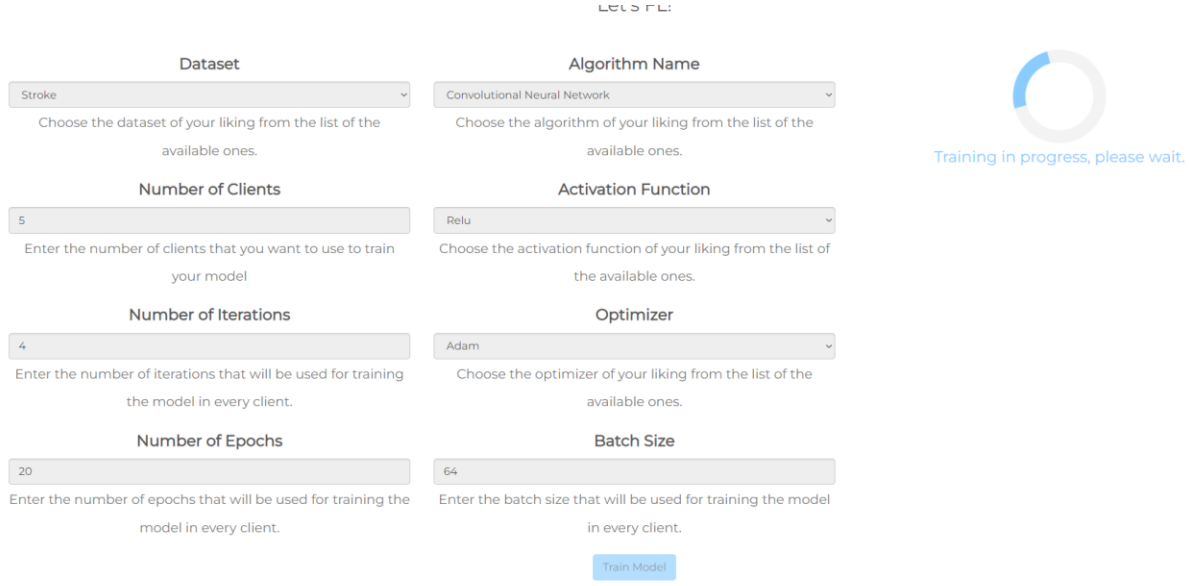
Πίνακας 12: Διαθέσιμες Παράμετροι Πειραμάτων

Παράμετρος	Διαθέσιμες Τιμές
Σύνολο Δεδομένων	«Stroke», «Covid -19», «Breast Cancer», «Kidney Disease», «Water Potability», «Weather Forecast», «Iris», «Car Evaluation»
Αριθμός Χρηστών	Ακέραιος αριθμός που ανήκει στο κλειστό διάστημα [1,10]
Αριθμός Επαναλήψεων	Ακέραιος αριθμός που ανήκει στο κλειστό διάστημα [1,10]
Πλήθος Περιόδων Εκπαίδευσης	Ακέραιος αριθμός που ανήκει στο κλειστό διάστημα [1,999]
Αλγόριθμος Μηχανικής Μάθησης	«Convolutional Neural Network», «Artificial Neural Network», «Deep Neural Network», «Logistic Regression»
Συνάρτηση Ενεργοποίησης	«Exponential», «Linear», «Relu», «Selu», «Sigmoid»
Συνάρτηση Βελτιστοποίησης	«Adadelta», «Adagrad», «Adam», «Adamax», «Ftrl», «Nadam», «RMSprop», «SGD»
Μέγεθος Υποσυνόλων Δεδομένων	Ακέραιος αριθμός που ανήκει στο κλειστό διάστημα [1,999]

Έστω ότι επιλέγονται οι ακόλουθες παράμετροι:

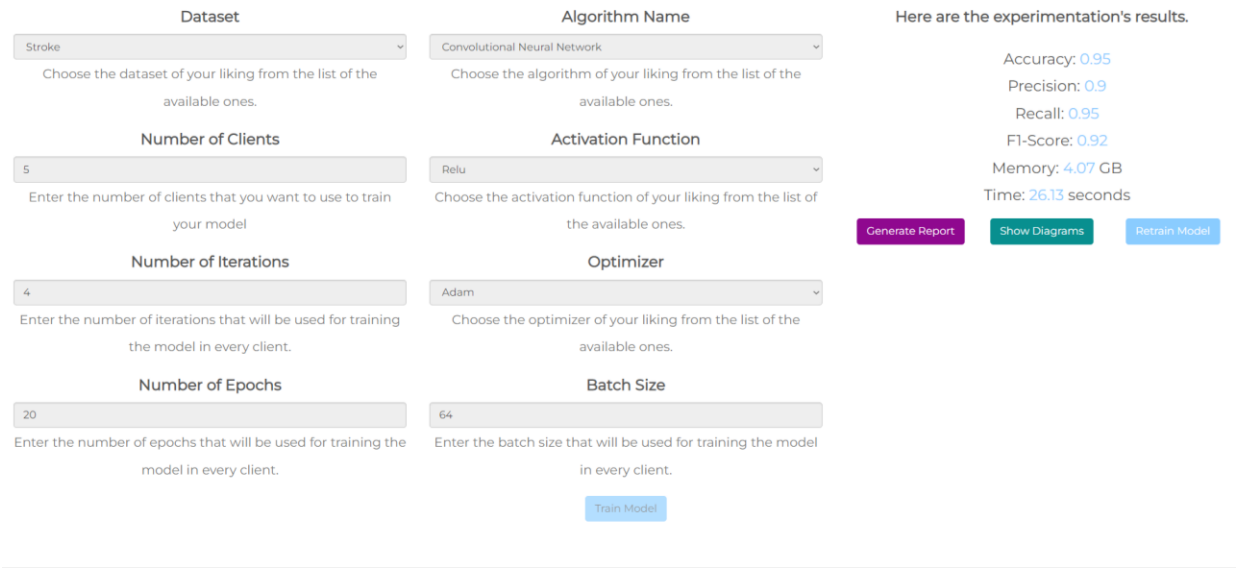
- **Σύνολο Δεδομένων**: «Stroke»
- **Αριθμός Χρηστών**: 5
- **Αριθμός Επαναλήψεων**: 4
- **Πλήθος Περιόδων Εκπαίδευσης**: 20
- **Αλγόριθμος Μηχανικής Μάθησης**: «Convolutional Neural Network»
- **Συνάρτηση Ενεργοποίησης**: «Relu»
- **Συνάρτηση Βελτιστοποίησης**: «Adam»
- **Μέγεθος Υποσυνόλων Δεδομένων**: 64

Στη συνέχεια, επιλέγεται το κουμπί «Train Model», ξεκινάει η εκπαίδευση και οι χρήστες ενημερώνονται με αντίστοιχο μήνυμα στην οθόνη, όπως φαίνεται στην **Εικόνα *13***.



Εικόνα 13: Πραγματοποίηση εκπαίδευσης με συγκεκριμένες παραμέτρους

Ύστερα από την επιτυχή ολοκλήρωση της εκπαίδευσης με τις συγκεκριμένους παραμέτρους, εμφανίζονται τα αντίστοιχα αποτελέσματα, όπως φαίνεται στην **Εικόνα *14***.



Εικόνα 14: Εμφάνιση αποτελεσμάτων εκπαίδευσης

Ειδικότερα, τα αποτελέσματα που εμφανίζονται συνοψίζονται στον ακόλουθο πίνακα.

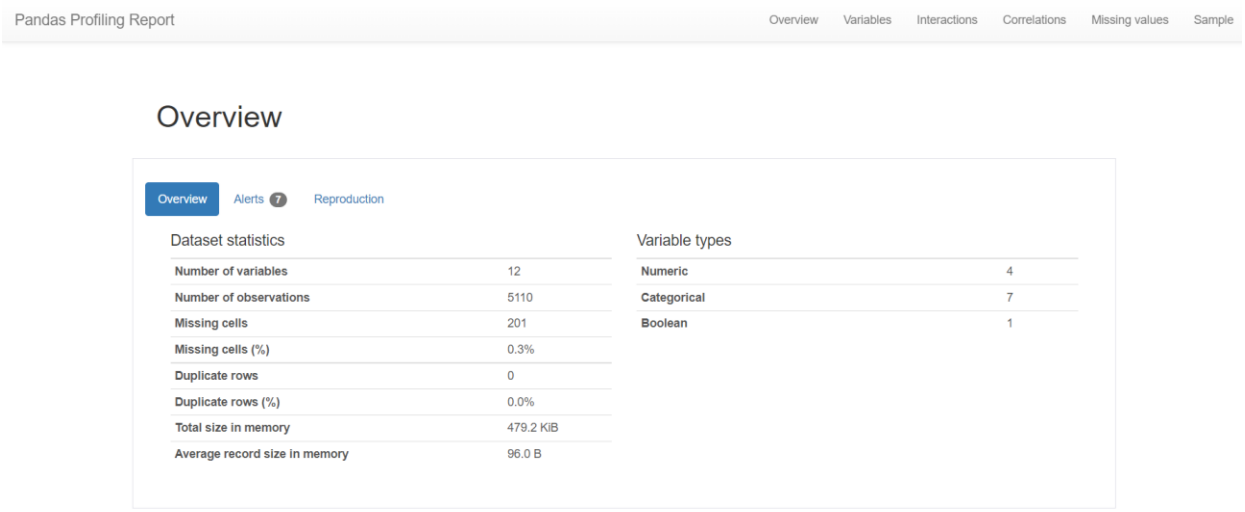
Πίνακας 13: Διαθέσιμα Αποτελέσματα Πειραμάτων

Αποτέλεσμα	Περιγραφή[3]
Accuracy	$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$
Precision	$Precision = \frac{TP}{TP + FP}$
Recall	$Recall = \frac{TP}{TP + FN}$
F1 - Score	$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall}$
Memory	Η μνήμη που αξιοποιήθηκε για τη πραγματοποίηση του πειράματος σε GB

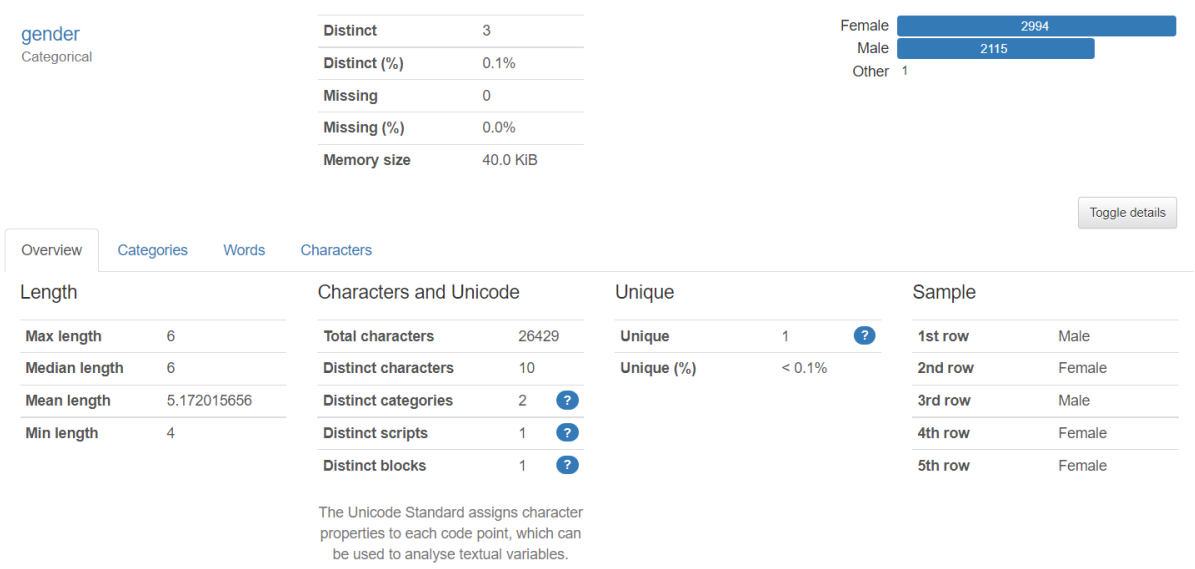
[3] True Positives (TP) - Αυτές είναι οι σωστά προβλεπόμενες θετικές τιμές που σημαίνει ότι η τιμή της πραγματικής κλάσης είναι ΑΛΗΘΗΣ και η τιμή της προβλεπόμενης κλάσης είναι επίσης ΑΛΗΘΗΣ.
True Negatives (TN) - Αυτές είναι οι σωστά προβλεπόμενες αρνητικές τιμές που σημαίνει ότι η τιμή της πραγματικής κλάσης είναι ΨΕΥΔΗΣ και η τιμή της προβλεπόμενης κλάσης είναι επίσης ΨΕΥΔΗΣ.
False Positives (FP) – Αυτές είναι οι λάθος προβλεπόμενες θετικές τιμές που σημαίνει ότι η τιμή της πραγματικής κλάσης είναι ΨΕΥΔΗΣ και η τιμή της προβλεπόμενης κλάσης είναι ΑΛΗΘΗΣ.
False Negatives (FN) – Αυτές είναι οι λάθος προβλεπόμενες θετικές τιμές που σημαίνει ότι η τιμή της πραγματικής κλάσης είναι ΑΛΗΘΗΣ και η τιμή της προβλεπόμενης κλάσης είναι ΨΕΥΔΗΣ.

Time	Ο χρόνος εκτέλεσης του πειράματος σε δευτερόλεπτα
Report	Λεπτομερές έγγραφο το οποίο περιλαμβάνει τα αποτελέσματα της περιγραφικής ανάλυσης που πραγματοποιήθηκε στο σύνολο δεδομένων πάνω στο οποίο εφαρμόστηκε η εκπαίδευση
Diagrams	Συγκριτικά διαγράμματα των πειραμάτων που έχουν πραγματοποιηθεί από τους χρήστες, βάσει διαφορετικών παραμέτρων

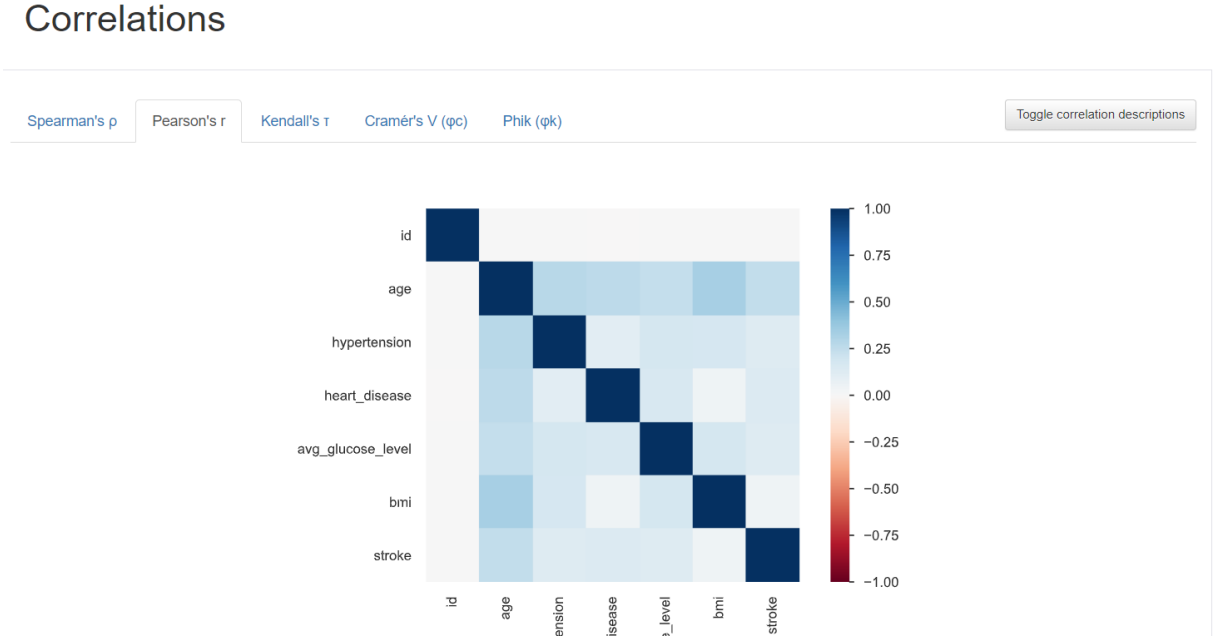
Εφόσον ο χρήστης επιλέξει το κουμπί «Generate Report», τότε δύναται να ανακτήσει το «Report» που περιγράφεται στον παραπάνω πίνακα και το οποίο, όπως φαίνεται στις ακόλουθες εικόνες, περιλαμβάνει πληθώρα πληροφοριών για κάθε χαρακτηριστικό του συνόλου δεδομένων εκπαίδευσης, οι οποίες αποτελούν τα αποτελέσματα της αντίστοιχης περιγραφικής ανάλυσης.



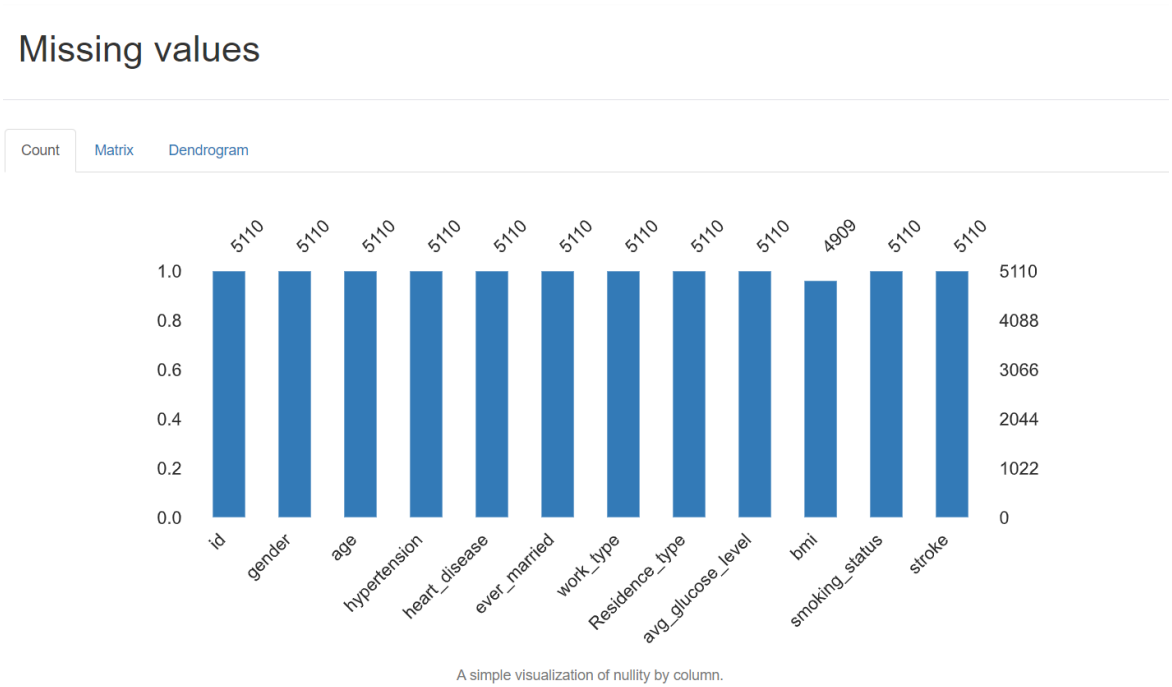
Εικόνα 15: Σύνοψη του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος



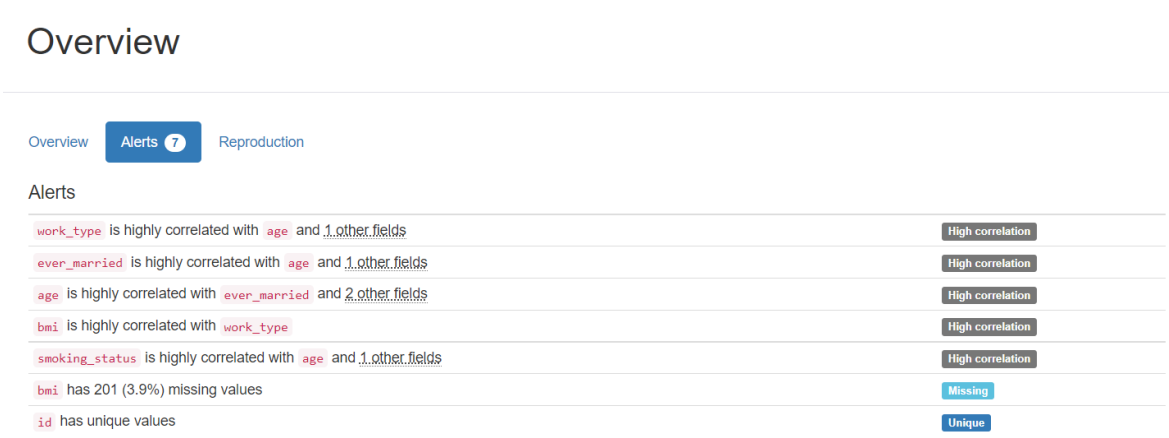
Εικόνα 16: Πληροφορίες συγκεκριμένου χαρακτηριστικού του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος



Εικόνα 17: Προβολή συσχέτισης Pearson χαρακτηριστικών του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος



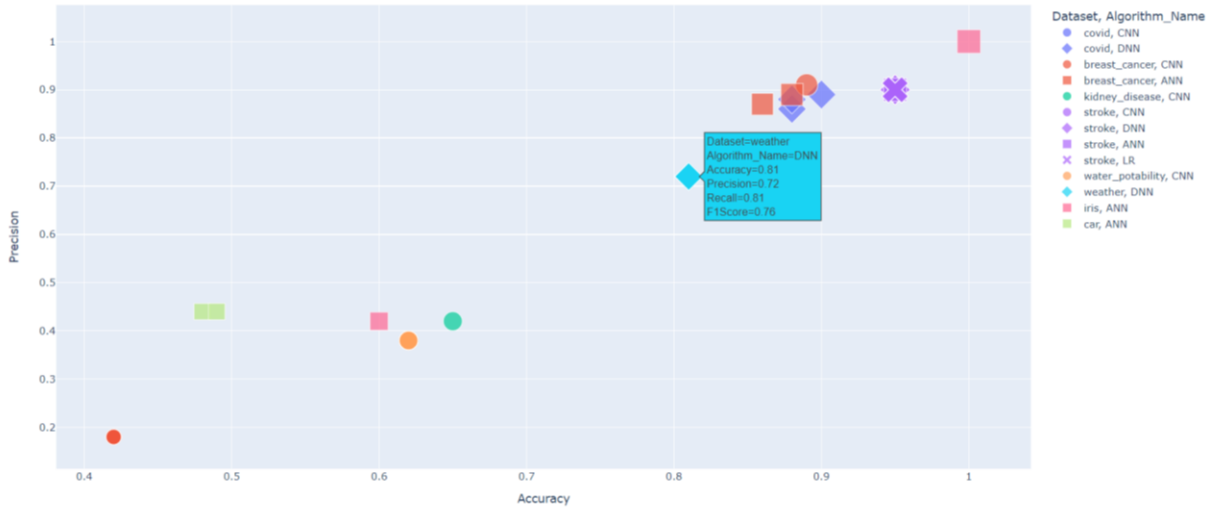
Εικόνα 18: Προβολή ελλιπών τιμών του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος



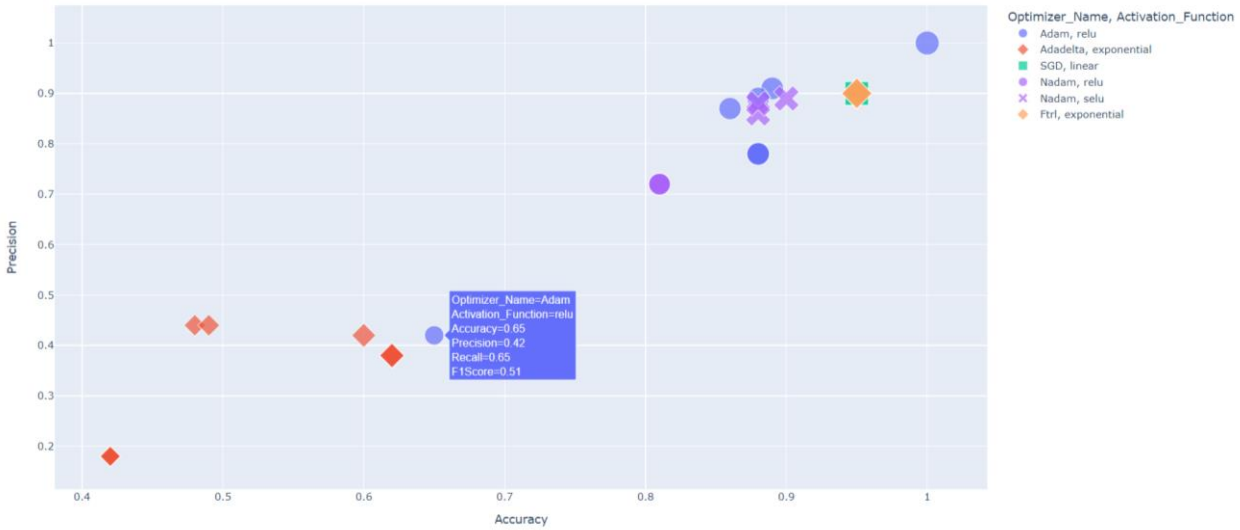
Εικόνα 19: Προβολή σημαντικών ειδοποιήσεων σχετικά με τα χαρακτηριστικά του συνόλου δεδομένων εκπαίδευσης ενδεικτικού παραδείγματος.

Εκτός από το παραπάνω «Report», αν ο χρήστης επιλέξει το κουμπί «Show Diagrams», δύναται να οπτικοποιήσει τα αποτελέσματα όλων των προηγούμενων πειραμάτων που έχει πραγματοποιήσει, έτσι ώστε να μπορέσει να συγκρίνει την αποτελεσματικότητα διαφορετικών παραμέτρων και την επίδραση που αυτές έχουν στην εκπαίδευση των μοντέλων μηχανικής μάθησης. Τα διαγράμματα είναι πέντε (5) και το καθένα από αυτά συγκρίνει/οπτικοποιεί διαφορετικές παραμέτρους των πειραμάτων. Ειδικότερα, αναφορικά με το πρώτο διάγραμμα, όπως φαίνεται στην **Εικόνα *20***, αυτό περιλαμβάνει τις παραμέτρους Accuracy και Precision,

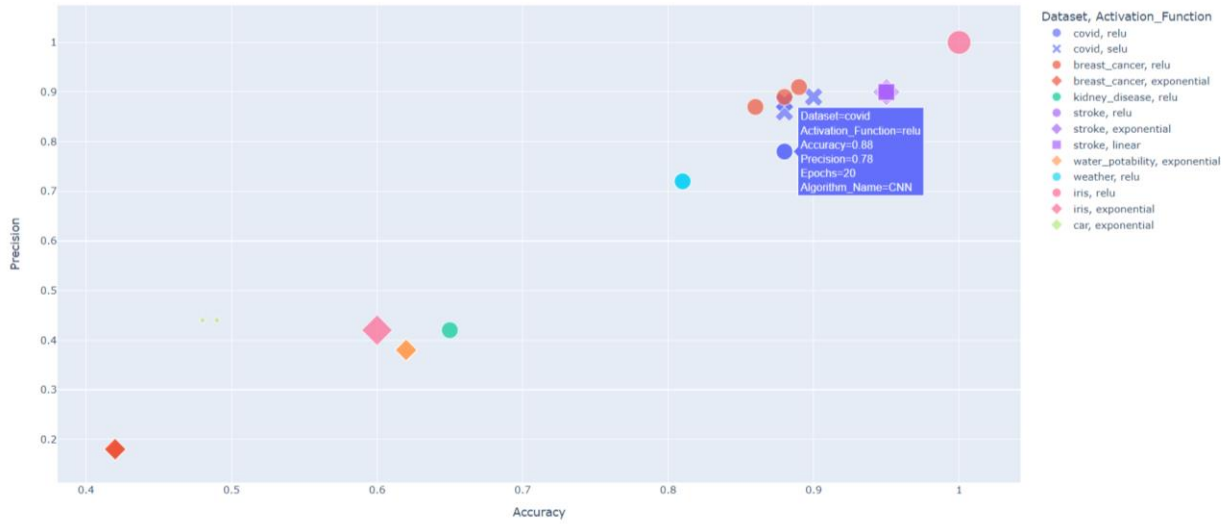
συναρτήσει του Recall, του F1 - Score, του Συνόλου Δεδομένων και του Αλγόριθμου Μηχανικής Μάθησης. Όσον αφορά το δεύτερο διάγραμμα, όπως φαίνεται στην **Εικόνα *21***, αυτό αναφέρεται στις παραμέτρους Accuracy και Precision, συναρτήσει του Recall, του F1 - Score, της Συνάρτησης Βελτιστοποίησης και της Συνάρτησης Ενεργοποίησης. Το τρίτο διάγραμμα, όπως παρουσιάζεται στην **Εικόνα *22***, αναφέρεται στις παραμέτρους Accuracy και Precision, συναρτήσει της Συνάρτησης Ενεργοποίησης, του Συνόλου Δεδομένων, του Αλγόριθμου Μηχανικής Μάθησης και του Πλήθους Περιόδων Εκπαίδευσης, ενώ το τέταρτο αφορά τους μέσους όρους των τιμών των Accuracy, Precision, Recall και F1 – Score ανά Αλγόριθμο Μηχανικής Μάθησης, όπως φαίνεται στην **Εικόνα *23***. Τέλος, το πέμπτο διάγραμμα περιλαμβάνει τις παραμέτρους της Χρησιμοποιούμενης Μνήμης και του Χρόνου Εκτέλεσης, συναρτήσει του Αλγόριθμου Μηχανικής Μάθησης, του Αριθμού Χρηστών και του Συνόλου Δεδομένων, όπως παρουσιάζεται στην **Εικόνα *24***.



Εικόνα 20: Διάγραμμα διασποράς των Accuracy και Precision των πειραμάτων, συναρτήσει του Recall, του F1 - Score, του Συνόλου Δεδομένων και του Αλγόριθμου Μηχανικής Μάθησης.

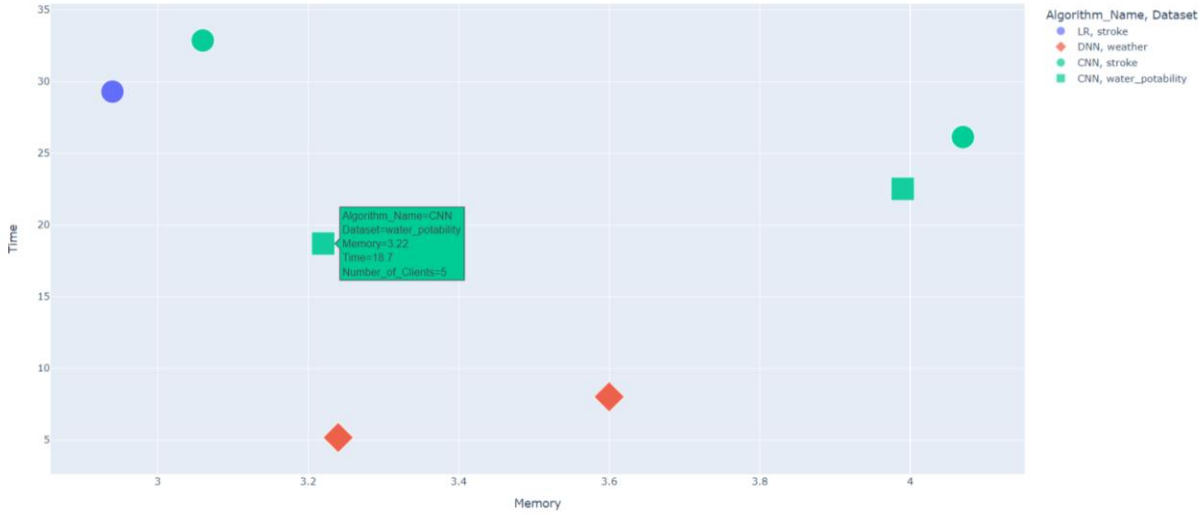


Εικόνα 21: Διάγραμμα διασποράς των Accuracy και Precision των Πειραμάτων, συναρτήσει του Recall, του F1 - Score, της Συνάρτησης Βελτιστοποίησης και της Συνάρτησης Ενεργοποίησης.



Εικόνα 22: Διάγραμμα διασποράς των Accuracy και Precision των Πειραμάτων, συναρτήσει της Συνάρτησης Ενεργοποίησης, του Συνόλου Δεδομένων, του Αλγόριθμου Μηχανικής Μάθησης και του Πλήθους Περιόδων Εκπαίδευσης.

Εικόνα 23: Μέσοι όροι των τιμών των Accuracy, Precision, Recall και F1 – Score ανά Αλγόριθμο Μηχανικής Μάθησης.



Εικόνα 24: Διάγραμμα διασποράς της Χρησιμοποιούμενης Μνήμης και του Χρόνου Εκτέλεσης των Πειραμάτων, συναρτήσει του Αλγόριθμου Μηχανικής Μάθησης, του Αριθμού Χρηστών και του Συνόλου Δεδομένων.

Δεδομένου πως οι χρήστες έχουν ολοκληρώσει κάποιο πείραμα, επιλέγοντας το κουμπί «Retrain Model», έχουν τη δυνατότητα να πραγματοποιήσουν, εκ νέου, κάποιο άλλο πείραμα.

4.2. Αποτελέσματα Ενδεικτικών Πειραμάτων

Στα πλαίσια της παρούσας διπλωματικής εργασίας πραγματοποιήθηκαν πληθώρα πειραμάτων, βάσει διαφορετικών παραμέτρων. Αξίζει να σημειωθεί πως, δεδομένου του πλήθους των διαθέσιμων παραμέτρων και του εύρους τιμών τις οποίες μπορούν να πάρουν, τα πραγματοποιηθέντα πειράματα καλύπτουν ένα ενδεικτικό κομμάτι των δυνατοτήτων τις εφαρμογής και των πειραμάτων τα οποία δύνανται να διεξαχθούν. Μία σύνοψη των πειραμάτων που έχουν πραγματοποιηθεί, παρουσιάζεται στον ακόλουθο πίνακα.

Πίνακας 14: Αποτελέσματα Πραγματοποιηθέντων Πειραμάτων

A/A	Τιμές Παραμέτρων	Αποτελέσματα
1	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Adam Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 2.82 Time: 14.33
2	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: ANN Συνάρτηση Ενεργοποίησης: Linear Συνάρτηση Βελτιστοποίησης: SGD Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 2.8 Time: 4.2
3	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 3 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 4.0 Time: 16.05
4	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 5 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 4.07

	Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Adam Μέγεθος Υποσυνόλων Δεδομένων: 64	Time: 26.13
5	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 5 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Ftrl Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 3.06 Time: 32.87
6	Σύνολο Δεδομένων: **Stroke** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 32	Accuracy: 0.95 Precision: 0.9 Recall: 0.95 F1 – Score: 0.92 Memory: 2.97 Time: 4.51
7	Σύνολο Δεδομένων: **Covid - 19** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Adam Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.88 Precision: 0.78 Recall: 0.88 F1 – Score: 0.83 Memory: 3.28 Time: 12.62
8	Σύνολο Δεδομένων: **Covid - 19** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: DNN Συνάρτηση Ενεργοποίησης: Selu Συνάρτηση Βελτιστοποίησης: Nadam Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.88 Precision: 0.86 Recall: 0.88 F1 – Score: 0.87 Memory: 3.64 Time: 11.77
9	Σύνολο Δεδομένων: **Covid - 19** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 50	Accuracy: 0.8 Precision: 0.77 Recall: 0.8 F1 – Score: 0.78 Memory: 2.67

	Αλγόριθμος Μηχανικής Μάθησης: Logistic Regression Συνάρτηση Ενεργοποίησης: Linear Συνάρτηση Βελτιστοποίησης: SGD Μέγεθος Υποσυνόλων Δεδομένων: 32	Time: 3.37
10	Σύνολο Δεδομένων: **Covid - 19** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 50 Αλγόριθμος Μηχανικής Μάθησης: DNN Συνάρτηση Ενεργοποίησης: Selu Συνάρτηση Βελτιστοποίησης: SGD Μέγεθος Υποσυνόλων Δεδομένων: 32	Accuracy: 0.92 Precision: 0.91 Recall: 0.92 F1 – Score: 0.91 Memory: 2.86 Time: 4.81
11	Σύνολο Δεδομένων: **Breast Cancer** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: ANN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Adam Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.86 Precision: 0.87 Recall: 0.86 F1 – Score: 0.86 Memory: 2.71 Time: 3.54
12	Σύνολο Δεδομένων: **Breast Cancer** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 50 Αλγόριθμος Μηχανικής Μάθησης: DNN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: SGD Μέγεθος Υποσυνόλων Δεδομένων: 128	Accuracy: 0.58 Precision: 0.33 Recall: 0.58 F1 – Score: 0.42 Memory: 2.85 Time: 4.5
13	Σύνολο Δεδομένων: **Breast Cancer** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.42 Precision: 0.18 Recall: 0.42 F1 – Score: 0.25 Memory: 3.59 Time: 10.59
14	Σύνολο Δεδομένων: **Kidney Disease** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5	Accuracy: 0.65 Precision: 0.42 Recall: 0.65

	Πλήθος Περιόδων Εκπαίδευσης: 50 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: RMSprop Μέγεθος Υποσυνόλων Δεδομένων: 64	F1 – Score: 0.51 Memory: 4.55 Time: 19.32
15	Σύνολο Δεδομένων: **Water Potability** Αριθμός Χρηστών: 4 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.62 Precision: 0.38 Recall: 0.62 F1 – Score: 0.47 Memory: 3.52 Time: 14.36
16	Σύνολο Δεδομένων: **Weather Forecast** Αριθμός Χρηστών: 5 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 20 Αλγόριθμος Μηχανικής Μάθησης: DNN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Nadam Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.81 Precision: 0.72 Recall: 0.81 F1 – Score: 0.76 Memory: 3.24 Time: 5.17
17	Σύνολο Δεδομένων: **Weather Forecast** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 100 Αλγόριθμος Μηχανικής Μάθησης: DNN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adagrad Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.82 Precision: 0.73 Recall: 0.82 F1 – Score: 0.76 Memory: 2.73 Time: 5.26
18	Σύνολο Δεδομένων: **Iris** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 40 Αλγόριθμος Μηχανικής Μάθησης: ANN Συνάρτηση Ενεργοποίησης: Exponential Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 5	Accuracy: 0.6 Precision: 0.42 Recall: 0.6 F1 – Score: 0.48 Memory: 2.58 Time: 2.73
19	Σύνολο Δεδομένων: **Iris** Αριθμός Χρηστών: 2 Αριθμός Επαναλήψεων: 5	Accuracy: 1.0 Precision: 1.0 Recall: 1.0

	Πλήθος Περιόδων Εκπαίδευσης: 40 Αλγόριθμος Μηχανικής Μάθησης: ANN Συνάρτηση Ενεργοποίησης: Relu Συνάρτηση Βελτιστοποίησης: Adadelta Μέγεθος Υποσυνόλων Δεδομένων: 5	F1 – Score: 1.0 Memory: 2.93 Time: 0.99
20	Σύνολο Δεδομένων: **Car Evaluation** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 40 Αλγόριθμος Μηχανικής Μάθησης: ANN Συνάρτηση Ενεργοποίησης: Linear Συνάρτηση Βελτιστοποίησης: RMSprop Μέγεθος Υποσυνόλων Δεδομένων: 5	Accuracy: 0.76 Precision: 0.7 Recall: 0.76 F1 – Score: 0.73 Memory: 2.99 Time: 20.58
21	Σύνολο Δεδομένων: **Car Evaluation** Αριθμός Χρηστών: 10 Αριθμός Επαναλήψεων: 5 Πλήθος Περιόδων Εκπαίδευσης: 50 Αλγόριθμος Μηχανικής Μάθησης: CNN Συνάρτηση Ενεργοποίησης: Linear Συνάρτηση Βελτιστοποίησης: SGD Μέγεθος Υποσυνόλων Δεδομένων: 64	Accuracy: 0.7 Precision: 0.56 Recall: 0.7 F1 – Score: 0.6 Memory: 3.7 Time: 8.38

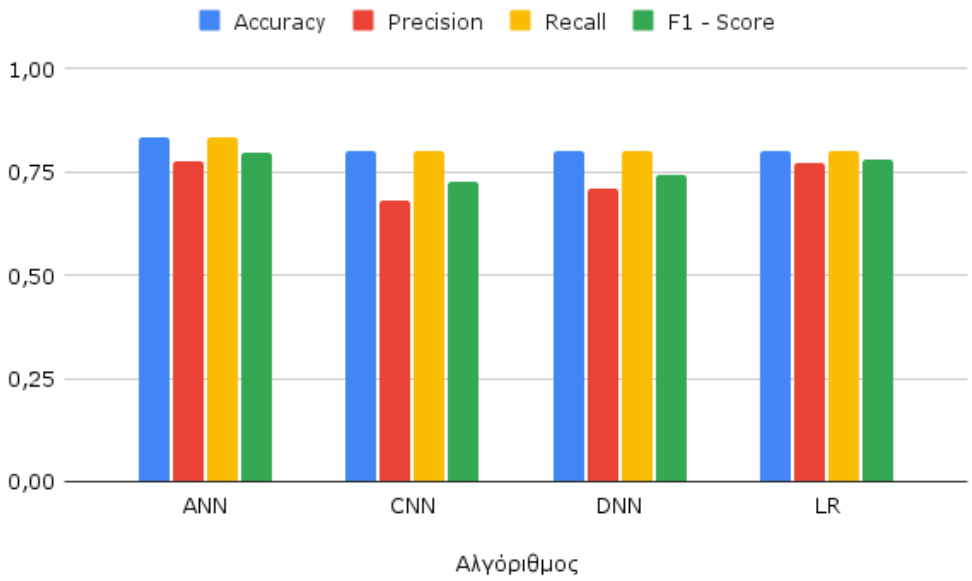
4.3. Σύγκριση Αποτελεσμάτων Ενδεικτικών Πειραμάτων

Στη παρούσα ενότητα πραγματοποιείται μία σύγκριση των αποτελεσμάτων των ενδεικτικών πειραμάτων, τα οποία διενεργήθηκαν στα πλαίσια της παρούσας εργασίας. Η συγκεκριμένη σύγκριση πραγματοποιείται βάσει των αποτελεσμάτων που προσφέρει η εφαρμογή και, ουσιαστικά, αποτελεί τη σύγκριση που θα πραγματοποιούσαν οι αναλυτές δεδομένων, έτσι ώστε να αξιολογήσουν την Ομοσπονδιακή Μάθηση και να επιλέξουν τους κατάλληλους αλγορίθμους και παραμέτρους για τα δικά τους σενάρια χρήσης. Οι συγκρίσεις πραγματοποιούνται συναρτήσει της ακρίβειας των προβλέψεων και τις απαιτήσεις σε υπολογιστικούς πόρους. Τα πειράματα διεξάχθηκαν σε υπολογιστή με τα ακόλουθα χαρακτηριστικά:

- Επεξεργαστής: Processor 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz
- Μνήμη: 16,0 GB (15,8 GB usable) RAM
- Λειτουργικό Σύστημα: Windows 10 Home (64-bit operating system, x64-based processor)

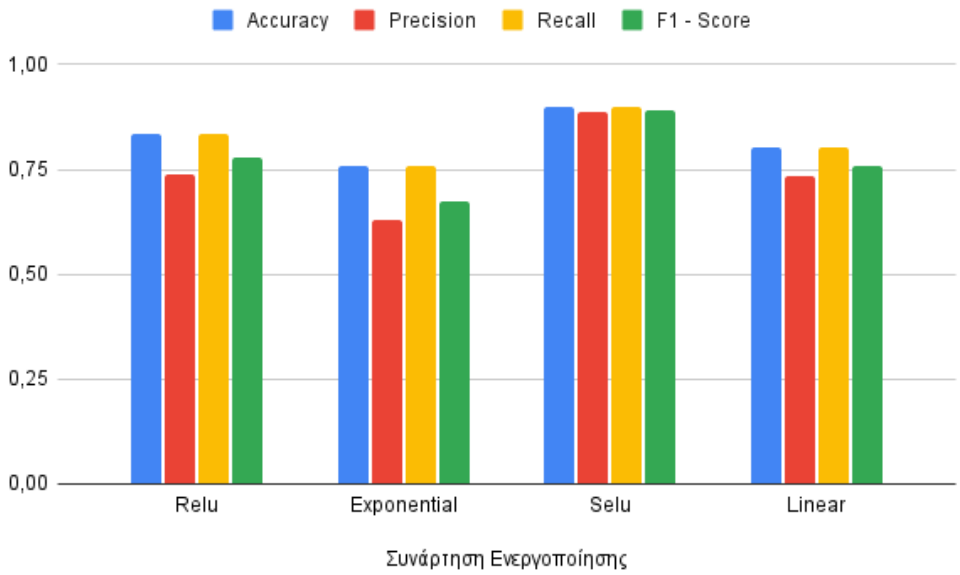
4.3.1. Ακρίβεια Προβλέψεων

Στα ακόλουθα διαγράμματα πραγματοποιείται μία σύγκριση του μέσου όρου των μετρικών «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του αλγόριθμου μηχανική μάθησης που χρησιμοποιήθηκε (**Εικόνα *25***), της συνάρτησης ενεργοποίησης που αξιοποιήθηκε (**Εικόνα *26***), της συνάρτησης βελτιστοποίησης που χρησιμοποιήθηκε (**Εικόνα *27***), του πλήθους χρηστών (**Εικόνα *28***), του πλήθους περιόδων (**Εικόνα *29***) και του μεγέθους υποσυνόλου δεδομένων εκπαίδευσης (**Εικόνα *30***).



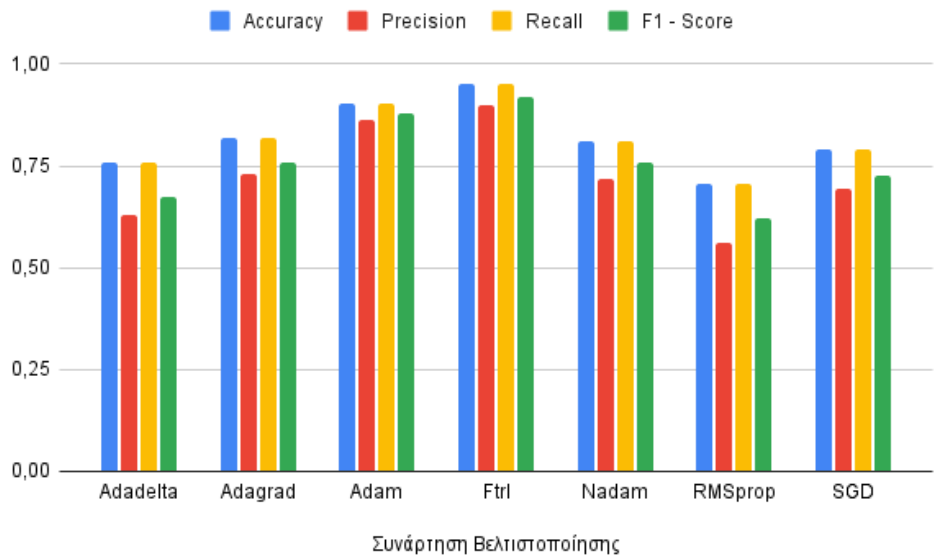
Εικόνα 25: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του αλγόριθμου μηχανική μάθησης.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως ο αλγόριθμος «Artificial Neural Networks» πετυχαίνει τις πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά ο αλγόριθμος «Logistic Regression». Βέβαια, αντίστοιχες μετρήσεις που πετυχαίνουν οι αλγόριθμοι «Convolutional Neural Networks» και «Deep Neural Networks» είναι επίσης ικανοποιητικές, καθώς διαφέρουν ελάχιστα με τους υπόλοιπους αλγορίθμους.



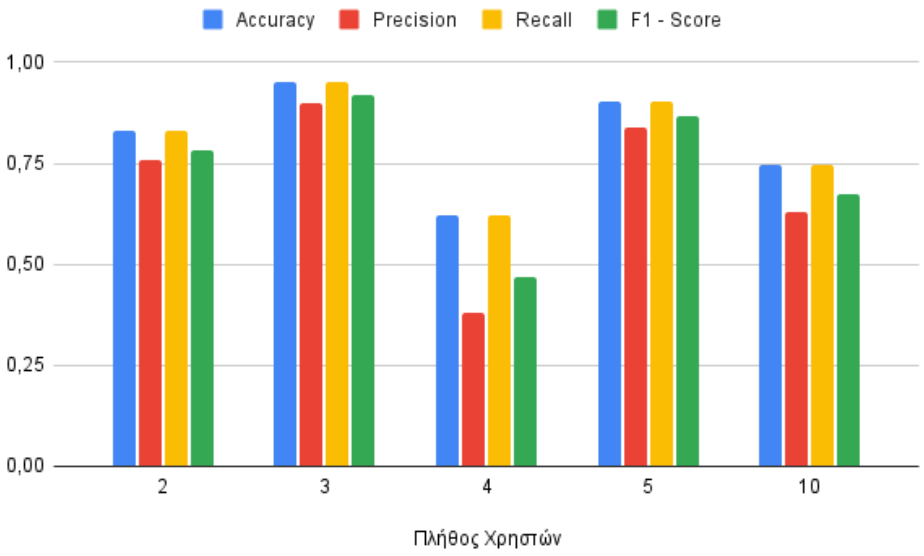
Εικόνα 26: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει της συνάρτησης ενεργοποίησης.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως η συνάρτηση ενεργοποίησης «Selu» πετυχαίνει τις πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά η συνάρτηση ενεργοποίησης «Linear». Η συνάρτηση ενεργοποίησης «Exponential» φαίνεται να πετυχαίνει τις λιγότερο ικανοποιητικές μετρήσεις. Τα παραπάνω αποτελέσματα σχετίζονται τόσο με τους αλγόριθμους μηχανικής μάθησης οι οποίοι αξιοποιούν τις παραπάνω συναρτήσεις, όπως επίσης και με τα σύνολα δεδομένων εκπαίδευσης που αξιοποιούνται (π.χ. μία συνάρτηση ενεργοποίησης μπορεί να είναι πολύ αποδοτική σε δεδομένα που ακολουθούν εκθετική κατανομή αλλά μία άλλη μπορεί να είναι πιο αποδοτική σε δεδομένα που έχουν γραμμική σχέση μεταξύ τους).



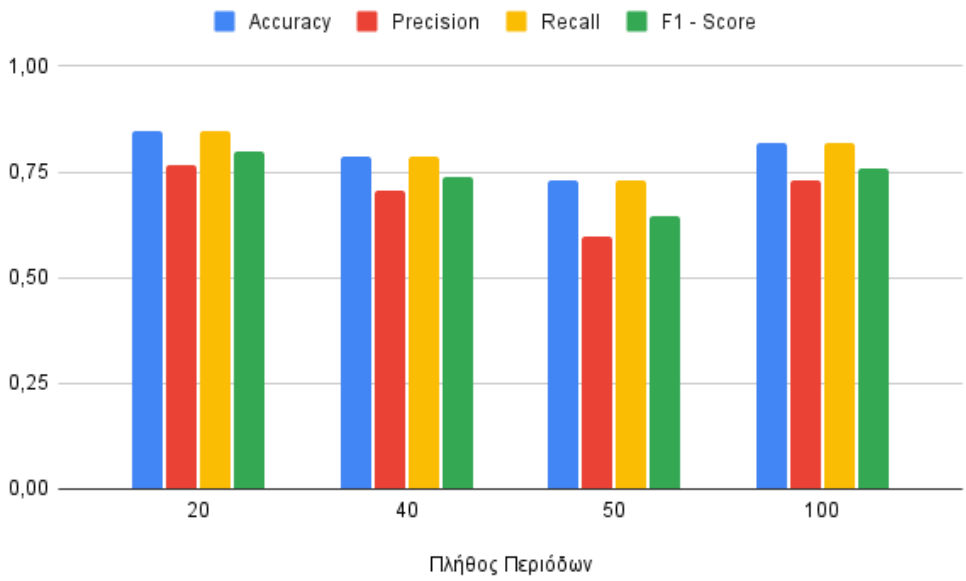
Εικόνα 27: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει της συνάρτησης βελτιστοποίησης.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως η συνάρτηση βελτιστοποίησης «Ftrl» πετυχαίνει τις πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά η συνάρτηση βελτιστοποίησης «Adam». Η συνάρτηση βελτιστοποίησης «RMSprop» φαίνεται να πετυχαίνει τις λιγότερο ικανοποιητικές μετρήσεις, ενώ οι συναρτήσεις βελτιστοποίησης «Adadelta», «Adagrad», «Nadam» και «SGD» πετυχαίνουν πανομοιότυπες μετρήσεις. Τα παραπάνω αποτελέσματα σχετίζονται τόσο με τους αλγόριθμους μηχανικής μάθησης οι οποίοι αξιοποιούν τις παραπάνω συναρτήσεις, όπως επίσης και με τα σύνολα δεδομένων εκπαίδευσης που αξιοποιούνται (π.χ. μία συνάρτηση βελτιστοποίησης μπορεί να είναι πολύ αποδοτική σε δεδομένα που ακολουθούν εκθετική κατανομή αλλά μία άλλη μπορεί να είναι πιο αποδοτική σε δεδομένα που έχουν γραμμική σχέση μεταξύ τους).



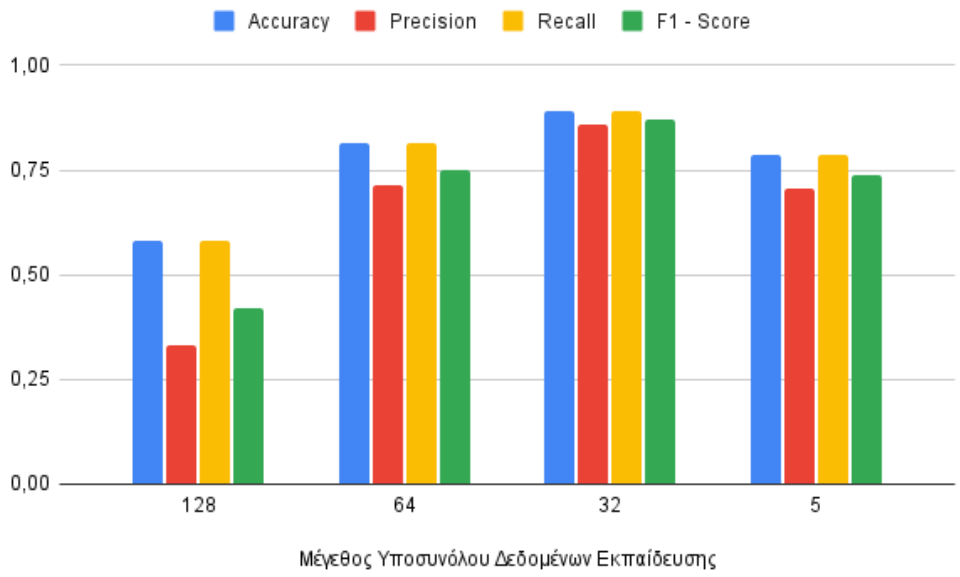
Εικόνα 28: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του πλήθους χρηστών.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως για πλήθος χρηστών ίσο με τρία (3) επιτυγχάνονται οι πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά το πλήθος χρηστών ίσο με το πέντε (5). Το πλήθος χρηστών ίσο με τέσσερα (4) φαίνεται να πετυχαίνει τις λιγότερο ικανοποιητικές μετρήσεις. Τα παραπάνω αποτελέσματα σχετίζονται αρκετά με τον τρόπο που πραγματοποιείται η εκπαίδευση στα πειράματα. Ειδικότερα, σε κάθε πείραμα υπάρχει ένα σύνολο δεδομένων το οποίο μπορεί να περιέχει εκατοντάδες, μέχρι και μερικές χιλιάδες εγγραφές και το οποίο, εν συνεχεία, διαμοιράζεται τυχαία σε χρήστες, ανάλογα με το πλήθος χρηστών που έχει οριστεί. Το παραπάνω σημαίνει ότι ενδέχεται να υπάρχουν φορές που ο διαμοιρασμός του συνόλου δεδομένων μπορεί να οδηγήσει στη δημιουργία υποσυνόλων δεδομένων τα οποία δεν είναι αντιπροσωπευτικά του αρχικού και, συνεπώς, επηρεάζεται η ακρίβεια των αλγορίθμων. Σε ένα πραγματικό σενάριο χρήσης, όπου υπάρχει πληθώρα αντιπροσωπευτικών δεδομένων για κάθε χρήστη, η ακρίβεια των προβλέψεων όχι μόνο δεν μειώνεται με την αύξηση του πλήθους των χρηστών αλλά, αντιθέτως, αυξάνεται.



Εικόνα 29: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του πλήθους περιόδων.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως για πλήθος περιόδων ίσο με εκατό (100) επιτυγχάνονται οι πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά το πλήθος περιόδων ίσο με το είκοσι (20). Το πλήθος περιόδων ίσο με πενήντα (50) φαίνεται να πετυχαίνει τις λιγότερο ικανοποιητικές μετρήσεις. Συνήθως, όσο αυξάνεται το πλήθος των περιόδων εκπαίδευσης, τόσο αυξάνεται και η ακρίβεια των αλγορίθμων μηχανικής μάθησης. Ωστόσο, στα συγκεκριμένα πειράματα, εναλλάσσονται αρκετές παράμετροι, όπως είναι για παράδειγμα το σύνολο δεδομένων και ο αλγόριθμος μηχανικής μάθησης. Γι' αυτό το λόγο δεν παρατηρείται καθαρά αυξητική τάση στην ακρίβεια των αλγορίθμων, όσο αυξάνεται το πλήθος των περιόδων.

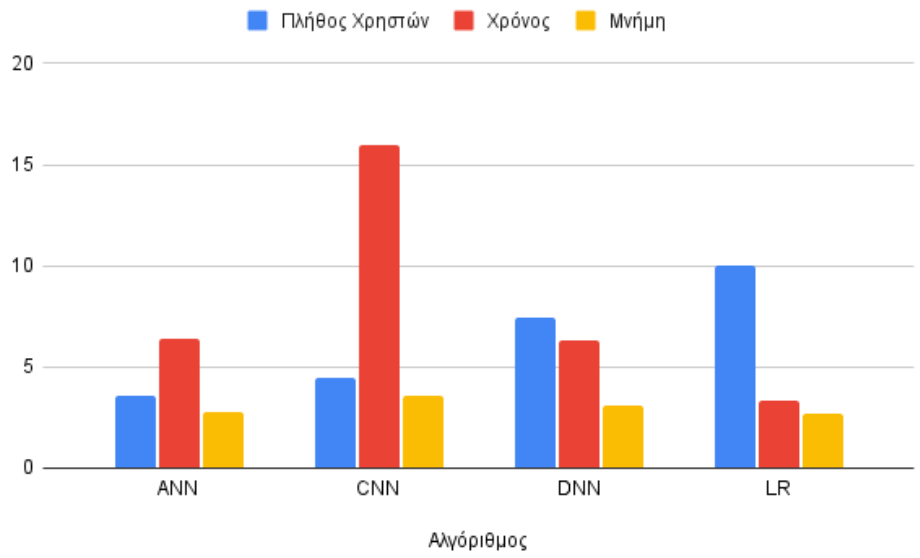


Εικόνα 30: Σύγκριση μέσου όρου «Accuracy», «Precision», «Recall» και «F1 - Score», συναρτήσει του μεγέθους υποσυνόλου δεδομένων εκπαίδευσης.

Με βάση το παραπάνω διάγραμμα, φαίνεται πως για μέγεθος υποσυνόλου δεδομένων εκπαίδευσης ίσο με τριάντα δύο (32) επιτυγχάνονται οι πιο υψηλές μετρήσεις αναφορικά με τα «Accuracy», «Precision», «Recall» και «F1 - Score», ενώ ακολουθεί, με μικρή διαφορά το μέγεθος υποσυνόλου δεδομένων εκπαίδευσης ίσο με το εξήντα τέσσερα (64). Το μέγεθος υποσυνόλου δεδομένων εκπαίδευσης ίσο με εκατό είκοσι οκτώ (128) φαίνεται να πετυχαίνει τις λιγότερο ικανοποιητικές μετρήσεις. Αν το μέγεθος του υποσυνόλου δεδομένων εκπαίδευσης είναι υπερβολικά μικρό ή υπερβολικά μεγάλο, τότε επηρεάζεται αρνητικά η ακρίβεια των αλγορίθμων.

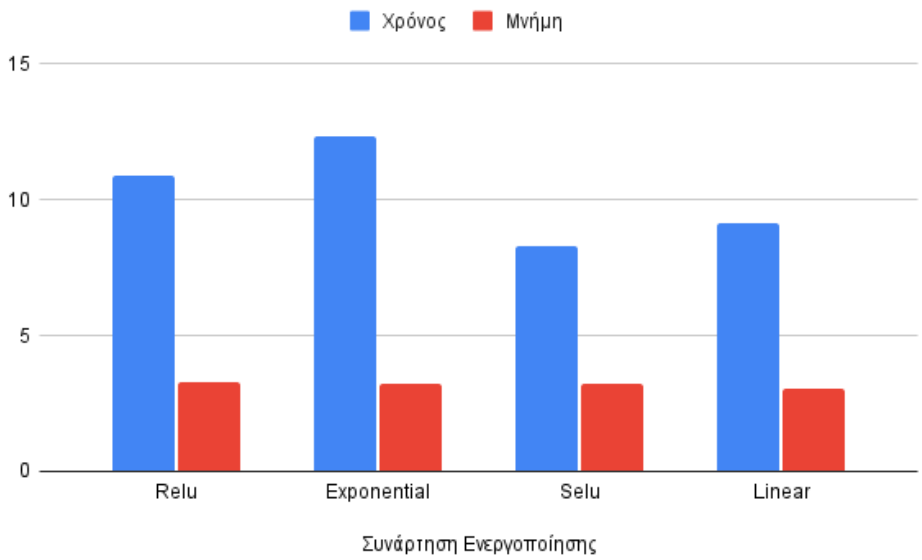
4.3.2. Απαιτήσεις σε Πόρους

Στα ακόλουθα διαγράμματα πραγματοποιείται μία σύγκριση του πλήθους χρηστών, του χρόνου εκτέλεσης και της μνήμης, συναρτήσει του αλγόριθμου μηχανική μάθησης που χρησιμοποιήθηκε (**Εικόνα *31***). Επιπρόσθετα, πραγματοποιείται μία σύγκριση του χρόνου εκτέλεσης και της μνήμης, συναρτήσει της συνάρτησης ενεργοποίησης που αξιοποιήθηκε (**Εικόνα *32***) και της συνάρτησης βελτιστοποίησης που χρησιμοποιήθηκε (**Εικόνα *33***).



Εικόνα 31: Σύγκριση πλήθους χρηστών, χρόνου εκτέλεσης και μνήμης, συναρτήσει του αλγόριθμου μηχανική μάθησης.

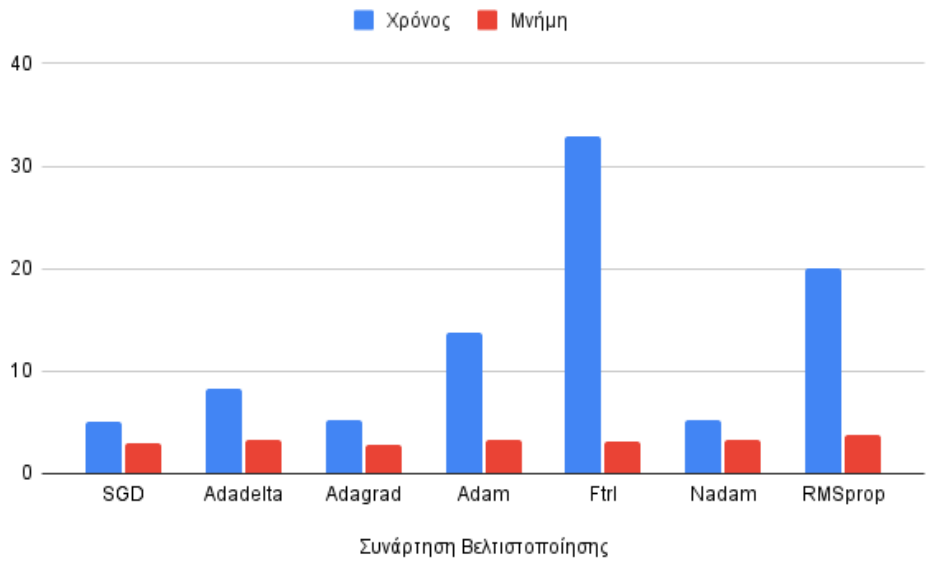
Με βάση το παραπάνω διάγραμμα, φαίνεται πως ο αλγόριθμος «Convolutional Neural Networks» έχει αυξημένο χρόνο εκτέλεσης και υψηλές απαιτήσεις σε υπολογιστικούς πόρους. Αντίθετα, ο αλγόριθμος «Logistic Regression» έχει μειωμένο χρόνο εκτέλεσης και μειωμένες απαιτήσεις σε υπολογιστικούς πόρους, κάτι που είναι λογικό καθώς είναι ο πιο απλός αλγόριθμος σε σχέση με τους υπόλοιπους. Οι αλγόριθμοι «Artificial Neural Networks» και «Deep Neural Networks» έχουν παρόμοιες μετρήσεις, με τον αλγόριθμο «Deep Neural Networks» να έχει αυξημένες απαιτήσεις σε χρόνο και μνήμη, λόγω της αυξημένης πολυπλοκότητάς του.



Εικόνα 32: Σύγκριση χρόνου εκτέλεσης και μνήμης, συναρτήσει της συνάρτησης ενεργοποίησης.

Σύμφωνα με το παραπάνω διάγραμμα, φαίνεται πως η συνάρτηση ενεργοποίησης «Exponential» έχει αυξημένο χρόνο εκτέλεσης, ενώ ακολουθεί η συνάρτηση ενεργοποίησης «Relu» με το δεύτερο χειρότερο χρόνο εκτέλεσης. Τον ελάχιστο χρόνο εκτέλεσης φαίνεται να έχει η συνάρτηση ενεργοποίησης «Selu». Αναφορικά με τη μνήμη που αξιοποιείται, όλες οι συναρτήσεις ενεργοποίησης φαίνεται να χρησιμοποιούν σχεδόν παρόμοιο ποσοστό μνήμης. Ωστόσο, η συνάρτηση ενεργοποίησης που φαίνεται να αξιοποιεί τη λιγότερη μνήμη είναι η «Linear», κάτι το οποίο μπορεί να αιτιολογηθεί λόγω της μειωμένης πολυπλοκότητάς της[4].

[4] Η συνάρτηση ενεργοποίησης «Linear», επίσης γνωστή ως συνάρτηση γραμμικής ενεργοποίησης, δεν αλλάζει το σταθμισμένο άθροισμα της εισόδου με κανέναν τρόπο και επιστρέφει απευθείας την τιμή.



Εικόνα 33: Σύγκριση χρόνου εκτέλεσης και μνήμης, συναρτήσει της συνάρτησης βελτιστοποίησης.

Σύμφωνα με το παραπάνω διάγραμμα, φαίνεται πως η συνάρτηση βελτιστοποίησης «Ftrl» έχει αυξημένο χρόνο εκτέλεσης, ενώ ακολουθεί η συνάρτηση βελτιστοποίησης «RMSprop» με το δεύτερο χειρότερο χρόνο εκτέλεσης. Επίσης αυξημένο χρόνο εκτέλεσης έχει και η συνάρτηση βελτιστοποίησης «Adam». Αντιθέτως, τον ελάχιστο χρόνο εκτέλεσης φαίνεται να έχει η συνάρτηση βελτιστοποίησης «SGD», ενώ οι συναρτήσεις βελτιστοποίησης «Adagrad» και «Nadam» έχουν εξίσου ικανοποιητικά αποτελέσματα αναφορικά με το χρόνο εκτέλεσης. Οι συναρτήσεις ενεργοποίησης «Adadelta» και «Adam» έχουν μέτριους χρόνους εκτέλεσης. Αναφορικά με τη μνήμη που αξιοποιείται, δεν παρατηρείται κάποια ιδιαίτερη διαφορά, καθώς όλες οι συναρτήσεις βελτιστοποίησης φαίνεται να αξιοποιούν παρόμοιο ποσοστό μνήμης.

5. Συμπεράσματα

Συνοψίζοντας, η παραγωγή δεδομένων είναι τεράστια και, συνεπώς, απαιτούνται νέοι τρόποι αποδοτικής διαχείρισης και ανάλυσης αυτών για την εξαγωγή χρήσιμης πληροφορίας και γνώσης, κάτι το οποίο αποτελεί ιδιαίτερη πρόκληση. Η ραγδαία αύξηση των δυνατοτήτων των υπολογιστικών πόρων, σε συνδυασμό με τις πρόσφατες εξελίξεις στο τομέα της Τεχνητής Νοημοσύνης, έχουν οδηγήσει στην ανάπτυξη νέων τεχνικών για την εκπαίδευση μοντέλων μηχανικής μάθησης βάσει των διαθέσιμων δεδομένων. Οι προαναφερθείσες τεχνικές πρέπει, εκτός από την αποδοτική διαχείριση και ανάλυση του όγκου των δεδομένων, να διασφαλίζουν και άλλες πτυχές των δεδομένων, όπως είναι η ιδιωτικότητα τους. Τα παραπάνω θα πρέπει να πραγματοποιούνται, χωρίς να διακυβεύεται η ποιότητα της ανάλυσης που πραγματοποιείται στα δεδομένα και η ακρίβεια των παραγόμενων προβλέψεων ενός αλγορίθμου μηχανικής μάθησης. Προς αυτή τη κατεύθυνση, πρόσφατα προτάθηκε η Ομοσπονδιακή Μάθηση, η οποία αποτελεί ένα νέο τρόπο εκπαίδευσης μοντέλων μηχανικής μάθησης. Στην ΟΜ, η εκπαίδευση δεν πραγματοποιείται βάσει ενός κεντρικού μοντέλου, όπως πραγματοποιείται στη παραδοσιακή μηχανική μάθηση, αλλά βάσει επιμέρους μοντέλων, τα οποία εκπαιδεύονται πάνω σε δεδομένα επιμέρους χρηστών. Η εκπαίδευση κάθε ξεχωριστού μοντέλου πραγματοποιείται τοπικά σε κάθε χρήστη, ενώ στη συνέχεια οι παράμετροι των μοντέλων αποστέλλονται σε ένα διακομιστή, ο οποίος δημιουργεί ένα ενιαίο μοντέλο σύμφωνα με αυτές και στη συνέχεια το αποστέλλει πίσω στους χρήστες για επανεκπαίδευση. Με αυτό το τρόπο, όχι μόνο αυξάνεται η ακρίβεια των αλγορίθμων μηχανικής μάθησης, αλλά αυξάνεται και η ποσότητα των δεδομένων που χρησιμοποιούνται για εκπαίδευση, ενώ συγχρόνως διασφαλίζεται και η ασφάλεια και η ιδιωτικότητα των δεδομένων των χρηστών.

Φυσικά, η επιλογή χρήσης του ομοσπονδιακού τρόπου για εκπαίδευση μοντέλων δεν είναι απλή. Η ΟΜ είναι πολύ αποδοτική σε συγκεκριμένα σενάρια χρήσης στα οποία τα δεδομένα είναι κατανεμημένα. Σε διαφορετικές περιπτώσεις, όπου και η ασφάλεια των δεδομένων ενδεχομένως δεν είναι προτεραιότητα (π.χ. ανωνυμοποιημένα δεδομένα), μπορούν να επιλεχθούν συμβατικές μέθοδοι και τεχνικές εκπαίδευσης. Σε αυτό το πλαίσιο, η παρούσα διπλωματική εργασία, αφού πρώτα αναλύει τα χαρακτηριστικά της ΟΜ και τους αλγορίθμους που έχουν αναπτυχθεί και μπορούν να αξιοποιηθούν και σε αυτή, προτείνει ένα ολοκληρωμένο περιβάλλον πραγματοποίησης πειραμάτων ομοσπονδιακής μάθησης. Το περιβάλλον αυτό παρέχει μία πληθώρα συνόλων δεδομένων και αλγορίθμων που μπορούν να επιλέξουν οι χρήστες, έτσι ώστε να πραγματοποιήσουν τα δικά τους πειράματα. Επιπρόσθετα, οι χρήστες μπορούν να αλλάξουν όλες τις παραμέτρους των πειραμάτων και των αλγορίθμων και να συγκρίνουν τα αποτελέσματα, καταλήγοντας σε αυτές που συμβάλλουν στη μεγιστοποίηση της ακρίβειας κάποιου αλγόριθμου μηχανικής μάθησης για κάποιο συγκεκριμένο σενάριο χρήσης. Επίσης, οι χρήστες μπορούν να συγκρίνουν τον ομοσπονδιακό τρόπο μάθησης με τον συμβατικό, καθώς μπορούν να καθορίσουν το πλήθος των χρηστών που ανήκουν σε μία ομοσπονδία. Στόχος των πειραμάτων είναι να καθοδηγήσουν τους χρήστες στην επιλογή κατάλληλου τρόπου μηχανικής μάθησης, κατάλληλου αλγορίθμου και κατάλληλων παραμέτρων

αυτού για τα εκάστοτε δικά τους σενάρια χρήσης που ενδεχομένως έχουν να υλοποιήσουν. Στη παρούσα διπλωματική εργασία παρατίθενται και τα αποτελέσματα από ενδεικτικά πειράματα που έχουν πραγματοποιηθεί, προσομοιώνοντας τα βήματα ενός πραγματικού χρήστη και παρέχοντας μία σύγκριση των αλγορίθμων που έχουν υλοποιηθεί στα πλαίσια της εργασίας.

Πιο ειδικά, όπως προαναφέρθηκε και στην Ενότητα 4.3, ο αλγόριθμος που είχε και την υψηλότερη ακρίβεια στις προβλέψεις του, δηλαδή υψηλότερες τιμές στις μετρικές «Accuracy», «Precision», «Recall» και «F1 - Score», ήταν ο «Artificial Neural Networks». Η συνάρτηση ενεργοποίησης που αξιοποιήθηκε για την επίτευξη των αντίστοιχων υψηλότερων μετρήσεων ήταν η «Selu», ενώ η αντίστοιχη συνάρτηση βελτιστοποίησης ήταν η «Ftrl». Όσον αφορά στο βέλτιστο πλήθος χρηστών, σύμφωνα με τις παραπάνω μετρήσεις, αυτό ήταν ίσο με τρία (3), ενώ το βέλτιστο πλήθος περιόδων ήταν ίσο με εκατό (100) και το βέλτιστο μέγεθος υποσυνόλου δεδομένων εκπαίδευσης βρέθηκε να ήταν ίσο με τριάντα δύο (32). Όσον αφορά τις ελάχιστες απαιτήσεις σε πόρους, και πιο συγκεκριμένα την απαιτούμενη μνήμη και τον αντίστοιχο χρόνο εκτέλεσης, αυτές αφορούσαν τον αλγόριθμο «Logistic Regression», κάτι που είναι λογικό καθώς είναι ο πιο απλός αλγόριθμος σε σχέση με τους υπόλοιπους. Επίσης, τον ελάχιστο χρόνο εκτέλεσης φαίνεται να έχουν η συνάρτηση ενεργοποίησης «Selu» και η συνάρτηση βελτιστοποίησης «SGD». Αναφορικά με το ποσοστό μνήμης που αξιοποιείται, όλες οι συναρτήσεις ενεργοποίησης και βελτιστοποίησης φαίνεται να χρησιμοποιούν σχεδόν το ίδιο, με αμελητέες αποκλίσεις.

Όσον αφορά τις μελλοντικές βελτιώσεις της παρούσας διπλωματικής εργασίας, αυτές περιγράφονται παρακάτω. Αρχικά, μία μελλοντική βελτίωση είναι η υλοποίηση και προσθήκη περισσότερων αλγόριθμων μηχανικής μάθησης, πέραν των τεσσάρων που έχουν ήδη υλοποιηθεί. Επίσης, θα είχε ενδιαφέρον η προσθήκη αλγορίθμων που σχετίζονται με τη συσταδοποίηση, καθώς τα σύνολα δεδομένων και οι αλγόριθμοι που αξιοποιήθηκαν στα πλαίσια της εργασίας, εστίαζαν περισσότερο σε προβλήματα κατηγοριοποίησης. Επιπρόσθετα, μία αρκετά μεγάλη εξέλιξη θα ήταν η παροχή της δυνατότητας στους χρήστες της εφαρμογής που αναπτύχθηκε να εισάγουν τα δικά τους σύνολα δεδομένων σε αυτή. Ωστόσο, τα δεδομένα αυτά θα πρέπει να «καθαρίζονται» προτού εκκινήσουν τα διάφορα πειράματα, καθώς μη αξιόπιστα/καθαρισμένα δεδομένα θα επηρεάσουν την αποτελεσματικότητα των αλγορίθμων. Συνεπώς, θα απαιτούνταν η ανάπτυξη και η ενσωμάτωση ενός αυτοματοποιημένου μηχανισμού καθαρισμού δεδομένων. Ο μηχανισμός αυτός θα πραγματοποιούσε καθαρισμό στα δεδομένα είτε βάσει κανόνων που έχουν αναπτύξει οι ίδιοι οι χρήστες και τους οποίους εισάγουν στην εφαρμογή μαζί με τα δεδομένα τους, είτε αυτόματα με χρήση κάποιας υπολογιστικής ευφυΐας, όπως είναι η Επεξεργασία Φυσικής Γλώσσας. Επιπρόσθετα, μία άλλη μελλοντική βελτίωση της εφαρμογής, θα ήταν και προσθήκη της δυνατότητας της ανωνυμοποίησης στα δεδομένα και η αντίστοιχη σύγκριση των διάφορων διαθέσιμων τεχνικών, κάτι το οποίο δεν πραγματοποιείται στα πλαίσια της συγκεκριμένης διπλωματικής εργασίας, καθώς τα δεδομένα που αξιοποιούνται για τα πειράματα είναι ήδη ανωνυμοποιημένα στη πηγή από την οποία προέρχονται. Τέλος, σε περίπτωση που δεν υπάρχουν περιορισμοί στους υπολογιστικούς πόρους, θα είχε ιδιαίτερο ενδιαφέρον η χρήση Μεγάλων Δεδομένων (Big Data) και η χρήση εκατοντάδων/χιλιάδων

χρηστών στα αντίστοιχα πειράματα, για να προσομοιωθούν, όσο το δυνατόν καλύτερα, πραγματικά σενάρια χρήσης μεγάλης κλίμακας.

Αναφορές

[1] New York Times – Facebook Data Breach, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html, last accessed: August 2022.

[2] Ευρωπαϊκή Επιτροπή - Προστασία δεδομένων στην ΕΕ, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el, last accessed: August 2022.

[3] Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. IEEE Communications Surveys & Tutorials, 23(2), 1342-1397.

[4] Niknam, S., Dhillon, H. S., & Reed, J. H. (2020). Federated learning for wireless communications: Motivation, opportunities, and challenges. IEEE Communications Magazine, 58(6), 46-51.

[5] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2016). Practical secure aggregation for federated learning on user-held data. arXiv preprint arXiv:1611.04482.

[6] Husnoo, M. A., Anwar, A., Chakrabortty, R. K., Doss, R., & Ryan, M. J. (2021). Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. IEEE Access.

[7] Liu, Y., & Zhao, Q. (2019). E-voting scheme using secret sharing and K-anonymity. World Wide Web, 22(4), 1657-1667.

[8] Li, Z., Huang, Z., Chen, C., & Hong, C. (2019). Quantification of the leakage in federated learning. arXiv preprint arXiv:1910.05467.

[9] Melis, L., Song, C., De Cristofaro, E., & Shmatikov, V. (2019, May). Exploiting unintended feature leakage in collaborative learning. In 2019 IEEE symposium on security and privacy (SP) (pp. 691-706). IEEE.

[10] Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. arXiv preprint arXiv:1712.07557.

[11] Triastcyn, A., & Faltings, B. (2020). Federated generative privacy. IEEE Intelligent Systems, 35(4), 50-57.

[12] Munjal, K., & Bhatia, R. (2022). A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems, 1-28.

[13] Gao, D., Ju, C., Wei, X., Liu, Y., Chen, T., & Yang, Q. (2019). Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography. arXiv preprint arXiv:1909.05784.

[14] Chen, T., Jin, X., Sun, Y., & Yin, W. (2020). Vafl: a method of vertical asynchronous federated learning. arXiv preprint arXiv:2007.06081.

[15] Liu, Y., Kang, Y., Xing, C., Chen, T., & Yang, Q. (2020). A secure federated transfer learning framework. IEEE Intelligent Systems, 35(4), 70-82.

[16] Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y., & Ranjan, R. (2018). Fog computing: Survey of trends, architectures, requirements, and research directions. IEEE access, 6, 47980-48009.

[17] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Roselander, J. (2019). Towards federated learning at scale: System design. Proceedings of Machine Learning and Systems, 1, 374-388.

[18] Chen, M., Mathews, R., Ouyang, T., & Beaufays, F. (2019). Federated learning of out-of-vocabulary words. arXiv preprint arXiv:1903.10635.

[19] Leroy, D., Coucke, A., Lavril, T., Gisselbrecht, T., & Dureau, J. (2019, May). Federated learning for keyword spotting. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6341-6345). IEEE.

[20] Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., ... & Ramage, D. (2018). Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604.

[21] Yang, T., Andrew, G., Eichner, H., Sun, H., Li, W., Kong, N., ... & Beaufays, F. (2018). Applied federated learning: Improving google keyboard query suggestions. arXiv preprint arXiv:1812.02903.

[22] Ramaswamy, S., Mathews, R., Rao, K., & Beaufays, F. (2019). Federated learning for emoji prediction in a mobile keyboard. arXiv preprint arXiv:1906.04329.

[23] Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X., & Chen, M. (2019). In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. IEEE Network, 33(5), 156-165.

[24] Qian, Y., Hu, L., Chen, J., Guan, X., Hassan, M. M., & Alelaiwi, A. (2019). Privacy-aware service placement for mobile edge computing via federated learning. Information Sciences, 505, 562-570.

[25] Feng, J., Rong, C., Sun, F., Guo, D., & Li, Y. (2020). PMF: A privacy-preserving human mobility prediction framework via federated learning. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4(1), 1-21.

[26] Sozinov, K., Vlassov, V., & Girdzijauskas, S. (2018, December). Human activity recognition using federated learning. In 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom) (pp. 1103-1111). IEEE.

[27] Aïvodji, U. M., Gambs, S., & Martin, A. (2019, May). IOTFLA: A secured and privacy-preserving smart home architecture implementing federated learning. In 2019 IEEE Security and Privacy Workshops (SPW) (pp. 175-180). IEEE.

[28] Yu, T., Li, T., Sun, Y., Nanda, S., Smith, V., Sekar, V., & Seshan, S. (2020, April). Learning context-aware policies from multiple smart homes via federated multi-task learning. In 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 104-115). IEEE.

[29] Liu, W., Chen, L., Chen, Y., & Zhang, W. (2020). Accelerating federated learning via momentum gradient descent. IEEE Transactions on Parallel and Distributed Systems, 31(8), 1754-1766.

[30] Hu, B., Gao, Y., Liu, L., & Ma, H. (2018, December). Federated region-learning: An edge computing-based framework for urban environment sensing. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

[31] Han, X., Yu, H., & Gu, H. (2019, August). Visual inspection with federated learning. In International Conference on Image Analysis and Recognition (pp. 52-64). Springer, Cham.

[32] Liu, W., Chen, L., Chen, Y., & Zhang, W. (2020). Accelerating federated learning via momentum gradient descent. IEEE Transactions on Parallel and Distributed Systems, 31(8), 1754-1766.

[33] Mowla, N. I., Tran, N. H., Doh, I., & Chae, K. (2019). Federated learning-based cognitive detection of jamming attack in flying ad-hoc network. IEEE Access, 8, 4338-4350.

[34] Saputra, Y. M., Hoang, D. T., Nguyen, D. N., Dutkiewicz, E., Mueck, M. D., & Srikanteswara, S. (2019, December). Energy demand prediction with federated learning for electric vehicle networks. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[35] Wang, Y., Tong, Y., & Shi, D. (2020, April). Federated latent dirichlet allocation: A local differential privacy-based framework. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 34, No. 04, pp. 6283-6290).

[36] Brisimi, T. S., Chen, R., Mela, T., Olshevsky, A., Paschalidis, I. C., & Shi, W. (2018). Federated learning of predictive models from federated electronic health records. International journal of medical informatics, 112, 59-67.

[37] Silva, S., Gutman, B. A., Romero, E., Thompson, P. M., Altmann, A., & Lorenzi, M. (2019, April). Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data. In 2019 IEEE 16th international symposium on biomedical imaging (ISBI 2019) (pp. 270-274). IEEE.

[38] Liu, Z., Li, T., Smith, V., & Sekar, V. (2019). Enhancing the privacy of federated learning with sketching. arXiv preprint arXiv:1911.01812.

[39] Gao, D., Ju, C., Wei, X., Liu, Y., Chen, T., & Yang, Q. (2019). Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography. arXiv preprint arXiv:1909.05784.

[40] Li, S., Cheng, Y., Liu, Y., Wang, W., & Chen, T. (2019). Abnormal client behavior detection in federated learning. arXiv preprint arXiv:1910.09933.

[41] Pfohl, S. R., Dai, A. M., & Heller, K. (2019). Federated and differentially private learning for electronic health records. arXiv preprint arXiv:1911.05861.

[42] Huang, L., Yin, Y., Fu, Z., Zhang, S., Deng, H., & Liu, D. (2018). LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data. arXiv preprint arXiv:1811.12629.

[43] Lee, J., Sun, J., Wang, F., Wang, S., Jun, C. H., & Jiang, X. (2018). Privacy-preserving patient similarity learning in a federated environment: development and analysis. JMIR medical informatics, 6(2), e7744.

[44] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 1-21.

[45] Han, J., Pei, J., & Tong, H. (2022). Data mining: concepts and techniques. Morgan kaufmann.

[46] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. the Journal of machine Learning research, 12, 2825-2830.

[47] Aha, D. W., Kibler, D., & Albert, M. K. (1991). Instance-based learning algorithms. Machine learning, 6(1), 37-66.

[48] Keerthi, S. S., Shevade, S. K., Bhattacharyya, C., & Murthy, K. R. K. (2001). Improvements to Platt's SMO algorithm for SVM classifier design. Neural computation, 13(3), 637-649.

[49] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.

[50] Ester, M., Kriegel, H. P., Sander, J., & Xu, X. (1996, August). A density-based algorithm for discovering clusters in large spatial databases with noise. In kdd (Vol. 96, No. 34, pp. 226-231).

[51] Sarker, I. H., Colman, A., Kabir, M. A., & Han, J. (2018). Individualized time-series segmentation for mining mobile phone user behavior. The Computer Journal, 61(3), 349-368.

[52] Wang, W., Yang, J., & Muntz, R. (1997, August). STING: A statistical information grid approach to spatial data mining. In Vldb (Vol. 97, pp. 186-195)

[53] Agrawal, R., Gehrke, J., Gunopulos, D., & Raghavan, P. (1998, June). Automatic subspace clustering of high dimensional data for data mining applications. In Proceedings of the 1998 ACM SIGMOD international conference on Management of data (pp. 94-105)

[54] Rasmussen, C. (1999). The infinite Gaussian mixture model. Advances in neural information processing systems, 12.

[55] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), 1-16.

[56] Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2018, September). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In International MICCAI Brainlesion Workshop (pp. 92-104). Springer, Cham.

[57] HTML, https://developer.mozilla.org/en-US/docs/Learn/HTML, last accessed: October 2022.

[58] Bootstrap, https://getbootstrap.com, last accessed: October 2022.

[59] CSS, https://developer.mozilla.org/en-US/docs/Web/CSS, last accessed: October 2022.

[60] JavaScript, https://www.javascript.com, last accessed: October 2022.

[61] jQuery, https://jquery.com, last accessed: October 2022.

[62] Python Programming Language, https://www.python.org, last accessed: October 2022.

[63] Flask, https://flask.palletsprojects.com/en/2.2.x/, last accessed: October 2022.

[64] Flask_Cors, https://flask-cors.readthedocs.io/en/latest/, last accessed: October 2022.

[65] Keras, https://keras.io, last accessed: October 2022.

[66] Matplotlib, https://matplotlib.org, last accessed: October 2022.

[67] NumPy, https://numpy.org, last accessed: October 2022.

[68] Pandas, https://pandas.pydata.org, last accessed: October 2022.

[69] Pillow, https://pillow.readthedocs.io/en/stable/, last accessed: October 2022.

[70] Plotly, https://plotly.com/python/, last accessed: October 2022.

[71] Psutil, https://psutil.readthedocs.io/en/latest/, last accessed: October 2022.

[72] Scikit_Learn, https://scikit-learn.org/stable/, last accessed: October 2022.

[73] TensorFlow, https://www.tensorflow.org, last accessed: October 2022.

[74] Pandas Profiling: https://pandas-profiling.ydata.ai/docs/master/index.html, last accessed: November 2022.

[75] Pandas Schema: https://pypi.org/project/pandas-schema/, last accessed: November 2022.

[76] Kaggle – Stroke Dataset, https://www.kaggle.com/datasets/fedesoriano/stroke-prediction-dataset, last accessed: October 2022.

[77] GitHub – Covid - 19 Dataset, https://github.com/burakalakuss/COVID-19-Clinical/tree/master/ Clinical%20Data, last accessed: October 2022.

[78] Kaggle – Breast Cancer Dataset, https://www.kaggle.com/code/buddhiniw/breast-cancer-prediction/data, last accessed: October 2022.

[79] Kaggle – Kidney Disease Dataset, https://www.kaggle.com/datasets/mansoordaku/ckdisease, last accessed: October 2022.

[80] Kaggle – Water Quality Dataset, https://www.kaggle.com/datasets/adityakadiwal/water-potability, last accessed: October 2022.

[81] Kaggle – Weather Forecast Dataset, https://www.kaggle.com/datasets/ananthr1/weather-prediction, last accessed: October 2022.

[82] Kaggle – Iris Dataset, https://www.kaggle.com/datasets/uciml/iris, last accessed: October 2022.

[83] UCI Machine Learning Repository – Car Evaluation Dataset, https://archive.ics.uci.edu/ml/datasets/ Car+Evaluation, last accessed: October 2022.

[84] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938.

[85] Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. IEEE transactions on neural networks and learning systems.

[86] Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K. R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. Proceedings of the IEEE, 109(3), 247-278.

[87] Connelly, L. (2020). Logistic regression. Medsurg Nursing, 29(5), 353-354.

[88] GitHub – GitHub Main Page, https://github.com, last accessed: November 2022.

[89] Python – Python Version 3.9.10, https://www.python.org/downloads/release/python-3910/, last accessed: November 2022.

[90] Git – Git Download, https://git-scm.com/downloads, last accessed: November 2022.

[91] Docker – Docker Main Page, https://www.docker.com, last accessed: November 2022.

[92] Docker – Docker Installation, https://docs.docker.com/engine/install/, last accessed: November 2022.