Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

# Εφαρμογή ομοσπονδιακής μάθησης για Network Slicing σε περιβάλλοντα 5G

Διπλωματικη Εργασια

του

**ΚΥΡΙΑΚΟΥ ΠΛΥΣΗ**

**Επιβλέπων:** Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2025

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

# Εφαρμογή ομοσπονδιακής μάθησης για Network Slicing σε περιβάλλοντα 5G

Διπλωματικη Εργασια

του

**ΚΥΡΙΑΚΟΥ ΠΛΥΣΗ**

**Επιβλέπων:** Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 17 Οκτωβρίου 2025.

| *(Υπογραφή)* | *(Υπογραφή)* | *(Υπογραφή)* |
|---|---|---|
| ..... | ..... | ..... |
| Δημήτριος Ασκούνης | Ιωάννης Ψαρράς | Ευάγγελος Μαρινάκης |
| Καθηγητής Ε.Μ.Π. | Καθηγητής Ε.Μ.Π. | Επίκουρος Καθηγητής Ε.Μ.Π. |

Αθήνα, Οκτώβριος 2025

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων



## ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

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

*(Υπογραφή)*

.....
Κυριάκος Πλυσής

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Ηλεκτρονικών Υπολογιστών

17 Οκτωβρίου 2025

# Περίληψη

Η ασφάλεια των δικτύων 5G αποτελεί κρίσιμο ζήτημα, καθώς η ευρεία υιοθέτησή τους σε εφαρμογές όπως οι τηλεπικοινωνίες, οι έξυπνες πόλεις και το Internet of Things (IoT) τα καθιστά ελκυστικό στόχο για κακόβουλες επιθέσεις. Η ανίχνευση εισβολών σε τέτοια δίκτυα παρουσιάζει προκλήσεις, λόγω της πολυπλοκότητάς τους, της κατανεμημένης φύσης των δεδομένων και της απαίτησης για προστασία της ιδιωτικότητας. Το Federated Learning (FL) έχει αναδειχθεί ως η κατάλληλη προσέγγιση για την ανάπτυξη συστημάτων ανίχνευσης εισβολών σε τέτοια περιβάλλοντα, επιτρέποντας την εκπαίδευση μοντέλων χωρίς την ανάγκη συγκέντρωσης των δεδομένων.

Στο πλαίσιο αυτής της εργασίας μελετάται η εφαρμογή της FL σε συστήματα ανίχνευσης εισβολών για δίκτυα 5G, με έμφαση στη ρεαλιστική διάσταση που εισάγει το Network Slicing. Για τον σκοπό αυτό χρησιμοποιείται το σύνολο δεδομένων 5G-SliciNDD, το οποίο περιλαμβάνει 14.456 ροές κίνησης, 52 χαρακτηριστικά και έναν διακριτό δείκτη για τον τύπο slice (eMBB, mMTC, URLLC). Το πρόβλημα διατυπώνεται ως δυαδική ταξινόμηση μεταξύ καλόβουλων και κακόβουλων ροών.

Αξιολογούνται τρεις διαφορετικές στρατηγικές συγκέντρωσης (FedAvg, FedAvgM, FedAdam), τόσο σε σενάρια ισόποσης κατανομής των δεδομένων όσο και σε σενάρια κατανομής βάσει Network Slicing, που προσομοιώνουν πιο ρεαλιστικές συνθήκες λειτουργίας. Τα αποτελέσματα επιβεβαιώνουν ότι η ισόποση κατανομή επιτρέπει τη βέλτιστη απόδοση των αποκεντρωμένων μοντέλων, με δείκτες F2 που προσεγγίζουν το 97%. Ωστόσο, η κατανομή βάσει network slices, αν και συνοδεύεται από αναμενόμενη πτώση απόδοσης, παρουσιάζει σταθερή βελτίωση με τη χρήση πιο εξελιγμένων στρατηγικών, φτάνοντας σε F2 Score έως και 94.19%.

Η εργασία αναδεικνύει τη σημασία της ρεαλιστικής αξιολόγησης FL-βασισμένων συστημάτων ανίχνευσης εισβολών σε δίκτυα 5G και δείχνει ότι, με την κατάλληλη επιλογή στρατηγικών συγκέντρωσης, η απόδοση σε πραγματικές συνθήκες μπορεί να πλησιάσει τα επίπεδα του ιδανικού σεναρίου ισόποσης κατανομής.

**Λέξεις-Κλειδιά**: 5G, Federated Learning, Δικτυακός Τεμαχισμός, Δυαδική Ταξινόμηση, Κυβερνοασφάλεια, Συστήματα Ανίχνευσης Εισβολών

# Abstract

The security of 5G networks is a critical issue, as their widespread adoption in applications such as smart cities and the Internet of Things (IoT) makes them an attractive target for malicious attacks. Intrusion detection in such networks presents challenges due to their complexity, the distributed nature of the data, and the requirement for privacy protection. Federated Learning (FL) has emerged as a suitable approach for developing intrusion detection systems in such environments, allowing models to be trained without the need to centralize the data.

This thesis investigates the application of FL to intrusion detection systems for 5G networks, with particular emphasis on the realistic dimension introduced by Network Slicing. For this purpose, the 5G-SliciNDD dataset is utilized, which contains 14,456 traffic flows, 52 features, and a distinct indicator for the slice type (eMBB, mMTC, URLLC). The problem is formulated as a binary classification task between Benign and Malicious flows.

Three different aggregation strategies (FedAvg, FedAvgM, FedAdam) are evaluated under both equal data distribution scenarios and Network Slicing-based distribution scenarios, which simulate more realistic operating conditions. The results confirm that equal distribution enables optimal performance of the decentralized models, with F2 scores approaching 97%. However, Network Slicing-based distribution, although accompanied by an expected performance drop, demonstrates steady improvement through the use of more advanced strategies, reaching an F2 Score of up to 94.19%.

This work highlights the importance of realistic evaluation of FL-based intrusion detection systems in 5G networks and demonstrates that, with the appropriate choice of aggregation strategies, performance under realistic conditions can approach that of the ideal equal distribution scenario.

**Keywords**: 5G, Federated Learning, Network Slicing, Binary Classification, Cybersecurity, Intrusion Detection Systems

# Περιεχόμενα

# Κατάλογος Σχημάτων

# Κατάλογος Πινάκων

Κεφάλαιο 1

# Εισαγωγή

## 1.1 Πλαίσιο

Η τεχνολογία των δικτύων 5G έχει επιφέρει ριζικές αλλαγές στον τρόπο που αντιλαμβανόμαστε και χρησιμοποιούμε τις ασύρματες επικοινωνίες. Χάρη σε χαρακτηριστικά όπως η υψηλή ταχύτητα μετάδοσης, η εξαιρετικά χαμηλή καθυστέρηση και η μαζική συνδεσιμότητα, τα 5G δίκτυα αποτελούν τη βάση για κρίσιμες και καινοτόμες εφαρμογές, όπως οι έξυπνες πόλεις, τα αυτόνομα οχήματα και το Internet of Things (IoT).

Μια από τις πιο θεμελιώδεις καινοτομίες που εισάγει το 5G είναι ο Δικτυακός Τεμαχισμός (Network Slicing). Μέσω αυτής της τεχνολογίας, η φυσική υποδομή του δικτύου «τεμαχίζεται» λογικά σε απομονωμένα κομμάτια (slices), το καθένα από τα οποία προσαρμόζεται στις ανάγκες διαφορετικών υπηρεσιών και εφαρμογών. Ενδεικτικά, τα slices eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low Latency Communications) και mMTC (massive Machine Type Communications) εξυπηρετούν απαιτήσεις που κυμαίνονται από γρήγορη μετάδοση δεδομένων μέχρι εξαιρετική αξιοπιστία ή μαζική συνδεσιμότητα συσκευών.

Αν και το Network Slicing προσφέρει ευελιξία και αποδοτικότητα, ταυτόχρονα εισάγει νέες προκλήσεις ασφαλείας. Κάθε slice λειτουργεί αυτόνομα, με ξεχωριστό λειτουργικό ρόλο και διαφορετικές απαιτήσεις ως προς την ασφάλεια. Συνεπώς, κάθε slice ενδέχεται να εμφανίζει διαφορετικά επίπεδα κινδύνου και να απαιτεί διαφοροποιημένη διαχείριση ασφάλειας. Οι παραδοσιακές, συγκεντρωτικές προσεγγίσεις ασφάλειας δεν επαρκούν πλέον για την πλήρη προστασία τέτοιων περίπλοκων και κατανεμημένων υποδομών.

Στο πλαίσιο αυτό, τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDS) που βασίζονται στη Μηχανική Μάθηση αποτελούν μια υποσχόμενη λύση. Ωστόσο, η εκπαίδευση αυτών των συστημάτων απαιτεί πρόσβαση σε μεγάλο όγκο δεδομένων, γεγονός που συγκρούεται με την ανάγκη διατήρησης της ιδιωτικότητας και τη φύση της κατανεμημένης αρχιτεκτονικής των 5G δικτύων.

Το Federated Learning (FL) έρχεται να καλύψει αυτό το κενό, επιτρέποντας την εκπαίδευση μοντέλων ανίχνευσης επιθέσεων χωρίς τη συγκέντρωση των δεδομένων σε κεντρικούς εξυπηρετητές. Με αυτόν τον τρόπο, οι συσκευές και οι υποδομές κάθε slice μπορούν να συμβάλουν στην ανίχνευση κακόβουλης δραστηριότητας, διατηρώντας τα δεδομένα τους τοπικά.

Η εφαρμογή τέτοιων καινοτόμων τεχνικών καθίσταται κρίσιμη για τη βελτίωση της ασφάλειας και της αξιοπιστίας των 5G υποδομών, λαμβάνοντας υπόψη τη δυναμική και την πολυπλοκότητα που εισάγει το Network Slicing.

## 1.2 Σκοπός

Σκοπός της παρούσας εργασίας είναι η διερεύνηση της εφαρμογής του FL σε συστήματα ανίχνευσης εισβολών για δίκτυα 5G, λαμβάνοντας υπόψη τη ρεαλιστική διάσταση του Network Slicing. Ειδικότερα, μελετάται πώς ο διαχωρισμός του δικτύου σε slices επηρεάζει τη λειτουργία και την απόδοση ενός FL-βασισμένου συστήματος ανίχνευσης επιθέσεων.

Βασικό αντικείμενο της εργασίας αποτελεί η αξιολόγηση της αποτελεσματικότητας διαφορετικών στρατηγικών συγκέντρωσης (aggregation strategies), όπως το FedAvg, το FedAvgM και το FedAdam, τόσο σε περιβάλλοντα όπου τα δεδομένα κατανέμονται σύμφωνα με τα slices όσο και σε περιπτώσεις ισόποσου διαχωρισμού τους. Παράλληλα, διερευνάται κατά πόσο ο τρόπος διαχωρισμού των δεδομένων επηρεάζει την αποδοτικότητα και την ικανότητα του συστήματος να ανιχνεύει κακόβουλη δραστηριότητα.

Η απάντηση στα παραπάνω ερωτήματα προκύπτει τόσο μέσω της βιβλιογραφικής επισκόπησης όσο και από την υλοποίηση και αξιολόγηση πειραματικού συστήματος. Η ανάλυση και σύγκριση των αποτελεσμάτων επιτρέπει την εξαγωγή συμπερασμάτων σχετικά με τη ρεαλιστική εφαρμογή του FL για την ενίσχυση της ασφάλειας στα 5G δίκτυα.

## 1.3 Συνεισφορά Εργασίας

Λαμβάνοντας υπόψη τη σημασία του Network Slicing και τις προκλήσεις που αυτό εισάγει για την ασφάλεια των 5G δικτύων, η παρούσα εργασία εστιάζει στην ανάπτυξη και αξιολόγηση ενός συστήματος ανίχνευσης εισβολών βασισμένου στο FL. Σε αντίθεση με μεγάλο μέρος της υπάρχουσας βιβλιογραφίας, όπου η αξιολόγηση τέτοιων συστημάτων πραγματοποιείται κυρίως σε ιδανικές, τεχνητές συνθήκες ισόποσης κατανομής των δεδομένων, η παρούσα προσέγγιση εξετάζει και το ρεαλιστικό σενάριο όπου η κατανομή των δεδομένων ακολουθεί τη λογική του Network Slicing.

Η εργασία αυτή συνεισφέρει με μια ολοκληρωμένη πειραματική μελέτη, στην οποία συγκρίνονται τρεις διαφορετικές στρατηγικές συγκέντρωσης (FedAvg, FedAvgM και FedAdam), τόσο σε σενάρια ισόποσης κατανομής όσο και σε σενάρια κατανομής βάσει Network Slicing. Μέσω αυτής της συγκριτικής ανάλυσης, αναδεικνύεται η επίδραση του τρόπου κατανομής των δεδομένων και η σημασία της επιλογής κατάλληλης στρατηγικής συγκέντρωσης για τη βελτίωση της απόδοσης του συστήματος.

Τα αποτελέσματα της μελέτης δείχνουν ότι, παρά τη μικρή αναμενόμενη πτώση απόδοσης που συνοδεύει τη ρεαλιστική προσέγγιση του Network Slicing, η χρήση πιο εξελιγμένων τεχνικών συγκέντρωσης μπορεί να περιορίσει σημαντικά αυτή τη διαφορά, καθιστώντας εφικτή τη ρεαλιστική και αποδοτική εφαρμογή συστημάτων ανίχνευσης εισβολών σε κατανεμημένα περιβάλλοντα 5G.

## 1.4 Διάρθρωση Εργασίας

Η εργασία αποτελείται από πέντε κεφάλαια. Στο Κεφάλαιο 2 παρουσιάζεται η Βιβλιογραφική Ανασκόπηση και οι Σχετικές Εργασίες, όπου αναλύεται η εξέλιξη και η αρχιτεκτονική των δικτύων 5G, η έννοια του Network Slicing, οι βασικές κυβερνοαπειλές που απειλούν τις υποδομές αυτών των δικτύων, καθώς και οι σύγχρονες προσεγγίσεις ανίχνευσης εισβολών με έμφαση στη Μηχανική Μάθηση, το Federated Learning και τα διαθέσιμα σύνολα δεδομένων

που αξιοποιούνται στη διεθνή βιβλιογραφία για τη μελέτη της ανίχνευσης επιθέσεων σε 5G και IoT περιβάλλοντα.

Το Κεφάλαιο 3 περιγράφει τη μεθοδολογία και την υλοποίηση της προτεινόμενης προσέγγισης. Περιλαμβάνει την επιλογή και προεπεξεργασία των δεδομένων, τη διαδικασία δημιουργίας υποσυνόλων τόσο βάσει Network Slicing όσο και μέσω ισόποσου διαχωρισμού, καθώς και τη στρατηγική εκπαίδευσης των FL μοντέλων.

Στο Κεφάλαιο 4 παρουσιάζονται τα αποτελέσματα της πειραματικής αξιολόγησης. Αρχικά περιγράφονται οι μετρικές αξιολόγησης, ενώ στη συνέχεια αναλύονται συγκριτικά τα αποτελέσματα των διαφορετικών προσεγγίσεων, τόσο για τα τοπικά μοντέλα όσο και για τα FL μοντέλα με τις διάφορες στρατηγικές συγκέντρωσης.

Τέλος, στο Κεφάλαιο 5 συνοψίζονται τα συμπεράσματα της εργασίας και προτείνονται κατευθύνσεις για μελλοντική έρευνα και βελτιώσεις.

Κεφάλαιο 2

# Βιβλιογραφική Ανασκόπηση και Σχετικές Εργασίες

## 2.1 5G Δίκτυα και Internet of Things

### 2.1.1 Από τα 1G στα 5G: Εξέλιξη των Κινητών Δικτύων

Η εξέλιξη των κινητών δικτύων τα τελευταία σαράντα χρόνια έχει μεταμορφώσει ριζικά τον τρόπο με τον οποίο επικοινωνούν οι άνθρωποι, οι συσκευές και οι υπηρεσίες. Από τα αναλογικά δίκτυα πρώτης γενιάς έως τα σημερινά ψηφιακά και υπερσυνδεδεμένα περιβάλλοντα της πέμπτης γενιάς, κάθε τεχνολογικό άλμα προσέφερε σημαντικές βελτιώσεις σε όρους ταχύτητας, αξιοπιστίας, ευελιξίας και εμβέλειας εφαρμογών.

Η απαρχή αυτής της πορείας ξεκίνησε με το 1G τη δεκαετία του 1980, το οποίο παρείχε αποκλειστικά αναλογική φωνητική επικοινωνία, με περιορισμένη ποιότητα, χαμηλή κάλυψη και ελάχιστες δυνατότητες ασφάλειας. Η μετάβαση στο 2G σηματοδότησε τη στροφή στην ψηφιακή μετάδοση, εισάγοντας υπηρεσίες όπως τα σύντομα γραπτά μηνύματα (SMS) και βελτιώνοντας τη σταθερότητα και την ποιότητα των κλήσεων. Με την έλευση του 3G, το ενδιαφέρον μετατοπίστηκε από τη φωνή στα δεδομένα. Για πρώτη φορά, έγινε δυνατή η ευρεία χρήση του διαδικτύου μέσω κινητού, καθώς και η αξιοποίηση πολυμεσικών εφαρμογών και υπηρεσιών όπως το mobile email, το video streaming και οι πρώτες εκδόσεις έξυπνων τηλεφώνων. Η επόμενη γενιά, το 4G, και κυρίως η τεχνολογία Long Term Evolution (LTE), έφερε κατακόρυφη αύξηση στις ταχύτητες μετάδοσης και μείωση στην καθυστέρηση, επιτρέποντας υπηρεσίες όπως το High Definition (HD) streaming, οι βιντεοκλήσεις και η μαζική υιοθέτηση φορητών εφαρμογών σε παγκόσμιο επίπεδο.

Σε αυτό το πλαίσιο, το 5G δεν έρχεται απλώς να βελτιώσει τις επιδόσεις του 4G, αλλά να επαναπροσδιορίσει συνολικά την αρχιτεκτονική και τη φιλοσοφία σχεδίασης των δικτύων. Σχεδιασμένο με σκοπό να υποστηρίξει ένα τεράστιο φάσμα εφαρμογών — από το IoT και την αυτοματοποιημένη βιομηχανία, έως τα αυτόνομα οχήματα και την επαυξημένη πραγματικότητα — το 5G στοχεύει σε ταχύτητες της τάξης των Gbps, και καθυστερήσεις κάτω του 1 ms [7].

### 2.1.2 Αρχιτεκτονική και Βασικά Χαρακτηριστικά των Δικτύων 5G

Όπως αναφέρθηκε στην προηγούμενη υποενότητα, το 5G εισάγει μια εντελώς νέα φιλοσοφία σχεδίασης για τα ασύρματα δίκτυα. Σε αντίθεση με τις προηγούμενες γενιές, οι οποίες βασίζονταν σε μονολιθικές και στατικά διαμορφωμένες υποδομές, το 5G σχεδιάστηκε εξαρχής για να είναι ευέλικτο, προσαρμοστικό και βασισμένο σε υπηρεσίες. Αυτή η προσέγγιση υλοποιείται μέσα από την υιοθέτηση της Service-Based Architecture (SBA) στον πυρήνα του δικτύου (5G Core (5GC).

#### 2.1.2.1 Service-Based Architecture (SBA)

Στον πυρήνα του 5G συναντάμε μία από τις σημαντικές διαφοροποιήσεις σε σχέση με τις προηγούμενες γενιές: την αρχιτεκτονική βασισμένη σε υπηρεσίες, γνωστή ως SBA. Σε αντίθεση με τις παλαιότερες προσεγγίσεις, όπου οι λειτουργικές μονάδες του δικτύου ήταν στενά συνδεδεμένες, προκαθορισμένες και στατικά διασυνδεδεμένες, το 5G υιοθετεί έναν πιο ευέλικτο και δυναμικό τρόπο οργάνωσης.

Η SBA βασίζεται στην ιδέα ότι κάθε βασική λειτουργία του δικτύου (π.χ. αυθεντικοποίηση, διαχείριση κινητικότητας, διαχείριση πολιτικής) πρέπει να υλοποιείται ως μια αυτόνομη, ανεξάρτητη και επαναχρησιμοποιήσιμη υπηρεσία. Αυτές οι υπηρεσίες δεν συνδέονται πλέον με σταθερές, άκαμπτες διεπαφές, αλλά επικοινωνούν μεταξύ τους μέσω κοινών και ανοιχτών προγραμματιστικών διεπαφών (Application Programming Interfaces (APIs)), επιτρέποντας έτσι τη δυναμική ανακάλυψη, ενεργοποίηση και συνεργασία των μονάδων εντός του πυρήνα.

Αυτό το μοντέλο επιτρέπει στο δίκτυο να είναι περισσότερο modular, δηλαδή να προσαρμόζεται ευκολότερα σε νέες απαιτήσεις και να υποστηρίζει προηγμένες λειτουργίες, όπως το Network Slicing ή την ενσωμάτωση εξωτερικών παρόχων υπηρεσιών, μέσω μηχανισμών ασφαλούς έκθεσης (exposure). Η SBA αποτελεί τον θεμέλιο λίθο της ευελιξίας, της επεκτασιμότητας και του προγραμματιζόμενου χαρακτήρα που χαρακτηρίζουν τα σύγχρονα δίκτυα 5G [8].

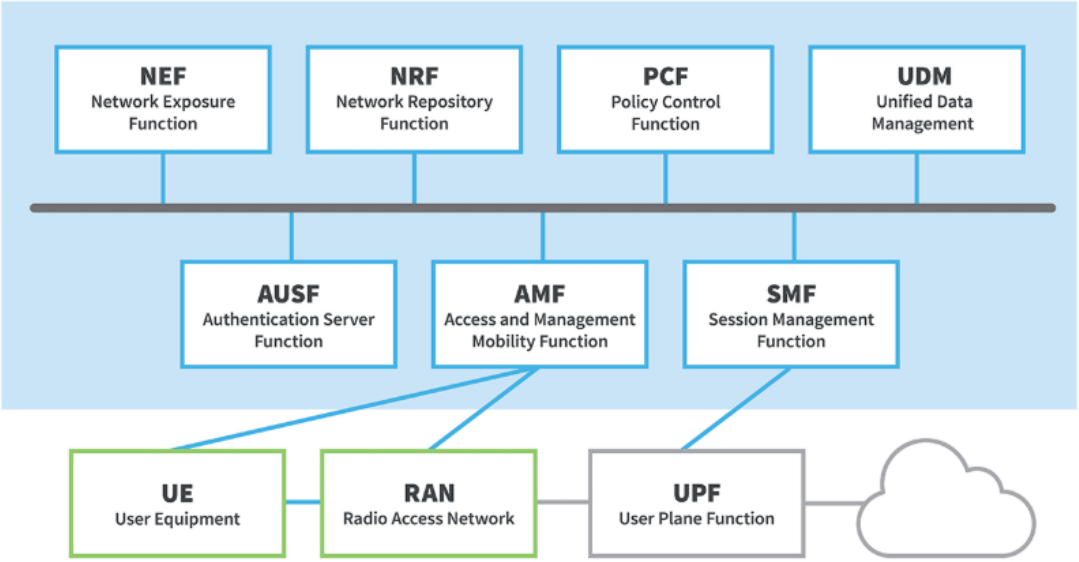
#### 2.1.2.2 Η SBA στον πυρήνα του δικτύου 5G

Η υλοποίηση της SBA στο (5GC) επιτυγχάνεται μέσω ενός συνόλου αυτόνομων λειτουργικών μονάδων, καθεμία από τις οποίες λειτουργεί ως ανεξάρτητη υπηρεσία. Οι μονάδες αυτές επικοινωνούν μεταξύ τους μέσω προκαθορισμένων και ασφαλών διεπαφών (APIs), επιτρέποντας την ευέλικτη ανταλλαγή πληροφορίας και την εύκολη αντικατάσταση ή αναβάθμιση μεμονωμένων στοιχείων χωρίς να διαταράσσεται η συνολική λειτουργία του δικτύου. Η αρχιτεκτονική αυτή υιοθετεί αρχές που θυμίζουν συστήματα μικροϋπηρεσιών (microservices), προσφέροντας σημαντικά οφέλη σε επεκτασιμότητα, διαλειτουργικότητα και διαχείριση.

Ενδεικτικά, η Access and Mobility Management Function (AMF) διαχειρίζεται την πρόσβαση των συσκευών και την κινητικότητα των χρηστών, ενώ η Session Management Function (SMF) είναι υπεύθυνη για τη διαχείριση των συνεδριών και την εκχώρηση διευθύνσεων Internet Protocol (IP). Παράλληλα, η User Plane Function (UPF) αναλαμβάνει τη μεταφορά δεδομένων στο επίπεδο χρήστη, με στόχο τη χαμηλή καθυστέρηση και την υψηλή απόδοση. Συμπληρωματικά, μονάδες όπως η Authentication Server Function (AUSF), για αυθεντικοποίηση, η Unified Data Management (UDM), για τη διαχείριση προφίλ συνδρομητών και η Policy Control Function (PCF), για τον έλεγχο πολιτικών πρόσβασης και ποιότητας υπηρεσίας, διασφαλίζουν την ορθή και ασφαλή λειτουργία του πυρήνα. Η Network Exposure Function (NEF) επιτρέπει την ασφαλή έκθεση υπηρεσιών σε τρίτους παρόχους μέσω ανοιχτών διεπαφών, ενώ η Network Repository Function (NRF)) λειτουργεί ως μηχανισμός ανακάλυψης υπηρεσιών και συντονισμού μεταξύ των μονάδων του πυρήνα [9].

Η αποσύνδεση αυτών των λειτουργιών και η αναδιάταξή τους ως ανεξάρτητες υπηρεσίες όχι μόνο ενισχύει την ευελιξία του συστήματος, αλλά διευκολύνει και την ενσωμάτωση προηγ-

μένων τεχνολογιών, όπως η εικονικοποίηση ( Network Functions Virtualization (NFV)) και ο προγραμματιζόμενος έλεγχος ( Software-Defined Networking (SDN)), που αναλύονται στη συνέχεια.
Στο σχήμα 2.1 αποτυπώνεται η δομή του 5GC και η αλληλεπίδραση μεταξύ των επιμέρους λειτουργικών μονάδων που αναφέρθηκαν παραπάνω.




Σχήμα 2.1: *Αρχιτεκτονική του 5G Core [1]*

#### 2.1.2.3 Next Generation Radio Access Network (NG-RAN)

Σε κάθε γενιά κυψελοειδών δικτύων, το Radio Access Network (RAN) αποτελεί το κρίσιμο τμήμα της αρχιτεκτονικής που είναι υπεύθυνο για τη σύνδεση των χρηστών με τον πυρήνα του δικτύου. Είναι το σημείο στο οποίο ο Εξοπλισμός Χρήστη (User Equipment (UE)) επικοινωνεί ασύρματα με σταθμούς βάσης, οι οποίοι στη συνέχεια διοχετεύουν την κίνηση προς τον κεντρικό πυρήνα. Στις προηγούμενες γενιές, όπως το 3G και το 4G, το RAN αποτελούνταν από κόμβους όπως οι NodeB και eNodeB, αντίστοιχα, οι οποίοι λειτουργούσαν με σταθερή λογική δρομολόγησης και περιορισμένη δυνατότητα συνεργασίας και ευελιξίας.

Στο 5G, το ραδιοδίκτυο πρόσβασης επανασχεδιάζεται πλήρως ως Next Generation Radio Access Network (NG-RAN), ακολουθώντας τις ίδιες αρχές ευελιξίας και επεκτασιμότητας που συναντώνται στο 5GC. Το NG-RAN δεν περιορίζεται πλέον σε στατικά προκαθορισμένους ρόλους, αλλά υποστηρίζει δυναμική λειτουργία, καλύτερη κατανομή πόρων και βελτιωμένο συντονισμό μεταξύ κόμβων, με στόχο την κάλυψη των απαιτήσεων για χαμηλή καθυστέρηση, μαζική συνδεσιμότητα και υψηλή αξιοπιστία.

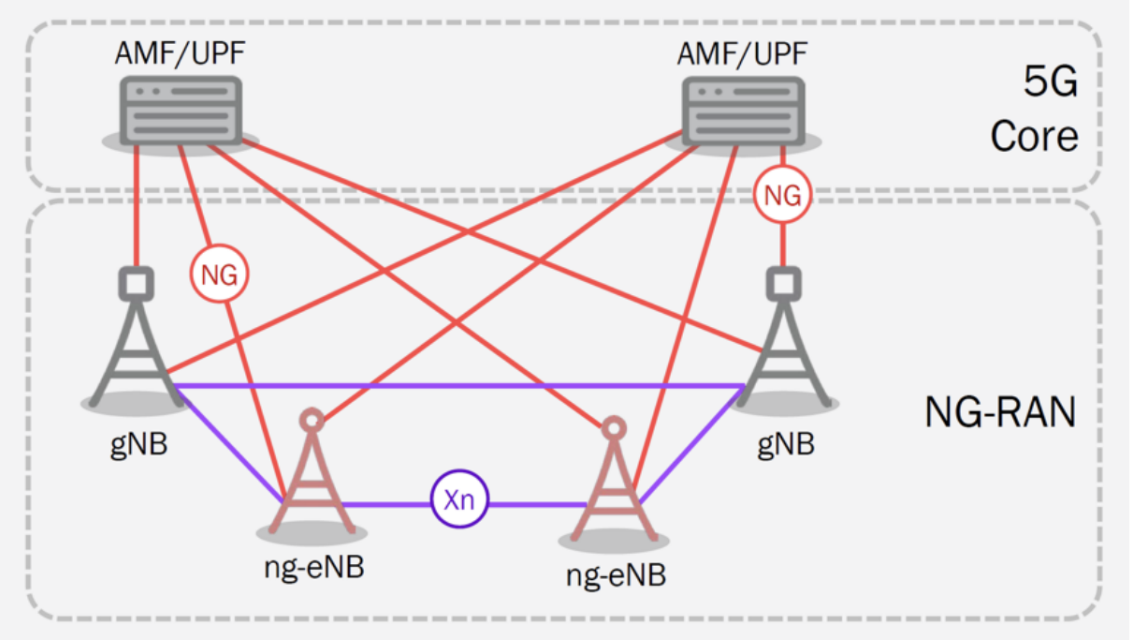
Οι βασικοί κόμβοι του NG-RAN είναι οι gNB (Next Generation NodeB), οι οποίοι εξυπηρετούν το 5G New Radio (NR) και υποστηρίζουν αποκλειστικά σύνδεση με τον 5GC, καθώς και οι ng-eNB, οι οποίοι επιτρέπουν τη συνύπαρξη και τη σταδιακή ενσωμάτωση του 5G σε υπάρχουσες LTE υποδομές. Οι κόμβοι αυτοί επικοινωνούν με τον πυρήνα μέσω της διεπαφής NG και μεταξύ τους μέσω της Xn, η οποία αντικαθιστά την παλαιότερη X2 και υποστηρίζει

καλύτερο συντονισμό μεταξύ σταθμών βάσης.

Η ανάπτυξη του NG-RAN μπορεί να ακολουθήσει δύο μοντέλα: το μη-αυτόνομο (Non-Standalone (NSA)) και το αυτόνομο (Standalone (SA)). Στην περίπτωση του NSA, η σύνδεση του χρήστη πραγματοποιείται μέσω του 5G NR για τη μεταφορά δεδομένων, αλλά ο έλεγχος εξακολουθεί να γίνεται μέσω του 4G LTE και του Evolved Packet Core (EPC). Αντιθέτως, στη λειτουργία SA, το δίκτυο στηρίζεται εξ ολοκλήρου στον νέο πυρήνα 5GC, αξιοποιώντας πλήρως τις δυνατότητες της SBA, της εικονικοποίησης και της προγραμματιζόμενης λειτουργίας [10].

Ο ρόλος του NG-RAN, σε συνδυασμό με τον ανασχεδιασμένο πυρήνα, είναι θεμελιώδης για την υλοποίηση κρίσιμων τεχνολογιών του 5G, όπως το Network Slicing και η υποστήριξη εφαρμογών εξαιρετικά χαμηλής καθυστέρησης. Η υλοποίηση αυτών των δυνατοτήτων προϋποθέτει καινοτόμες τεχνικές ελέγχου και διαχείρισης, όπως αυτές που προσφέρουν οι τεχνολογίες SDN και NFV, οι οποίες αναλύονται στην επόμενη παράγραφο.

Η αρχιτεκτονική του NG-RAN, καθώς και η σύνδεσή του με τον πυρήνα 5GC, παρουσιάζεται στο Σχήμα 2.2.




Σχήμα 2.2: *Αρχιτεκτονική του NG-RAN και η διασύνδεσή του με τον πυρήνα 5GC, με ενδεικτικές μονάδες όπως gNB, ng-eNB, AMF και UPF [2].*

#### 2.1.2.4 Εικονικοποίηση και Προγραμματιζόμενη Λειτουργία στο 5G (NFV & SDN)

Ένα από τα πιο καινοτόμα χαρακτηριστικά του 5G είναι η δυνατότητα προγραμματιζόμενης λειτουργίας του δικτύου (programmability). Η έννοια αυτή αναφέρεται στην ικανότητα δυναμικής διαχείρισης, τροποποίησης και επαναδιαμόρφωσης των λειτουργιών και των ροών του δικτύου μέσω λογισμικού, χωρίς να απαιτούνται παρεμβάσεις σε φυσικό επίπεδο. Για την υλοποίηση αυτού του οράματος, δύο βασικές τεχνολογίες υιοθετούνται: η NFV και το SDN.

Η NFV επιτρέπει την αντικατάσταση παραδοσιακών, υλοποιημένων σε εξειδικευμένο υλικό (hardware) δικτυακών λειτουργιών, με εικονικές εκδοχές αυτών (Virtual Network Functions (VNFs)) που εκτελούνται σε κοινό υπολογιστικό περιβάλλον. Λειτουργίες όπως η δρομολόγηση, η ανάλυση πακέτων ή τα firewalls μπορούν πλέον να υλοποιούνται ως λογισμικό, ανεξάρτητο από τον φυσικό εξοπλισμό, επιτρέποντας μεγαλύτερη ευελιξία, ταχύτερη εγκατάσταση και χαμηλότερο κόστος [11].

Συμπληρωματικά, το SDN προσφέρει ένα νέο μοντέλο ελέγχου του δικτύου, αποσυνδέοντας το επίπεδο ελέγχου (Control Plane) από το επίπεδο προώθησης δεδομένων (Data Plane). Μέσω του SDN controller, το δίκτυο μπορεί να ελέγχεται κεντρικά, επιτρέποντας την προσαρμογή των πολιτικών δρομολόγησης, τη βελτιστοποίηση της απόδοσης, αλλά και την εφαρμογή δυναμικών μηχανισμών ασφάλειας. Το μοντέλο αυτό είναι ιδιαίτερα συμβατό με την αρχιτεκτονική SBA, αφού προσφέρει τις απαραίτητες δυνατότητες για την ευέλικτη συνεργασία και ενορχήστρωση των δικτυακών λειτουργιών [12].

Η ενσωμάτωση των τεχνολογιών NFV και SDN στον πυρήνα και στο ραδιοδίκτυο του 5G μετατρέπει το δίκτυο σε ένα πλήρως προγραμματιζόμενο σύστημα, ικανό να προσαρμόζεται σε πραγματικό χρόνο στις ανάγκες διαφορετικών υπηρεσιών και εφαρμογών. Αυτή η ευελιξία είναι καθοριστική για την υποστήριξη προσεγγίσεων όπως το Network Slicing, το IoT και οι εφαρμογές με αυστηρές απαιτήσεις καθυστέρησης ή αξιοπιστίας.

### 2.1.3 Το Internet of Things στο πλαίσιο του 5G

Το IoT αναφέρεται σε ένα οικοσύστημα διασυνδεδεμένων φυσικών συσκευών, αισθητήρων, οχημάτων, βιομηχανικών μονάδων και άλλων αντικειμένων, τα οποία έχουν τη δυνατότητα συλλογής, αποστολής και λήψης δεδομένων μέσω δικτύων επικοινωνίας. Η βασική ιδέα πίσω από το IoT είναι η δημιουργία ενός περιβάλλοντος όπου ο φυσικός κόσμος και τα ψηφιακά συστήματα μπορούν να αλληλεπιδρούν σε πραγματικό χρόνο, χωρίς ανθρώπινη παρέμβαση.

Η εφαρμογή του IoT εκτείνεται σε πολυάριθμους τομείς: από τις έξυπνες πόλεις και τη βιομηχανία 4.0, μέχρι την υγειονομική περίθαλψη, τις μεταφορές και την αγροτική παραγωγή. Παρόλο που οι βασικές αρχές του IoT είναι γνωστές εδώ και αρκετά χρόνια, η μαζική υλοποίησή του ήταν μέχρι πρότινος περιορισμένη από τεχνικούς φραγμούς, όπως οι περιορισμένες ταχύτητες μετάδοσης, η υψηλή καθυστέρηση και η αδυναμία υποστήριξης ταυτόχρονης σύνδεσης εκατομμυρίων συσκευών [13].

Το 5G έρχεται να ανατρέψει τα παραπάνω εμπόδια, παρέχοντας τις τεχνολογικές δυνατότητες που απαιτούνται για την πλήρη αξιοποίηση του IoT. Η αυξημένη χωρητικότητα του ραδιοδικτύου, η δυνατότητα μαζικής συνδεσιμότητας (massive connectivity), η εξαιρετικά χαμηλή καθυστέρηση (ultra-low latency) και η υψηλή αξιοπιστία του 5G καθιστούν δυνατή τη δημιουργία περιβαλλόντων όπου εκατομμύρια συσκευές μπορούν να επικοινωνούν αποδοτικά και σε πραγματικό χρόνο [14].

Επιπλέον, η αρχιτεκτονική του 5G προσφέρει σημαντική προσαρμοστικότητα, καθώς επιτρέπει τη διαχείριση των συσκευών και των υπηρεσιών του IoT μέσω προγραμματιζόμενων μηχανισμών όπως το SDN, αλλά και μέσω εικονικοποιημένων υποδομών (NFV), όπως παρουσιάστηκε προηγουμένως. Η δυνατότητα διαχωρισμού του δικτύου σε εξειδικευμένα λειτουργικά τμήματα (Network Slices), καθένα εκ των οποίων μπορεί να εξυπηρετεί διαφορετικούς τύπους IoT εφαρμογών, αποτελεί ένα επιπλέον στρατηγικό πλεονέκτημα που αναδεικνύεται

στην επόμενη υποενότητα [15].

Συνολικά, το 5G λειτουργεί ως καταλύτης για την εξάπλωση του IoT, δημιουργώντας τις υποδομές για έξυπνα συστήματα που βασίζονται σε συνεχή ροή πληροφορίας, αλληλεπίδραση μεταξύ συσκευών, και ταχεία λήψη αποφάσεων σε πραγματικό χρόνο.

### 2.1.4 Δικτυακός Τεμαχισμός (Network Slicing)

Μια από τις πιο καινοτόμες δυνατότητες που εισάγει το 5G είναι η τεχνολογία του δικτυακού τεμαχισμού (Network Slicing). Ο τεμαχισμός επιτρέπει τη δημιουργία πολλαπλών λογικών, πλήρως απομονωμένων ΄τομών΄ (slices) εντός του ίδιου φυσικού δικτύου. Κάθε slice λειτουργεί ως ένα ξεχωριστό εικονικό δίκτυο με προσαρμοσμένα χαρακτηριστικά απόδοσης, ασφάλειας και πολιτικών διαχείρισης, εξυπηρετώντας διαφορετικές υπηρεσίες ή κάθετες αγορές (verticals).

Η υλοποίηση του Network Slicing βασίζεται στον συνδυασμό των τεχνολογιών SBA, NFV και SDN, οι οποίες παρουσιάστηκαν στις προηγούμενες υποενότητες. Η εικονικοποίηση των λειτουργιών του πυρήνα και του ραδιοδικτύου, σε συνδυασμό με τον προγραμματιζόμενο έλεγχο της δικτυακής συμπεριφοράς, επιτρέπει τη δυναμική δημιουργία, παραμετροποίηση και διαχείριση σλιςες σε πραγματικό χρόνο. Κάθε slice μπορεί να διαθέτει αποκλειστικούς ή διαμοιραζόμενους πόρους, ξεχωριστές ρυθμίσεις ποιότητας υπηρεσίας (Quality of Service (QoS)) και εξειδικευμένες πολιτικές ασφάλειας, χωρίς να επηρεάζει ή να επηρεάζεται από άλλα slices [16].

Αναλόγως των απαιτήσεων της εφαρμογής, κάθε slice μπορεί να είναι βελτιστοποιημένο για διαφορετικά προφίλ χρήσης. Η προδιαγραφή του 5G καθορίζει τρεις βασικές κατηγορίες slices [17]:

- **Enhanced Mobile Broadband (eMBB):** Υποστηρίζει υπηρεσίες που απαιτούν υψηλό εύρος ζώνης και ταχύτητες μετάδοσης, όπως 4K/8K βίντεο, AR/VR εφαρμογές και cloud gaming.

- **Massive Machine Type Communications (mMTC):** Σχεδιασμένο για σενάρια μαζικής συνδεσιμότητας με χαμηλό ενεργειακό αποτύπωμα, όπως αισθητήρες σε έξυπνες πόλεις, παρακολούθηση περιβάλλοντος ή βιομηχανικό IoT.

- **Ultra-Reliable Low-Latency Communications (URLLC):** Στοχεύει σε εφαρμογές με αυστηρές απαιτήσεις αξιοπιστίας και καθυστέρησης κάτω από 1μς, όπως η τηλεχειρουργική, τα αυτόνομα οχήματα και τα συστήματα ελέγχου σε κρίσιμες υποδομές.

Ένα χαρακτηριστικό παράδειγμα αξιοποίησης του Network Slicing είναι ένα έξυπνο εργοστάσιο παραγωγής. Εκεί, ένα slice eMBB μπορεί να εξυπηρετεί την αναμετάδοση βίντεο υψηλής ανάλυσης για επιτήρηση ή απομακρυσμένο έλεγχο, ένα slice mMTC να διαχειρίζεται τη συλλογή δεδομένων από εκατοντάδες αισθητήρες παραγωγής, και ένα slice URLLC να εξυπηρετεί την ανταλλαγή κρίσιμων εντολών σε πραγματικό χρόνο μεταξύ ρομποτικών μηχανημάτων. Κάθε slice λειτουργεί ανεξάρτητα και διασφαλίζει την απαιτούμενη ποιότητα υπηρεσίας, χωρίς παρεμβολές ή συμφόρηση από τις υπόλοιπες λειτουργίες.

Ο τεμαχισμός του δικτύου αποτελεί κεντρικό πυλώνα για την υποστήριξη της πολυμορφίας των υπηρεσιών που υπόσχεται το 5G. Η δυνατότητα παροχής εξατομικευμένων slices σε διαφορετικούς παρόχους, οργανισμούς ή εφαρμογές, ενισχύει την ευελιξία, την ασφάλεια και τη συνολική αποδοτικότητα του συστήματος.

Συνοψίζοντας, τα δίκτυα πέμπτης γενιάς φέρνουν επαναστατικές αλλαγές στον τρόπο με τον οποίο σχεδιάζονται, υλοποιούνται και χρησιμοποιούνται τα ασύρματα δίκτυα. Μέσα από την υιοθέτηση αρχιτεκτονικών όπως το SBA, τις τεχνολογίες NFV και SDN, καθώς και την έννοια του Network Slicing, το 5G καθιστά δυνατή την παροχή εξειδικευμένων και εξαιρετικά αποδοτικών υπηρεσιών. Ωστόσο, αυτή η αυξημένη ευελιξία και πολυπλοκότητα συνοδεύεται από νέες προκλήσεις ασφαλείας και πιθανά τρωτά σημεία. Η επόμενη ενότητα εξετάζει τις κύριες κυβερνοαπειλές που σχετίζονται με το οικοσύστημα του 5G, ξεκινώντας από τις επιθέσεις DoS/DDoS, οι οποίες μπορούν να διαταράξουν κρίσιμες λειτουργίες του δικτύου.

## 2.2 Κυβερνοαπειλές στο 5G

Η ριζική αναδιάρθρωση της αρχιτεκτονικής των δικτύων 5G φέρνει στο προσκήνιο όχι μόνο τεχνολογικές καινοτομίες αλλά και έναν διευρυμένο χώρο πιθανών επιθέσεων. Καθώς τα δίκτυα γίνονται πιο ευέλικτα, κατανεμημένα και δυναμικά, αυξάνονται και τα σημεία στα οποία μπορούν να στοχεύσουν κακόβουλοι παράγοντες. Από την επιφάνεια πρόσβασης έως το υποκείμενο δίκτυο και την υποδομή cloud, κάθε επίπεδο μπορεί να αποτελέσει σημείο ευπάθειας. Στην παρούσα ενότητα εξετάζονται βασικές κατηγορίες κυβερνοαπειλών που σχετίζονται με την υποδομή και τη λειτουργία των δικτύων 5G, περιλαμβάνοντας επιθέσεις όπως οι DoS/DDoS, οι αναγνωριστικές ενέργειες και οι επιθέσεις MitM.

### 2.2.1 Επιθέσεις DoS και DDoS

Οι επιθέσεις DoS και DDoS αποτελούν σημαντικές προκλήσεις για την απόδοση και την ασφάλεια των δικτύων 5G, κυρίως λόγω του μεγάλου αριθμού συνδεδεμένων συσκευών που χαρακτηρίζουν αυτά τα δίκτυα. Ο στόχος αυτών των επιθέσεων είναι η εξάντληση των πόρων του παρόχου δικτύου, με αποτέλεσμα τη μείωση της ποιότητας των υπηρεσιών και την αδυναμία εξυπηρέτησης των χρηστών. Στις DDoS επιθέσεις, οι δράστες συχνά αξιοποιούν παραβιασμένες συσκευές, δημιουργώντας μεγάλα botnets που μπορούν να εκτοξεύσουν μαζικά αιτήματα προς την υποδομή του δικτύου, επηρεάζοντας τόσο τις συσκευές των χρηστών όσο και τη συνολική λειτουργικότητα του δικτύου. [18]

Για την πραγματοποίηση επιθέσεων DoS και DDoS στα δίκτυα 5G, οι κακόβουλοι χρήστες εστιάζουν στους πόρους που σχετίζονται με τη συνδεσιμότητα και το εύρος ζώνης, καθώς αυτά είναι κρίσιμα για την παροχή υπηρεσιών υψηλού επιπέδου. Μερικές αδυναμίες που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι περιλαμβάνουν [19]:

- **Επίπεδο Σηματοδοσίας**: Η διακοπή της σηματοδοσίας επηρεάζει τη διαδικασία πιστοποίησης χρηστών και τη δυναμική κατανομή εύρους ζώνης, περιορίζοντας την κινητικότητα των χρηστών.
- **Επίπεδο Δεδομένων Χρήστη**: Η παρεμπόδιση της αμφίδρομης επικοινωνίας μεταξύ διακομιστών και συνδεδεμένων συσκευών οδηγεί σε διακοπές στις υπηρεσίες.
- **Επίπεδο Διαχείρισης**: Στόχος είναι η διατάραξη των λειτουργιών που υποστηρίζουν

τα επίπεδα χρήστη και σηματοδοσίας, με αποτέλεσμα την αστάθεια του δικτύου.

- **Ραδιοφωνικοί Πόροι**: Οι επιθέσεις σε αυτούς τους πόρους δυσχεραίνουν την πρόσβαση των συνδρομητών στο δίκτυο.
- **Υποστηρικτικές Υποδομές**: Επηρεάζονται συστήματα που διαχειρίζονται λογιστικές πληροφορίες ή υπηρεσίες υποστήριξης.
- **Υποδομές Cloud**: Οι κακόβουλες ενέργειες μπορούν να προκαλέσουν εξάντληση φυσικών και λογικών πόρων, όπως διακομιστών, αποθηκευτικών χώρων και εικονικών μηχανών.

Ένας από τους πιο διαδεδομένους τύπους αυτών των επιθέσεων είναι τα flood attacks, οι οποίες επικεντρώνονται στην υπερφόρτωση του δικτύου με υπερβολικά μεγάλο όγκο δεδομένων σε σύντομο χρονικό διάστημα [20]. Για παράδειγμα:

- **SYN Flood**: Πρόκειται για μορφή επίθεσης DoS που εκμεταλλεύεται τη διαδικασία τριών βημάτων ελέγχου σύνδεσης (TCP three-way handshake). Η διαδικασία αυτή αποτελεί τον καθιερωμένο μηχανισμό με τον οποίο δύο συστήματα συμφωνούν να δημιουργήσουν αξιόπιστη σύνδεση στο πρωτόκολλο TCP. Αρχικά, ο υπολογιστής-πελάτης στέλνει πακέτο SYN (synchronize) για να αιτηθεί τη σύνδεση. Ο διακομιστής απαντά με πακέτο SYN-ACK επιβεβαιώνοντας την αποδοχή και, τέλος, ο πελάτης αποστέλλει πακέτο ACK ολοκληρώνοντας τη διαδικασία. Στην επίθεση SYN Flood, ο επιτιθέμενος αποστέλλει μαζικά πακέτα SYN, χωρίς όμως να ολοκληρώνει ποτέ τη σύνδεση. Ως αποτέλεσμα, παραμένουν ανοιχτές ημιτελείς συνδέσεις στη μνήμη του διακομιστή, εξαντλώντας τους διαθέσιμους πόρους του και καθιστώντας τον μη διαθέσιμο.
- **UDP Flood**: Σε αυτή την περίπτωση, ο επιτιθέμενος στέλνει μεγάλο όγκο πακέτων UDP (User Datagram Protocol) σε τυχαίες ή συγκεκριμένες θύρες του συστήματος. Το σύστημα-στόχος προσπαθεί να απαντήσει ή να επεξεργαστεί τα πακέτα, οδηγώντας σε υπερφόρτωση των πόρων του.
- **ICMP Flood (Ping Flood)**: Η επίθεση αυτή βασίζεται στην αποστολή τεράστιου αριθμού πακέτων ICMP (Internet Control Message Protocol), συνήθως Echo Request (γνωστών ως ping). Ο στόχος καλείται να απαντήσει σε κάθε μήνυμα, γεγονός που μπορεί να προκαλέσει συμφόρηση ή αδυναμία εξυπηρέτησης.
- **HTTP Flood**: Σε αυτή τη μορφή επίθεσης, ο επιτιθέμενος κατακλύζει έναν διακομιστή ιστού με πολλαπλά έγκυρα αιτήματα HTTP, όπως GET ή POST. Παρόλο που δεν απαιτείται ιδιαίτερα υψηλό εύρος ζώνης, η συνεχής επεξεργασία των αιτημάτων μπορεί να εξαντλήσει τους υπολογιστικούς πόρους του διακομιστή, οδηγώντας σε άρνηση υπηρεσίας.

Επιπλέον, μια άλλη τεχνική που χρησιμοποιείται στις επιθέσεις DoS/DDoS είναι οι slow-rate attacks, οι οποίες διαφέρουν από τις παραδοσιακές επιθέσεις flooding. Σε αυτές, ο επιτιθέμενος στέλνει δεδομένα με πολύ αργό ρυθμό για να διατηρήσει ανοικτές συνδέσεις,

καταναλώνοντας τους πόρους του συστήματος χωρίς να ανιχνεύεται εύκολα. Ένα παράδειγμα είναι η Slowloris, όπου ο επιτιθέμενος διατηρεί πολλαπλές ημιτελείς συνδέσεις HTTP με έναν διακομιστή, εξαντλώντας τις διαθέσιμες συνδέσεις [21].

Οι επιτιθέμενοι μπορούν επίσης να στοχεύσουν τους λογικούς και φυσικούς πόρους του εξοπλισμού χρήστη (UE), όπως η μνήμη, η μπαταρία, οι μονάδες επεξεργασίας, οι αισθητήρες και το λειτουργικό σύστημα. Η εξάντληση αυτών των πόρων περιορίζει τη δυνατότητα πρόσβασης των χρηστών στο δίκτυο, ενώ μπορεί να προκαλέσει αλυσιδωτές αντιδράσεις που επηρεάζουν την ευρύτερη υποδομή.

Οι επιπτώσεις αυτών των επιθέσεων μπορούν να είναι ιδιαίτερα σοβαρές, επηρεάζοντας κρίσιμες υποδομές, όπως τα δίκτυα υγείας, μεταφορών και ενέργειας. Οι συντονισμένες επιθέσεις μέσω γεωγραφικά διασκορπισμένων μηχανών ή παραβιασμένων IoT συσκευών μπορούν να προκαλέσουν ευρείας κλίμακας διακοπές υπηρεσιών, επισημαίνοντας την ανάγκη για μια εξελικτική στρατηγική ασφάλειας.

### 2.2.2 Reconnaissance Attacks

Οι αναγνωριστικές επιθέσεις αποτελούν το πρώτο στάδιο σε πολλές κυβερνοεπιθέσεις, καθώς επιτρέπουν στους επιτιθέμενους να συλλέξουν πληροφορίες για το στόχο τους πριν προχωρήσουν σε πιο καταστροφικές ενέργειες. Οι επιτιθέμενοι χρησιμοποιούν τεχνικές όπως η σάρωση θυρών και η ανάλυση πακέτων για να εντοπίσουν αδυναμίες, ανοιχτές θύρες και εκτεθειμένες υπηρεσίες σε ένα δίκτυο. Στα δίκτυα 5G, όπου η διαχείριση τεράστιου όγκου δεδομένων και συσκευών είναι κρίσιμη, τέτοιες επιθέσεις μπορούν να προκαλέσουν σοβαρούς κινδύνους ασφάλειας [22].

Μία από τις πιο συνηθισμένες μορφές αναγνωριστικών επιθέσεων είναι η σάρωση θυρών. Οι επιτιθέμενοι στέλνουν αιτήματα σε μια σειρά από θύρες ενός συστήματος και αναλύουν τις απαντήσεις για να εντοπίσουν ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται. Στα δίκτυα 5G, όπου οι συσκευές UE μπορούν να έχουν έως και 65.546 θύρες, οι οποίες διακρίνονται σε γνωστές θύρες (0–1023), καταχωρημένες θύρες (1024–49151) και ιδιωτικές θύρες (49152–65535), η σάρωση μπορεί να αποκαλύψει κρίσιμες πληροφορίες για το στόχο [23].

Οι πιο κοινές τεχνικές σάρωσης περιλαμβάνουν:

- **TCP Scanning**: Αξιοποιεί τη διαδικασία τριών βημάτων ελέγχου σύνδεσης (TCP three-way handshake), κατά την οποία ανταλλάσσονται πακέτα SYN (Synchronize), SYN-ACK και ACK για τη δημιουργία αξιόπιστης σύνδεσης. Η τεχνική αυτή παρέχει λεπτομερείς πληροφορίες για τις διαθέσιμες θύρες και υπηρεσίες, ενώ μπορεί να είναι δύσκολα ανιχνεύσιμη, καθώς προσομοιάζει με νόμιμη κυκλοφορία.

- **Stealth Scanning**: Εφαρμόζει εναλλακτικές τεχνικές αποστολής πακέτων, όπως SYN, FIN (Finish) ή άλλες ειδικές σημαίες (flags), ώστε να παρακάμψει τα συστήματα ανίχνευσης και να εντοπίσει ανοιχτές θύρες χωρίς να ολοκληρώσει το πλήρες handshake.

- **Bounce Scanning**: Αξιοποιεί τρίτα συστήματα, όπως διακομιστές που υποστηρίζουν το πρωτόκολλο File Transfer Protocol (FTP), για να επαναπροωθήσει τα πακέτα ανίχνευσης. Με αυτόν τον τρόπο, ο επιτιθέμενος αποκρύπτει την πραγματική του διεύθυνση IP και καθιστά δυσκολότερο τον εντοπισμό του.

- **UDP Scanning**: Στοχεύει θύρες που χρησιμοποιούν το User Datagram Protocol (UDP), ένα πρωτόκολλο χωρίς επιβεβαίωση σύνδεσης. Αν και παρέχει λιγότερες πληροφορίες σε σχέση με το TCP Scanning, μπορεί να αποκαλύψει υπηρεσίες που βασίζονται στο UDP.

Μία ακόμη μορφή αναγνωριστικής επίθεσης είναι η ανάλυση πακέτων, όπου οι επιτιθέμενοι παρακολουθούν την κίνηση δεδομένων στο δίκτυο για να συλλέξουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια χρηστών, δομές αρχιτεκτονικής δικτύου και τύπους υπηρεσιών. Στα δίκτυα 5G, η πολυπλοκότητα των πακέτων και η ποικιλία των πρωτοκόλλων που χρησιμοποιούνται τα καθιστούν ιδανικό στόχο για τέτοιου είδους επιθέσεις. Χρησιμοποιώντας ειδικά εργαλεία, όπως το Wireshark [24], οι επιτιθέμενοι μπορούν να αποκτήσουν λεπτομέρειες για τη διαμόρφωση του δικτύου και να εντοπίσουν ευάλωτα σημεία.

### 2.2.3 Επιθέσεις Man-in-the-Middle

Οι επιθέσεις MitM αποτελούν μια από τις πιο σοβαρές απειλές για τα δίκτυα 5G, καθώς επιτρέπουν στους επιτιθέμενους να παρεμβαίνουν στην επικοινωνία μεταξύ δύο μερών χωρίς την γνώση τους. Στόχος του επιτιθέμενου είναι να υποκλέψει, να τροποποιήσει ή να διαγράψει δεδομένα που ανταλλάσσονται, θέτοντας σε κίνδυνο την ασφάλεια και την εμπιστευτικότητα των πληροφοριών [25].

Οι επιθέσεις MitM πραγματοποιούνται μέσω της παραβίασης της εμπιστευτικής σύνδεσης σε διάφορα επίπεδα του δικτύου. Ο επιτιθέμενος μπορεί να αναλάβει ρόλο διαμεσολαβητή μεταξύ του εξοπλισμού χρήστη και του δικτύου, ανακατευθύνοντας τη ροή δεδομένων ή δημιουργώντας ψεύτικα σημεία πρόσβασης. Αυτές οι επιθέσεις είναι ιδιαίτερα επικίνδυνες στα δίκτυα 5G, λόγω του μεγάλου αριθμού συνδεδεμένων συσκευών και της πολυπλοκότητας των επικοινωνιών τους [26].

Οι πιο κοινές τεχνικές και τύποι επιθέσεων MitM περιλαμβάνουν:

- **ARP Spoofing**: Οι επιτιθέμενοι παραποιούν τις συσχετίσεις του Address Resolution Protocol (ARP), δηλαδή τον αντιστοιχισμό μεταξύ διευθύνσεων Internet Protocol (IP) και Media Access Control (MAC) στο επίπεδο Ethernet. Με αυτόν τον τρόπο, μπορούν να ανακατευθύνουν την κυκλοφορία δεδομένων μέσω της συσκευής τους ή να διακόψουν τη σύνδεση.

- **DNS Spoofing**: Οι κακόβουλοι χρήστες παραποιούν απαντήσεις του Domain Name System (DNS), ανακατευθύνοντας τους χρήστες σε ψεύτικες ιστοσελίδες ή κακόβουλους διακομιστές, χωρίς να το αντιλαμβάνονται.

- **Rogue Access Points**: Δημιουργούνται κακόβουλα σημεία ασύρματης πρόσβασης (Wi-Fi Access Points), τα οποία μιμούνται νόμιμα δίκτυα. Οι ανυποψίαστοι χρήστες συνδέονται σε αυτά, επιτρέποντας την υποκλοπή δεδομένων ή την εκμετάλλευση της σύνδεσής τους.

- **SSL Stripping**: Οι επιτιθέμενοι υποβαθμίζουν σκόπιμα μια ασφαλή σύνδεση Hyper-Text Transfer Protocol Secure (HTTPS) σε μη κρυπτογραφημένη σύνδεση HTTP. Αυτό τους επιτρέπει να υποκλέψουν δεδομένα που διαφορετικά θα μεταδίδονταν με ασφάλεια.

- **Packet Injection**: Οι επιτιθέμενοι εισάγουν κακόβουλα ή τροποποιημένα πακέτα δεδομένων μέσα στη ροή της επικοινωνίας μεταξύ δύο συσκευών. Με αυτόν τον τρόπο μπορούν να παραποιήσουν πληροφορίες ή να διακόψουν τη σύνδεση.

Συνεπώς, στα δίκτυα 5G, οι επιθέσεις MitM μπορούν να προκαλέσουν σημαντικές διαταραχές στη λειτουργικότητα και την ασφάλεια του συστήματος. Μέσω αυτών των επιθέσεων, οι επιτιθέμενοι αποκτούν πρόσβαση σε ευαίσθητες πληροφορίες, όπως διαπιστευτήρια χρηστών, κωδικούς πρόσβασης και δεδομένα σύνδεσης, απειλώντας την εμπιστευτικότητα της επικοινωνίας. Επιπλέον, έχουν τη δυνατότητα να τροποποιούν ή να διαγράφουν δεδομένα, υπονομεύοντας την ακρίβεια και την αξιοπιστία κρίσιμων υπηρεσιών. Οι πληροφορίες που αποκτώνται από τέτοιες επιθέσεις μπορούν επίσης να αξιοποιηθούν για τη διενέργεια πιο εκτεταμένων επιθέσεων, όπως οι DoS επιθέσεις, ενισχύοντας τις αρνητικές επιπτώσεις στην ασφάλεια και τη λειτουργικότητα του δικτύου.

### 2.2.4 Τρόποι Αντιμετώπισης Κυβερνοεπιθέσεων

Η προστασία των δικτύων 5G από κυβερνοεπιθέσεις αποτελεί βασική προτεραιότητα, δεδομένης της πολυπλοκότητας και του εύρους των απειλών που συνοδεύουν αυτή την τεχνολογία. Ενδεικτικά, επιθέσεις όπως αυτές που αναλύσαμε προηγουμένως, όπως οι DoS/DDoS, οι MitM και οι αναγνωριστικές επιθέσεις, είναι από τις πιο διαδεδομένες και έχουν τη δυνατότητα να διαταράξουν σημαντικά τη λειτουργικότητα και την ασφάλεια του δικτύου, αναδεικνύοντας την ανάγκη εφαρμογής αποτελεσματικών στρατηγικών προστασίας [27].

Η ασφάλεια των επικοινωνιών διαδραματίζει κεντρικό ρόλο στην αποτροπή υποκλοπών και στην προστασία της ακεραιότητας των δεδομένων. Η χρήση κρυπτογράφησης μέσω των πρωτοκόλλων HTTPS και TLS, και η εφαρμογή μεθόδων πιστοποίησης εξασφαλίζουν την εμπιστευτικότητα της ανταλλαγής δεδομένων. Επιπλέον, η περιορισμένη πρόσβαση σε κρίσιμες υποδομές μέσω κατάλληλων μέτρων, όπως τα τείχη προστασίας, μειώνει τις πιθανότητες επιτυχούς επίθεσης.

Παράλληλα, τα συστήματα που ανιχνεύουν και αποτρέπουν ύποπτη δραστηριότητα είναι ζωτικής σημασίας για την αποτελεσματική προστασία του δικτύου. Η συνεχής παρακολούθηση της δικτυακής δραστηριότητας και η εφαρμογή τεχνολογιών ανάλυσης δεδομένων επιτρέπουν την έγκαιρη αναγνώριση ανωμαλιών και την άμεση αντίδραση σε ενδεχόμενες απειλές. Καθώς οι επιθέσεις εξελίσσονται, η ενσωμάτωση μέτρων ασφαλείας από τη φάση σχεδιασμού των δικτύων αποτελεί κρίσιμη στρατηγική για την ανθεκτικότητα του συστήματος [28].

Η ανάγκη για συνεχώς βελτιούμενα μέτρα προστασίας καθιστά σαφές ότι η ανίχνευση επιθέσεων και η πρόληψή τους δεν μπορούν να βασίζονται αποκλειστικά σε στατικά μέτρα ασφαλείας. Η χρήση έξυπνων συστημάτων, όπως τα IDS, αναδεικνύεται ως βασικό εργαλείο για την προστασία των δικτύων 5G. Με έμφαση στις δυνατότητες ακριβούς και ταχείας ανίχνευσης, αυτά τα συστήματα αποτελούν το επόμενο κρίσιμο βήμα για τη διασφάλιση της σταθερότητας, της αξιοπιστίας και της ασφάλειας των υπηρεσιών τους. Η παρούσα εργασία επικεντρώνεται στη διερεύνηση και ανάπτυξη ενός τέτοιου συστήματος, ειδικά προσαρμοσμένου στις μοναδικές απαιτήσεις των δικτύων 5G [29].

### 2.2.5 Συστήματα Ανίχνευσης Εισβολής

Τα ΙΔΣ αναλύουν διάφορα περιβάλλοντα για τον εντοπισμό κακόβουλων δραστηριοτήτων, διαχωρίζοντάς τες από κανονικές και επιθυμητές συμπεριφορές. Υπάρχουν δύο κύριες μέθοδοι ανίχνευσης ανωμαλιών: η ανίχνευση βάσει υπογραφών (signature-based) και η ανίχνευση ανωμαλιών (anomaly-based). Τα συστήματα βάσει υπογραφών συγκρίνουν τις δραστηριότητες με προκαθορισμένα μοτίβα, αλλά αδυνατούν να εντοπίσουν άγνωστες επιθέσεις. Από την άλλη, τα συστήματα ανίχνευσης ανωμαλιών επικεντρώνονται στην ανίχνευση επιθέσεων zero-day, βασισμένα σε πρότυπα συμπεριφοράς. Ενώ και οι δύο μέθοδοι χρησιμοποιούν μηχανική μάθηση εδώ και χρόνια, οι περιορισμοί στα ποσοστά ανίχνευσης έχουν στρέψει την έρευνα σε μοντέλα βαθιάς μάθησης [30].

Μια άλλη κατηγοριοποίηση των IDS βασίζεται στο περιβάλλον που παρακολουθείται. Τα Host-based IDS εγκαθίστανται σε hosts και ειδοποιούν τους χρήστες για προβλήματα, ενώ τα Network Intrusion Detection Systems (NIDS) επικεντρώνονται στην παρακολούθηση της κυκλοφορίας δικτύου. Τα NIDS τοποθετούνται σε στρατηγικά σημεία, και παρακολουθούν εισερχόμενα και εξερχόμενα πακέτα. Αναλύουν αντίγραφα της κυκλοφορίας για να διασφαλιστεί ότι τα έγκυρα πακέτα δεν επιβραδύνονται, καθιστώντας τα ιδανικά για την ανίχνευση κακόβουλων δραστηριοτήτων σε πραγματικό χρόνο [31].

## 2.3 Μηχανική Μάθηση

### 2.3.1 Εισαγωγή

Η Μηχανική Μάθηση (Machine Learning (ML)) αποτελεί έναν από τους βασικούς κλάδους της Τεχνητής Νοημοσύνης (Artificial Intelligence (AI)), εστιάζοντας στην ανάπτυξη αλγορίθμων που έχουν τη δυνατότητα να μαθαίνουν και να βελτιώνονται μέσω της ανάλυσης δεδομένων, χωρίς να απαιτείται ρητός προγραμματισμός. Ο κύριος στόχος της είναι η ανάπτυξη μοντέλων που μπορούν να αναγνωρίζουν μοτίβα, να πραγματοποιούν προβλέψεις και να υποστηρίζουν τη λήψη αποφάσεων με αυτοματοποιημένο τρόπο [32].

Η αξιοποίηση της Μηχανικής Μάθησης εκτείνεται σε ένα ευρύ φάσμα εφαρμογών, από την υγειονομική περίθαλψη (π.χ. διάγνωση ασθενειών μέσω ανάλυσης ιατρικών εικόνων) και τα χρηματοοικονομικά (π.χ. πρόβλεψη τάσεων αγοράς) έως τον τομέα της ενέργειας (π.χ. βελτιστοποίηση κατανάλωσης πόρων) και την ασφάλεια δικτύων, όπου συμβάλλει στην ανίχνευση ανωμαλιών και κακόβουλων δραστηριοτήτων [33], [34].

Στο πλαίσιο αυτής της διατριβής, η Μηχανική Μάθηση είναι ιδιαίτερα σχετική καθώς αξιοποιείται για την ανίχνευση ανωμαλιών και εισβολών σε περιβάλλοντα δικτύων 5G και IoT. Τα συστήματα αυτά, λόγω του αυξημένου όγκου δεδομένων και της πολυπλοκότητας των σύγχρονων δικτύων, απαιτούν ισχυρούς αλγορίθμους που μπορούν να διακρίνουν μεταξύ κανονικής και κακόβουλης δραστηριότητας με υψηλή ακρίβεια [35].

Για να κατανοήσουμε πλήρως τη σημασία της Μηχανικής Μάθησης στη συγκεκριμένη μελέτη, είναι απαραίτητο να εξετάσουμε τις βασικές αρχές και έννοιές της, καθώς και τις διαφορές μεταξύ των κύριων κατηγοριών της, που θα παρουσιαστούν στην επόμενη ενότητα.

### 2.3.2 Βασικές έννοιες και αρχές Μηχανικής Μάθησης

Η μηχανική μάθηση στηρίζεται στην ικανότητα ενός υπολογιστικού συστήματος να μαθαίνει αυτόνομα, δηλαδή να βελτιώνει την απόδοσή του χωρίς ανθρώπινη παρέμβαση. Η διαδικασία αυτή ξεκινά από την παροχή κατάλληλων δεδομένων εισόδου (training data), τα οποία μπορεί να περιλαμβάνουν ετικέτες που υποδεικνύουν σε ποια κατηγορία ανήκει το κάθε δείγμα. Η παρουσία ετικετών εξαρτάται από τον τύπο μάθησης που χρησιμοποιείται—για παράδειγμα, η επιβλεπόμενη μάθηση (supervised learning) βασίζεται σε δεδομένα με ετικέτες, ενώ η μη επιβλεπόμενη μάθηση (unsupervised learning) λειτουργεί χωρίς αυτές. Στη συνέχεια, ένας αλγόριθμος μάθησης εκτελείται σε επαναληπτικές φάσεις, προσαρμόζοντας σταδιακά τις παραμέτρους του ώστε να δημιουργήσει ένα μοντέλο ικανό να εξάγει χρήσιμα συμπεράσματα ή να πραγματοποιεί προβλέψεις [36].

Σημαντικό ρόλο στη διαδικασία αυτή διαδραματίζουν τα χαρακτηριστικά (features), δηλαδή οι μετρήσιμες ποσότητες που περιγράφουν τα δεδομένα. Τα χαρακτηριστικά μπορούν να είναι αριθμητικά (numeric) ή κατηγοριοποιημένα (categorical), και η επιλογή τους επηρεάζει άμεσα την απόδοση του μοντέλου. Οι αλγόριθμοι μάθησης χρησιμοποιούν αυτά τα χαρακτηριστικά για να εντοπίσουν πρότυπα και σχέσεις στα δεδομένα. Για παράδειγμα, οι αλγόριθμοι δέντρων αποφάσεων (decision trees) μπορούν να διαχειριστούν και τους δύο τύπους χαρακτηριστικών, ενώ αλγόριθμοι όπως η γραμμική παλινδρόμηση (linear regression) απαιτούν αποκλειστικά αριθμητικά δεδομένα. Ο συνδυασμός αυτών των χαρακτηριστικών δημιουργεί διανύσματα χαρακτηριστικών (feature vectors), τα οποία σχηματίζουν τον συνολικό χώρο χαρακτηριστικών (feature space) στον οποίο λειτουργούν τα μοντέλα μάθησης.

Μία από τις βασικές προκλήσεις της μηχανικής μάθησης είναι η αποτελεσματική διαχείριση του αριθμού των χαρακτηριστικών,καθώς η παρουσία πολλών χαρακτηριστικών δεν συνεπάγεται απαραίτητα καλύτερη απόδοση. Σε πολλές περιπτώσεις, ορισμένα από τα χαρακτηριστικά μπορεί να είναι περιττά ή να μην συνεισφέρουν στην ακρίβεια του μοντέλου, οδηγώντας σε αυξημένο χρόνο εκπαίδευσης και ενδεχομένως σε χαμηλότερη ακρίβεια. Το φαινόμενο αυτό είναι γνωστό ως curse of dimensionality [37]. Για την αντιμετώπιση αυτού του προβλήματος, χρησιμοποιούνται τεχνικές μείωσης διαστάσεων, όπως η Ανάλυση Κύριων Συνιστωσών (Principal Component Analysis (PCA) [38], οι οποίες επιτρέπουν τη συμπίεση του χώρου χαρακτηριστικών χωρίς σημαντική απώλεια πληροφορίας. Με τον τρόπο αυτό, η διαδικασία μάθησης γίνεται πιο αποδοτική και το τελικό μοντέλο μπορεί να επιτύχει υψηλότερη ακρίβεια.

Με την κατανόηση των βασικών αρχών της Μηχανικής Μάθησης, μπορούμε πλέον να εξετάσουμε τις κύριες κατηγορίες της και τον ρόλο που διαδραματίζουν στην επίλυση σύνθετων προβλημάτων σε διάφορους τομείς εφαρμογής.

### 2.3.3 Κατηγοριές Μηχανικής Μάθησης

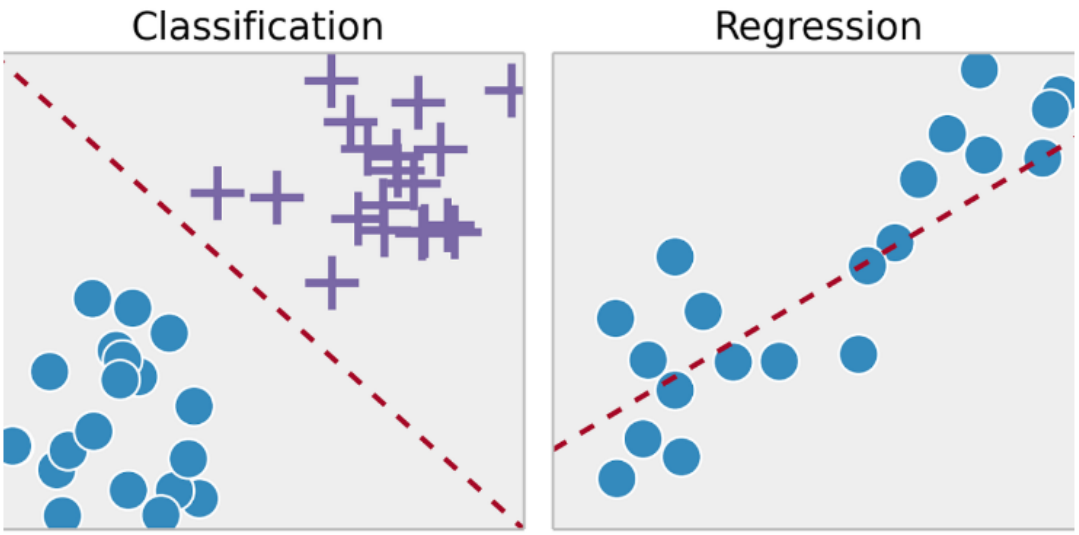
Τα συστήματα μηχανικής μάθησης διακρίνονται σε διαφορετικές κατηγορίες, ανάλογα με την παρουσία ή απουσία ανθρώπινης επίβλεψης κατά τη διαδικασία εκπαίδευσης. Επιπλέον, η ταξινόμηση των συστημάτων μπορεί να βασιστεί σε κριτήρια όπως η ικανότητά τους να ανιχνεύουν μοτίβα στα δεδομένα και να δημιουργούν προβλεπτικά μοντέλα. Στη συνέχεια, παρουσιάζονται οι κύριες κατηγορίες της Μηχανικής Μάθησης και ο ρόλος τους στην ανάλυση δεδομένων.

### Επιβλεπόμενη Μάθηση (Supervised Learning)

Η επιβλεπόμενη μάθηση βασίζεται στη χρήση δεδομένων που περιλαμβάνουν προκαθορισμένες ετικέτες (labels), επιτρέποντας στο μοντέλο να μάθει από γνωστά παραδείγματα. Κατά τη διάρκεια της εκπαίδευσης, ο αλγόριθμος αναπτύσσει τη δυνατότητα να συνδέει τα χαρακτηριστικά των δεδομένων με τις αντίστοιχες ετικέτες, με στόχο να πραγματοποιεί ακριβείς προβλέψεις σε νέα, άγνωστα δεδομένα [39]. Οι εφαρμογές της επιβλεπόμενης μάθησης περιλαμβάνουν δύο βασικούς τύπους:

- **Ταξινόμηση (Classification):** Στην πρώτη περίπτωση, ο αλγόριθμος λαμβάνει δεδομένα ταξινομημένα σε διακριτές κατηγορίες και, μετά την εκπαίδευση, μπορεί να προβλέπει την κατηγορία νέων δεδομένων. Για παράδειγμα, η αναγνώριση εικόνων χρησιμοποιεί ταξινόμηση για να αναγνωρίσει αντικείμενα σε φωτογραφίες [40].
- **Παλινδρόμηση (Regression):** Στην παλινδρόμηση, το σύστημα προβλέπει συνεχείς αριθμητικές τιμές αντί για διακριτές κατηγορίες. Για παράδειγμα, η πρόβλεψη των τιμών κατοικιών βασίζεται σε δεδομένα όπως η τοποθεσία και το μέγεθος του ακινήτου [41].

Ορισμένοι αλγόριθμοι, όπως η λογιστική παλινδρόμηση (Logistic Regression), γεφυρώνουν το χάσμα μεταξύ των δύο κατηγοριών, καθώς μπορούν να χρησιμοποιηθούν τόσο για προβλήματα ταξινόμησης όσο και για την εκτίμηση πιθανοτήτων.



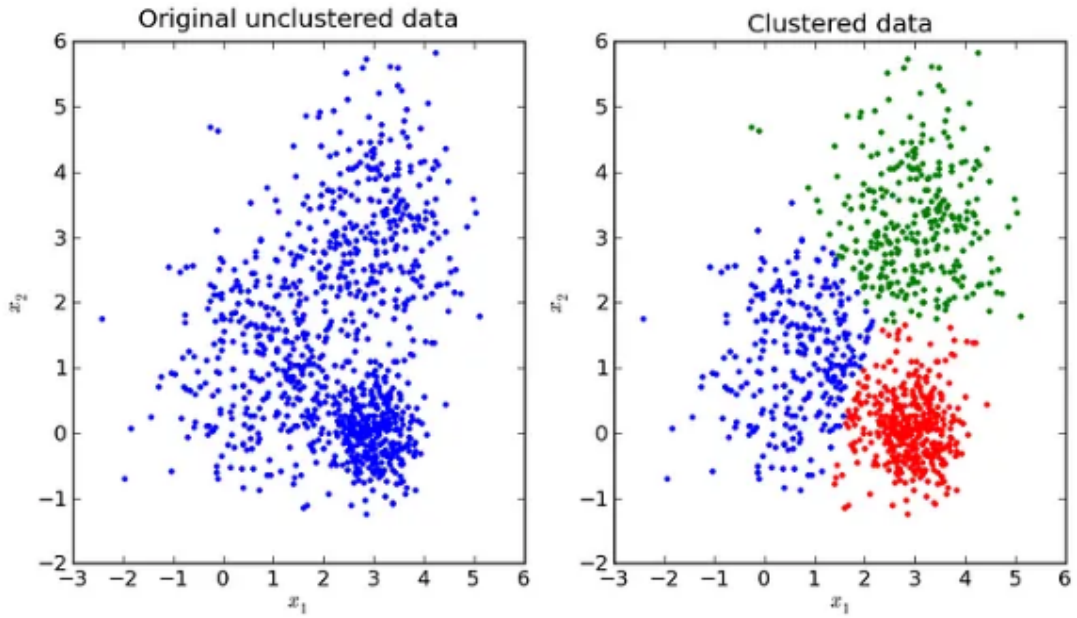

Σχήμα 2.3: *Παραδείγματα Ταξινόμησης και Παλινδρόμησης [3]*

### Μη-Επιβλεπόμενη Μάθηση (Unsupervised Learning)

Σε αντίθεση με την επιβλεπόμενη μάθηση, η μη-επιβλεπόμενη μάθηση λειτουργεί χωρίς την ύπαρξη ετικετών στα δεδομένα εκπαίδευσης. Ο στόχος είναι η ανίχνευση κρυφών μοτίβων εντός των δεδομένων και η κατηγοριοποίηση των δεδομένων σε ομάδες (clusters), βάσει των ομοιοτήτων τους. [42]. Οι πιο συχνά χρησιμοποιούμενοι αλγόριθμοι στη μη-επιβλεπόμενη μάθηση περιλαμβάνουν:

- **Ομαδοποίηση (Clustering):** Τεχνικές όπως ο αλγόριθμος K-Means χωρίζουν τα δεδομένα σε ομάδες βάσει της ομοιότητας των χαρακτηριστικών τους [43].
- **Ανίχνευση ανωμαλιών (Anomaly Detection):** Εφαρμόζεται για την εντόπιση δεδομένων που αποκλίνουν σημαντικά από το σύνολο, όπως στην ανίχνευση ύποπτων συναλλαγών σε χρηματοοικονομικές εφαρμογές [44].
- **Μείωση διαστάσεων (Dimensionality Reduction):** Μέθοδοι όπως η PCA συμπιέζουν τα δεδομένα, διατηρώντας τις πιο σημαντικές πληροφορίες [45].

Η μη-επιβλεπόμενη μάθηση είναι ιδανική για τη διερεύνηση σύνθετων δεδομένων, ειδικά σε περιπτώσεις όπου δεν υπάρχουν προκαθορισμένες κατηγορίες ή ετικέτες.




Σχήμα 2.4: *Παραδείγματα Δεδομένων στη Μη-Επιβλεπόμενη Μάθηση. Αριστερά: Ακατηγοριοποίητα δεδομένα (Unclustered Data). Δεξιά: Δεδομένα που έχουν ομαδοποιηθεί σε ομάδες (Clustered Data) μέσω αλγορίθμου ομαδοποίησης [4]*

### Ενισχυτική Μάθηση (Reinforcement Learning)

Η ενισχυτική μάθηση είναι μια διαφορετική προσέγγιση, όπου ένα σύστημα, γνωστό και ως πράκτορας, μαθαίνει μέσω αλληλεπίδρασης με το περιβάλλον του. Οι αποφάσεις που λαμβάνει αξιολογούνται μέσω ανταμοιβών ή ποινών, και μέσω αυτής της διαδικασίας ο πράκτορας βελτιστοποιεί τις ενέργειές του για να επιτύχει έναν συγκεκριμένο στόχο. Μερικές εφαρμογές της ενισχυτικής μάθησης περιλαμβάνουν τα αυτόνομα οχήματα, ρομποτική και στρατηγικά παιχνίδια [46].

### Άλλες Μέθοδοι Μάθησης

Εκτός από τις κύριες κατηγορίες Μηχανικής Μάθησης, υπάρχουν και άλλες μορφές μάθησης, όπως η ημι-επιβλεπόμενη μάθηση (semi-supervised learning), όπου μόνο ένα μέρος των

δεδομένων περιέχει ετικέτες, συνδυάζοντας τα χαρακτηριστικά της επιβλεπόμενης και μη-επιβλεπόμενης μάθησης. Αυτές οι μέθοδοι είναι ιδιαίτερα χρήσιμες σε περιπτώσεις όπου η σήμανση δεδομένων είναι κοστοβόρα ή χρονοβόρα.

### 2.3.4 Επιλογή Χαρακτηριστικών

Η επιλογή χαρακτηριστικών (Feature Selection) αποτελεί ένα κρίσιμο βήμα στη διαδικασία προεπεξεργασίας δεδομένων στη Μηχανική Μάθηση, καθώς επηρεάζει άμεσα την απόδοση, την υπολογιστική αποδοτικότητα και τη γενικευσιμότητα των μοντέλων. Στόχος είναι η διατήρηση των πιο σχετικών χαρακτηριστικών, μειώνοντας ταυτόχρονα τον όγκο των δεδομένων και αποφεύγοντας την εισαγωγή μη χρήσιμης ή πλεονάζουσας πληροφορίας.

Κατά τη διαδικασία επιλογής χαρακτηριστικών, η ύπαρξη μεγάλου αριθμού μεταβλητών μπορεί να οδηγήσει σε υπερπροσαρμογή (overfitting), αυξημένο υπολογιστικό κόστος και δυσκολία στην ερμηνεία των αποτελεσμάτων. Επομένως, η αφαίρεση άσχετων ή ιδιαίτερα συσχετισμένων μεταβλητών βελτιώνει την ικανότητα των μοντέλων να μάθουν ουσιώδη μοτίβα χωρίς να προσαρμόζονται υπερβολικά στις ιδιαιτερότητες των δεδομένων εκπαίδευσης [47].

Παρακάτω, περιγράφουμε τις τρεις βασικές μεθόδους επιλογής χαρακτηριστικών, κάθε μία από τις οποίες εφαρμόζει διαφορετική προσέγγιση για τη διατήρηση των πιο σημαντικών μεταβλητών. Ανάλογα με τις ανάγκες της εκάστοτε εφαρμογής μηχανικής μάθησης, μπορούν να χρησιμοποιηθούν στατιστικές μέθοδοι, τεχνικές βελτιστοποίησης ή ενσωματωμένες προσεγγίσεις εντός των αλγορίθμων εκπαίδευσης.

#### Filter Methods

Αρχικά, η πιο διαδεδομένη μέθοδος επιλογής χαρακτηριστικών είναι η μέθοδος φιλτραρίσματος, η οποία χρησιμοποιεί στατιστικές τεχνικές για να αξιολογήσει την σημασία των χαρακτηριστικών, ανεξάρτητα από ποιο μοντέλο θα εφαρμοστεί. Η πιο συνηθισμένη τεχνική είναι ο Συντελεστής Συσχέτισης (Correlation Coefficient) [48], ο οποίος μετρά τη γραμμική σχέση μεταξύ δύο μεταβλητών. Για δύο μεταβλητές $X$ και $Y$, ο συντελεστής συσχέτισης υπολογίζεται ως εξής:

$$r_{X,Y} = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}} \tag{2.1}$$

όπου:

- $X_i$, $Y_i$ είναι οι παρατηρήσεις των μεταβλητών $X$ και $Y$,
- $\bar{X}$ και $\bar{Y}$ είναι οι μέσοι όροι των $X$ και $Y$ αντίστοιχα,
- $r_{X,Y}$ κυμαίνεται από $-1$ (τέλεια αρνητική συσχέτιση) έως 1 (τέλεια θετική συσχέτιση).

Τα χαρακτηριστικά με χαμηλό απόλυτο συντελεστή συσχέτισης απορρίπτονται, ενώ αυτά με ισχυρή συσχέτιση διατηρούνται.

#### Wrapper Methods

Μια ακόμη προσέγγιση για την επιλογή χαρακτηριστικών είναι οι μεθόδοι Wrapper οι οποίοι επιλέγουν υποσύνολα χαρακτηριστικών με βάση την απόδοση ενός μοντέλου μηχανικής

μάθησης. Τα χαρακτηριστικά που συμβάλλουν στην καλύτερη απόδοση διατηρούνται, ενώ τα λιγότερο σημαντικά απορρίπτονται. Μεταξύ των πιο διαδεδομένων τεχνικών αυτής της κατηγορίας περιλαμβάνονται οι αλγόριθμοι (Genetic Algorithms - GA) και BPSO (Binary Particle Swarm Optimization), οι οποίοι χρησιμοποιούν στοχαστικές διαδικασίες βελτιστοποίησης για την επιλογή του βέλτιστου υποσυνόλου χαρακτηριστικών. Ο BPSO, συγκεκριμένα, προσομοιώνει τη συμπεριφορά ενός πληθυσμού ¨σωματιδίων' που κινούνται σε έναν δυαδικό χώρο αναζήτησης, διερευνώντας διαφορετικούς συνδυασμούς χαρακτηριστικών, με στόχο τη βελτίωση της απόδοσης του μοντέλου [49].

Στο BPSO, κάθε ¨σωματίδιο' αντιπροσωπεύει ένα υποψήφιο υποσύνολο χαρακτηριστικών ως ένα δυαδικό διάνυσμα $X = [x_1, x_2, \ldots, x_d]$, όπου $x_i \in \{0, 1\}$ δηλώνει την επιλογή ή όχι του χαρακτηριστικού $i$. Η ταχύτητα του σωματιδίου $V = [v_1, v_2, \ldots, v_d]$ επηρεάζει την πιθανότητα αλλαγής της κατάστασης κάθε $x_i$.

Η επικαιροποίηση της ταχύτητας και της θέσης γίνεται ως εξής:

$$v_i^{t+1} = wv_i^t + c_1 r_1 (pbest_i - x_i^t) + c_2 r_2 (gbest_i - x_i^t) \tag{2.2}$$

$$x_i^{t+1} = \begin{cases} 1, & \text{if } \sigma(v_i^{t+1}) > r_3 \\ 0, & \text{otherwise} \end{cases} \tag{2.3}$$

όπου:

- $w$ είναι ο συντελεστής αδράνειας,
- $c_1$, $c_2$ οι συντελεστές γνωστικής και κοινωνικής συνιστώσας,
- $r_1$, $r_2$, $r_3$ τυχαίοι αριθμοί στο διάστημα $[0, 1]$,
- $pbest_i$ η καλύτερη προηγούμενη θέση του σωματιδίου,
- $gbest_i$ η καλύτερη θέση του σμήνους,
- $\sigma(v)$ η συνάρτηση σιγμοειδούς:

$$\sigma(v) = \frac{1}{1 + e^{-v}} \tag{2.4}$$

**Embedded Methods**

Σε αντίθεση με τις προηγούμενες μεθόδους, οι ενσωματωμένες μέθοδοι επιλέγουν τα σημαντικά χαρακτηριστικά κατά την εκπαίδευση του μοντέλου. Για παράδειγμα, το μοντέλο Random Forest υπολογίζει τη σχετική σημασία κάθε χαρακτηριστικού βάσει της συμβολής του στη λήψη αποφάσεων, επιτρέποντας την αφαίρεση μη σημαντικών μεταβλητών. Αντίστοιχα, η Lasso Regression εφαρμόζει κανονικοποίηση, οδηγώντας στη μηδενική τιμή των συντελεστών των λιγότερο σημαντικών χαρακτηριστικών, αποκλείοντάς τα από το μοντέλο. Σε σύγκριση με τις μεθόδους φιλτραρίσματος, οι ενσωματωμένες μέθοδοι λαμβάνουν υπόψη την αλληλεπίδραση μεταξύ των χαρακτηριστικών, ενώ ταυτόχρονα είναι πιο αποδοτικές από τις wrapper

methods, καθώς δεν απαιτούν την εκπαίδευση πολλαπλών μοντέλων για τη δοκιμή διαφορετικών συνδυασμών χαρακτηριστικών [50].

### 2.3.5 Παραδοσιακά Μοντέλα Μηχανικής Μάθησης

Αφού γίνει η επιλογή των κατάλληλων χαρακτηριστικών, το επόμενο στάδιο στη διαδικασία της μηχανικής μάθησης είναι η επιλογή του μοντέλου που θα χρησιμοποιηθεί για την ανάλυση και την πρόβλεψη. Τα παραδοσιακά μοντέλα μηχανικής μάθησης έχουν αποτελέσει τη βάση για πολλές εφαρμογές, προσφέροντας αποδοτικές και ερμηνεύσιμες λύσεις σε προβλήματα ταξινόμησης, παλινδρόμησης και ανίχνευσης ανωμαλιών.

Τα μοντέλα αυτά χαρακτηρίζονται από τη χρήση μαθηματικών και στατιστικών τεχνικών για την εύρεση σχέσεων στα δεδομένα. Αν και η απόδοσή τους μπορεί να επηρεαστεί από την πολυπλοκότητα των δεδομένων και την ποιότητα των χαρακτηριστικών, παραμένουν ιδιαίτερα χρήσιμα λόγω της χαμηλής υπολογιστικής απαίτησης και της δυνατότητας ερμηνείας των αποφάσεων. Παρακάτω περιγράφονται οι πιο συνηθισμένες προσεγγίσεις στα παραδοσιακά μοντέλα μηχανικής μάθησης [51].

#### Δέντρα Απόφασεων

Τα δέντρα απόφασης είναι ένα από τα πιο δημοφιλή μοντέλα μηχανικής μάθησης, λόγω της απλότητάς τους και της ικανότητάς τους να διαχειρίζονται τόσο κατηγορικά όσο και αριθμητικά δεδομένα. Η διαδικασία εκμάθησης βασίζεται στη διάσπαση των δεδομένων σε υποσύνολα μέσω διαδοχικών αποφάσεων, σχηματίζοντας μια δενδροειδή δομή. Το αποτέλεσμα είναι ένα μοντέλο που μπορεί να ερμηνευθεί εύκολα και να εξηγήσει τις αποφάσεις του. Ωστόσο, τα δέντρα απόφασης είναι επιρρεπή σε υπερπροσαρμογή, ειδικά όταν έχουν μεγάλο βάθος [52].

#### Random Forests

Ένα άλλο μοντέλο είναι το Random Forest το οποίο αποτελεί μια εξέλιξη των δέντρων απόφασης, καθώς βασίζονται στη δημιουργία πολλαπλών ανεξάρτητων δέντρων, των οποίων οι προβλέψεις συνδυάζονται για την εξαγωγή του τελικού αποτελέσματος. Η χρήση πολλαπλών δέντρων μειώνει την πιθανότητα υπερπροσαρμογής και βελτιώνει τη γενίκευση του μοντέλου. Επιπλέον, το Random Forest παρέχει ενδείξεις για τη σημαντικότητα των χαρακτηριστικών, διευκολύνοντας την επιλογή των πιο σχετικών μεταβλητών [53].

#### Support Vector Machines - SVMs

Οι μηχανές διανυσμάτων υποστήριξης (SVMs) είναι μοντέλα ταξινόμησης που βασίζονται στη χρήση υπερεπιπέδων (hyperplanes) για το διαχωρισμό των δεδομένων σε διαφορετικές κατηγορίες. Η βασική ιδέα είναι να βρεθεί το υπερεπίπεδο που μεγιστοποιεί την απόσταση ανάμεσα στις κατηγορίες, προσφέροντας έτσι μεγαλύτερη ανθεκτικότητα σε θόρυβο και δεδομένα εκτός κατανομής. Τα SVMs είναι ιδιαίτερα χρήσιμα σε προβλήματα με μη γραμμικά όρια απόφασης, καθώς μπορούν να επεκταθούν μέσω πυρηνικών συναρτήσεων (kernel functions) [54].

#### Naïve Bayes

Το μοντέλο Naïve Bayes βασίζεται στο θεώρημα του Βαψες για την πρόβλεψη της πιθανότητας

εμφάνισης μιας κατηγορίας δεδομένης μιας συνθήκης. Υποθέτει ότι τα χαρακτηριστικά είναι ανεξάρτητα μεταξύ τους, κάτι που στις περισσότερες περιπτώσεις δεν ισχύει, αλλά παρά ταύτα προσφέρει ικανοποιητικά αποτελέσματα, ιδιαίτερα σε προβλήματα ταξινόμησης κειμένου και αναγνώρισης προτύπων. Η ευκολία εκπαίδευσης και η ταχύτητα επεξεργασίας το καθιστούν χρήσιμο για εφαρμογές πραγματικού χρόνου [55].

**k-Nearest Neighbors (k-NN)**

Ο αλγόριθμος k-NN είναι μια απλή αλλά ισχυρή μέθοδος ταξινόμησης και παλινδρόμησης, η οποία βασίζεται στη γειτνίαση των δεδομένων. Όταν ένα νέο δείγμα πρέπει να ταξινομηθεί, συγκρίνεται με τα κ πιο κοντινά του γειτονικά σημεία και κατατάσσεται στην κατηγορία που εμφανίζεται συχνότερα σε αυτά. Αν και το k-NN δεν απαιτεί εκπαίδευση, έχει υψηλό υπολογιστικό κόστος κατά την πρόβλεψη, καθώς απαιτεί τη σύγκριση κάθε νέου δείγματος με ολόκληρο το σύνολο δεδομένων [56].

Τα παραδοσιακά μοντέλα μηχανικής μάθησης συνεχίζουν να χρησιμοποιούνται ευρέως, καθώς προσφέρουν αποδοτικές και ερμηνεύσιμες λύσεις, ιδιαίτερα σε περιπτώσεις όπου η επεξηγησιμότητα είναι κρίσιμη. Παρόλο που οι μέθοδοι αυτές έχουν περιορισμούς σε πολύπλοκα δεδομένα, μπορούν να συνδυαστούν με πιο προηγμένες τεχνικές, όπως τα νευρωνικά δίκτυα, για τη δημιουργία υβριδικών συστημάτων που αξιοποιούν τα πλεονεκτήματα και των δύο προσεγγίσεων.

### 2.3.6 Νευρωνικά Δίκτυα

Τα νευρωνικά δίκτυα (Neural Networks - NNs) αποτελούν μια από τις πιο ισχυρές και ευέλικτες προσεγγίσεις στη μηχανική μάθηση, εμπνευσμένα από τη λειτουργία του ανθρώπινου εγκεφάλου. Σε αντίθεση με τα παραδοσιακά μοντέλα μηχανικής μάθησης, τα οποία συχνά βασίζονται σε αυστηρά καθορισμένους κανόνες ή στατιστικές υποθέσεις, τα νευρωνικά δίκτυα έχουν την ικανότητα να ανακαλύπτουν πολύπλοκα πρότυπα στα δεδομένα, ακόμα και όταν οι σχέσεις μεταξύ των μεταβλητών δεν είναι προφανείς [57].

**Βασική Δομή των Νευρωνικών Δικτύων**

Ένα τυπικό νευρωνικό δίκτυο αποτελείται από τρία βασικά είδη επιπέδων (layers):

- **Είσοδος (Input Layer):** Περιλαμβάνει τους νευρώνες που λαμβάνουν τα δεδομένα εισόδου και τα προωθούν στα επόμενα επίπεδα χωρίς να πραγματοποιούν υπολογισμούς. Ουσιαστικά, λειτουργεί ως σημείο εκκίνησης για τη ροή των δεδομένων.
- **Κρυφά Επίπεδα (Hidden Layers):** Τα ενδιάμεσα επίπεδα, στα οποία πραγματοποιούνται οι περισσότερες υπολογιστικές διαδικασίες μέσω γραμμικών και μη γραμμικών μετασχηματισμών. Σε κάθε νευρώνα εκτελείται η ακόλουθη πράξη:

$$z = \mathbf{w}^T \mathbf{x} + b \tag{2.5}$$

όπου:

  - $\mathbf{x}$ είναι το διάνυσμα εισόδου,

– $\mathbf{w}$ τα βάρη,

– $b$ η προκατάληψη (bias).

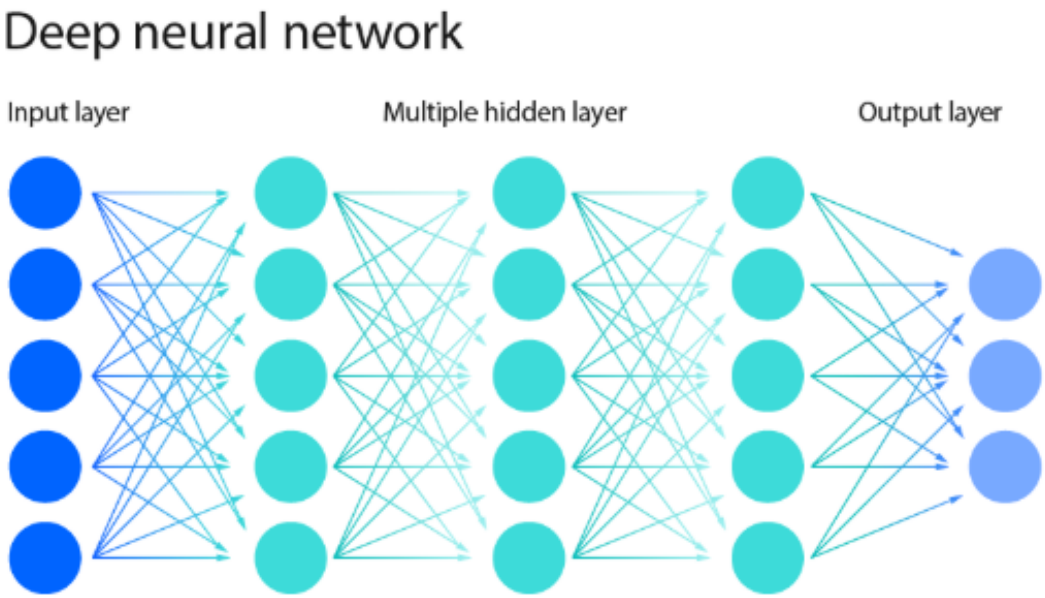
Αφού υπολογιστεί το $z$, εφαρμόζεται μια μη γραμμική συνάρτηση ενεργοποίησης (activation function) όπως η ReLU ή η Sigmoid για την εισαγωγή μη γραμμικότητας στο δίκτυο:

$$a = \phi(z) \tag{2.6}$$

Η έξοδος $a$ από κάθε νευρώνα λειτουργεί ως είσοδος για τους νευρώνες του επόμενου επιπέδου.

- **Έξοδος (Output Layer):** Το τελευταίο επίπεδο του δικτύου, το οποίο παράγει την τελική πρόβλεψη ή ταξινόμηση.

Στο παρακάτω διάγραμμα 2.5, απεικονίζεται η αρχιτεκτονική ενός νευρωνικού δικτύου:




Σχήμα 2.5: *Αναπαράσταση της βασικής δομής ενός νευρωνικού δικτύου [5]*

### Διαδικασία Εκπαίδευσης και Βελτιστοποίησης

Η εκπαίδευση ενός νευρωνικού δικτύου πραγματοποιείται μέσω αλγορίθμων βελτιστοποίησης, με πιο διαδεδομένη τη μέθοδο Backpropagation, όπου τα βάρη των συνδέσεων προσαρμόζονται σταδιακά για να μειωθεί το σφάλμα της πρόβλεψης. Ο πιο συνηθισμένος αλγόριθμος που χρησιμοποιείται για την ενημέρωση των βαρών είναι ο (Gradient Descent), καθώς και οι πιο εξελιγμένες παραλλαγές του, όπως:

- Stochastic Gradient Descent (SGD) [58]
- Adam Optimizer [59]

- RMSprop [60]

Η επιλογή της κατάλληλης μεθόδου εκπαίδευσης εξαρτάται από το μέγεθος του συνόλου δεδομένων, την πολυπλοκότητα του προβλήματος και την ανάγκη για γρήγορη σύγκλιση.

### Βασικοί Τύποι Νευρωνικών Δικτύων

Υπάρχουν διάφορες κατηγορίες νευρωνικών δικτύων, ανάλογα με την αρχιτεκτονική και τον τρόπο που επεξεργάζονται τα δεδομένα:

- **Πολυστρωματικά Αντιληπτικά (Multi-Layer Perceptrons (MLPs))**: Τα MLPs υλοποιούν την κλασική δομή νευρωνικών δικτύων, όπως περιγράφηκε παραπάνω, χρησιμοποιώντας πλήρως συνδεδεμένα επίπεδα. Κάθε νευρώνας ενός επιπέδου συνδέεται με όλους τους νευρώνες του επόμενου, και η υπολογιστική διαδικασία ακολουθεί τις βασικές σχέσεις (2.5), (2.6). Η απλότητά τους τα καθιστά κατάλληλα για προβλήματα παλινδρόμησης και ταξινόμησης, ωστόσο η απόδοσή τους περιορίζεται σε πολύπλοκα δεδομένα, όπως εικόνες ή ακολουθίες, όπου απαιτούνται εξειδικευμένες αρχιτεκτονικές [61].

- **Συνελικτικά Νευρωνικά Δίκτυα (Convolutional Neural Networks - CNNs):** Τα CNNs έχουν σχεδιαστεί για την ανάλυση δεδομένων με χωρική δομή, όπως εικόνες, αξιοποιώντας συνελικτικά φίλτρα (convolutional filters) για την εξαγωγή τοπικών χαρακτηριστικών. Η σύνδεση μεταξύ φίλτρου $K$ και είσόδου $I$ περιγράφεται από τη σχέση:

$$S(i,j) = (I * K)(i,j) = \sum_m \sum_n I(i+m, j+n) K(m,n) \tag{2.7}$$

  Παρόλο που τα CNNs διακρίνονται για την ικανότητά τους να εντοπίζουν πολύπλοκα πρότυπα και ιεραρχίες χαρακτηριστικών σε δεδομένα με χωρική δομή, απαιτούν σημαντικούς υπολογιστικούς πόρους και μεγάλα σύνολα δεδομένων για την αποφυγή υπερπροσαρμογής, γεγονός που τα καθιστά λιγότερο αποδοτικά σε προβλήματα μικρής κλίμακας ή χωρίς χωρικές συσχετίσεις [62].

- **Αναδρομικά Νευρωνικά Δίκτυα (Recurrent Neural Networks - RNNs):** Τα RNNs έχουν σχεδιαστεί για την επεξεργασία δεδομένων ακολουθίας, όπου η σειρά των στοιχείων έχει σημασία, όπως στην ανάλυση κειμένου, την πρόβλεψη χρονοσειρών και την αναγνώριση φωνής. Ενσωματώνουν πληροφορίες από προηγούμενες χρονικές στιγμές μέσω αναδρομικών συνδέσεων, επιτρέποντας στο δίκτυο να διατηρεί 'μνήμη' προηγούμενων καταστάσεων.

  Η βασική λειτουργία ενός RNN ορίζεται από την ακόλουθη εξίσωση:

$$h_t = \phi(W_h h_{t-1} + W_x x_t + b) \tag{2.8}$$

  όπου:

  – $h_t$ είναι η κρυφή κατάσταση στη χρονική στιγμή $t$,

- $h_{t-1}$ είναι η κρυφή κατάσταση της προηγούμενης χρονικής στιγμής,
- $x_t$ είναι η είσοδος στη χρονική στιγμή $t$,
- $W_h$ και $W_x$ είναι τα βάρη για την προηγούμενη κατάσταση και την τρέχουσα είσοδο αντίστοιχα,
- $b$ είναι το βιας,
- $\phi$ είναι η συνάρτηση ενεργοποίησης

Αν και τα RNNs είναι αποτελεσματικά στην ανάλυση ακολουθιών, παρουσιάζουν προβλήματα όπως το (vanishing και exploding gradient) κατά τη διαδικασία εκπαίδευσης. Το φαινόμενο vanishing προκαλεί τη σταδιακή μείωση των παραγώγων σε πολύ μικρές τιμές, με αποτέλεσμα το μοντέλο να αδυνατεί να μάθει μακροχρόνιες εξαρτήσεις. Από την άλλη, το exploding grdient οδηγεί σε πολύ μεγάλες τιμές παραγώγων, προκαλώντας αστάθεια και αριθμητικά σφάλματα κατά την εκπαίδευση. Για την αντιμετώπιση αυτών των ζητημάτων, αναπτύχθηκαν πιο εξελιγμένες αρχιτεκτονικές RNN, όπως τα Long Short-Term Memory (LSTM) και τα Gated Recurrent Units (GRU), τα οποία επιτρέπουν τη διατήρηση πληροφοριών για μεγαλύτερες ακολουθίες [63].

- **Νευρωνικά Δίκτυα Μετασχηματιστών (Transformers):** Οι Transformers εισήγαγαν μια επαναστατική προσέγγιση στην επεξεργασία ακολουθιακών δεδομένων, καταργώντας την ανάγκη για επαναληπτικές δομές όπως τα RNNs. Βασίζονται εξ ολοκλήρου σε Attention Mechanisms, οι οποίοι επιτρέπουν στο δίκτυο να εστιάζει σε σημαντικές πληροφορίες εντός της ακολουθίας, ανεξαρτήτως θέσης. Ο κεντρικός μηχανισμός είναι το Self-Attention, που υπολογίζεται μέσω της εξίσωσης:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{2.9}$$

όπου:

- $Q$ είναι οι ερωτήσεις (Queries),
- $K$ τα κλειδιά (Keys),
- $V$ οι τιμές (Values),
- και $d_k$ είναι η διάσταση των κλειδιών.

Η αρχιτεκτονική των Transformers επέτρεψε τη δημιουργία μοντέλων όπως το BERT [64] και το GPT [65], τα οποία έχουν επιτύχει εξαιρετικά αποτελέσματα σε καθήκοντα φυσικής γλώσσας και άλλες εφαρμογές ακολουθιακών δεδομένων. Παρόλο που είναι υπολογιστικά απαιτητικά, προσφέρουν εξαιρετική απόδοση και δυνατότητες παράλληλης επεξεργασίας.

Συγκριτικά με τα Παραδοσιακά Μοντέλα Μηχανικής Μάθησης, τα νευρωνικά δίκτυα προσφέρουν σημαντικά πλεονεκτήματα, ιδιαίτερα σε σύνθετα προβλήματα με μεγάλο όγκο δεδομένων. Ωστόσο, απαιτούν περισσότερους υπολογιστικούς πόρους, μεγαλύτερους χρόνους εκπαίδευσης και είναι πιο επιρρεπή σε υπερπροσαρμογή. Για τον λόγο αυτό, η χρήση τεχνικών

όπως η Κανονικοποίηση (Regularization) και η Ενίσχυση Δεδομένων (Data Augmentation) είναι συχνά απαραίτητη για τη βελτίωση της απόδοσης. Η εξέλιξή τους, ιδιαίτερα με τη χρήση βαθιάς μάθησης (Deep Learning), επιτρέπει τη δημιουργία ακόμη πιο αποδοτικών και ευέλικτων μοντέλων, καθιστώντας τα αναπόσπαστο κομμάτι των σύγχρονων προσεγγίσεων στη μηχανική μάθηση.

## 2.4 Federated Learning

### 2.4.1 Εισαγωγή

Το FL παρουσιάστηκε για πρώτη φορά από την Google πριν από περίπου μία δεκαετία [66], εισάγοντας μια καινοτόμο προσέγγιση στην εκπαίδευση μοντέλων Μηχανικής Μάθησης. Σε αντίθεση με τις παραδοσιακές μεθόδους, όπου τα δεδομένα συγκεντρώνονται σε έναν κεντρικό διακομιστή για την εκπαίδευση του μοντέλου, το FL επιτρέπει την εκπαίδευση να πραγματοποιείται τοπικά στις συσκευές ή στους κόμβους που κατέχουν τα δεδομένα. Αντί να μεταφέρονται τα ίδια τα δεδομένα, μόνο οι ενημερώσεις των μοντέλων (όπως τα βάρη και οι παράμετροι) αποστέλλονται σε έναν κεντρικό διακομιστή για συγχώνευση.

Αυτή η αποκεντρωμένη προσέγγιση ανταποκρίνεται σε κρίσιμες ανησυχίες που σχετίζονται με την ιδιωτικότητα των δεδομένων και την ασφάλεια, μειώνοντας παράλληλα τον επικοινωνιακό φόρτο και το κόστος μεταφοράς δεδομένων μέσω δικτύου [67]. Ειδικά σε περιβάλλοντα όπου τα δεδομένα είναι ευαίσθητα (π.χ., στον τομέα της υγείας ή των οικονομικών), το FL προσφέρει ένα πλαίσιο όπου τα δεδομένα παραμένουν τοπικά, διασφαλίζοντας τη συμμόρφωση με κανονισμούς όπως το General Data Protection Regulation (GDPR).

Από την αρχική του σύλληψη, το FL έχει εξελιχθεί σε μία από τις πιο υποσχόμενες τεχνολογίες για τη διαχείριση μεγάλων, ετερογενών και κατανεμημένων συνόλων δεδομένων. Έχει βρει εφαρμογή σε ποικίλους τομείς, όπως:

- Δκτυα 5G και IoT, όπου η τοπική επεξεργασία μειώνει την καθυστέρηση και τον φόρτο δικτύου.
- Υγειονομικές υπηρεσίες, όπου η ανάλυση των ευαίσθητων δεδομένων των ασθενών πραγματοποιείται χωρίς να παραβιάζεται η ιδιωτικότητα τους.
- Βιομηχανικά συστήματα και χρηματοοικονομικές υπηρεσίες, όπου η διατήρηση της ασφάλειας και η μείωση του λειτουργικού κόστους είναι καθοριστικής σημασίας.

Παρά τα πλεονεκτήματά του FL, παρουσιάζονται και σημαντικές προκλήσεις. Η διαχείριση μη ομοιογενών δεδομένων (Non-Independent and Identically Distributed (non-IID) data), οι αυξημένες απαιτήσεις σε υπολογιστικούς πόρους και η αντιμετώπιση ζητημάτων ασφάλειας, όπως επιθέσεις poisoning και eavesdropping [68], καθιστούν την υλοποίηση και τη βελτιστοποίησή του πολύπλοκη διαδικασία [69]. Αυτές οι προκλήσεις καθιστούν αναγκαία την ανάπτυξη βελτιωμένων αλγορίθμων συγκέντρωσης και πρωτοκόλλων ασφαλείας, τα οποία θα εξετάσουμε στα επόμενα τμήματα.

### 2.4.2 Πλεονεκτήματα του Federated Learning

Το FL αποτελεί μια επαναστατική προσέγγιση στη μηχανική μάθηση, προσφέροντας πολυάριθμα πλεονεκτήματα σε περιβάλλοντα με κατανεμημένα δεδομένα και αυξημένες απαιτήσεις

για την ασφάλεια, ιδιωτικότητα και απόδοση.

Ένα από τα κύρια χαρακτηριστικά του FL είναι η διατήρηση της ιδιωτικότητας, καθώς τα δεδομένα παραμένουν τοπικά στις συσκευές και μόνο οι ενημερώσεις του μοντέλου κοινοποιούνται. Αυτή η προσέγγιση εξασφαλίζει τη συμμόρφωση με αυστηρούς κανονισμούς προστασίας δεδομένων, όπως το GDPR, γεγονός που καθιστά το FL ιδιαίτερα κατάλληλο για τομείς όπως η υγεία και τα χρηματοοικονομικά.

Η αποκεντρωμένη φύση του FL επιτρέπει τη διαχείριση ετερογενών δεδομένων, διατηρώντας την ακρίβεια των μοντέλων ακόμη και σε περιβάλλοντα όπου οι κατανομές μεταξύ των κόμβων δεν είναι ομοιογενείς. Επιπλέον, υποστηρίζει κατανεμημένες αρχιτεκτονικές, μειώνοντας την εξάρτηση από κεντρικούς διακομιστές και τον κίνδυνο αποτυχίας λόγω μονοσήμαντων σημείων αποτυχίας. Η ανθεκτικότητα αυτή ενισχύεται περαιτέρω από την ικανότητα του να παραμένει λειτουργικό σε περιπτώσεις προσωρινής αποσύνδεσης κόμβων, καθιστώντας το ιδανικό για δίκτυα με περιορισμένη ή ασυνεχή συνδεσιμότητα [70].

Ένα ακόμη βασικό πλεονέκτημα είναι η δυνατότητα κλιμάκωσής του. Μπορεί να ενσωματώσει εκατομμύρια συσκευές, από smartphones έως συσκευές IoT, εξασφαλίζοντας αξιόπιστη εκπαίδευση μοντέλων σε μεγάλης κλίμακας κατανεμημένα δίκτυα. Αυτή η κλιμάκωση συμπληρώνεται από την ενεργειακή αποδοτικότητα, καθώς το FL ελαχιστοποιεί την ανάγκη μετάδοσης μεγάλων συνόλων δεδομένων, κάτι που είναι κρίσιμο για συσκευές με περιορισμένη ενέργεια, όπως οι αισθητήρες IoT και Edge Devices, όπως μικροελεγκτές ή φορητές συσκευές. Επιπλέον, μειώνει το κόστος επικοινωνίας, μεταφέροντας μόνο παραμέτρους του μοντέλου αντί για ολόκληρα σύνολα δεδομένων, καθιστώντας το κατάλληλο για περιβάλλοντα με χαμηλό εύρος ζώνης [71].

Η προώθηση συνεργασίας μεταξύ οργανισμών αποτελεί ακόμα ένα πλεονέκτημα, καθώς το FL επιτρέπει σε διαφορετικούς οργανισμούς να εκπαιδεύουν κοινά μοντέλα χωρίς την ανάγκη ανταλλαγής ευαίσθητων δεδομένων. Αυτή η δυνατότητα είναι κρίσιμη για εφαρμογές σε ευαίσθητους τομείς, όπως η υγειονομική περίθαλψη, όπου η ανταλλαγή δεδομένων περιορίζεται από κανονισμούς και πολιτικές εμπιστευτικότητας. Επίσης, το FL είναι ιδιαίτερα ευέλικτο, υποστηρίζοντας εφαρμογές σε ένα ευρύ φάσμα τομέων, από έξυπνες πόλεις (Smart Cities) και IoT, έως χρηματοοικονομικές υπηρεσίες και βιομηχανικά περιβάλλοντα [72].

Παράλληλα, το FL ενισχύει την ασφάλεια των δεδομένων, μειώνοντας τον κίνδυνο παραβίασης κατά τη μεταφορά τους, μέσω της χρήσης προσαρμοσμένων πρωτοκόλλων και τεχνικών κρυπτογράφησης, όπως η ομομορφική κρυπτογράφηση (homomorphic encryption) και τα Trusted Execution Environments (TEEs). Η χρήση αυτών των τεχνολογιών παρέχει προστασία από επιθέσεις, όπως data poisoning και επιθέσεις Membership Inference [73], εξασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων [74].

Το FL υποστηρίζει την επεξεργασία πραγματικών δεδομένων σε πραγματικό χρόνο, επιτρέποντας την ταχεία ενημέρωση και εφαρμογή μοντέλων. Αυτή η δυνατότητα είναι κρίσιμη για εφαρμογές που απαιτούν γρήγορη προσαρμογή, όπως τα αυτοκινούμενα οχήματα. Ταυτόχρονα, τα συνεργαζόμενα μοντέλα που προκύπτουν μέσω του FL ενισχύουν τη συνολική απόδοση, επιτρέποντας στις συσκευές να επωφελούνται από τα δεδομένα άλλων συσκευών χωρίς να παραβιάζεται η ιδιωτικότητα [75].

Τέλος, διευκολύνει την κανονικοποίηση των μοντέλων, συμβάλλοντας στη μείωση του overfitting, δηλαδή του φαινομένου κατά το οποίο το μοντέλο ¨μαθαίνει' υπερβολικά καλά τα

δεδομένα εκπαίδευσης, με αποτέλεσμα να μην μπορεί να γενικευτεί σωστά σε νέα, άγνωστα δεδομένα. Παράλληλα, επιτρέπει στις συσκευές και τους οργανισμούς να διατηρούν την πλήρη κυριαρχία των δεδομένων τους, αποφεύγοντας την ανάγκη για εξωτερικές λύσεις αποθήκευσης.

Αυτά τα πλεονεκτήματα καθιστούν το FL εξαιρετικά αποδοτικό και ασφαλές για χρήση σε δίκτυα 5G και IoT, όπου η διαχείριση μεγάλου όγκου κατανεμημένων δεδομένων είναι υψίστης σημασίας.

### 2.4.3 Κατηγορίες Federated Learning

Η εξέλιξη του FL έχει οδηγήσει στη δημιουργία διαφόρων κατηγοριών που ανταποκρίνονται στις ποικίλες ανάγκες και προκλήσεις που προκύπτουν κατά την εφαρμογή του. Αυτές οι κατηγορίες αντιπροσωπεύουν διαφορετικές προσεγγίσεις ως προς τον τρόπο συντονισμού και διαχείρισης, τη φύση των δεδομένων και τη σχέση τους μεταξύ των κόμβων, καθώς και το πλαίσιο συνεργασίας και το μέγεθος των συμμετεχόντων. Οι λεπτομέρειες αυτών των κατηγοριών εξετάζονται αναλυτικά παρακάτω.

#### 2.4.3.1 Κατηγοριοποίηση βάσει Αρχιτεκτονικής Συντονισμού

Η πρώτη κατηγορία επικεντρώνεται στον τρόπο συντονισμού της διαδικασίας εκπαίδευσης [76]. Η διάκριση σε Κεντρικό και Αποκεντρωμένο FL καθορίζει τον βαθμό ελέγχου, τη ροή των δεδομένων και τις προκλήσεις που προκύπτουν.

- **Κεντρικό Federated Learning (CFL):**
  Το Κεντρικό FL αποτελεί την παραδοσιακή προσέγγιση, όπου η διαδικασία εκπαίδευσης συντονίζεται από έναν κεντρικό διακομιστή. Οι τοπικοί κόμβοι εκπαιδεύουν το μοντέλο με βάση τα τοπικά δεδομένα τους και αποστέλλουν τις παραμέτρους στον κεντρικό διακομιστή για συγχώνευση. Αυτή η μέθοδος είναι απλή στην υλοποίηση αλλά παρουσιάζει περιορισμούς, όπως η εξάρτηση από τον διακομιστή (μονοσήμαντο σημείο αποτυχίας — single point of failure) και ζητήματα ιδιωτικότητας και ασφάλειας [77].

- **Αποκεντρωμένο Federated Learning (DFL):**
  Από την άλλη το αποκεντρωμένο FL, γνωστό και ως "serverless" ή "distributed FL", καταργεί την ανάγκη για κεντρικό διακομιστή. Οι κόμβοι ανταλλάσσουν δεδομένα και παραμέτρους απευθείας μεταξύ τους, μειώνοντας τον κίνδυνο αποτυχίας λόγω μονοσήμαντων σημείων. Παρόλα αυτά, η έλλειψη κεντρικού συντονισμού αυξάνει την πολυπλοκότητα διαχείρισης, τον φόρτο επικοινωνίας και τις απαιτήσεις ασφαλείας [78].

#### 2.4.3.2 Κατηγοριοποίηση βάσει Δομής και Σχέσης Δεδομένων

Το δεύτερο κριτήριο κατηγοριοποίησης αφορά τη φύση των δεδομένων και τη σχέση τους μεταξύ των κόμβων. Ανάλογα με το επίπεδο κοινών χαρακτηριστικών και τη διασύνδεση των δεδομένων, διαμορφώνονται διαφορετικοί τύποι συνεργασίας [79].

- **Οριζόντιο Federated Learning (Horizontal Federated Learning - HFL):**
  Το οριζόντιο FL εφαρμόζεται όταν τα δεδομένα μεταξύ των κόμβων έχουν κοινά χαρακτηριστικά αλλά διαφορετικά δείγματα [80]. Για παράδειγμα, δύο νοσοκομεία που

παρακολουθούν παρόμοιους βιομετρικούς δείκτες διαφορετικών ασθενών μπορούν να συνεργαστούν για τη βελτίωση ενός μοντέλου πρόγνωσης χωρίς να ανταλλάξουν τα δεδομένα τους. Αυτή η προσέγγιση είναι ιδιαίτερα χρήσιμη σε περιπτώσεις όπου οι οργανισμοί ανήκουν στην ίδια βιομηχανία και καταγράφουν παρόμοιες παραμέτρους. Οι βασικές προκλήσεις περιλαμβάνουν την αντιμετώπιση της ανισορροπίας των δεδομένων και την προστασία από επιθέσεις που στοχεύουν τις ενημερώσεις του μοντέλου.

- **Κάθετο Federated Learning (Vertical Federated Learning - VFL):**
  Το κάθετο FL στοχεύει στη συνεργασία μεταξύ κόμβων που διαθέτουν διαφορετικά χαρακτηριστικά αλλά μοιράζονται κοινούς χρήστες ή αντικείμενα ενδιαφέροντος [81]. Για παράδειγμα, μια τράπεζα με χρηματοοικονομικά δεδομένα μπορεί να συνεργαστεί με μια πλατφόρμα ηλεκτρονικού εμπορίου, η οποία έχει δεδομένα συμπεριφοράς πελατών, για τη βελτίωση των μοντέλων αξιολόγησης πιστοληπτικής ικανότητας. Η κύρια πρόκληση εδώ είναι η ασφαλής στοίχιση των δεδομένων και η διατήρηση της ιδιωτικότητας, δεδομένου ότι τα χαρακτηριστικά είναι διαφορετικά.

- **Federated Transfer Learning (FTL):**
  Μια ακόμη κατηγορία είναι το FTL, το οποίο επιτρέπει τη συνεργασία μεταξύ κόμβων που δεν μοιράζονται ούτε κοινό χώρο χαρακτηριστικών ούτε κοινά δείγματα [82]. Αυτή η προσέγγιση είναι ιδανική για περιπτώσεις όπου τα δεδομένα είναι περιορισμένα ή ετερογενή. Για παράδειγμα, η εκπαίδευση ενός μοντέλου πρόβλεψης σε διαφορετικές γεωγραφικές περιοχές, με ελάχιστη επικάλυψη δεδομένων, μπορεί να επιτευχθεί μέσω του Federated Transfer Learning. Η αποτελεσματικότητα αυτής της μεθόδου εξαρτάται από την ικανότητα των αλγορίθμων να προσαρμόζουν γνώσεις από διαφορετικά σύνολα δεδομένων.

- **Federated Reinforcement Learning (FRL):**
  Τέλος, το FRL επεκτείνει τις αρχές του Reinforcement Learning σε κατανεμημένα περιβάλλοντα [83]. Αντί να ανταλλάσσονται δεδομένα, οι πράκτορες (agents) κοινοποιούν μοντέλα πολιτικής ή τιμών. Για παράδειγμα, τα αυτόνομα οχήματα μπορούν να εκπαιδεύονται σε διαφορετικά περιβάλλοντα και να μοιράζονται τις στρατιγηκές που έχουν μάθει χωρίς να διακυβεύονται τοπικά δεδομένα. Η κύρια πρόκληση είναι η διασφάλιση της συνοχής μεταξύ των διαφορετικών πρακτόρων και η ελαχιστοποίηση του επικοινωνιακού κόστους.

#### 2.4.3.3 Κατηγοριοποίηση βάσει Πλαισίου Συνεργασίας

Ο τρίτη κατηγορία αφορά το πλαίσιο συνεργασίας και το μέγεθος των συμμετεχόντων.Εστιάζει στις εφαρμογές που απαιτούν συνεργασία μεταξύ διαφορετικών ομάδων ή συσκευών. Αυτή η κατηγοριοποίηση καθορίζει τη φύση των συμμετεχόντων (οργανισμοί ή συσκευές) και τον τρόπο με τον οποίο οι περιορισμοί επικοινωνίας και ενέργειας επηρεάζουν την εφαρμογή [84].

- **Cross-Silo FL (CSFL):**
  Αρχικά. το CSFL επικεντρώνεται σε συνεργασίες μεταξύ μεγάλων, αξιόπιστων οργανισμών ή ΄σιλό· (π.χ., πανεπιστήμια, νοσοκομεία ή εταιρείες) [85]. Σε αυτό το πλαίσιο, οι

συμμετέχοντες είναι περιορισμένοι σε αριθμό και συνήθως εμπιστεύονται ο ένας τον άλλο, επιτρέποντας πιο σταθερή και ελεγχόμενη ανταλλαγή ενημερώσεων του μοντέλου. Η μέθοδος αυτή μπορεί να εφαρμοστεί τόσο σε οριζόντιο όσο και σε κάθετο FL, ανάλογα με τα χαρακτηριστικά των δεδομένων που κατέχει κάθε ΄σιλό΄. Το CSFL είναι ιδανικό για εφαρμογές που απαιτούν αυξημένη ακρίβεια και συνεπή υπολογιστική ισχύ, όπως η ιατρική ανάλυση και η ακαδημαϊκή έρευνα.

- **Cross-Device FL (CDFL):**
  Το CDFL στοχεύει στη συνεργασία μεταξύ μεγάλου αριθμού κόμβων χαμηλής υπολογιστικής ισχύος, όπως κινητά τηλέφωνα, IoT συσκευές, ή ακόμα και οικιακές συσκευές [86]. Σε αυτό το πλαίσιο, οι συσκευές αυτές συνήθως ανήκουν σε διαφορετικούς χρήστες και έχουν περιορισμούς στη μνήμη και την ενέργεια. Η μέθοδος αυτή εφαρμόζεται κυρίως στο οριζόντιο FL, καθώς οι συσκευές διαθέτουν δεδομένα με παρόμοια χαρακτηριστικά, αλλά διαφορετικά δείγματα. Οι προκλήσεις του CDFL περιλαμβάνουν την αποτελεσματική διαχείριση της επικοινωνίας, την ασφάλεια από επιθέσεις, και τη βελτιστοποίηση των ενεργειακών απαιτήσεων. Αυτό το καθιστά κατάλληλο για εφαρμογές όπως η προσαρμοσμένη εκπαίδευση μοντέλων σε κινητές συσκευές και οι προτάσεις περιεχομένου.

Αυτή η πολυεπίπεδη κατηγοριοποίηση του FL προσφέρει την ευελιξία να προσαρμόζεται σε διάφορες απαιτήσεις και σενάρια εφαρμογής. Η επιλογή της κατάλληλης προσέγγισης εξαρτάται από τη φύση των δεδομένων, τη διαθεσιμότητα πόρων και τις ανάγκες ιδιωτικότητας και ασφάλειας.

### 2.4.4 Federated Learning Frameworks

Η ανάπτυξη του FL οδήγησε στη δημιουργία διαφόρων εξειδικευμένων πλαισίων λογισμικού (frameworks) που διευκολύνουν την υλοποίηση, τη διαχείριση και την ανάπτυξη αποκεντρωμένων μοντέλων μηχανικής μάθησης. Αυτά τα frameworks προσφέρουν ποικίλες λειτουργίες και καλύπτουν διαφορετικές ανάγκες, από πειραματικά περιβάλλοντα έως μεγάλης κλίμακας επιχειρηματικές εφαρμογές. Στη συνέχεια, παρουσιάζονται μερικά από τα πιο διαδεδομένα frameworks για FL.

#### 2.4.4.1 PySyft

Αρχικά, το PySyft είναι ένα ανοιχτού κώδικα framework το οποίο βασίζεται στη βιβλιοθήκη PyTorch. Ειδικεύεται στην ασφαλή και ιδιωτική μηχανική μάθηση, υποστηρίζοντας τεχνικές όπως το FL, το Differential Privacy (DP) και Encrypted Computation [87]. Επίσης, προσφέρει εργαλεία για την υλοποίηση κρυπτογραφικών τεχνικών όπως η Ομομορφική Κρυπτογράφηση και το Secure Multi-Party Computation (SMPC) [88], επιτρέποντας την ασφαλή ανταλλαγή μοντέλων χωρίς την αποκάλυψη των δεδομένων εκπαίδευσης. Η ευελιξία του και η συμβατότητά του με τις βιβλιοθήκες PyTorch και TensorFlow το καθιστούν ιδανικό για εφαρμογές που απαιτούν αυξημένη προστασία δεδομένων, όπως ο τομέας της υγείας και οι τραπεζικές υπηρεσίες [89] [90].

#### 2.4.4.2 Flower (Flwr)

Ακόμα ένα framework είναι το Flower, το οποίο αποτελεί ένα από τα πιο ευέλικτα και εύχρηστα frameworks για FL. Πρόκειται για ένα πλαίσιο ανοιχτού κώδικα, σχεδιασμένο να υποστηρίζει διαφορετικές πλατφόρμες και βιβλιοθήκες μηχανικής μάθησης όπως PyTorch, TensorFlow, και Scikit-learn[91]. Το Flower διευκολύνει την υλοποίηση τόσο σε cross-device όσο και σε cross-silo σενάρια, παρέχοντας υψηλή κλιμακωσιμότητα και τη δυνατότητα προσαρμογής των συναρτήσεων συγκέντρωσης. Επιπλέον, η αρχιτεκτονική του επιτρέπει τη διαχείριση μεγάλου αριθμού clients, καθιστώντας το κατάλληλο για περιβάλλοντα όπως το IoT και κινητές συσκευές [92].

#### 2.4.4.3 TensorFlow Federated (TFF)

Το TensorFlow Federated (TFF) αναπτύχθηκε από την Google και είναι ένα από τα πιο δημοφιλή frameworks για την υλοποίηση FL σε περιβάλλοντα που χρησιμοποιούν το TensorFlow. Το TFF προσφέρει πλήρη ενσωμάτωση με το οικοσύστημα του TensorFlow, επιτρέποντας τη χρήση προκαθορισμένων αλγορίθμων όπως το Federated Averaging (FedAvg). Επίσης παρέχει εργαλεία για την προσομοίωση κατανεμημένων συστημάτων σε τοπικά περιβάλλοντα, διευκολύνοντας τον πειραματισμό πριν από την υλοποίηση σε πραγματικά δίκτυα. Χάρη στην απλότητά του, αποτελεί ιδανική επιλογή για οργανισμούς που χρησιμοποιούν ήδη το TensorFlow στις εφαρμογές τους [93].

#### 2.4.4.4 IBM Federated Learning (IBM FL)

Το IBM FL είναι μια επιχειρηματική πλατφόρμα για την υλοποίηση FL σε μεγάλης κλίμακας περιβάλλοντα. Το IBM FL εστιάζει στην ασφάλεια και τη συμμόρφωση με κανονισμούς, προσφέροντας υποστήριξη για τεχνικές όπως το DP και η Ομομορφική Κρυπτογράφηση. Επιπλέον, παρέχει ενσωμάτωση με τις υπηρεσίες IBM Watson και άλλες εταιρικές λύσεις, καθιστώντας το κατάλληλο για οργανισμούς με αυξημένες ανάγκες για διαχείριση δεδομένων [94]. Το IBM FL επιτρέπει την προσαρμογή αλγορίθμων συγκέντρωσης και την παρακολούθηση της απόδοσης του μοντέλου σε πραγματικό χρόνο, προσφέροντας ένα ολοκληρωμένο περιβάλλον για την ανάπτυξη και τη διαχείριση FL εφαρμογών [95].

#### 2.4.4.5 FATE (Federated AI Technology Enabler)

Τέλος, το FATE είναι ένα framework ανοιχτού κώδικα που επικεντρώνεται στην παροχή βιομηχανικών λύσεων για FL. Το FATE υποστηρίζει διάφορους τύπους FL, όπως το HFL και το VFL, καθώς και προηγμένες τεχνικές ασφαλούς υπολογισμού, όπως το Encryption και το SMPC. Το framework αυτό είναι ιδανικό για περιβάλλοντα όπου απαιτείται η ανταλλαγή ευαίσθητων δεδομένων μεταξύ διαφορετικών οργανισμών, όπως στον τραπεζικό τομέα και τις τηλεπικοινωνίες. Η αρχιτεκτονική του επιτρέπει την επεκτασιμότητα και την ευκολία ενσωμάτωσης σε πολύπλοκα πληροφοριακά συστήματα [96].

#### 2.4.4.6 Σύγκριση και Επιλογή Frameworks

Πίνακας 2.1: *Σύγκριση FL Frameworks*

| Framework | Γλώσσα | Εστίαση | Κρυπτογραφία |
|---|---|---|---|
| **PySyft** | Python | Ασφάλεια, Privacy | Ναι |
| **Flower** | Python | Ευελιξία, Cross-Platform | Όχι |
| **TensorFlow FL** | Python | TensorFlow Integration | Όχι |
| **IBM FL** | Python/Java | Επιχειρηματική Χρήση | Ναι |
| **FATE** | Python/Java | Βιομηχανικό FL | Ναι |

Η επιλογή του κατάλληλου framework εξαρτάται από τις ανάγκες του έργου. Ο Πίνακας 2.1 παρουσιάζει μια συνοπτική σύγκριση βασικών χαρακτηριστικών των πιο διαδεδομένων πλαισίων FL. Για παράδειγμα, σε πειραματικές εφαρμογές, το Flower προσφέρει την απαραίτητη ευελιξία, ενώ για αυξημένη ασφάλεια και προστασία προσωπικών δεδομένων, τα PySyft και FATE αποτελούν καλύτερες επιλογές. Εφαρμογές που χρησιμοποιούν ήδη το TensorFlow μπορούν να επωφεληθούν από τη στενή ενσωμάτωση που προσφέρει το TensorFlow Federated, ενώ το IBM FL απευθύνεται κυρίως σε επιχειρηματικά περιβάλλοντα με αυστηρές απαιτήσεις συμμόρφωσης και ασφάλειας.

### 2.4.5 Συναρτήσεις Συγκέντρωσης

Προηγουμένως αναφέραμε ότι στο FL, η εκπαίδευση των μοντέλων πραγματοποιείται τοπικά στις συσκευές ή στους κόμβους που κατέχουν τα δεδομένα, διατηρώντας έτσι την ιδιωτικότητα και μειώνοντας τον επικοινωνιακό φόρτο. Ωστόσο, για να προκύψει ένα ενιαίο, παγκόσμιο μοντέλο, οι ενημερώσεις που προέρχονται από τους επιμέρους κόμβους πρέπει να συνδυαστούν αποτελεσματικά. Αυτή η διαδικασία επιτυγχάνεται μέσω των συναρτήσεων συγκέντρωσης (aggregation functions), οι οποίες συγχωνεύουν τις τοπικές ενημερώσεις σε ένα κοινό μοντέλο. Η επιλογή της κατάλληλης συνάρτησης συγκέντρωσης διαδραματίζει καθοριστικό ρόλο στην απόδοση, τη σταθερότητα και την ικανότητα γενίκευσης του παγκόσμιου μοντέλου, καθώς επηρεάζει τον τρόπο με τον οποίο οι ενημερώσεις από διαφορετικούς clients ενσωματώνονται [97].

Ανάλογα με τις ιδιαιτερότητες του συστήματος και των δεδομένων, μπορούν να χρησιμοποιηθούν διαφορετικές προσεγγίσεις συγκέντρωσης, όπως:

- **Federated Averaging (FedAvg):** Πρόκειται για την πιο διαδεδομένη μέθοδο, στην οποία οι ενημερώσεις των τοπικών μοντέλων σταθμίζονται βάσει του μεγέθους του dataset κάθε client και στη συνέχεια υπολογίζεται ο μέσος όρος των παραμέτρων. Το FedAvg προσφέρει υψηλή απόδοση και είναι αποδοτικό σε κατανεμημένα περιβάλλοντα, ωστόσο μπορεί να επηρεαστεί από τη μη ομοιομορφία των δεδομένων (data heterogeneity), καθώς δεν λαμβάνει υπόψη την κατεύθυνση ή δυναμική των ενημερώσεων [98].

- **FedAvgM**: Μια επέκταση του FedAvg είναι το FedAvgM το οποίο ενσωματώνει την έννοια της ορμής (momentum) στον server. Στοχεύει στη βελτίωση της σταθερότητας κατά τη σύγκλιση, ιδιαίτερα όταν οι τοπικές ενημερώσεις διαφέρουν σημαντικά λόγω ετερογένειας στα δεδομένα. Παρ' όλα αυτά, η απόδοσή του εξαρτάται σε μεγάλο βαθμό από την κατάλληλη ρύθμιση υπερπαραμέτρων, όπως ο ρυθμός ορμής [99].

- **FedAdam**: Ακόμα μια παραλλαγή του FedAvg είναι η συνάρτηση FedAdam, η οποία χρησιμοποιεί τον βελτιστοποιητή Adam στον server για την ενημέρωση των παραμέτρων. Η συνάρτηση αυτή, έχει δείξει βελτιωμένη απόδοση σε σενάρια με υψηλή ετερογένεια ή σύνθετη δυναμική εκπαίδευσης. Ωστόσο, η πολυπλοκότητα της προσαρμογής των παραμέτρων (όπως οι ρυθμοί εκμάθησης και οι βελτιστοποιητικοί συντελεστές) μπορεί να καθιστά τη χρήση του πιο απαιτητική σε πρακτικές εφαρμογές [100].

- **Federated Median (FedMedian):** Αυτή η μέθοδος χρησιμοποιεί τη διάμεσο των τοπικών ενημερώσεων αντί για τον μέσο όρο που χρησιμοποιούν οι συναρτήσεις που προαναφέρθηκαν. Για αυτό τον λόγο, παρουσιάζει αυξημένη ανθεκτικότητα σε ακραίες τιμές και είναι ιδιαίτερα χρήσιμη σε περιβάλλοντα όπου υπάρχουν αποκλίνοντες (byzantine clients). Ωστόσο, ενδέχεται να μειώνει την ταχύτητα σύγκλισης όταν οι ενημερώσεις των πελατών είναι συνεπείς και αξιόπιστες [101].

- **Krum και Multi-Krum:** Πρόκειται για πιο εξελιγμένες τεχνικές που στοχεύουν στην προστασία του μοντέλου από επιθέσεις και μη αξιόπιστες ενημερώσεις. Επιλέγουν μόνο τις ενημερώσεις που βρίσκονται πλησιέστερα μεταξύ τους, απορρίπτοντας τις πιο ακραίες τιμές. Με αυτόν το τρόπο προσφέρουν αυξημένη ανθεκτικότητα, αλλά είναι υπολογιστικά αρκετά πιο απαιτητικές και μπορεί να καθυστερούν τη συνολική διαδικασία εκπαίδευσης [102].

- **Trimmed Mean:** Η συνάρτηση Trimmed Mean απορρίπτει ένα ποσοστό από τις μεγαλύτερες και μικρότερες τιμές των ενημερώσεων πριν υπολογίσει τον μέσο όρο. Είναι ιδιαίτερα χρήσιμη σε περιπτώσεις όπου υπάρχει υψηλός θόρυβος στα δεδομένα. Ωστόσο, η επιλογή του κατάλληλου ποσοστού αποκοπής είναι κρίσιμη και μπορεί να επηρεάσει σημαντικά την ακρίβεια του μοντέλου [103].

Λαμβάνοντας υπόψη τα χαρακτηριστικά των συναρτήσεων που παρουσιάστηκαν παραπάνω, κάθε συνάρτηση συγκέντρωσης παρουσιάζει διαφορετικά πλεονεκτήματα και περιορισμούς, ανάλογα με τις απαιτήσεις του συστήματος και τη φύση των δεδομένων. Η επιλογή της κατάλληλης συνάρτησης συγκέντρωσης εξαρτάται σε μεγάλο βαθμό από την ετερογένεια μεταξύ των πελατών, την παρουσία αποκλινουσών ενημερώσεων καθώς και το επίπεδο ανθεκτικότητας που απαιτείται έναντι επιθέσεων. Οι βασικές τεχνικές, όπως το FedAvg, είναι αποδοτικές για μεγάλα κατανεμημένα συστήματα με σχετικά ομοιογενή δεδομένα, ενώ πιο εξειδικευμένες μέθοδοι, όπως το Krum και το FedMedian, προτιμώνται σε περιβάλλοντα που απαιτούν αυξημένη ασφάλεια και σταθερότητα.

## 2.5 Σχετικές Εργασίες

### 2.5.1 FL Εφαρμογές 5G-NIDD

Το 5G Network Intrusion Detection Dataset (5G-NIDD) dataset [;] αποτελεί ένα σημαντικό σύνολο δεδομένων ανίχνευσης εισβολών δικτύου, δημιουργημένο σε πραγματικό περιβάλλον 5G. Περιλαμβάνει ποικίλους τύπους επιθέσεων, όπως DoS (ICMP Flood, UDP Flood, SYN Flood, HTTP Flood, Slowrate DoS) και σαρώσεις θυρών (SYN Scan, TCP Connect Scan, UDP Scan), καθώς και κανονική κυκλοφορία από πραγματικές κινητές συσκευές. Η

αξιολόγηση μεθόδων μηχανικής μάθησης, όπως Decision Tree, Random Forest, KNN, Naive Bayes και MLP (Multi-Layer Perceptron), έδειξε ότι το MLP πέτυχε την υψηλότερη ακρίβεια ανίχνευσης, αγγίζοντας το 97.89%. Παράλληλα, στη μελέτη [;], εφαρμόστηκε αρχιτεκτονική FL με δύο clients , όπου αξιολογήθηκαν Aggregation Functions όπως FedAvg, FedProx, FedAdam, FedAdagrad και FedYogi να προσφέρουν σημαντική ακρίβεια, με το FedAvg να υπερισχύει (ακρίβεια 97.89%). Παράλληλα, χρησιμοποιήθηκε μια προσαρμοσμένη αρχιτεκτονική MLP για την ταξινόμηση εννέα κατηγοριών επιθέσεων, με τεχνικές κανονικοποίησης χαρακτηριστικών και SMOTE να εξισορροπούν τις κατηγορίες δεδομένων. Η κατανομή των δεδομένων σε μη-ομοιογενείς συνθήκες αντικατοπτρίζει την πραγματική ετερογένεια των δικτύων 5G, ενισχύοντας την αξιοπιστία της μεθόδου.

Προχωρώντας πέρα από τα παραδοσιακά μοντέλα FL, η μελέτη [;] εισάγει το DeepFedKDAD, ένα καινοτόμο πλαίσιο που συνδυάζει υβριδικό μοντέλο CNN-BiLSTM με Deep Federated Knowledge Distillation (FKD). Αυτή η προσέγγιση όχι μόνο διασφαλίζει την ιδιωτικότητα μέσω ανταλλαγής logits αλλά και μειώνει την επικοινωνιακή επιβάρυνση, καθιστώντας την ιδανική για κατανεμημένα περιβάλλοντα. Η χρήση της κατανομής Dirichlet για την προσομοίωση μη-ομοιόμορφων κατανομών δεδομένων επιβεβαιώνει την ικανότητα του πλαισίου να λειτουργεί σε ετερογενή περιβάλλοντα. Με ακρίβεια που φτάνει το 99.96%, το DeepFedKDAD αποδεικνύει ανώτερη απόδοση σε σχέση με παραδοσιακούς αλγορίθμους FedAvg, εξασφαλίζοντας ταχύτερη σύγκλιση.

Η ασφάλεια των δικτύων επόμενης γενιάς εξετάζεται περαιτέρω στη μελέτη [;], η οποία εστιάζει στην αρχιτεκτονική multi-process FL για τη βελτιστοποίηση της ασφάλειας στα δίκτυα 6G-V2X. Μέσω της ανεξάρτητης εκπαίδευσης τοπικών μοντέλων και της χρήσης stacking για συγχώνευση, επιτυγχάνεται βελτιωμένη απόδοση ταξινόμησης, ιδιαίτερα σε συνθήκες non-IID που αντικατοπτρίζουν την ετερογένεια στα κατανεμημένα οχηματικά δίκτυα. Παρόλο που η πολυπλοκότητα της διαδικασίας σταςκινγ εισάγει προκλήσεις, τα αποτελέσματα δείχνουν σημαντικές βελτιώσεις στην ακρίβεια, ενισχύοντας τη χρησιμότητα της προσέγγισης.

Τέλος, η μελέτη [;] παρουσιάζει το TenaxDoS, ένα πλαίσιο που συνδυάζει Continual Learning και FL για την αντιμετώπιση προκλήσεων, όπως το φαινόμενο "catastrophic forgetting". Τα τοπικά μοντέλα, βασισμένα σε αρχιτεκτονική MLP, εκπαιδεύονται στους κόμβους ακρών και συγχωνεύουν τις παραμέτρους τους με τον αλγόριθμο FedAvg. Τα αποτελέσματα αναδεικνύουν την αποτελεσματικότητα του TenaxDoS, επιτυγχάνοντας σημαντικές βελτιώσεις στην ακρίβεια και τη συνολική απόδοση.

### 2.5.2 FL Εφαρμογές στο ToN IoT dataset

Το ToN IoT dataset σχεδιάστηκε για να καλύψει τις αδυναμίες προηγούμενων συνόλων δεδομένων στον τομέα της κυβερνοασφάλειας, ενσωματώνοντας δεδομένα από ποικίλες πηγές και παρέχοντας 9 κατηγορίες επιθέσεων, όπως DoS, DDoS, ransomware και MitM. Σκοπός του είναι να υποστηρίξει συστήματα μηχανικής μάθησης στην ανίχνευση σύγχρονων απειλών [104].

Διάφορες μελέτες έχουν αξιοποιήσει το σύνολο δεδομένων σε περιβάλλοντα FL για την ανίχνευση επιθέσεων σε IoT δίκτυα. Μέθοδοι συσσώρευσης, όπως το FedAvg, το Fed+, το FedProx, και το FedYogi, χρησιμοποιήθηκαν για την αντιμετώπιση της μη ομοιογενούς φύσης των δεδομένων, με το Fed+ και το FedYogi να επιδεικνύουν καλύτερες επιδόσεις [105].

Τα δεδομένα διανεμήθηκαν σε πελάτες βάσει σεναρίων, όπως Basic, Balanced και Mixed, με στόχο την προσομοίωση πραγματικών συνθηκών [106].

Τα μοντέλα που χρησιμοποιήθηκαν περιλάμβαναν Logistic Regression, DNNs και Deep Belief Networks (DBN), με το DBN να υπερέχει σε επιδόσεις με F1-Score 72% [107]. Οι μελέτες ανέδειξαν την ανάγκη προηγμένων στρατηγικών σύγκλισης για την αντιμετώπιση προκλήσεων, όπως η ανισορροπία και η πολυπλοκότητα των δεδομένων, επιβεβαιώνοντας την αξία του FL για την ανίχνευση επιθέσεων σε IoT περιβάλλοντα.

### 2.5.3 FL Εφαρμογές στο Bot-IoT dataset

Το Bot-IoT dataset σχεδιάστηκε για να αντιμετωπίσει τα προβλήματα που παρουσιάζουν τα υπάρχοντα σύνολα δεδομένων κυβερνοασφάλειας, όπως η περιορισμένη ποικιλία επιθέσεων και η έλλειψη ρεαλιστικής κυκλοφορίας IoT, περιλαμβάνοντας δεδομένα φυσιολογικής και κακόβουλης κίνησης, καθώς και επιθέσεις όπως DoS, DDoS, reconnaissance και information theft [108].

Διάφορες μελέτες έχουν αξιοποιήσει το Bot-IoT σε περιβάλλοντα FL για την ανίχνευση επιθέσεων botnet σε IoT δίκτυα, εφαρμόζοντας μεθόδους συσσώρευσης, όπως το FedAvg, FedProx και FedYogi [109].

Τα δεδομένα διανεμήθηκαν κατανεμημένα σε πελάτες, προσομοιώνοντας σενάρια με μη ομοιογενή κατανομή, όπως zero-day επιθέσεις, και χρησιμοποιήθηκαν αρχιτεκτονικές όπως 1D-CNN και Deep Neural Networks. Τα αποτελέσματα έδειξαν ακρίβεια ανίχνευσης άνω του 90%, ενώ μελέτες ανέδειξαν προκλήσεις, όπως η ανισορροπία των δεδομένων και ο χρόνος σύγκλισης των μοντέλων [110].

Επιπλέον, η ενσωμάτωση συστημάτων μετριασμού επιθέσεων και η σύνδεση με Host-based Intrusion Detection and Prevention System (HIDPS) προσφέρει αποτελεσματική διαχείριση ανωμαλιών σε πραγματικά περιβάλλοντα, όπως το botnet Mirai.

### 2.5.4 FL Εφαρμογές στο Edge-IIoTset dataset

Το Edge-IIoTset αποτελεί ένα από τα πιο ρεαλιστικά και ολοκληρωμένα datasets για την ανάπτυξη συστημάτων ανίχνευσης εισβολών σε IoT περιβάλλοντα, παρέχοντας δεδομένα από πολυεπίπεδη αρχιτεκτονική, όπως Cloud Computing, Edge Computing και Blockchain Networks, που περιλαμβάνουν τόσο κανονική όσο και κακόβουλη κυκλοφορία. Οι πρώτες μελέτες επικεντρώθηκαν στην αντιμετώπιση της μη-ομοιόμορφης κατανομής δεδομένων με τη χρήση FL μεθοδολογιών, όπως το FedAvg και το FedProx, επιτυγχάνοντας ακρίβεια 85% για μοντέλα DNN και DBN, παρότι υπήρχαν προκλήσεις λόγω της πολυπλοκότητας των δεδομένων [111].

Σε επόμενες εργασίες, η χρήση του FL βελτιώθηκε για να ενισχύσει την ιδιωτικότητα και την ακρίβεια, με επιδόσεις 92.49% για τα RNN και 91.34% για τα CNN, μειώνοντας την εξάρτηση από την κεντρική αποθήκευση δεδομένων αλλά παραμένοντας ευάλωτο σε ζητήματα ετερογένειας [112].

Επιπλέον, τεχνικές Zero Trust και προσομοίωση ρεαλιστικών περιβαλλόντων με κατανομή δεδομένων σε 3, 9 και 15 clients ενίσχυσαν την αποτελεσματικότητα των CNN σε επιθέσεις, όπως SQL Injection και Ransomware, φτάνοντας ακρίβειες 92%, αν και οι υπολογιστικές απαιτήσεις παραμένουν εμπόδιο [113].

Συνολικά, οι μελέτες ανέδειξαν τη σημασία του Edge-IIoTset για την προώθηση αποδο-

τικών IDS σε IoT περιβάλλοντα, ενώ παράλληλα επισήμαναν την ανάγκη για λύσεις που να αντιμετωπίζουν τις προκλήσεις κλίμακας και απόδοσης.

### 2.5.5 ML Εφαρμογές

Η μελέτη [;] εξετάζει την ανίχνευση ανωμαλιών σε δίκτυα 5G, αξιοποιώντας ως βάση το 5G-NIDD και προτείνοντας μια εμπλουτισμένη και εκτενέστερα επεξεργασμένη εκδοχή του, γνωστή ως 5G-SliciNDD. Το νέο αυτό dataset σχεδιάστηκε ειδικά για να ενσωματώνει την έννοια του δικτυακού τεμαχισμού (Network Slicing) στο πλαίσιο της ανίχνευσης εισβολών. Περιλαμβάνει 14,456 εγγραφές με 52 χαρακτηριστικά, εκ των οποίων το 51.18% αφορά κακόβουλη και το 48.82% κανονική κυκλοφορία. Κατά την προεπεξεργασία, ελλείπουσες τιμές αντικαταστάθηκαν με μέσες τιμές, ενώ εφαρμόστηκε κανονικοποίηση χαρακτηριστικών. Χρησιμοποιήθηκαν τεχνικές επιλογής χαρακτηριστικών, όπως Correlation Coefficient και Binary Particle Swarm Optimization, για τη δημιουργία μοντέλων, όπως DT, kNN, NB, Extreme Gradient Boosting (xGB) και Τεχνητά Νευρωνικά Δίκτυα (ANN). Το μοντέλο Hard Voting (HV) απέδωσε την καλύτερη απόδοση με ακρίβεια 99.8%, αποδεικνύοντας την αποτελεσματικότητά του στην ανίχνευση ανωμαλιών. Παράλληλα, αναδεικνύεται η αξία των ensemble μοντέλων για ισχυρή ανίχνευση ανωμαλιών, με προκλήσεις όπως η διαχείριση μη ισορροπημένων δεδομένων και η αποδοτικότητα σε πραγματικό χρόνο.

Η μελέτη [;] παρουσιάζει το 5GC PFCP Intrusion Detection Dataset, που στοχεύει στην ανάπτυξη Συστημάτων Ανίχνευσης Εισβολών για δίκτυα 5G. Το σύνολο δεδομένων ενσωματώνει λειτουργίες όπως το Session Management Function και το User Plane Function και περιλαμβάνει τέσσερις τύπους επιθέσεων PFCP: PFCP Session Establishment Flood Attack, PFCP Session Deletion Flood DoS Attack, και PFCP Session Modification Flood Attack. Προσφέρει ισορροπημένα δεδομένα για διαφορετικούς χρονισμούς ροής (15s, 60s, 120s), περιλαμβάνοντας 86 χαρακτηριστικά TCP/IP και 36 PFCP. Η μελέτη υπογραμμίζει τις προκλήσεις ασφάλειας στον πυρήνα δικτύων 5G και τις δυνατότητες τεχνικών Μηχανικής και Βαθιάς Μάθησης για την αντιμετώπισή τους.

Κεφάλαιο 3

# Μεθοδολογία και Υλοποίηση

## 3.1 Ζητούμενο

Η παρούσα διπλωματική εργασία επικεντρώνεται στη μελέτη της ανίχνευσης κακόβουλης δραστηριότητας σε περιβάλλοντα 5G μέσω τεχνικών ML και FL. Βασικός στόχος είναι η ανάπτυξη και αξιολόγηση ενός IDS που μπορεί να λειτουργεί αποτελεσματικά σε αποκεντρωμένα περιβάλλοντα, αξιοποιώντας το FL για την εκπαίδευση μοντέλων χωρίς τη μεταφορά δεδομένων.

Κεντρικό στοιχείο της προσέγγισης αποτελεί η ένταξη του Network Slicing στη μεθοδολογία αξιολόγησης, προσομοιώνοντας πιο ρεαλιστικά σενάρια λειτουργίας ενός 5G δικτύου, όπου διαφορετικές κατηγορίες slices (eMBB, mMTC, URLLC) αξιοποιούν την ίδια υποδομή. Στόχος είναι η διερεύνηση του κατά πόσο ένα FL-based IDS μπορεί να διατηρήσει υψηλή απόδοση και σε τέτοιες μη ομοιογενείς, κατανεμημένες συνθήκες.

Αρχικά, υλοποιείται ένα βασικό σενάριο FL, όπου το σύνολο δεδομένων διαχωρίζεται βάσει Network Slicing και χρησιμοποιείται η απλή συνάρτηση συγκέντρωσης FedAvg, ώστε να αξιολογηθεί η επίδοση του συστήματος σε μια ρεαλιστική και απαιτητική συνθήκη. Παράλληλα, για σκοπούς σύγκρισης, εφαρμόζεται η ίδια συνάρτηση σε σενάριο ισόποσης κατανομής των δεδομένων, προσομοιώνοντας μια πιο ιδανική, ισορροπημένη κατάσταση. Στη συνέχεια, εξετάζεται η χρήση πιο εξελιγμένων συναρτήσεων συγκέντρωσης (FedAvgM και FedAdam) και στα δύο σενάρια κατανομής, με στόχο τη βελτίωση της απόδοσης, ιδιαίτερα στην πιο απαιτητική περίπτωση του Network Slicing.

Η διαδικασία αυτή οδηγεί στη δημιουργία έξι διαφορετικών μοντέλων, τα οποία αξιολογούνται συγκριτικά ως προς την ακρίβεια, τη σταθερότητα και τη δυνατότητα γενίκευσης. Η εργασία στοχεύει να συνεισφέρει στη βαθύτερη κατανόηση των επιδόσεων του FL σε πραγματικές συνθήκες 5G, αναδεικνύοντας παράλληλα τη σημασία της επιλογής κατάλληλων συναρτήσεων συγκέντρωσης και κατανομής δεδομένων για τη βέλτιστη ανίχνευση επιθέσεων.

## 3.2 Σύνολο Δεδομένων

### 3.2.1 Περιγραφή Συνόλου Δεδομένων

Στην προηγούμενη ενότητα, παρουσιάστηκαν σημαντικές ερευνητικές προσπάθειες που σχετίζονται με την ανίχνευση επιθέσεων σε δίκτυα 5G, με ιδιαίτερη έμφαση στο 5G-NIDD, το οποίο αποτελεί ένα από τα πιο διαδεδομένα και αναγνωρισμένα δημόσια σύνολα δεδομένων στον τομέα. Το 5G-NIDD έχει χρησιμοποιηθεί ευρέως στη βιβλιογραφία για την αξιολόγηση αλγορίθμων μηχανικής μάθησης και βαθιάς μάθησης σε σενάρια κυβερνοασφάλειας για δίκτυα επόμενης γενιάς.

Βασιζόμενο στο 5G-NIDD, το 5G-SliciNDD αποτελεί ένα εμπλουτισμένο και εκτενέστερα

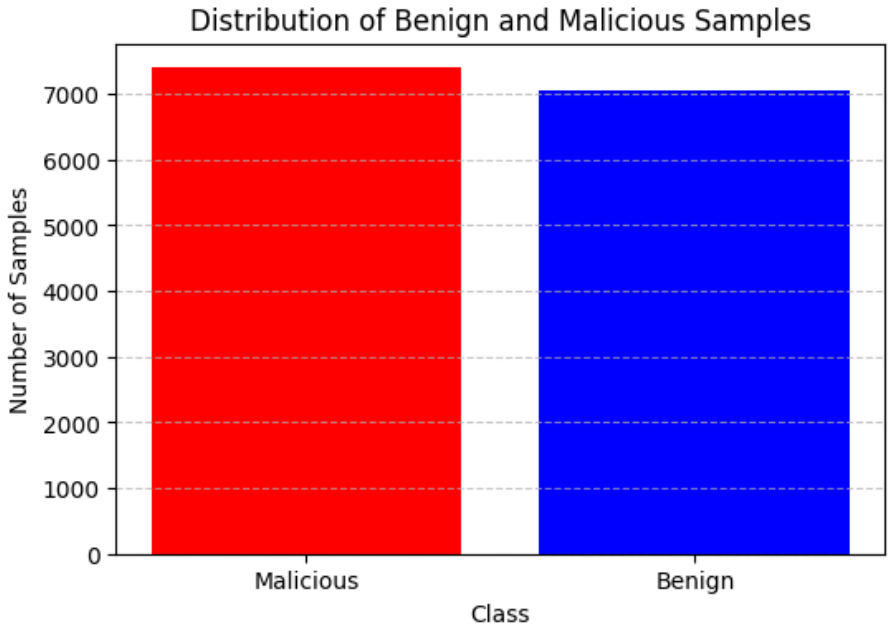
επεξεργασμένο σύνολο δεδομένων, σχεδιασμένο ειδικά για να ενσωματώνει την έννοια του δικτυακού τεμαχισμού (network slicing) στο πλαίσιο της ανίχνευσης εισβολών. Πρόκειται για το βασικό dataset που χρησιμοποιείται στην παρούσα εργασία.

Το 5G-SliciNDD dataset συνδυάζει δεδομένα κίνησης από διαφορετικούς τύπους slices και έχει διαχωριστεί σε τρία επιμέρους υποσύνολα, ανάλογα με το είδος του slice: eMBB (enhanced Mobile Broadband), mMTC (massive Machine-Type Communications) και URLLC (Ultra-Reliable Low-Latency Communications). Η αναλυτική περιγραφή των κατηγοριών αυτών έχει παρουσιαστεί στην ενότητα 2.1.4.

Ο τεμαχισμός αυτός επιτρέπει την ανάλυση και σύγκριση της συμπεριφοράς των επιθέσεων ανά τύπο slice, προσφέροντας μια πιο στοχευμένη κατανόηση των προκλήσεων ασφάλειας σε κάθε σενάριο χρήσης. Το σύνολο δεδομένων αποτελείται συνολικά από 14.456 εγγραφές και 52 χαρακτηριστικά, ενώ το πρόβλημα που εξετάζεται διατυπώνεται ως δυαδική ταξινόμηση μεταξύ Benign και Malicious ροών. Η κατανομή των κατηγοριών είναι σχετικά ισορροπημένη, με 7.057 δείγματα Benign και 7.399 δείγματα Malicious, γεγονός που περιορίζει την πιθανότητα μεροληψίας και επιτρέπει πιο αντικειμενική αξιολόγηση των μοντέλων.

Αν και το αρχικό 5G-NIDD περιλαμβάνει λεπτομερή κατηγοριοποίηση επιθέσεων (όπως DoS, DDoS, Reconnaissance κ.λπ.), στην παρούσα εργασία επιλέγεται μια αφαιρετική προσέγγιση που συγκεντρώνεται στη συνολική διάκριση benign και malicious δραστηριότητας. Σημειώνεται, ωστόσο, ότι αρκετά από τα Malicious δείγματα του 5G-SliciNDD φέρουν χαρακτηριστικά που μπορούν να συσχετιστούν με συγκεκριμένες κατηγορίες επιθέσεων από το αρχικό 5G-NIDD, όπως θα αναδειχθεί έμμεσα κατά την ανάλυση των χαρακτηριστικών στα επόμενα στάδια της μεθοδολογίας.

Παρακάτω παρουσιάζεται το πλήθος των δειγμάτων ανά κατηγορία:




Σχήμα 3.1: *Κατανομή των δειγμάτων ανά κατηγορία (Benign και Malicious) στο σύνολο δεδομένων 5G-SliciNDD*

### 3.2.2 Περιγραφή Χαρακτηριστικών

Το αρχικό σύνολο δεδομένων περιλαμβάνει 52 χαρακτηριστικά, τα οποία περιγράφουν πληροφορία σχετική με την κυκλοφορία του δικτύου, όπως αριθμός πακέτων, όγκος δεδομένων, χρόνοι έναρξης/λήξης, καθώς και κατηγορικές ετικέτες όπως το όνομα της εφαρμογής, η κατεύθυνση της ροής και το όνομα του σλιςε. Τα χαρακτηριστικά αυτά είναι είτε αριθμητικά (π.χ. SrcPkts, DstBytes), είτε κατηγορικά (π.χ. Proto, App, Slice), είτε δυαδικά.

Στις επόμενες ενότητες, περιγράφονται οι τεχνικές που εφαρμόστηκαν για την επεξεργασία των χαρακτηριστικών αυτών, καθώς και οι μέθοδοι επιλογής των πιο σημαντικών για το τελικό μοντέλο. Στον Πίνακα 3.1 παρουσιάζονται όλα τα χαρακτηριστικά του συνόλου δεδομένων, μαζί με τον τύπο τους (αριθμητικός ή κατηγορικός) και το ποσοστό απουσίας τιμών (missing values).

| **Feature** | **Type** | **Missing (%)** | **Feature** | **Type** | **Missing (%)** |
|---|---|---|---|---|---|
| X | Numerical | 0.00 | dMeanPktSz | Numerical | 0.00 |
| Seq | Numerical | 0.00 | Load | Numerical | 0.00 |
| Dur | Numerical | 0.00 | SrcLoad | Numerical | 0.00 |
| RunTime | Numerical | 0.00 | DstLoad | Numerical | 0.00 |
| Mean | Numerical | 0.00 | Loss | Numerical | 0.00 |
| Sum | Numerical | 0.00 | SrcLoss | Numerical | 0.00 |
| Min | Numerical | 0.00 | DstLoss | Numerical | 0.00 |
| Max | Numerical | 0.00 | pLoss | Numerical | 0.00 |
| Proto | Categorical | 0.00 | SrcGap | Numerical | 21.53 |
| sTos | Numerical | 0.01 | DstGap | Numerical | 21.53 |
| dTos | Numerical | 26.89 | Rate | Numerical | 0.00 |
| sDSb | Categorical | 0.00 | SrcRate | Numerical | 0.00 |
| dDSb | Categorical | 0.00 | DstRate | Numerical | 0.00 |
| sTtl | Numerical | 0.01 | State | Categorical | 0.00 |
| dTtl | Numerical | 27.14 | SrcWin | Numerical | 22.34 |
| sHops | Numerical | 0.01 | DstWin | Numerical | 29.35 |
| dHops | Numerical | 26.97 | sVid | Numerical | 97.41 |
| Cause | Categorical | 0.00 | dVid | Numerical | 99.97 |
| TotPkts | Numerical | 0.00 | SrcTCPBase | Numerical | 21.53 |
| SrcPkts | Numerical | 0.00 | DstTCPBase | Numerical | 30.33 |
| DstPkts | Numerical | 0.00 | TcpRtt | Numerical | 0.00 |
| TotBytes | Numerical | 0.00 | SynAck | Numerical | 0.00 |
| SrcBytes | Numerical | 0.00 | AckDat | Numerical | 0.00 |
| DstBytes | Numerical | 0.00 | UniqueID | Numerical | 0.00 |
| Offset | Numerical | 0.00 | predicted | Categorical | 0.00 |
| sMeanPktSz | Numerical | 0.00 | Label | Binary | 0.00 |

Πίνακας 3.1: *Dataset features with type and percentage of missing values*

## 3.3 Προεπεξεργασία και Επιλογή Χαρακτηριστικών

### 3.3.1 Εργαλεία

Για την υλοποίηση της παρούσας εργασίας χρησιμοποιήθηκε η γλώσσα προγραμματισμού Python 3.11, μέσω του περιβάλλοντος Jupyter Notebook, ενσωματωμένου στο Visual Studio Code. Το συγκεκριμένο περιβάλλον προσφέρει ευελιξία στην ανάπτυξη, εκτέλεση και

παρουσίαση των πειραμάτων μηχανικής μάθησης.

Οι βασικές βιβλιοθήκες που χρησιμοποιήθηκαν είναι:

- pandas, numpy – για διαχείριση και επεξεργασία πινάκων δεδομένων
- scikit-learn – για τεχνικές προεπεξεργασίας, επιλογής χαρακτηριστικών και αξιολόγησης μοντέλων
- matplotlib, seaborn – για οπτικοποίηση στατιστικών και χαρακτηριστικών
- pyswarm – για την υλοποίηση του αλγορίθμου Binary Particle Swarm Optimization (BPSO)

Όλα τα πειράματα εκτελέστηκαν τοπικά, με πλήρη έλεγχο στη ροή δεδομένων και τις παραμέτρους των μοντέλων.

### 3.3.2 Προεπεξεργασία Δεδομένων

Στο παρόν στάδιο πραγματοποιήθηκε προσεκτική προετοιμασία του αρχικού συνόλου δεδομένων 5G-SliciNDD ώστε να καταστεί κατάλληλο για την εκπαίδευση μοντέλων Μηχανικής Μάθησης και FL. Η διαδικασία περιλάμβανε τα εξής τέσσερα βασικά βήματα:

#### Κωδικοποίηση Κατηγορικών Μεταβλητών

Όλες οι μη αριθμητικές στήλες του συνόλου δεδομένων μετατράπηκαν σε αριθμητικές μέσω Label Encoding. Η συγκεκριμένη μέθοδος επιλέχθηκε έναντι άλλων, όπως το One-Hot Encoding, καθώς οι κατηγορικές μεταβλητές του dataset ήταν κυρίως δυαδικές ή περιείχαν περιορισμένο αριθμό διακριτών τιμών, χωρίς σημασιολογική ιεραρχία. Επομένως, η δημιουργία επιπλέον χαρακτηριστικών μέσω One-Hot Encoding θα αύξανε άσκοπα τη διαστατικότητα των δεδομένων χωρίς ουσιαστικό όφελος. Επιπλέον, τα μοντέλα που χρησιμοποιήθηκαν στην εργασία δεν επηρεάζονται αρνητικά από την ακέραιη αναπαράσταση των κατηγοριών, καθιστώντας το Label Encoding μια απλή και αποδοτική επιλογή.

#### Διαχείριση Ελλιπών Τιμών

Η παρουσία ελλιπών τιμών στο σύνολο δεδομένων καταγράφηκε στον Πίνακα 3.1, όπου παρουσιάζεται για κάθε χαρακτηριστικό το ποσοστό των NaN τιμών. Στις περιπτώσεις όπου το ποσοστό αυτό ήταν εξαιρετικά υψηλό, όπως στα χαρακτηριστικά sVid (97.41%) και dVid (99.97%) , τα χαρακτηριστικά αφαιρέθηκαν από το σύνολο δεδομένων ώστε να αποφευχθεί η εισαγωγή θορύβου.

Για τα υπόλοιπα χαρακτηριστικά με μικρότερα ποσοστά απωλειών, εφαρμόστηκε τεχνική συμπλήρωσης μέσω υπολογισμού του μέσου όρου της κάθε στήλης (mean imputation). Η επιλογή αυτή επιτρέπει τη διατήρηση της πληρότητας των δεδομένων χωρίς την απώλεια παρατηρήσεων και θεωρείται κατάλληλη για αριθμητικά τραφφις χαρακτηριστικά που δεν παρουσιάζουν έντονες χρονικές μεταβολές. Επιπλέον, τα χαρακτηριστικά αυτά θα αξιολογηθούν περαιτέρω σε επόμενο στάδιο μέσω μεθόδων επιλογής χαρακτηριστικών, όπως η συσχέτιση και ο αλγόριθμος BPSO, περιορίζοντας έτσι τον κίνδυνο εισαγωγής μη χρήσιμων μεταβλητών στο τελικό μοντέλο.

**Κανονικοποίηση Αριθμητικών Χαρακτηριστικών**
Όλα τα αριθμητικά χαρακτηριστικά κανονικοποιήθηκαν στο διάστημα [0, 1] μέσω της μεθόδου Min-Max Scaling. Η κανονικοποίηση αυτή βελτιώνει τη σταθερότητα και την ταχύτητα σύγκλισης κατά την εκπαίδευση των μοντέλων, εξισορροπώντας την επίδραση κάθε χαρακτηριστικού.

**Αποθήκευση Επεξεργασμένων Δεδομένων**
Το τελικό επεξεργασμένο σύνολο αποθηκεύτηκε σε αρχείο τύπου CSV, ώστε να είναι διαθέσιμο για τις επόμενες φάσεις της μεθοδολογίας — όπως η επιλογή χαρακτηριστικών και η δημιουργία υποσυνόλων για τα πειράματα FL.

Η παραπάνω διαδικασία αποτελεί κρίσιμο βήμα για τη διασφάλιση της ποιότητας και αξιοπιστίας των δεδομένων που χρησιμοποιήθηκαν στα μοντέλα εκμάθησης.

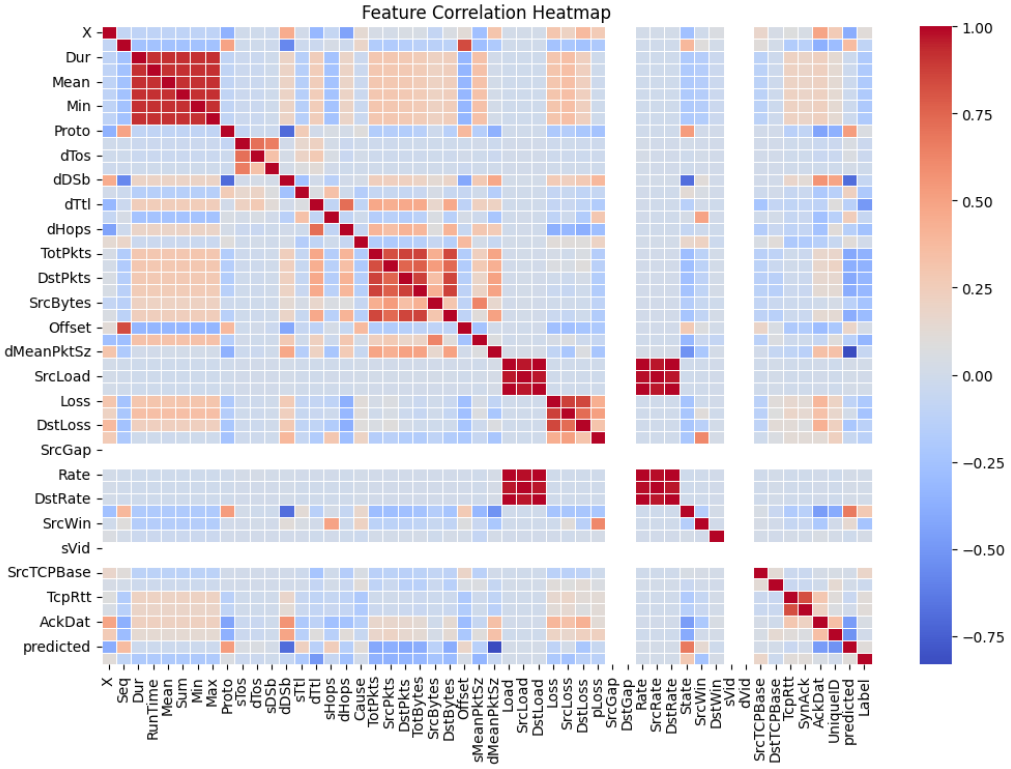
### 3.3.3 Ανάλυση Δεδομένων

Μετά την ολοκλήρωση της προεπεξεργασίας, ακολούθησε η φάση της ανάλυσης των χαρακτηριστικών με στόχο τη μείωση της διάστασης και τη βελτίωση της ποιότητας των δεδομένων εισόδου. Η διαδικασία περιλάμβανε διαδοχικά στάδια φιλτραρίσματος, βελτιστοποίησης και οπτικοποίησης, ώστε να διασφαλιστεί ότι τα τελικά σύνολα δεδομένων ήταν κατάλληλα για την εκπαίδευση αξιόπιστων και αποδοτικών μοντέλων.

#### 3.3.3.1 Φιλτράρισμα βάσει Συσχέτισης

Αρχικά υπολογίστηκε ο πίνακας συσχέτισης (correlation matrix) μεταξύ όλων των χαρακτηριστικών και της ετικέτας Label. Με βάση την απόλυτη τιμή της συσχέτισης, εφαρμόστηκε φίλτρο διατήρησης μόνο των χαρακτηριστικών με συσχέτιση άνω του κατωφλίου $\text{corr} > |0.1|$. Το συγκεκριμένο όριο επιλέχθηκε ώστε να διατηρηθεί ένας επαρκής αριθμός χαρακτηριστικών για περαιτέρω αξιολόγηση μέσω υβριδικού μοντέλου επιλογής χαρακτηριστικών, στο οποίο θα συνδυαστεί το φίλτρο συσχέτισης με αλγοριθμικές μεθόδους όπως το BPSO. Η αύξηση του κατωφλίου θα οδηγούσε σε σημαντική απώλεια χαρακτηριστικών ήδη από το πρώτο στάδιο, περιορίζοντας την ευελιξία του συνδυαστικού μηχανισμού. Ως εκ τούτου, το $|0.1|$ κρίθηκε ως κατάλληλο σημείο εκκίνησης για την υβριδική διαδικασία φιλτραρίσματος.

Για την οπτικοποίηση των σχέσεων μεταξύ των επιλεγμένων χαρακτηριστικών και την αξιολόγηση της πληροφορικής πυκνότητάς τους, δημιουργήθηκε το ακόλουθο heatmap συσχέτισης:




Σχήμα 3.2: *Πίνακας συσχέτισης μεταξύ χαρακτηριστικών μετά την εφαρμογή κατωφλίου 0.1*

Όπως παρατηρείται στον παραπάνω πίνακα συσχέτισης 3.2, η εφαρμογή του κατωφλίου corr $>$ |0.1| οδήγησε σε σημαντική μείωση του αριθμού χαρακτηριστικών, από 52 σε 26. Παρά τη μείωση αυτή, διατηρήθηκαν μεταβλητές με έντονη γραμμική συσχέτιση προς την κλάση Label, γεγονός που επιβεβαιώνεται από την παρουσία διακριτών περιοχών έντονης συσχέτισης στο heatmap. Η αρχική αυτή μείωση διαστάσεων αποτέλεσε τη βάση για την επόμενη φάση βελτιστοποίησης μέσω BPSO.

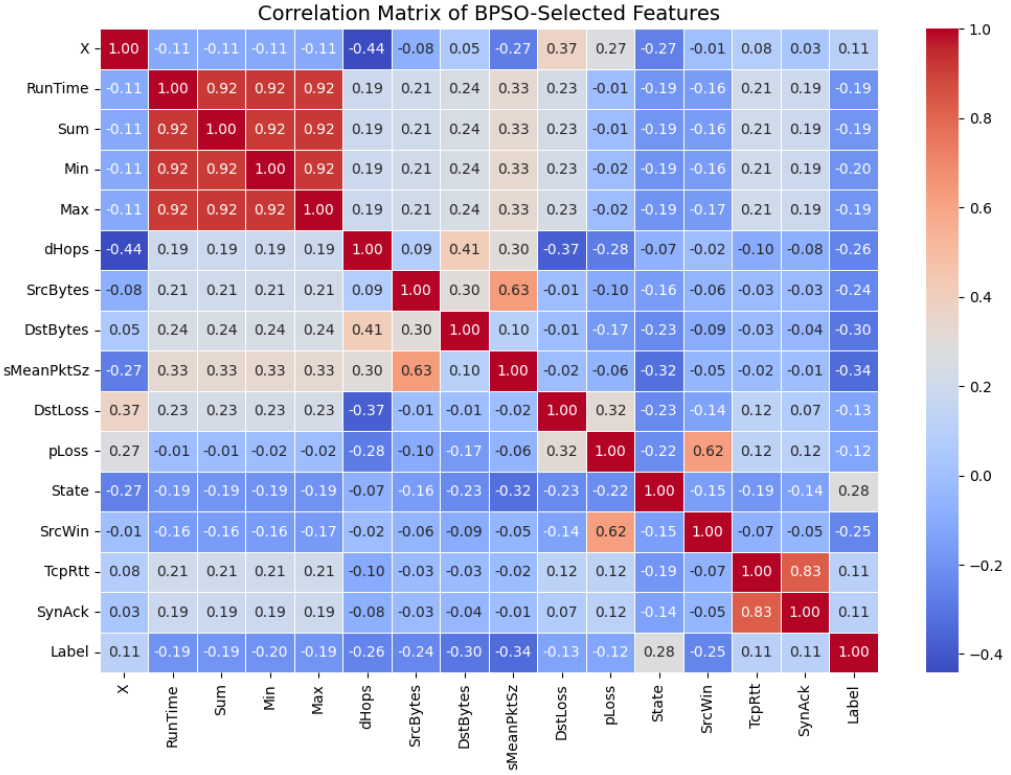
### 3.3.3.2 Συνδυαστική Προσέγγιση Επιλογής Χαρακτηριστικών

Η χρήση του παραπάνω threshold, αν και αποτελεσματική ως αρχικό φίλτρο, δεν εγγυάται απαραίτητα το βέλτιστο υποσύνολο χαρακτηριστικών. Για τον λόγο αυτό, επιλέχθηκε η χρήση μιας υβριδικής προσέγγισης που συνδυάζει το φιλτράρισμα μέσω του threshold με μία τεχνική βελτιστοποίησης βασισμένη στην απόδοση του μοντέλου. Συγκεκριμένα, εφαρμόστηκε ο αλγόριθμος Binary Particle Swarm Optimization (BPSO), ο οποίος αναζητά το υποσύνολο χαρακτηριστικών που μεγιστοποιεί την ακρίβεια ενός Decision Tree Classifier με cross-validation.

Αξίζει να σημειωθεί ότι ο BPSO είναι στοχαστικός αλγόριθμος, γεγονός που σημαίνει ότι κάθε εκτέλεση μπορεί να οδηγήσει σε διαφορετικό υποσύνολο επιλεγμένων χαρακτηριστικών. Για την αντιμετώπιση αυτής της μεταβλητότητας και την ενίσχυση της σταθερότητας των αποτελεσμάτων, η διαδικασία εκτελέστηκε επαναληπτικά. Καταγράφηκαν τα χαρακτηριστικά που επιλέγονταν συχνότερα σε διαφορετικές εκτελέσεις και, τελικά, επιλέχθηκε το σύνολο που εμφάνιζε τον μεγαλύτερο βαθμό επαναληψιμότητας. Η προσέγγιση αυτή διασφάλισε την αντιπροσωπευτικότητα και αξιοπιστία του τελικού συνόλου.

Αφού εντοπίστηκε το τελικό και πιο σταθερό υποσύνολο χαρακτηριστικών μέσω της δια-

δικασίας επιλογής του BPSO, κρίθηκε σημαντικό να αξιολογηθεί και οπτικά. Παρακάτω ακολουθεί ο πίνακας συσχέτισης με βάση τα χαρακτηριστικά που περιλαμβάνονται στο τελικό φιλτραρισμένο σύνολο:




Σχήμα 3.3: *Πίνακας συσχέτισης για τα χαρακτηριστικά που επιλέχθηκαν από τον αλγόριθμο BPSO*

Το σύνολο των 16 χαρακτηριστικών που επιλέχθηκαν πιο συστηματικά από τον BPSO παρουσιάζεται στον Πίνακα 3.2. Περιλαμβάνονται κυρίως αριθμητικές μεταβλητές σχετικές με τον όγκο και τη ροή δεδομένων, καθώς και ορισμένες κατηγορικές που σχετίζονται με το πρωτόκολλο και την κατάσταση της σύνδεσης.

| # | Feature | Type | Correlation with Label |
|---|---|---|---|
| 1 | X | Numerical | 0.11 |
| 2 | RunTime | Numerical | 0.19 |
| 3 | Sum | Numerical | 0.19 |
| 4 | Min | Numerical | 0.20 |
| 5 | Max | Numerical | 0.19 |
| 6 | dHops | Numerical | 0.26 |
| 7 | SrcBytes | Numerical | 0.24 |
| 8 | DstBytes | Numerical | 0.30 |
| 9 | sMeanPktSz | Numerical | 0.34 |
| 10 | pLoss | Numerical | 0.12 |
| 11 | State | Categorical | 0.28 |
| 12 | SrcWin | Numerical | 0.25 |
| 13 | TcpRtt | Numerical | 0.11 |
| 14 | SynAck | Numerical | 0.11 |
| 15 | DstPkts | Numerical | 0.13 |
| 16 | Label | Binary | 1.00 |

Πίνακας 3.2: *Τελικό σύνολο 16 χαρακτηριστικών που επιλέχθηκαν μέσω BPSO και η συσχέτισή τους με την ετικέτα*

Όπως φαίνεται στον παραπάνω πίνακα συσχέτισης 3.3, η πυκνότητα των συσχετίσεων έχει μειωθεί αισθητά, με τις περισσότερες μεταβλητές να παρουσιάζουν χαμηλή αλληλεξάρτηση μεταξύ τους. Αυτό υποδηλώνει ότι η επιλογή που πραγματοποίησε ο αλγόριθμος επικεντρώθηκε σε συμπληρωματικές μεταβλητές με ισχυρή συμβολή στο πρόβλημα ταξινόμησης, περιορίζοντας παράλληλα την πλεονάζουσα πληροφορία του αρχικού συνόλου.

Η συνδυαστική χρήση threshold και BPSO επέτρεψε τη σταδιακή μείωση των χαρακτηριστικών, διατηρώντας εκείνα με τη μεγαλύτερη συνεισφορά στην πρόβλεψη. Τα παραγόμενα heatmaps βοήθησαν στην κατανόηση της δομής του τελικού συνόλου και ανέδειξαν ποια χαρακτηριστικά παρουσιάζουν ισχυρότερη συσχέτιση με την ετικέτα (Label). Στη συνέχεια, εστιάζουμε στα τρία σημαντικότερα εξ αυτών, προκειμένου να μελετηθεί πιο αναλυτικά η επίδρασή τους.

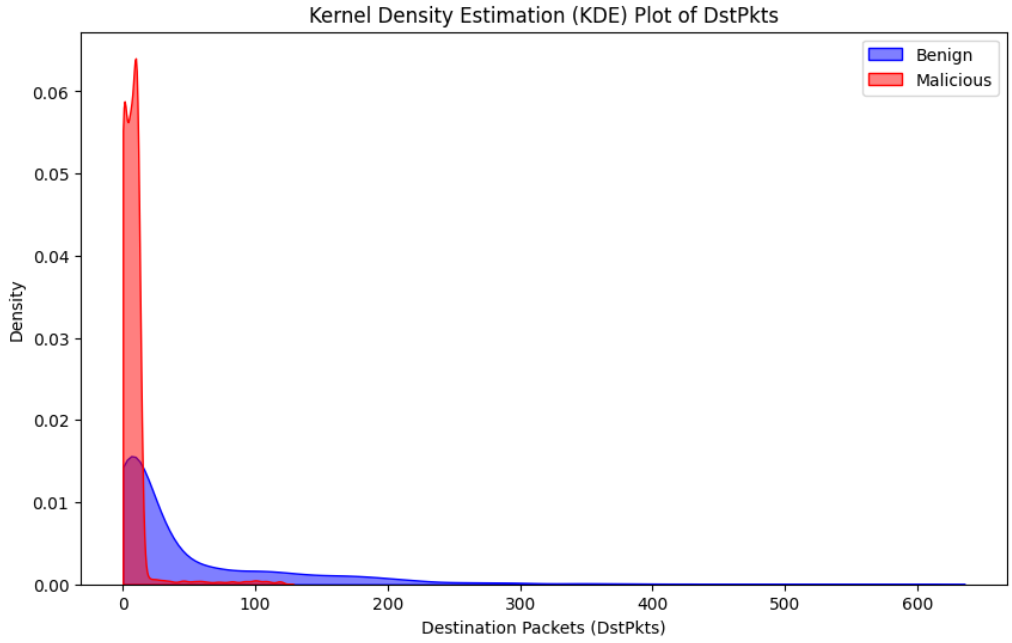
### 3.3.4 Ανάλυση Ισχυρών Χαρακτηριστικών

Έπειτα από την εφαρμογή των τεχνικών επιλογής χαρακτηριστικών και τη δημιουργία του τελικού φιλτραρισμένου συνόλου μέσω BPSO, πραγματοποιήθηκε περαιτέρω διερεύνηση των χαρακτηριστικών που εμφάνισαν τη μεγαλύτερη συσχέτιση με την ετικέτα Label. Όπως διαπιστώνεται εύκολα στον πίνακα συσχέτισης 3.3, τα χαρακτηριστικά DstPkts, State και sMeanPktSz εμφανίζουν τις ισχυρότερες συσχετίσεις με την ετικέτα και επιλέχθηκαν για στοχευμένη ανάλυση. Η μελέτη των κατανομών τους που ακολουθεί επιδιώκει να αναδείξει τη διακριτική τους ικανότητα και να ενισχύσει την ερμηνευσιμότητα του συνόλου δεδομένων.

#### 3.3.4.1 Ανάλυση του DstPkts

Το χαρακτηριστικό DstPkts (Destination Packets) εκφράζει τον αριθμό πακέτων που αποστέλλονται προς τον προορισμό κατά τη διάρκεια μιας ροής δικτύου. Παρατηρήθηκε ότι η κατανομή των τιμών του διαφοροποιείται αισθητά μεταξύ των κατηγοριών Benign και Malicious, υποδεικνύοντας ότι μπορεί να συμβάλει στη διάκριση μεταξύ φυσιολογικής και κακόβου-

λης συμπεριφοράς. Η τιμή συσχέτισης που καταγράφηκε ήταν 0.3. Στο παρακάτω γράφημα, απεικονίζεται η κατανομή του χαρακτηριστικού μέσω Kernel Density Estimation (KDE):



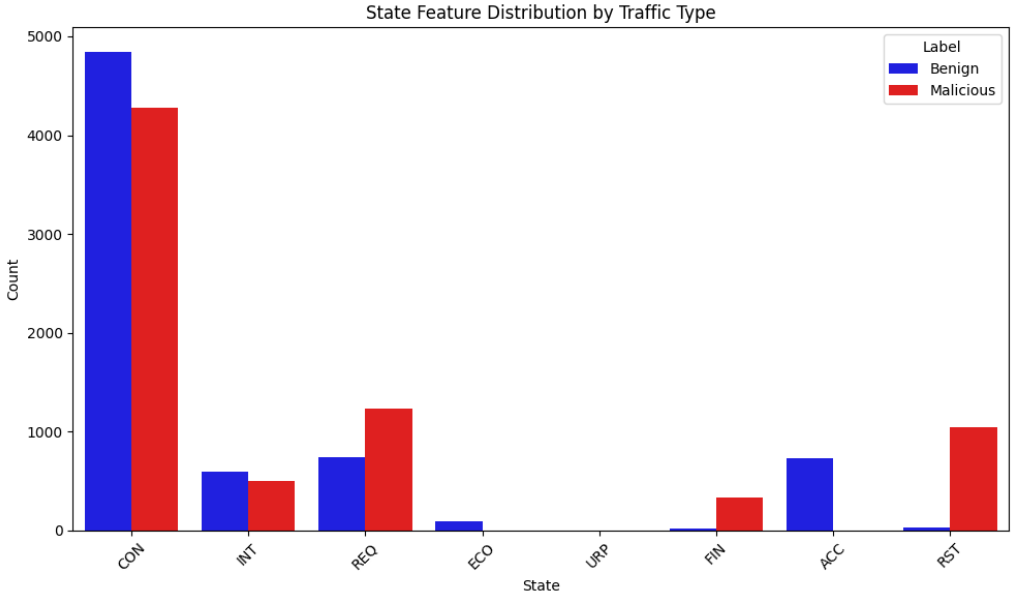

Σχήμα 3.4: *Κατανομή του χαρακτηριστικού DstPkts μέσω KDE για τις κατηγορίες Benign και Malicious*

Στο παραπάνω Διάγραμμα 3.4, οι κακόβουλες ροές (Malicious) συγκεντρώνονται γύρω από την τιμή 0 με έντονα συμπυκνωμένη κατανομή, σε αντίθεση με τις κανονικές ροές (Benign) που εμφανίζουν μεγαλύτερη διασπορά. Συγκεκριμένα, η πυκνότητα των Malicious κορυφώνεται γύρω από το 0 με τιμή περίπου 0.07, ενώ η αντίστοιχη των Benign είναι σημαντικά χαμηλότερη, περίπου 0.015. Η κατανομή των Benign εκτείνεται σε πολύ ευρύτερο φάσμα τιμών (από περίπου 0 έως 600), γεγονός που υποδεικνύει υψηλότερο αριθμό πακέτων προς τον προορισμό σε κανονικές συνδέσεις.

Η συμπεριφορά αυτή πιθανόν αντικατοπτρίζει επιθέσεις τύπου scanning, DoS ή probing, όπου ο τελικός προορισμός δεν ανταποκρίνεται ή απαντά ελάχιστα, με αποτέλεσμα να εμφανίζονται ροές με εξαιρετικά χαμηλό αριθμό πακέτων. Παρόλο που στην παρούσα εργασία η ταξινόμηση είναι δυαδική (Benign ή Malicious), το αρχικό dataset 5G-NIDD, από το οποίο προέρχεται το 5G-SliciNDD, περιλαμβάνει συγκεκριμένες κατηγορίες επιθέσεων. Έτσι, μεταβλητές όπως το DstPkts μπορούν να λειτουργήσουν ως έμμεσοι δείκτες για τον εντοπισμό τέτοιων επιθέσεων.

#### 3.3.4.2 Ανάλυση του State

Ένα ακόμη χαρακτηριστικό που ανέδειξε υψηλή συσχέτιση με την ετικέτα (0.28) είναι το State, το οποίο αποτελεί κατηγορική μεταβλητή και αποτυπώνει την κατάσταση μιας ροής ή σύνδεσης. Η ανάλυσή του είναι ιδιαίτερα σημαντική, καθώς επιτρέπει την παρατήρηση τυπικών προτύπων συμπεριφοράς που ενδέχεται να σχετίζονται με νόμιμη ή κακόβουλη δραστηριότητα.




Σχήμα 3.5: *Κατανομή του χαρακτηριστικού State ανά κατηγορία ετικέτας*

Στο Διάγραμμα 3.5, αποτυπώνεται η κατανομή της μεταβλητής State ως προς τις κατηγορίες Benign και Malicious. Παρακάτω παρουσιάζεται συνοπτικά η συχνότητα εμφάνισης κάθε τιμής της μεταβλητής ανά ετικέτα:

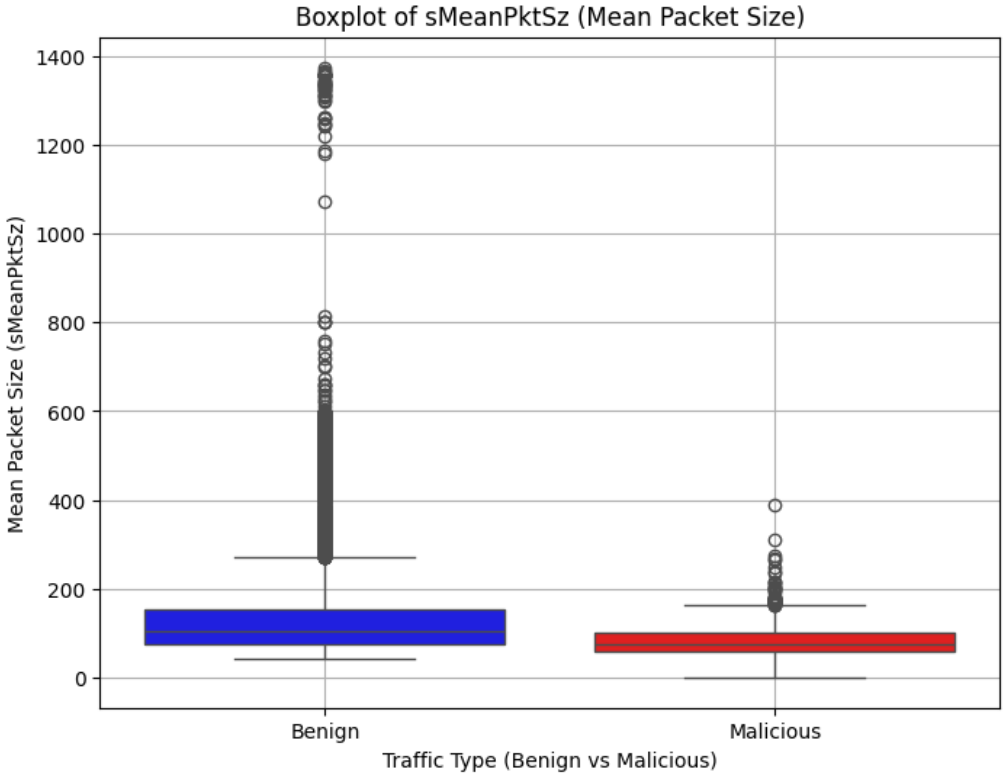
| State | Benign | Malicious |
|---|---|---|
| ACC | 733 | 0 |
| CON | 4848 | 4282 |
| ECO | 93 | 4 |
| FIN | 17 | 336 |
| INT | 593 | 501 |
| REQ | 737 | 1233 |
| RST | 32 | 1043 |
| URP | 4 | 0 |

Πίνακας 3.3: *Κατανομή παρατηρήσεων ανά τιμή της μεταβλητής State και ετικέτα*

Αναλύοντας την κατανομή των τιμών της μεταβλητής State, όπως παρουσιάζεται στον Πίνακα 3.3, εντοπίζονται χαρακτηριστικά μοτίβα που αναδεικνύουν τη συμβολή της στη διάκριση μεταξύ κανονικής και κακόβουλης κίνησης. Η τιμή ACC εμφανίζεται αποκλειστικά σε Benign εγγραφές, καθιστώντας την πιθανό δείκτη νόμιμης δραστηριότητας. Αντίθετα, οι καταστάσεις FIN και RST, που σχετίζονται με τερματισμό ή αιφνίδια διακοπή συνδέσεων, απαντώνται κυρίως σε Malicious ροές, γεγονός που υποδηλώνει συσχέτιση με επιθετικές συμπεριφορές. Η κατάσταση REQ εμφανίζει επίσης έντονη κλίση προς την κακόβουλη κατηγορία, με σχεδόν διπλάσιες εγγραφές σε σχέση με τις Benign. Αντιθέτως, η CON καταγράφεται συχνά και στις δύο κατηγορίες, γεγονός που περιορίζει τη διακριτική της ικανότητα. Τέλος, οι σπάνιες τιμές ECO και URP απαντώνται σχεδόν αποκλειστικά σε Benign ροές. Η συνολική εικόνα υποδεικνύει ότι η μεταβλητή State διαθέτει σαφή διαγνωστική αξία, καθώς ορισμένες από τις επιμέρους τιμές της εμφανίζουν υψηλή συσχέτιση με τη φύση της δικτυακής δραστηριότητας.

#### 3.3.4.3 Ανάλυση του sMeanPktSz

Ολοκληρώνοντας την ανάλυση των τριών πιο συσχετισμένων χαρακτηριστικών, εξετάζεται η μεταβλητή sMeanPktSz (0.34), η οποία αποτυπώνει το μέσο μέγεθος πακέτων που αποστέλλονται από τον αποστολέα. Σε αντίθεση με τα προηγούμενα χαρακτηριστικά —το αριθμητικό DstPkts και το κα categorial State—, η μεταβλητή sMeanPktSz προσφέρει ποσοτική πληροφορία για τη ροή των δεδομένων. Για την καλύτερη κατανόηση της διασποράς και των ακραίων τιμών της, αξιοποιείται η απεικόνιση μέσω boxplot.




Σχήμα 3.6: *Boxplot του χαρακτηριστικού sMeanPktSz για τις κατηγορίες Benign και Malicious*

Όπως φαίνεται στο Διάγραμμα 3.6, η μεταβλητή sMeanPktSz παρουσιάζει αξιοσημείωτες διαφορές μεταξύ των κατηγοριών Benign και Malicious. Τα Benign δείγματα εμφανίζουν σαφώς μεγαλύτερη διασπορά τιμών, με το 75ο εκατοστημόριο (X3) να φτάνει περίπου τα 152.5 bytes, σε αντίθεση με τα Malicious δείγματα, για τα οποία το X3 δεν ξεπερνά τα 99.9 bytes. Το ενδοτεταρτημοριακό εύρος (IXP) είναι σχεδόν διπλάσιο στα Benign (78.5) σε σύγκριση με τα Malicious (41.9), γεγονός που υποδηλώνει μεγαλύτερη ποικιλομορφία στα μεγέθη πακέτων σε κανονική δικτυακή δραστηριότητα.

Παράλληλα, εντοπίζονται αρκετοί ακραίοι outliers μόνο στην κατηγορία Benign, με τιμές που αγγίζουν ή και ξεπερνούν τα 1400 bytes. Σημειώνεται ότι σχεδόν όλα τα δείγματα με sMeanPktSz $>$ 350 bytes ανήκουν στην κατηγορία Benign, ενισχύοντας τη διακριτική ικανότητα της μεταβλητής. Αντίθετα, η κατανομή των Malicious δειγμάτων περιορίζεται σχεδόν αποκλειστικά στην περιοχή 0–200 bytes, υποδεικνύοντας ότι τα κακόβουλα πακέτα είναι κατά κύριο λόγο μικρού μεγέθους — ένα εύρημα που συνάδει με επιθέσεις τύπου scanning

ή flooding. Συνολικά, η μεταβλητή sMeanPktSz αναδεικνύεται ως ιδιαίτερα ισχυρός δείκτης για τη διάκριση μεταξύ νόμιμης και κακόβουλης δικτυακής δραστηριότητας.

#### 3.3.4.4 Συμπεράσματα Χαρακτηριστικών

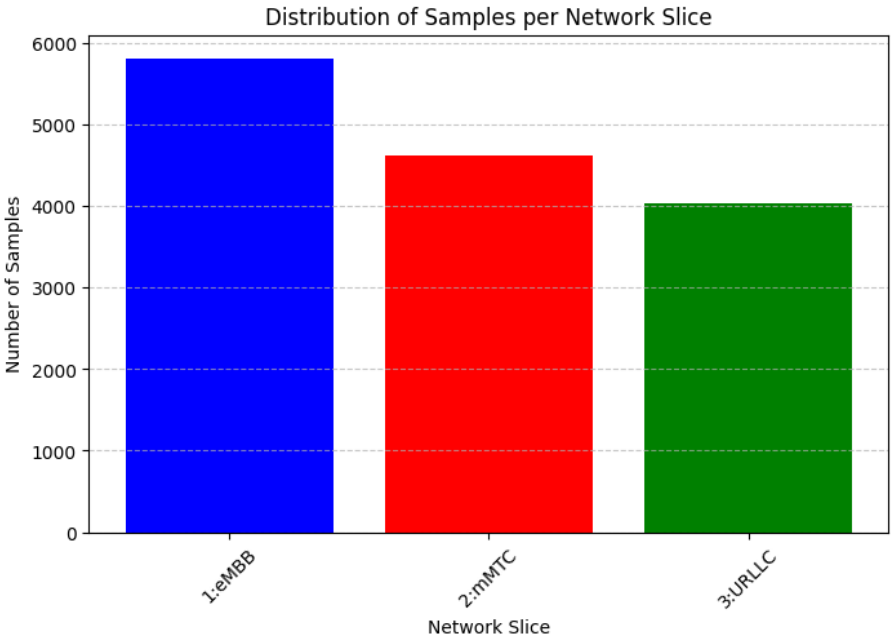
Η διαδικασία ανάλυσης των χαρακτηριστικών οδήγησε στην επιλογή ενός σταθερού και αντιπροσωπευτικού συνόλου μεταβλητών με ισχυρή συσχέτιση με την ετικέτα Label. Μέσα από τη στοχευμένη μελέτη επιμέρους χαρακτηριστικών, ενισχύθηκε η ερμηνευσιμότητα του συνόλου δεδομένων και αναδείχθηκαν κρίσιμα μοτίβα διαφοροποίησης μεταξύ νόμιμης και κακόβουλης κίνησης. Με βάση τα συμπεράσματα αυτής της ανάλυσης, προχωρούμε στην περιγραφή της διαδικασίας εκπαίδευσης των μοντέλων και της αρχιτεκτονικής του πειραματικού πλαισίου.

## 3.4 Δημιουργία Υποσυνόλων για Federated Learning

Καταλήγοντας στο τελικό φιλτραρισμένο σύνολο δεδομένων, το επόμενο βήμα της μεθοδολογίας αφορά την κατάλληλη προετοιμασία των υποσυνόλων για τις ανάγκες της εκπαίδευσης σε περιβάλλον FL. Η ανάπτυξη ενός τέτοιου περιβάλλοντος απαιτεί τη διάσπαση του συνόλου σε επιμέρους υποσύνολα που προσομοιώνουν διαφορετικούς απομονωμένους clients.

Στην παρούσα εργασία δημιουργήθηκαν δύο ξεχωριστές δομές διαχωρισμού των δεδομένων: μία βάσει του network slicing και μία με ισομερή τυχαία κατανομή (equal split), προκειμένου να διερευνηθεί η επίδραση της μορφής κατανομής στην απόδοση των ομοσπονδιακών μοντέλων. Η πρώτη περίπτωση αντικατοπτρίζει ένα πιο ρεαλιστικό σενάριο λειτουργίας δικτύου, όπου οι clients εκπροσωπούν διαφορετικές τομές (slices) του δικτύου με ενδεχομένως άνισα ή μη ομοιογενή χαρακτηριστικά. Αντίθετα, η ισομερής τυχαία κατανομή εξαλείφει την επίδραση της τομής, παρέχοντας ένα θεωρητικά πιο ουδέτερο και ομοιογενές περιβάλλον εκπαίδευσης.

Παράλληλα, πραγματοποιήθηκε ο απαραίτητος διαχωρισμός σε validation sets και τελικής δοκιμής (test sets) για την αξιόπιστη αξιολόγηση των global μοντέλων. Η διαδικασία αυτή αποτέλεσε κρίσιμο βήμα για την υλοποίηση και την αντικειμενική σύγκριση διαφορετικών σεναρίων εκπαίδευσης. Όπως φαίνεται στο Σχήμα 3.7, η συνολική κατανομή των εγγραφών ανά slice είναι σχετικά ισομερής, κάτι που αποτυπώνεται και στον παρακάτω Πίνακα 3.4.

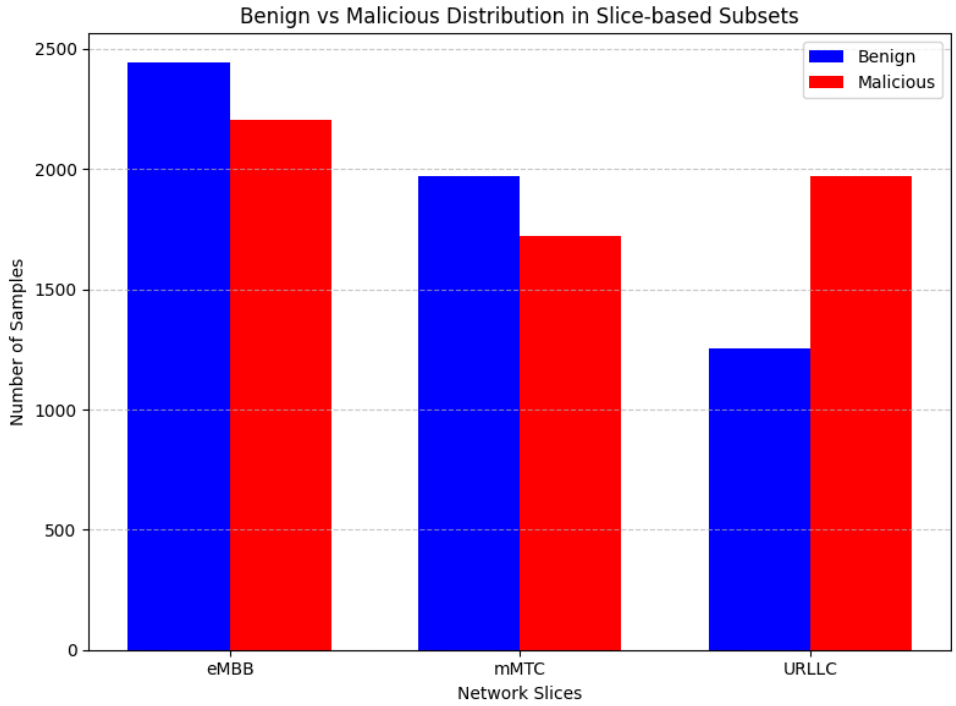



Σχήμα 3.7: *Κατανομή των δειγμάτων ανά slice στο σύνολο εκπαίδευσης*

### 3.4.1 Διαχωρισμός βάσει Network Slices

Ο πρώτος διαχωρισμός του συνόλου δεδομένων αφορά τη δημιουργία υποσυνόλων εκπαίδευσης με βάση την κατηγορία network slice. Αρχικά, το φιλτραρισμένο σύνολο δεδομένων υποβλήθηκε σε stratified split με βάση το πεδίο predicted, ώστε να δημιουργηθεί ένα καθολικό test set 20% με διατηρημένες τις αναλογίες μεταξύ eMBB, mMTC και URLLC. Το υπόλοιπο 80% αποτέλεσε το training set για το FL. Στη συνέχεια, το training set διαχωρίστηκε σε τρία αυτόνομα υποσύνολα, ανάλογα με την τιμή του πεδίου predicted, οδηγώντας στη δημιουργία των αρχείων eMBB_bpso_global.csv, mMTC_bpso_global.csv και URLLC_bpso_global.csv. Η διαδικασία αυτή προσομοιώνει σενάρια FL, όπου κάθε slice λειτουργεί ως απομονωμένος client με εξειδικευμένα δεδομένα ανά κατηγορία χρήσης.

Στο Διάγραμμα 3.8, απεικονίζεται η κατανομή των Benign και Malicious δειγμάτων στα τελικά slice-based υποσύνολα εκπαίδευσης, μετά την αφαίρεση του 20% που χρησιμοποιήθηκε για το καθολικό test set. Όπως φαίνεται, κάθε slice περιλαμβάνει ικανό αριθμό δειγμάτων και από τις δύο κατηγορίες ετικετών, επιτρέποντας την εκπαίδευση τοπικών μοντέλων με ρεαλιστικές συνθήκες. Στον Πίνακα 3.4 παρουσιάζεται η λεπτομερής κατανομή των δειγμάτων ανά slice, τόσο πριν όσο και μετά τον διαχωρισμό. Παρατηρείται ότι τα υποσύνολα eMBB και mMTC παρουσιάζουν σχετικά ισορροπημένη αναλογία μεταξύ Benign και Malicious παραδειγμάτων, ενώ στο URLLC υπερτερούν τα Malicious δείγματα — γεγονός που ανταναχλά τη φυσική κατανομή του αρχικού συνόλου δεδομένων.



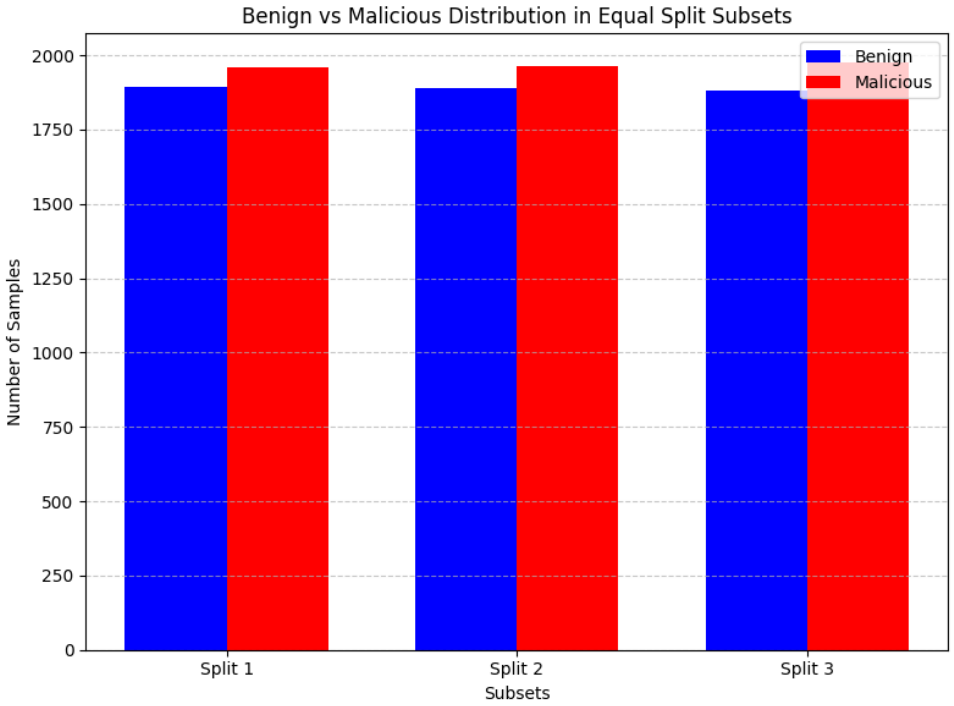

Σχήμα 3.8: *Κατανομή Benign και Malicious δειγμάτων ανά slice-based υποσύνολο*

Πίνακας 3.4: *Κατανομή των δειγμάτων για εκπαίδευση ανά slice και ετικέτα (Benign / Malicious), πριν και μετά τον διαχωρισμό για validation/test*

| **Slice** | **Benign** | **Malicious** | **Σύνολο** |
|---|---|---|---|
| eMBB (πριν) | 3.052 | 2.756 | 5.808 |
| eMBB (μετά) | 2.442 | 2.204 | 4.646 |
| mMTC (πριν) | 2.464 | 2.151 | 4.615 |
| mMTC (μετά) | 1.971 | 1.721 | 3.692 |
| URLLC (πριν) | 1.568 | 2.465 | 4.033 |
| URLLC (μετά) | 1.254 | 1.972 | 3.226 |

### 3.4.2 Ισόποσα Υποσύνολα (Equal Splits)

Η δεύτερη μέθοδος διαχωρισμού βασίστηκε στο ίδιο training set (80%) που προέκυψε μετά την αφαίρεση του καθολικού test set. Το σύνολο αυτό ανακατεύτηκε (shuffling) και στη συνέχεια χωρίστηκε ισομερώς σε τρία μέρη, χωρίς να ληφθεί υπόψη η κατηγορία slice. Τα τελικά υποσύνολα split1.csv, split2.csv και split3.csv περιλαμβάνουν παρόμοιο αριθμό δειγμάτων ανά ετικέτα, γεγονός που οφείλεται στην ισορροπία του αρχικού συνόλου. Η προσέγγιση αυτή προσομοιώνει περιβάλλον όπου οι συμμετέχοντες διαθέτουν ισοδύναμα αλλά θεματικά ετερογενή δεδομένα. .



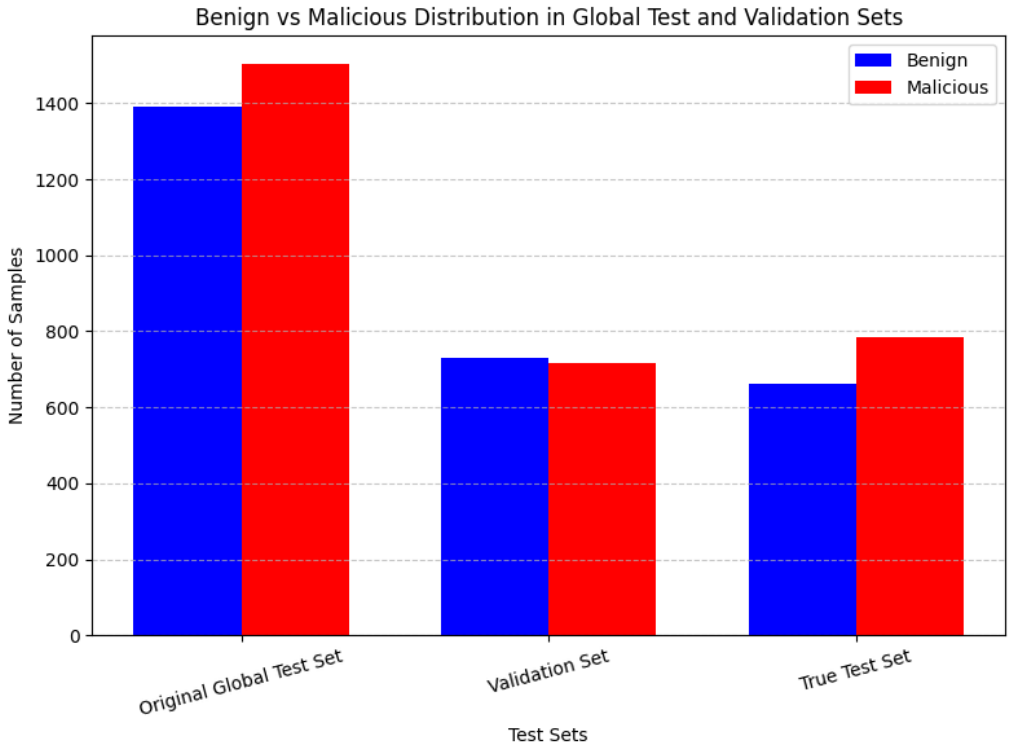

Σχήμα 3.9: *Κατανομή Benign και Malicious δειγμάτων στα ισόποσα υποσύνολα Equal Split*

### 3.4.3 Διαχωρισμός Validation και Test Set

Όπως προαναφέρθηκε, από το συνολικό σύνολο δεδομένων αφαιρέθηκε ένα ποσοστό 20%, το οποίο αποτέλεσε το καθολικό test set για τις ανάγκες αξιολόγησης. Στη συνέχεια, το σύνολο αυτό διαχωρίστηκε περαιτέρω σε δύο ίσα μέρη: το validation set και το true test set. Η διάκριση αυτή κρίθηκε απαραίτητη λόγω της διαφορετικής χρήσης τους στα πειραματικά σενάρια.

Κατά την εκπαίδευση τοπικών μοντέλων (ένα ανά slice), χρησιμοποιείται εσωτερικά ένα 10% του κάθε υποσυνόλου για σκοπούς επικύρωσης, ενώ η τελική αξιολόγηση πραγματοποιείται στο global test set. Αντίθετα, στα σενάρια FL, το validation set που προήλθε από το αρχικό test set χρησιμοποιείται καθολικά από τον server κατά τη διάρκεια της εκπαίδευσης (π.χ., για early stopping), και το true test set χρησιμοποιείται αποκλειστικά για την τελική αποτίμηση του παγκόσμιου μοντέλου.

Τα αντίστοιχα αρχεία που δημιουργήθηκαν είναι: global_val_set.csv και global_true_test_set.csv, ενώ στο Σχήμα 3.10 απεικονίζεται η δομή του διαχωρισμού.




Σχήμα 3.10: *Οπτική απεικόνιση του διαχωρισμού validation και test set από το καθολικό σύνολο δοκιμής*

| **Υποσύνολο** | **Benign** | **Malicious** | **Σύνολο** |
|---|---|---|---|
| Global Test Set (Αρχικό) | 1.390 | 1.502 | 2.892 |
| Validation Set | 729 | 717 | 1.446 |
| True Test Set | 661 | 785 | 1.446 |

Πίνακας 3.5: *Κατανομή των Benign και Malicious δειγμάτων στο αρχικό Global Test Set, καθώς και στα παράγωγα Validation και True Test Sets*

Συνολικά, η παραπάνω διαδικασία οδήγησε στη δημιουργία εννέα διακριτών συνόλων δεδομένων: έξι για την εκπαίδευση (τρεις clients ανά τρόπο διαχωρισμού), δύο για την καθολική επικύρωση και δοκιμή, καθώς και το αρχικό τεστ σετ. Με την προετοιμασία αυτή να έχει ολοκληρωθεί, το επόμενο βήμα είναι η διαμόρφωση του περιβάλλοντος FL και η υλοποίηση της διαδικασίας εκπαίδευσης.

## 3.5 Στρατηγική Εκπαίδευσης με Federated Learning

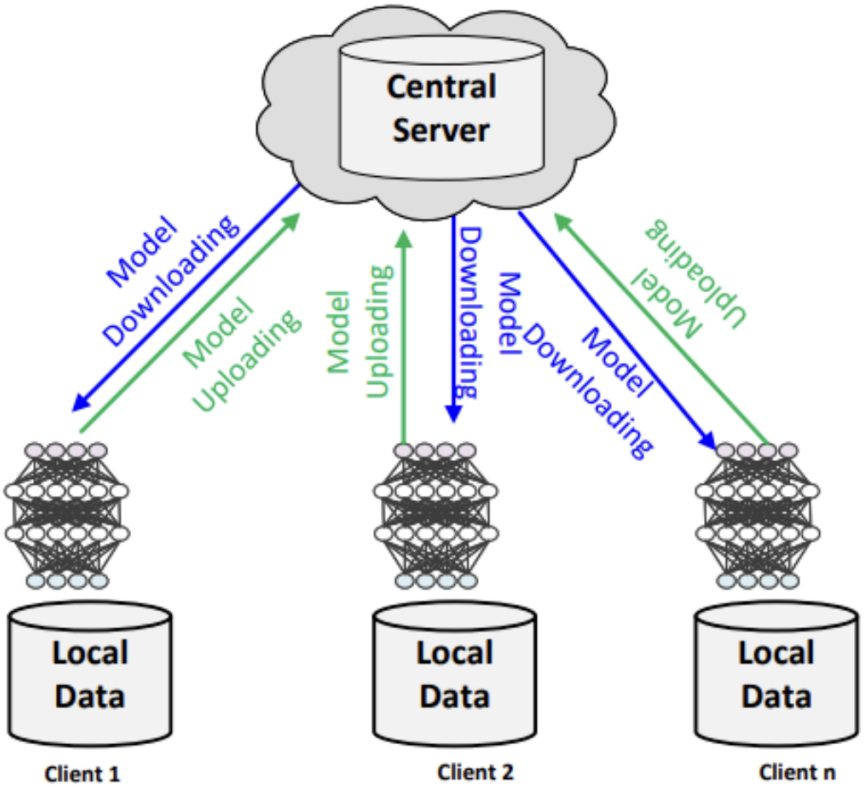
Μετά την προετοιμασία και τη δομημένη οργάνωση των υποσυνόλων δεδομένων, το επόμενο στάδιο της μεθοδολογίας αφορά τον σχεδιασμό και την υλοποίηση της στρατηγικής εκπαίδευσης. Η διαδικασία αυτή περιλαμβάνει την επιλογή του κατάλληλου FL framework, την αρχιτεκτονική του συστήματος, τις μεθόδους συγκέντρωσης, καθώς και τις τεχνικές ελέγχου και αξιολόγησης.

### 3.5.1 Πλαίσιο Ανάπτυξης

Όπως παρουσιάστηκε στην ενότητα 2.4.4, υπάρχουν πολλά διαθέσιμα frameworks για την υλοποίηση FL, καθένα με διαφορετικό προσανατολισμό και δυνατότητες. Για τις ανάγκες της παρούσας εργασίας, επιλέχθηκε το Flower (FLWR), ένα ανοικτού κώδικα και ευέλικτο πλαίσιο, το οποίο κρίθηκε καταλληλότερο για πειραματικού τύπου υλοποιήσεις. Η επιλογή βασίστηκε κυρίως στην απλότητα του API, την υποστήριξη για cross-silo FL σενάρια, καθώς και στη δυνατότητα ενσωμάτωσης με ευρέως χρησιμοποιούμενες βιβλιοθήκες όπως τα PyTorch, TensorFlow και scikit-learn [114]. Επιπλέον, η τεκμηρίωση και η κοινότητα υποστήριξης του Flower διευκόλυναν την ταχεία ανάπτυξη και τροποποίηση του συστήματος, προσφέροντας την απαραίτητη ευελιξία για τη διαμόρφωση και αξιολόγηση διαφορετικών στρατηγικών εκπαίδευσης.

### 3.5.2 Οργάνωση Κώδικα και Δομή Project

Το project δομήθηκε με καθαρό διαχωρισμό ρόλων μεταξύ του server και των clients. Ο server υλοποιεί την κεντρική λογική εκπαίδευσης, καθορίζει τις παραμέτρους του παγκόσμιου μοντέλου και εφαρμόζει τις στρατηγικές συγκέντρωσης. Κάθε client φορτώνει ένα διαφορετικό υποσύνολο δεδομένων (slice-based ή equal split) και εκπαιδεύει τοπικά το μοντέλο του. Όλες οι λειτουργίες οργανώθηκαν σε ξεχωριστά αρχεία Python για τον server, τους clients και τις βοηθητικές συναρτήσεις (utils). Η κωδικοποίηση πραγματοποιήθηκε εκτός του Jupyter σε αρχεία .py, για να υποστηρίζεται η κατανεμημένη εκτέλεση μέσω Command Line Interface (CLI). Η γενική αρχιτεκτονική της επικοινωνίας μεταξύ server και clients παρουσιάζεται ενδεικτικά στο Σχήμα 3.11, όπου απεικονίζεται η βασική ροή πληροφορίας σε περιβάλλον FL.




Σχήμα 3.11: *Απλοποιημένη απεικόνιση της αρχιτεκτονικής Federated Learning, όπου ο server συντονίζει την εκπαίδευση μέσω πολλαπλών απομονωμένων clients [6].*

### 3.5.3 Μοντέλο Machine Learning και Τοπική Λειτουργία Clients

Πριν την εφαρμογή των σεναρίων Federated Learning, αναπτύχθηκε και ρυθμίστηκε ένα απλό πλήρως συνδεδεμένο νευρωνικό δίκτυο, κατάλληλο για την εκτέλεση δυαδικής ταξινόμησης ροών δικτύου (κακόβουλες ή νόμιμες). Η αρχιτεκτονική του μοντέλου διατηρήθηκε σκόπιμα απλή, προκειμένου να περιοριστούν οι υπολογιστικές απαιτήσεις να εξασφαλίζεται η ομαλή εκπαίδευση σε όλους τους clients. Συγκεκριμένα, το δίκτυο περιλαμβάνει δύο κρυφά επίπεδα με ενεργοποιήσεις ReLU και ένα τελικό επίπεδο με έναν νευρώνα και sigmoid ενεργοποίηση, κατάλληλο για δυαδική ταξινόμηση.

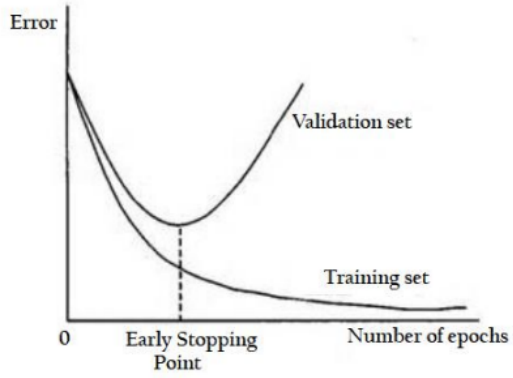
Για τη βελτιστοποίηση της απόδοσης του μοντέλου εφαρμόστηκε διαδικασία ρύθμισης υπερπαραμέτρων (hyperparameter tuning) με χρήση της μεθόδου grid search. Στη μέθοδο αυτή, για κάθε επιλεγμένη υπερπαράμετρο ορίζεται ένα σύνολο πιθανών τιμών και στη συνέχεια δοκιμάζονται συστηματικά όλοι οι πιθανοί συνδυασμοί τους, προκειμένου να εντοπιστεί η διαμόρφωση που μεγιστοποιεί την απόδοση του μοντέλου.

Οι υπερπαράμετροι που εξετάστηκαν περιλαμβάνουν τον αριθμό νευρώνων σε κάθε κρυφό επίπεδο, τον ρυθμό εκμάθησης (learning rate) και το μέγεθος παρτίδας (batch size). Για λόγους περιορισμού της πολυπλοκότητας και του χρόνου εκτέλεσης, η βασική αρχιτεκτονική του δικτύου παρέμεινε σταθερή, με δύο κρυφά επίπεδα και ReLU ενεργοποιήσεις.

Παράλληλα, χρησιμοποιήθηκε η τεχνική του early stopping, η οποία επιτρέπει τον αυτόματο τερματισμό της εκπαίδευσης όταν δεν παρατηρείται περαιτέρω βελτίωση στο validation loss,

περιορίζοντας έτσι το φαινόμενο της υπερεκπαίδευσης (overfitting) [115]. Συγκεκριμένα, το early stopping παρακολουθεί την απόδοση του μοντέλου σε κάθε εποχή και η εκπαίδευση σταματά αν το validation loss δεν μειωθεί για τρία συνεχόμενα epochs (patience = 3). Η ρύθμιση αυτή θεωρείται επαρκής ώστε να αποφεύγονται τόσο οι πρόωρες διακοπές λόγω τυχαίων διακυμάνσεων όσο και η άσκοπη συνέχιση της εκπαίδευσης. Με τον τρόπο αυτό, το μοντέλο διατηρεί τη δυνατότητα γενίκευσης και αποδίδει ικανοποιητικά και σε μη ορατά δεδομένα.

Η λογική του Early Stopping απεικονίζεται σχηματικά στο Σχήμα 3.12, όπου παρουσιάζεται η μεταβολή του αλιδατιον λοσς σε συνάρτηση με τα εποχης.




Σχήμα 3.12: *Ενδεικτική απεικόνιση της λειτουργίας του Early Stopping κατά την εκπαίδευση*

Ο Πίνακας 3.6 συνοψίζει τις τιμές που δοκιμάστηκαν για κάθε υπερπαράμετρο, καθώς και την τελική επιλογή που υιοθετήθηκε στο βέλτιστο μοντέλο.

| **Hyperparameter** | **Grid** | **Value** |
|---|---|---|
| Αριθμός νευρώνων στο 1ο επίπεδο | {8, 16, 32} | 16 |
| Αριθμός νευρώνων στο 2ο επίπεδο | {4, 8, 16} | 8 |
| Learning rate | {0.001, 0.0005, 0.0001} | 0.001 |
| Batch size | {32, 64, 128} | 64 |
| Activation function | {ReLU} | ReLU |
| Loss function | Binary Crossentropy | Binary Crossentropy |
| Optimizer | Adam | Adam |
| Early Stopping | Yes (patience = 3) | Yes |

Πίνακας 3.6: *Τιμές Grid Search και επιλεγμένες τιμές για το μοντέλο Machine Learning*

Το ίδιο ακριβώς μοντέλο χρησιμοποιείται αμετάβλητο ως τοπικό μοντέλο σε κάθε client του συστήματος FL, ανεξαρτήτως στρατηγικής συγκέντρωσης ή τρόπου κατανομής δεδομένων. Με τον τρόπο αυτό διασφαλίζεται η δίκαιη και συγκρίσιμη αξιολόγηση των διαφορετικών σεναρίων, καθώς η απόδοση επηρεάζεται αποκλειστικά από τη διαδικασία εκπαίδευσης και όχι από διαφοροποιήσεις στην αρχιτεκτονική ή στις παραμέτρους του μοντέλου.

### 3.5.4 Λειτουργία Server Συναρτήσεις Συγκέντρωσης

Ο server του Flower ελέγχει τη ροή της εκπαίδευσης, συγχωνεύοντας τα τοπικά μοντέλα των clients σε κάθε γύρο μέσω συναρτήσεων συγκέντρωσης. Στην παρούσα εργασία εφαρ-

μόστηκαν τρεις στρατηγικές: FedAvg, FedAvgM και FedAdam. Η FedAvg χρησιμοποιήθηκε ως σημείο αναφοράς για τη σταθμισμένη μέση τιμή, η FedAvgM για τη σταθεροποίηση μέσω ορμής και η FedAdam για πιο προσαρμοστική ενημέρωση των παραμέτρων. Η επιλογή αυτών βασίστηκε σε ευρήματα της βιβλιογραφίας και στη θεωρητική ανάλυση της Ενότητας 2.4.5, λαμβάνοντας υπόψη την πιθανή ετερογένεια των clients.

## 3.6 Μετρικές Αξιολόγησης

Για την αξιολόγηση της απόδοσης των μοντέλων ταξινόμησης χρησιμοποιήθηκαν πέντε βασικές μετρικές: Accuracy, Precision, Recall, F1 Score και F2 Score. Παρακάτω περιγράφεται αναλυτικά ο ρόλος κάθε μέτρου καθώς και ο τρόπος υπολογισμού του.

### Accuracy

Το Accuracy εκφράζει το ποσοστό των σωστά ταξινομημένων δειγμάτων επί του συνόλου.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3.1}$$

Όπου:

- TP (True Positives): κακόβουλες ροές που ταξινομήθηκαν σωστά ως κακόβουλες
- TN (True Negatives): νόμιμες ροές που ταξινομήθηκαν σωστά ως νόμιμες
- FP (False Positives): νόμιμες ροές που ταξινομήθηκαν λανθασμένα ως κακόβουλες
- FN (False Negatives): κακόβουλες ροές που ταξινομήθηκαν λανθασμένα ως νόμιμες

### Precision

Το Precision μετράει την ακρίβεια της πρόβλεψης θετικών περιπτώσεων, δηλαδή πόσες από τις ροές που ταξινομήθηκαν ως κακόβουλες ήταν πράγματι κακόβουλες.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{3.2}$$

### Recall

Η Recall (ή Sensitivity) δείχνει το ποσοστό των πραγματικών κακόβουλων ροών που εντοπίστηκαν σωστά από το μοντέλο. Είναι κρίσιμη σε εφαρμογές ασφάλειας.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3.3}$$

### F1 Score

Το F1 Score είναι ο αρμονικός μέσος των Precision και Recall, προσφέροντας έναν συμβιβασμό μεταξύ αυτών.

$$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{3.4}$$

### F2 Score

Το F2 Score είναι μια γενίκευση του F1 Score, που δίνει περισσότερη έμφαση στην Recall. Στην περίπτωσή μας, χρησιμοποιήθηκε με $\beta = 2$, ώστε να ενισχύεται η σημασία της ανίχνευσης

των κακόβουλων ροών.

$$\mathrm{F}_\beta = (1+\beta^2) \cdot \frac{\mathrm{Precision} \cdot \mathrm{Recall}}{(\beta^2 \cdot \mathrm{Precision}) + \mathrm{Recall}}, \quad \beta = 2 \tag{3.5}$$

Η επιλογή του F2 Score ως κύριο κριτήριο βασίστηκε στο γεγονός ότι η παράβλεψη μιας κακόβουλης ροής (FN) θεωρείται πιο επικίνδυνη από την εσφαλμένη επισήμανση μιας νόμιμης (FP), καθιστώντας την Recall-ευαίσθητη αξιολόγηση καταλληλότερη για την παρούσα εργασία.

Κεφάλαιο 4

# Αποτελέσματα

## 4.1 Εισαγωγή

Το παρόν κεφάλαιο επικεντρώνεται στην παρουσίαση και ανάλυση των αποτελεσμάτων που προέκυψαν από την εφαρμογή διαφορετικών στρατηγικών FL. Όπως περιγράφηκε στο προηγούμενο κεφάλαιο, αξιολογήθηκαν συνολικά έξι περιπτώσεις εκπαίδευσης, που προκύπτουν από τον συνδυασμό τριών στρατηγικών συγκέντρωσης (FedAvg, FedAvgM, FedAdam) και δύο τύπων κατανομής δεδομένων (Equal Split και Network Slicing).

Για κάθε μία από τις έξι περιπτώσεις, εκπαιδεύτηκαν πολλαπλά παγκόσμια μοντέλα, αποθηκεύοντας τα βάρη τους ανά γύρο. Στη συνέχεια, αξιολογήθηκε κάθε αποθηκευμένο μοντέλο στο τελικό test set, και επιλέχθηκε εκείνο με την υψηλότερη τιμή F2 Score. Το συγκεκριμένο μέτρο χρησιμοποιήθηκε ως βασικό κριτήριο επιλογής, καθώς δίνει έμφαση στην ανάκληση (Recall), η οποία θεωρείται κρίσιμη σε σενάρια ανίχνευσης εισβολών — όπου η εσφαλμένη κατάταξη μιας κακόβουλης ροής ως νόμιμης μπορεί να έχει σοβαρές επιπτώσεις.

Παράλληλα, στις τέσσερις από τις έξι περιπτώσεις (FedAvgM και FedAdam, για Splits και Slices), εφαρμόστηκε διαδικασία λεπτομερούς προσαρμογής παραμέτρων (fine-tuning), προκειμένου να βελτιστοποιηθεί η απόδοση των αντίστοιχων παγκόσμιων μοντέλων. Οι τιμές των υπερπαραμέτρων επιλέχθηκαν πειραματικά, βασισμένες σε επαναλαμβανόμενες δοκιμές και ανάλυση των μετρικών απόδοσης.

Τέλος, για σκοπούς γενικότερης σύγκρισης, αξιολογήθηκε και ένα συγκεντρωτικό μοντέλο ML, το οποίο εκπαιδεύτηκε τοπικά και παρουσιάζεται στο τέλος του κεφαλαίου ως σημείο αναφοράς.

## 4.2 Αποτελέσματα ανά Περίπτωση Federated Learning

### 4.2.1 Τοπικό Μοντέλο Machine Learning

Για την αξιολόγηση του μοντέλου ML, το οποίο εκπαιδεύτηκε στο πλήρες επεξεργασμένο σύνολο δεδομένων πριν την εφαρμογή του FL , χρησιμοποιήθηκε το global test set, το οποίο χρησιμοποιείται εξίσου και για την αξιολόγηση των FL μοντέλων. Ο confusion matrix, ο οποίος συνοψίζει τη συχνότητα σωστών και λανθασμένων προβλέψεων για κάθε κλάση, παρατίθεται παρακάτω:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} = \frac{770 + 635}{770 + 635 + 26 + 15} = 0.9717 \tag{4.1}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} = \frac{770}{770 + 26} = 0.9673 \tag{4.2}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} = \frac{770}{770 + 15} = 0.9810 \tag{4.3}$$

$$\text{F1 Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2 \cdot 0.9673 \cdot 0.9810}{0.9673 + 0.9810} = 0.9741 \tag{4.4}$$

$$\text{F2 Score} = \frac{5 \cdot \text{Precision} \cdot \text{Recall}}{4 \cdot \text{Precision} + \text{Recall}} = \frac{5 \cdot 0.9673 \cdot 0.9810}{4 \cdot 0.9673 + 0.9810} = 0.9775 \tag{4.5}$$

| **Μετρική** | **Τιμή** |
|---|---|
| Accuracy | 0.9717 |
| Precision | 0.9673 |
| Recall | 0.9810 |
| F1 Score | 0.9741 |
| F2 Score | 0.9775 |

Πίνακας 4.1: *Αποτελέσματα μοντέλου Machine Learning*

### 4.2.2 Αποτελέσματα Federated Learning με FedAvg

#### 4.2.2.1 Αποτέλεσμα FedAvg με Ισοκατανομή Δεδομένων

Σε αυτή την περίπτωση εφαρμόστηκε η στρατηγική συγκέντρωσης FedAvg, με τα δεδομένα να έχουν κατανεμηθεί ομοιόμορφα σε τρεις clients, χωρίς θεματική εξειδίκευση ανά τομή δικτύου. Κάθε client εκπαιδεύει τοπικά το ίδιο μοντέλο ML που περιγράφηκε προηγουμένως και αποστέλλει τα βάρη στον κεντρικό server για ομοιόμορφη μέση συγκέντρωση.

Η αξιολόγηση του τελικού συγκεντρωτικού μοντέλου πραγματοποιήθηκε στο κοινό global test set, χρησιμοποιώντας τα ίδια κριτήρια όπως και στο προηγούμενο τοπικά εκπαιδευμένο μοντέλο. Ο confusion matrix, ο οποίος συνοψίζει τη συχνότητα σωστών και λανθασμένων προβλέψεων για κάθε κλάση, παρατίθεται παρακάτω:

Οι βασικές μετρικές υπολογίστηκαν βάσει των παραπάνω τιμών ως εξής:

$$\text{Accuracy} = \frac{637 + 762}{637 + 762 + 24 + 23} = \frac{1399}{1446} = 0.9675 \tag{4.6}$$

$$\text{Precision} = \frac{762}{762 + 24} = \frac{762}{786} = 0.9695 \tag{4.7}$$

$$\text{Recall} = \frac{762}{762 + 23} = \frac{762}{785} = 0.9707 \tag{4.8}$$

$$\text{F1 Score} = \frac{2 \cdot 0.9695 \cdot 0.9707}{0.9695 + 0.9707} = 0.9701 \tag{4.9}$$

$$\text{F2 Score} = \frac{5 \cdot 0.9695 \cdot 0.9707}{4 \cdot 0.9695 + 0.9707} = 0.9704 \tag{4.10}$$

| Μετρική | Τιμή |
|---|---|
| Accuracy | 0.9675 |
| Precision | 0.9695 |
| Recall | 0.9707 |
| F1 Score | 0.9701 |
| F2 Score | 0.9704 |

Πίνακας 4.2: *Αποτελέσματα μοντέλου FedAvg με Equal Splits*

#### 4.2.2.2 Αποτέλεσμα FedAvg με Κατανομή κατά Network Slices

Για τη δεύτερη περίπτωση, χρησιμοποιήθηκε η στρατηγική FedAvg με κατανομή των δεδομένων κατά network slices στους τρεις clients. Το μοντέλο εκπαιδεύτηκε σε συνολικά 35 γύρους και τα καλύτερα βάρη επιλέχθηκαν βάσει της απόδοσης στο σύνολο επικύρωσης. Η τελική αξιολόγηση πραγματοποιήθηκε στο κοινό global test set, και ο confusion matrix είχε την εξής μορφή:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{765 + 544}{765 + 544 + 117 + 20} = 0.9053 \tag{4.11}$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{765}{765 + 117} = 0.8673 \tag{4.12}$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{765}{765 + 20} = 0.9745 \tag{4.13}$$

$$\text{F1 Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2 \cdot 0.8673 \cdot 0.9745}{0.8673 + 0.9745} = 0.9178 \tag{4.14}$$

$$\text{F2 Score} = \frac{5 \cdot \text{Precision} \cdot \text{Recall}}{4 \cdot \text{Precision} + \text{Recall}} = \frac{5 \cdot 0.8673 \cdot 0.9745}{4 \cdot 0.8673 + 0.9745} = 0.9039 \tag{4.15}$$

| Μετρική | Τιμή |
|---|---|
| Accuracy | 0.9053 |
| Precision | 0.8673 |
| Recall | 0.9745 |
| F1 Score | 0.9178 |
| F2 Score | 0.9039 |

Πίνακας 4.3: *Αποτελέσματα FedAvg με Network Slices Split*

### 4.2.3 Αποτελέσματα Federated Learning με FedAvgM

Η στρατηγική FedAvgM αποτελεί μια παραλλαγή του FedAvg, στην οποία εισάγεται ο μηχανισμός της επιτάχυνσης μέσω ορμής (momentum). Αυτό στοχεύει στην ταχύτερη και πιο σταθερή σύγκλιση του παγκόσμιου μοντέλου κατά τη διάρκεια των γύρων εκπαίδευσης.

Πριν την τελική εκπαίδευση με τη στρατηγική FedAvgM, εφαρμόστηκε μια διφασική διαδικασία επιλογής υπερπαραμέτρων, προκειμένου να επιτευχθεί βέλτιστη απόδοση και σταθερότητα κατά τη διάρκεια της εκπαίδευσης.

- Στην πρώτη φάση, πραγματοποιήθηκε διερευνητική αναζήτηση (exploratory grid search) με σχετικά υψηλές τιμές του ρυθμού μάθησης (Learning Rate) και της παραμέτρου ορμής (Momentum), ώστε να εντοπιστούν περιοχές με υψηλό δυναμικό απόδοσης, ακόμα και αν η εκπαίδευση παρουσίαζε αστάθεια.
- Στη δεύτερη φάση, χρησιμοποιήθηκαν τα αποθηκευμένα βάρη από τις καλύτερες στιγμές αυτών των εκτελέσεων ως αρχικά σημεία, και η εκπαίδευση συνεχίστηκε με πολύ μικρότερες τιμές του Learning Rate, με στόχο τη σταθερή βελτίωση της απόδοσης.

Η προσέγγιση αυτή αξιοποιεί τα πλεονεκτήματα της γρήγορης σύγκλισης στην αρχή και της σταθερής βελτιστοποίησης στη συνέχεια, παρόμοια με τεχνικές όπως το warm restart ή το fine-tuning from high-energy checkpoints.

Οι υπερπαράμετροι που δοκιμάστηκαν σε κάθε φάση παρουσιάζονται στους παρακάτω πίνακες:

| Hyperparameter | Grid |
|---|---|
| Learning Rate | {0.1, 0.3, 0.6, 0.8} |
| Momentum | {0.80, 0.85, 0.90, 0.95} |

Πίνακας 4.4: *Επιλεγμένοι συνδυασμοί υπερπαραμέτρων στη φάση εξερεύνησης (Phase 1 – Exploratory Grid Search)*

| Hyperparameter | Grid |
|---|---|
| Learning Rate | {0.001, 0.003, 0.005} |
| Momentum | {0.85, 0.90, 0.95} |

Πίνακας 4.5: *Συνδυασμοί λεπτομερούς βελτιστοποίησης στη Φάση 2 (Fine-Tuning)*

Η τελική επιλογή υπερπαραμέτρων για κάθε μοντέλο παρουσιάζεται αναλυτικά στα αντίστοιχα υποκεφάλαια που ακολουθούν.

#### 4.2.3.1 Αποτέλεσμα FedAvgM με Ισοκατανομή Δεδομένων (Equal Splits)

Για το συγκεκριμένο σενάριο, χρησιμοποιήθηκαν αρχικά τα αποθηκευμένα βάρη από τα καλύτερα στιγμιότυπα της πρώτης φάσης διερεύνησης υπερπαραμέτρων (Phase 1), όπως περιγράφηκε προηγουμένως. Στη συνέχεια, πραγματοποιήθηκε δεύτερη φάση λεπτομερούς εκπαίδευσης (Phase 2) με μικρότερες τιμές Learning Rate και Momentum, με αρχικοποίηση από αυτά τα βάρη.

Ο συνδυασμός υπερπαραμέτρων που οδήγησε στο βέλτιστο τελικό αποτέλεσμα για την περίπτωση της ισοκατανομής ήταν: Learning Rate = 0.001 και Momentum = 0.95. Το τελικό μοντέλο επιλέχθηκε βάσει της μέγιστης τιμής της μετρικής F2 Score και αξιολογήθηκε στο κοινό global test set. Ο confusion matrix που προέκυψε παρουσιάζεται παρακάτω:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{757 + 632}{757 + 632 + 29 + 28} = 0.9606 \tag{4.16}$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{757}{757 + 29} = 0.9631 \tag{4.17}$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{757}{757 + 28} = 0.9643 \tag{4.18}$$

$$\text{F1 Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2 \cdot 0.9631 \cdot 0.9643}{0.9631 + 0.9643} = 0.9637 \tag{4.19}$$

$$\text{F2 Score} = \frac{5 \cdot \text{Precision} \cdot \text{Recall}}{4 \cdot \text{Precision} + \text{Recall}} = \frac{5 \cdot 0.9631 \cdot 0.9643}{4 \cdot 0.9631 + 0.9643} = 0.9640 \tag{4.20}$$

| **Μετρική** | **Τιμή** |
|---|---|
| Accuracy | 0.9606 |
| Precision | 0.9631 |
| Recall | 0.9643 |
| F1 Score | 0.9637 |
| F2 Score | 0.9640 |

Πίνακας 4.6: *Αποτελέσματα FedAvgM με Equal Splits*

#### 4.2.3.2 Αποτέλεσμα FedAvgM με Κατανομή κατά Network Slices

Αντίστοιχα με την προηγούμενη περίπτωση, η εκπαίδευση πραγματοποιήθηκε με τη στρατηγική FedAvgM, εφαρμόζοντας αυτή τη φορά κατανομή των δεδομένων στους clients βάσει των αντίστοιχων network slices (URLLC, mMTC, eMBB). Το μοντέλο εκπαιδεύτηκε με αρχικοποίηση από αποθηκευμένα βάρη της πρώτης φάσης (Phase 1), και στη συνέχεια βελτιστοποιήθηκε σε δεύτερη φάση (Phase 2) με χαμηλότερες τιμές υπερπαραμέτρων.

Ο συνδυασμός Learning Rate = 0.0005 και Momentum = 0.90 παρήγαγε το καλύτερο αποτέλεσμα κατά τη δεύτερη φάση, σύμφωνα με τη μετρική F2 Score. Η τελική αξιολόγηση του μοντέλου πραγματοποιήθηκε στο κοινό global test set, και τα αποτελέσματα συνοψίζονται παρακάτω με βάση τον confusion matrix και τις κύριες μετρικές ταξινόμησης.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{759 + 595}{759 + 595 + 66 + 26} = \frac{1354}{1446} = 0.9364 \tag{4.21}$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{759}{759 + 66} = \frac{759}{825} = 0.9200 \tag{4.22}$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{759}{759 + 26} = \frac{759}{785} = 0.9669 \tag{4.23}$$

$$\text{F1 Score} = \frac{2 \cdot 0.9200 \cdot 0.9669}{0.9200 + 0.9669} = 0.9429 \tag{4.24}$$

$$\text{F2 Score} = \frac{5 \cdot 0.9200 \cdot 0.9669}{4 \cdot 0.9200 + 0.9669} = 0.9361 \tag{4.25}$$

| **Μετρική** | **Τιμή** |
|---|---|
| Accuracy | 0.9364 |
| Precision | 0.9200 |
| Recall | 0.9669 |
| F1 Score | 0.9429 |
| F2 Score | 0.9361 |

Πίνακας 4.7: *Αποτελέσματα FedAvgM με Network Slices*

### 4.2.4 Αποτελέσματα με FedAdam

Η στρατηγική FedAdam αποτελεί επέκταση του κλασικού Federated Averaging, ενσωματώνοντας τις έννοιες της προσαρμοστικής βελτιστοποίησης μέσω των υπερπαραμέτρων Learning Rate ($\eta$), Momentum ($\beta_1$) και Second Moment Estimate ($\beta_2$). Στο πλαίσιο της παρούσας εργασίας, η τιμή του $\beta_2$ παρέμεινε σταθερή (0.99), ενώ οι $\eta$ και $\beta_1$ αποτέλεσαν αντικείμενο διερεύνησης.

Όπως και στην περίπτωση του FedAvgM, εφαρμόστηκε μια διφασική προσέγγιση επιλογής υπερπαραμέτρων:

- Στην πρώτη φάση, πραγματοποιήθηκε exploratory grid search σε σχετικά υψηλές τιμές $\eta$ και $\beta_1$, προκειμένου να εντοπιστούν συνδυασμοί που οδηγούσαν σε υψηλές, έστω και προσωρινές, αποδόσεις.

- Στη δεύτερη φάση, τα καλύτερα μοντέλα από την πρώτη φάση χρησιμοποιήθηκαν ως σημεία αρχικοποίησης για εκπαίδευση με χαμηλότερες τιμές $\eta$, με στόχο την πιο σταθερή και βελτιωμένη σύγκλιση. Η επιλογή των τελικών μοντέλων έγινε βάσει της υψηλότερης τιμής F2 Score στο validation set.

Οι συνδυασμοί υπερπαραμέτρων που εξετάστηκαν σε κάθε φάση παρουσιάζονται στους ακόλουθους πίνακες:

| Hyperparameter | Grid |
|---|---|
| $\eta$ (Learning Rate) | {0.01, 0.04, 0.07 0,09,} |
| $\beta_1$ (Momentum) | {0.80, 0.85, 0.90, 0.95} |

Πίνακας 4.8: *Επιλεγμένοι συνδυασμοί υπερπαραμέτρων στη φάση εξερεύνησης για FedAdam (Phase 1 – Exploratory Grid Search)*

| Υπερπαραμέτρος | Grid |
|---|---|
| $\eta$ (Learning Rate) | {0.001, 0.0005} |
| $\beta_1$ (Momentum) | {0.90, 0,92, 0.95} |

Πίνακας 4.9: *Συνδυασμοί υπερπαραμέτρων για λεπτομερή εκπαίδευση με FedAdam (Phase 2 – Fine-Tuning)*

Στις υποενότητες που ακολουθούν, παρουσιάζονται τα τελικά αποτελέσματα για κάθε τύπο κατανομής δεδομένων.

#### 4.2.4.1 Αποτέλεσμα FedAdam με Ισομερή Κατανομή

Σε αυτή την περίπτωση, η στρατηγική FedAdam εφαρμόστηκε με ισομερή κατανομή του προεπεξεργασμένου συνόλου εκπαίδευσης στους τρεις clients. Η επιλογή υπερπαραμέτρων βασίστηκε στη διαδικασία δύο φάσεων που περιγράφηκε νωρίτερα, με τη βέλτιστη επίδοση να επιτυγχάνεται για $\eta = 0.001$ και $\beta_1 = 0.95$, ενώ η τιμή του $\beta_2$ διατηρήθηκε σταθερή στο 0.99.

Το αντίστοιχο μοντέλο, που παρουσίασε τη μέγιστη τιμή F2 Score στο validation set, αξιολογήθηκε τελικά στο κοινό global test set. Ο confusion matrix και οι υπολογισμοί των βασικών μετρικών για την κλάση Malicious παρουσιάζονται στη συνέχεια:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{771 + 625}{771 + 625 + 36 + 14} = \frac{1396}{1446} = 0.9654 \tag{4.26}$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{771}{771 + 36} = \frac{771}{807} = 0.9554 \tag{4.27}$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{771}{771 + 14} = \frac{771}{785} = 0.9822 \tag{4.28}$$

$$\text{F1 Score} = \frac{2 \cdot 0.9554 \cdot 0.9822}{0.9554 + 0.9822} = 0.9686 \tag{4.29}$$

$$\text{F2 Score} = \frac{5 \cdot 0.9554 \cdot 0.9822}{4 \cdot 0.9554 + 0.9822} = 0.9653 \tag{4.30}$$

| **Μετρική** | **Τιμή** |
|---|---|
| Accuracy | 0.9654 |
| Precision | 0.9554 |
| Recall | 0.9822 |
| F1 Score | 0.9686 |
| F2 Score | 0.9653 |

Πίνακας 4.10: *Αποτελέσματα FedAdam με Equal Splits*

#### 4.2.4.2 Αποτέλεσμα FedAdam με Κατανομή κατά Network Slices

Ολοκληρώνοντας την ανάλυση των έξι περιπτώσεων, εξετάζεται η εφαρμογή της στρατηγικής FedAdam με κατανομή των δεδομένων βάσει των network slices στους τρεις clients. Όπως και στις προηγούμενες περιπτώσεις, εφαρμόστηκε η διφασική διαδικασία επιλογής υπερπαραμέτρων, με τον συνδυασμό $\eta = 0.001$ και $\beta_1 = 0.95$ να προσφέρει την υψηλότερη τιμή F2 Score.

Το τελικό μοντέλο αξιολογήθηκε στο κοινό global test set, και τα αποτελέσματα της ταξινόμησης συνοψίζονται παρακάτω:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{740 + 622}{740 + 622 + 39 + 45} = \frac{1362}{1446} = 0.9419 \tag{4.31}$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{740}{740 + 39} = \frac{740}{779} = 0.9499 \tag{4.32}$$

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{740}{740 + 45} = \frac{740}{785} = 0.9427 \tag{4.33}$$

$$\text{F1 Score} = \frac{2 \cdot 0.9499 \cdot 0.9427}{0.9499 + 0.9427} = 0.9463 \tag{4.34}$$

$$\text{F2 Score} = \frac{5 \cdot 0.9499 \cdot 0.9427}{4 \cdot 0.9499 + 0.9427} = 0.9419 \tag{4.35}$$

| **Μετρική** | **Τιμή** |
|---|---|
| Accuracy | 0.9419 |
| Precision | 0.9499 |
| Recall | 0.9427 |
| F1 Score | 0.9463 |
| F2 Score | 0.9419 |

Πίνακας 4.11: *Αποτελέσματα FedAdam με Slices*

Οι έξι περιπτώσεις εκπαίδευσης που εξετάστηκαν περιλαμβάνουν διαφορετικούς συνδυασμούς στρατηγικών συγκέντρωσης και κατανομών δεδομένων. Η ενότητα αυτή κατέγραψε τα αποτελέσματα κάθε περίπτωσης με βάση επιλεγμένες μετρικές απόδοσης. Στο επόμενο τμήμα ακολουθεί συγκριτική επισκόπηση των μοντέλων με σκοπό την ανάδειξη των πιο αποτελεσματικών προσεγγίσεων.

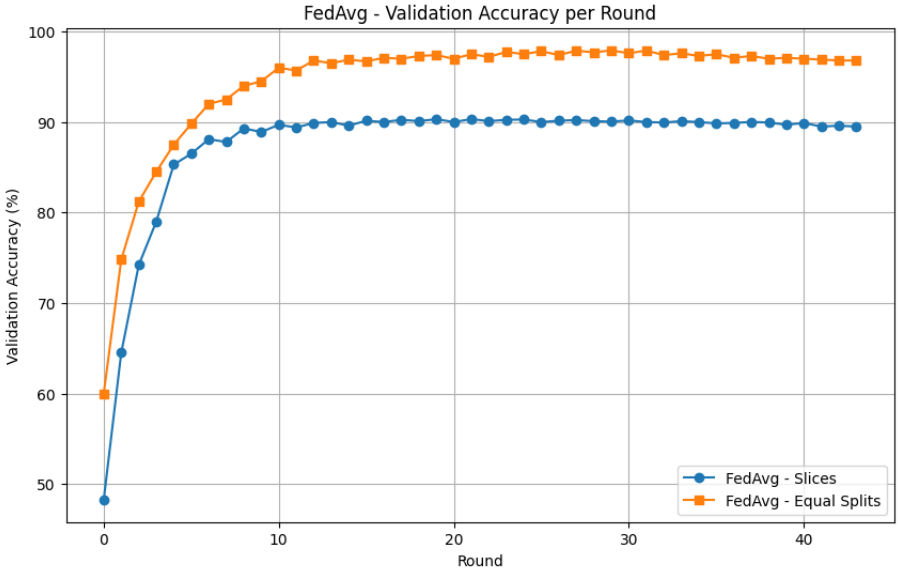
## 4.3 Συγκριτική Αξιολόγηση

Η παρούσα ενότητα συνοψίζει και συγκρίνει τα αποτελέσματα όλων των περιπτώσεων εκπαίδευσης FL που παρουσιάστηκαν προηγουμένως, προκειμένου να εξαχθούν συμπεράσματα σχετικά με την αποτελεσματικότητα κάθε στρατηγικής και κατανομής δεδομένων.

### 4.3.1 Πορεία Εκπαίδευσης και Σύγκλισης

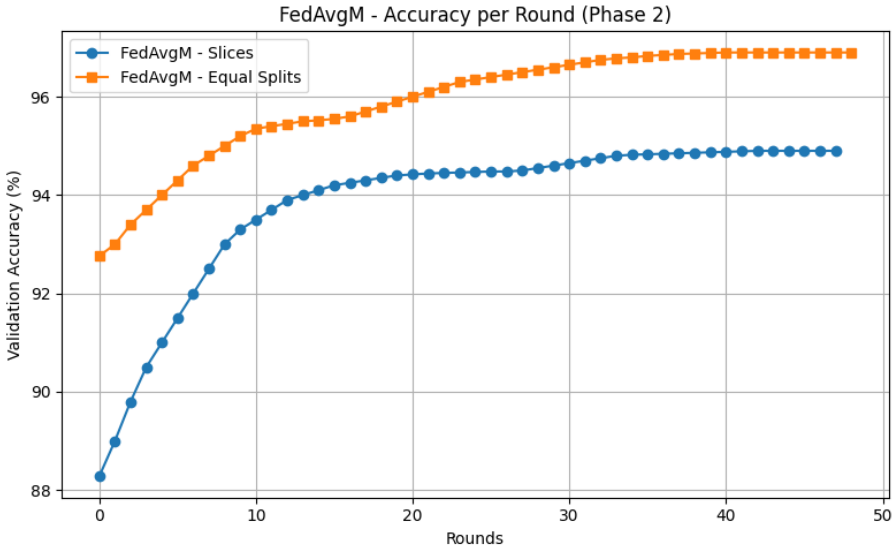
Πέρα από τις τελικές μετρικές απόδοσης, ιδιαίτερο ενδιαφέρον παρουσιάζει και η πορεία σύγκλισης του συστήματος κατά τη διάρκεια της εκπαίδευσης. Στα ακόλουθα σχήματα παρουσιάζεται η εξέλιξη του Validation Accuracy ανά γύρο για κάθε συνάρτηση συγκέντρωσης, τόσο στην περίπτωση ισοκατανομής δεδομένων όσο και στην περίπτωση κατανομής κατά Network Slices.

Για την καλύτερη κατανόηση της πορείας εκπαίδευσης, το Σχήμα 4.1 απεικονίζει την εξέλιξη του Validation Accuracy ανά γύρο για τη στρατηγική FedAvg.



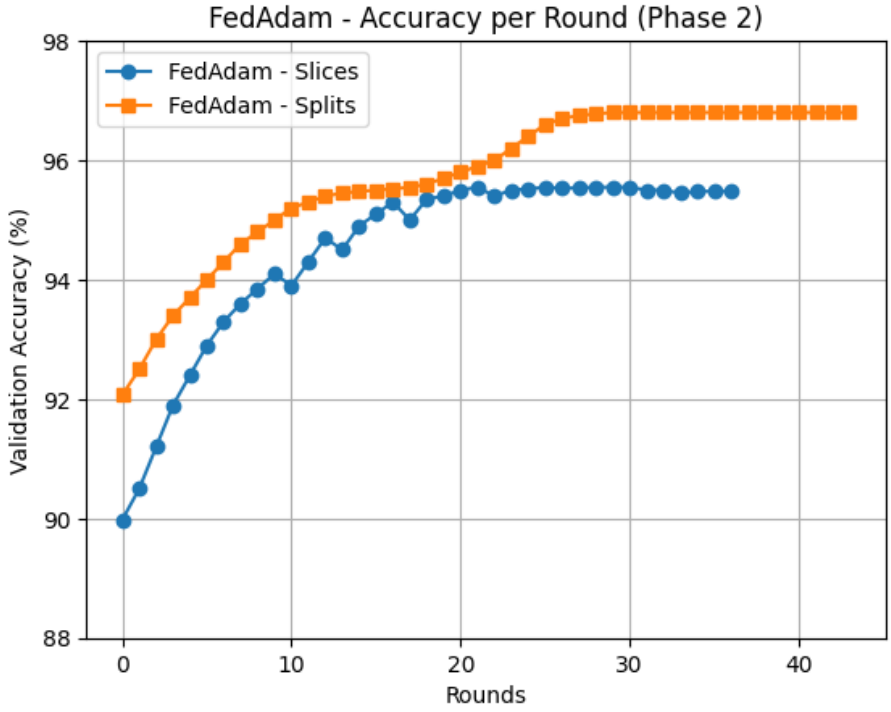

Σχήμα 4.1: *Validation Accuracy per round για τη στρατηγική FedAvg.*

Στο Σχήμα 4.2 παρουσιάζεται η πορεία του Validation Accuracy στη δεύτερη φάση εκπαίδευσης με τη στρατηγική FedAvgM, τόσο για το σενάριο ισοκατανομής όσο και για την κατανομή κατά Network Slices.




Σχήμα 4.2: *Εξέλιξη Validation Accuracy per round για τη στρατηγική FedAvgM (Phase 2).*

Τέλος, το Σχήμα 4.3 απεικονίζει τη μεταβολή του Validation Accuracy στη δεύτερη φάση εκπαίδευσης με τη στρατηγική FedAdam.



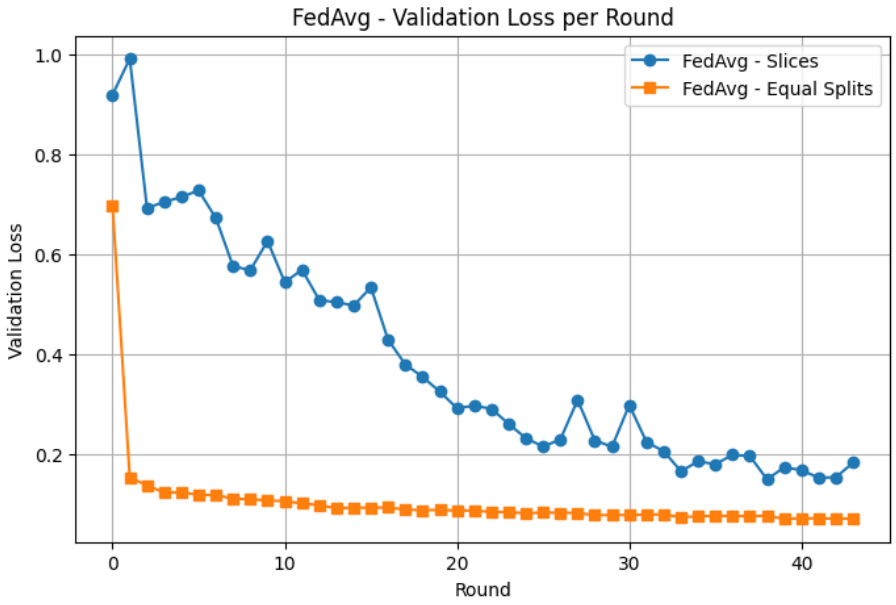

Σχήμα 4.3: *Εξέλιξη Validation Accuracy per round για τη στρατηγική FedAdam.*

Όπως παρατηρείται σε όλα τα παραπάνω σχήματα, σε κάθε περίπτωση η καμπύλη του Validation Accuracy για το σενάριο ισοκατανομής δεδομένων (Splits) υπερτερεί συστηματικά έναντι της αντίστοιχης καμπύλης για το Network Slicing (Slices), καθ' όλη τη διάρκεια της εκπαίδευσης. Το φαινόμενο αυτό επιβεβαιώνει τη δυσκολία που εισάγει η μη ισομερής και πιο ρεαλιστική κατανομή των δεδομένων ανά slice, υπογραμμίζοντας τη σημασία της επιλογής κατάλληλων τεχνικών συγκέντρωσης για τη βελτίωση της απόδοσης σε τέτοιες συνθήκες.

### 4.3.2 Πορεία του Validation Loss κατά τη διάρκεια της Εκπαίδευσης

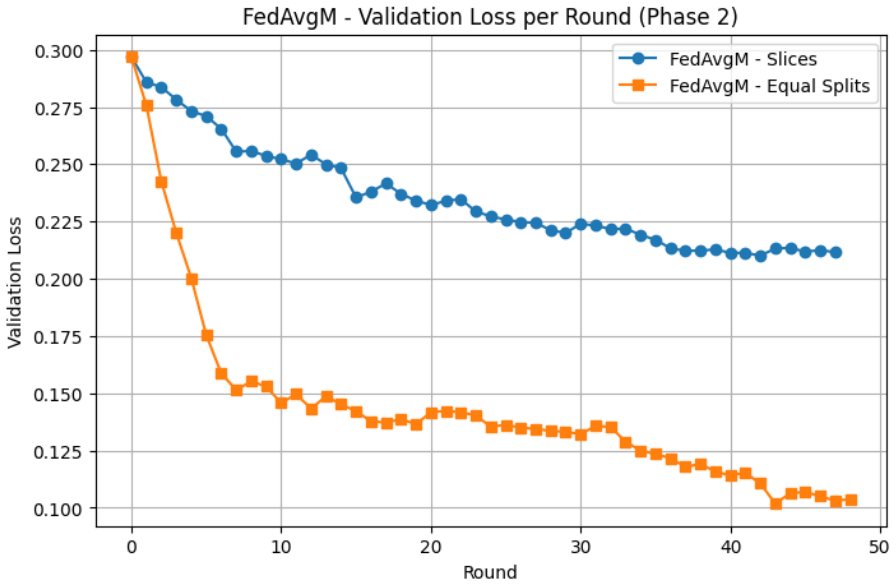
Εκτός από τις τελικές μετρικές αξιολόγησης και το Validation Accuracy, ιδιαίτερη σημασία έχει και η παρακολούθηση της πορείας του Validation Loss κατά τη διάρκεια των γύρων εκπαίδευσης, καθώς παρέχει πληροφορίες για τη σύγκλιση των μοντέλων και τη σταθερότητα της διαδικασίας εκπαίδευσης. Στα παρακάτω σχήματα παρουσιάζεται η εξέλιξη του Validation Loss για κάθε συνάρτηση συγκέντρωσης, τόσο στην περίπτωση ισοκατανομής δεδομένων όσο και στην περίπτωση κατανομής κατά Network Slices.

Το Σχήμα 4.4 απεικονίζει τη μεταβολή του Validation Loss ανά γύρο για τη στρατηγική FedAvg.



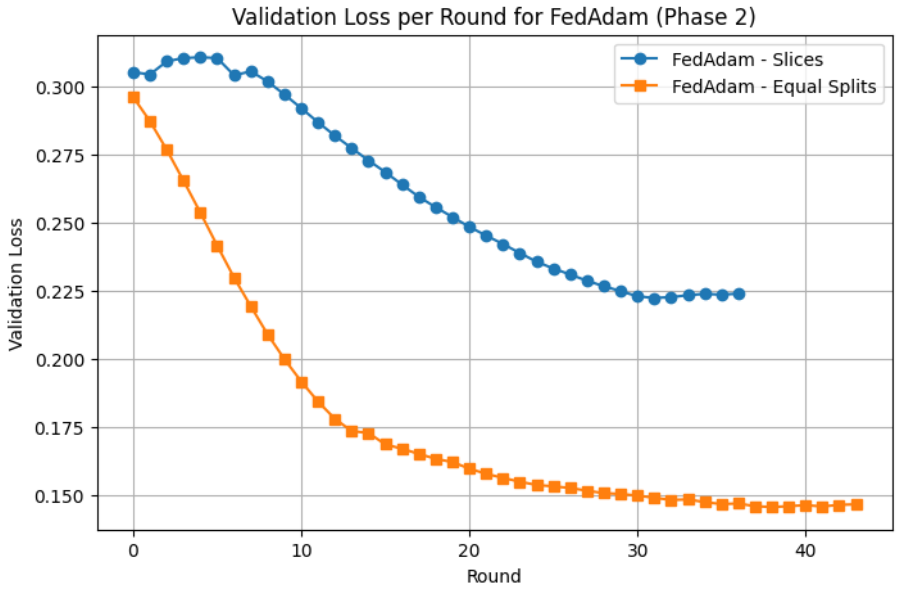

Σχήμα 4.4: *Εξέλιξη του Validation Loss ανά γύρο για τη στρατηγική FedAvg.*

Στη συνέχεια, το Σχήμα 4.5 παρουσιάζει την πορεία του Validation Loss κατά τη δεύτερη φάση εκπαίδευσης με τη στρατηγική FedAvgM, για τις δύο διαφορετικές κατανομές δεδομένων.




Σχήμα 4.5: *Εξέλιξη του Validation Loss ανά γύρο για τη στρατηγική FedAvgM (Phase 2).*

Τέλος, το Σχήμα 4.6 απεικονίζει τη μεταβολή του Validation Loss στη δεύτερη φάση εκπαίδευσης με τη στρατηγική FedAdam.




Σχήμα 4.6: *Εξέλιξη του Validation Loss ανά γύρο για τη στρατηγική FedAdam.*

Όπως παρατηρείται, σε όλες τις στρατηγικές, η καμπύλη του Validation Loss στην περίπτωση ισοκατανομής δεδομένων (Splits) μειώνεται ταχύτερα και σταθερότερα σε σχέση με την περίπτωση κατανομής κατά Network Slices (Slices). Το φαινόμενο αυτό αντικατοπτρίζει τη δυσκολία που εισάγει η μη ισομερής κατανομή των δεδομένων, καθώς και τη μεγαλύτερη πρόκληση στην επίτευξη καλής σύγκλισης υπό πιο ρεαλιστικές και μη ιδανικές συνθήκες. Επιπλέον, παρατηρείται ότι τα σενάρια με ισοκατανομή επιτυγχάνουν τελικά και χαμηλότερη τιμή Validation Loss σε κάθε συνάρτηση συγκέντρωσης.

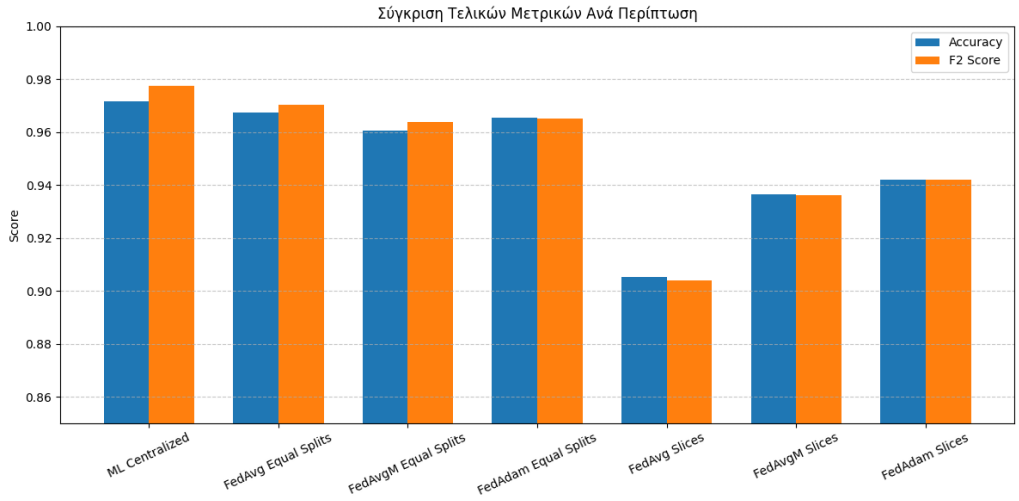
### 4.3.3 Σύγκριση Τελικών Αποτελεσμάτων

Ο Πίνακας 4.12 παρουσιάζει συγκεντρωτικά τις κύριες μετρικές απόδοσης (ακρίβεια, ακρίβεια θετικής κλάσης, ανάκληση, F1 και F2 score) για το τελικό μοντέλο κάθε περίπτωσης.

| **Στρατηγική** | **Κατανομή** | Accuracy | Precision | Recall | F1 | F2 |
|---|---|---|---|---|---|---|
| ML | Centralized | 0.9717 | 0.9673 | 0.9810 | 0.9741 | 0.9775 |
| FedAvg | Equal Splits | 0.9675 | 0.9695 | 0.9707 | 0.9701 | 0.9704 |
| FedAvg | Network Slices | 0.9053 | 0.8673 | 0.9745 | 0.9178 | 0.9039 |
| FedAvgM | Equal Splits | 0.9606 | 0.9631 | 0.9643 | 0.9637 | 0.9640 |
| FedAvgM | Network Slices | 0.9364 | 0.9200 | 0.9669 | 0.9429 | 0.9361 |
| FedAdam | Equal Splits | 0.9654 | 0.9554 | 0.9822 | 0.9686 | 0.9653 |
| FedAdam | Network Slices | 0.9419 | 0.9499 | 0.9427 | 0.9463 | 0.9419 |

Πίνακας 4.12: *Συγκεντρωτικός πίνακας αποτελεσμάτων για το τοπικό μοντέλο ML και όλες τις περιπτώσεις εκπαίδευσης FL.*

Για την ευκολότερη σύγκριση των περιπτώσεων και την καλύτερη απεικόνιση των διαφορών μεταξύ στρατηγικών και κατανομών, στο Σχήμα 4.7 παρουσιάζεται γράφημα με τις τιμές της ακρίβειας και του δείκτη F2 για κάθε μοντέλο.




Σχήμα 4.7: *Σύγκριση της Accuracy και του F2 Score για όλες τις περιπτώσεις εκπαίδευσης.*

Όπως ήταν αναμενόμενο, το συγκεντρωτικό ML μοντέλο που εκπαιδεύτηκε σε όλα τα διαθέσιμα δεδομένα παρουσίασε την υψηλότερη συνολική απόδοση, με Accuracy 97.17%, F1 Score 97.41% και F2 Score 97.75%. Αυτό οφείλεται στο γεγονός ότι στη συγκεντρωτική (centralized) εκπαίδευση το μοντέλο έχει πλήρη και ισορροπημένη εικόνα του συνόλου δεδομένων, αποφεύγοντας τις προκλήσεις που σχετίζονται με τη μη ομοιογενή κατανομή (non-IID) ή τους περιορισμένους τοπικούς όγκους δεδομένων που παρατηρούνται στις αποκεντρωμένες περιπτώσεις.

Αξιολογώντας τις αποκεντρωμένες περιπτώσεις, παρατηρείται ότι η στρατηγική FedAvg με ισοκατανομή δεδομένων (Equal Splits) προσέγγισε αρκετά την απόδοση της συγκεντρωτικής εκπαίδευσης, επιτυγχάνοντας F1 Score 97.01% και F2 Score 97.04%. Αντίθετα, η ίδια στρατηγική με κατανομή κατά network slices παρουσίασε αισθητή πτώση απόδοσης, κυρίως λόγω της ανισορροπίας δεδομένων ανά client, γεγονός που αντικατοπτρίζεται στην χαμηλότερη ακρίβεια 90.53% και στον δείκτη F2 που μειώθηκε σε 90.39%.

Παρόμοιο μοτίβο παρατηρείται και για τη βελτιωμένη στρατηγική FedAvgM. Η χρήση ορμής (momentum) συνέβαλε σε πιο σταθερή σύγκλιση και βελτίωση της ακρίβειας, ιδιαίτερα στην περίπτωση της ισοκατανομής, όπου ο δείκτης F2 έφτασε το 96.40%. Ωστόσο, η κατανομή κατά network slices και πάλι επιβάρυνε την τελική απόδοση, με F2 Score 93.61%.

Τέλος, η πιο σύνθετη στρατηγική FedAdam, που συνδυάζει στοιχεία του Adam Optimizer στο FL, πέτυχε απόδοση αντίστοιχη του FedAvgM για την ισοκατανομή (F2 Score 96.53%), ενώ παρουσίασε σχετική βελτίωση έναντι του FedAvgM στην περίπτωση των network slices (F2 Score 94.19%), χωρίς ωστόσο να φτάνει τα επίπεδα του συγκεντρωτικού μοντέλου.

Η σύγκριση των αποτελεσμάτων όλων των περιπτώσεων αναδεικνύει τη σημαντική επίδραση τόσο του τρόπου κατανομής των δεδομένων όσο και της επιλογής στρατηγικής συγκέντρωσης στην τελική απόδοση των μοντέλων. Η ανάλυση αυτή παρέχει χρήσιμες ενδείξεις σχετικά με τις προκλήσεις και τις δυνατότητες του FL σε σενάρια ασφαλείας 5G δικτύων.

Κεφάλαιο 5

# Συμπεράσματα και Μελλοντική Εργασία

## 5.1 Συμπεράσματα

Η παρούσα διπλωματική εργασία επικεντρώθηκε στην ανάπτυξη και αξιολόγηση ενός Συστήματος Ανίχνευσης Εισβολών βασισμένου στο FL για δίκτυα 5G, λαμβάνοντας υπόψη τις ρεαλιστικές προκλήσεις που εισάγει το Network Slicing. Αντί να περιοριστεί σε ιδανικές, ισομερώς κατανεμημένες συνθήκες δεδομένων, η εργασία διερεύνησε την απόδοση του συστήματος σε σενάρια που προσομοιώνουν τη δομή των πραγματικών 5G δικτύων, όπου διαφορετικές κατηγορίες slices (eMBB, mMTC, URLLC) συνυπάρχουν στην ίδια υποδομή.

Τα αποτελέσματα που παρουσιάστηκαν στον Πίνακα 4.12 και αναλύθηκαν συγκριτικά στην ενότητα 4.3, ανέδειξαν με σαφήνεια τη σημασία αυτής της προσέγγισης. Όπως ήταν αναμενόμενο, τα σενάρια Equal Splits, όπου τα δεδομένα κατανέμονται ισόποσα και ισορροπημένα στους clients, οδήγησαν στη βέλτιστη απόδοση των αποκεντρωμένων μοντέλων, με δείκτες F2 που άγγιξαν το 97% και προσέγγισαν τη συγκεντρωτική εκπαίδευση. Αξιοσημείωτο είναι ότι η χρήση πιο σύνθετων συναρτήσεων συγκέντρωσης, όπως το FedAvgM και το FedAdam, στην περίπτωση των Equal Splits, δεν οδήγησε σε περαιτέρω βελτίωση των αποτελεσμάτων, αλλά διατήρησε αντίστοιχα υψηλά επίπεδα απόδοσης, επιβεβαιώνοντας ότι σε ιδανικά ισορροπημένες συνθήκες ακόμα και η βασική στρατηγική FedAvg είναι επαρκής.

Ωστόσο, το πραγματικό ενδιαφέρον εντοπίζεται στην περίπτωση του Network Slicing. Παρά τη φυσιολογική πτώση απόδοσης λόγω της ανισορροπίας και ετερογένειας των δεδομένων ανά slice, η χρήση πιο εξελιγμένων τεχνικών συγκέντρωσης, όπως το FedAvgM και το FedAdam, οδήγησε σε σημαντική βελτίωση των αποτελεσμάτων, με τον δείκτη F2 να φτάνει έως και το 94.19%.

Τα ευρήματα αυτά επιβεβαιώνουν ότι η αξιολόγηση ενός FL-based IDS σε ρεαλιστικές συνθήκες, όπως αυτές που εισάγει το Network Slicing, είναι απαραίτητη για την εξαγωγή αξιόπιστων συμπερασμάτων σχετικά με την αποτελεσματικότητα τέτοιων συστημάτων σε πραγματικά 5G περιβάλλοντα. Επιπλέον, καταδεικνύεται ότι η επιλογή κατάλληλων συναρτήσεων συγκέντρωσης μπορεί να μετριάσει τις προκλήσεις που σχετίζονται με τη μη ομοιογενή κατανομή δεδομένων, φέρνοντας την απόδοση πιο κοντά σε αυτήν του ιδανικού σεναρίου ισοκατανομής.

## 5.2 Μελλοντική Εργασία - Προεκτάσεις

Τα ευρήματα της μελέτης επιβεβαιώνουν τη δυνατότητα εφαρμογής του Federated Learning στην ανίχνευση εισβολών σε δίκτυα 5G, αποδεικνύοντας ότι ακόμη και σε απαιτητικά σενάρια, όπως εκείνα που εισάγει το Network Slicing, η απόδοση μπορεί να διατηρηθεί σε υψηλά επίπεδα. Ωστόσο, το ζήτημα παραμένει ανοιχτό και επιδέχεται περαιτέρω διερεύνησης.

Ένα από τα επόμενα βήματα αφορά την αξιολόγηση πιο εξελιγμένων τοπικών μοντέλων. Η χρήση πιο σύνθετων αρχιτεκτονικών, όπως βαθύτερα νευρωνικά δίκτυα, Recurrent Neural Networks ή μοντέλα τύπου Transformers, ενδέχεται να ενισχύσει την ικανότητα του συστήματος να εντοπίζει επιθέσεις σε πιο περίπλοκα και δυναμικά περιβάλλοντα.

Παράλληλα, η εισαγωγή δυναμικών ή προσαρμοζόμενων στρατηγικών συγκέντρωσης αποτελεί ένα πολλά υποσχόμενο πεδίο. Η δυνατότητα των συναρτήσεων συγκέντρωσης να προσαρμόζονται στη διαφορετική κατανομή και φύση των δεδομένων ανά slice θα μπορούσε να βελτιώσει ακόμη περισσότερο τα αποτελέσματα, ιδιαίτερα σε συνθήκες έντονης ανισορροπίας.

Επιπλέον, η αξιολόγηση του συστήματος με χρήση πιο ρεαλιστικών ή και πραγματικών συνόλων δεδομένων, που περιλαμβάνουν σύνθετα μοτίβα επιθέσεων ή προέρχονται από πραγματικές υποδομές 5G, κρίνεται απαραίτητη για την ενίσχυση της αξιοπιστίας και της πρακτικής αξίας των συμπερασμάτων. Στο σημείο αυτό αξίζει να επισημανθεί ότι η διαθεσιμότητα τέτοιων δημόσιων συνόλων δεδομένων παραμένει περιορισμένη, γεγονός που δυσχεραίνει τη συγκριτική αξιολόγηση και την αναπαραγωγή των ερευνών. Η δημιουργία και δημοσιοποίηση νέων, ποικιλόμορφων συνόλων δεδομένων 5G, τα οποία θα ενσωματώνουν διαφορετικά σενάρια χρήσης και επιθέσεων, θα αποτελούσε σημαντική συμβολή στη συγκεκριμένη ερευνητική κατεύθυνση.

Τέλος, μία φυσική επέκταση της μελέτης είναι η μετάβαση από τη δυαδική στην πολυκατηγορική ταξινόμηση επιθέσεων. Η ικανότητα διάκρισης διαφορετικών τύπων κακόβουλης δραστηριότητας, πέρα από την απλή αναγνώριση Benign και Malicious ροών, αποτελεί απαραίτητη προϋπόθεση για την πλήρη αξιοποίηση ενός FL - based IDS σε πραγματικά σενάρια.

Η περαιτέρω εξέλιξη των παραπάνω πτυχών μπορεί να οδηγήσει στη δημιουργία πιο αποδοτικών, ανθεκτικών και ευέλικτων συστημάτων ανίχνευσης εισβολών, κατάλληλων για τις αυξημένες απαιτήσεις ασφαλείας των σύγχρονων 5G υποδομών.

# Βιβλιογραφία


[1] Hasanah Putri, Alfin Hikmaturokhman, Izanoordina Ahmad, Radial Anwar και Rafli Akbar. *Fifth generation core: the performance enhancement of virtual private server and bare metal. Bulletin of Electrical Engineering and Informatics*, 13(4):2408–2417, 2024.

[2] 3GPP. *3GPP TS 38.401 V15.2.0, NG-RAN; Architecture description (Release 15), September 2018.* Τεχνική Αναφορά με αριθμό, 3rd Generation Partnership Project (3GPP), Sophia Antipolis, 2018.

[3] MathWorks. *Machine Learning in MATLAB*, 2024.

[4] MathWorks. *Machine Learning in MATLAB*, 2024.

[5] Aliya Fahmi, Aziz Khan, Zahida Maqbool και Thabet Abdeljawad. *Circular intuitionistic fuzzy Hamacher aggregation operators for multi-attribute decision-making. Scientific reports*, 15(1):5618, 2025.

[6] Qazi Waqas Khan, Anam Nawaz Khan, Atif Rizwan, Rashid Ahmad, Salabat Khan και Do Hyeun Kim. *Decentralized machine learning training:*
*}a survey on synchronization,*
*}consolidation, and topologies. IEEE Access*, 11:68031–68050, 2023.

[7] Seizo Onoe. *Evolution of 5G Mobile Technology Toward*
*}2020 and Beyond. 2016 IEEE International Solid-State Circuits Conference (ISSCC)*, San Francisco, 2016. IEEE.

[8] Jiegang Lu, Limin Xiao, Zhigang, Ming Zhao και Wenbo Wang. *5G Enhanced Service-based Core Design. 28th Wireless and Optical Communications Conference (WOCC 2019)*, Beijing, 2019. IEEE.

[9] Endri Goshi, Michael Jarschel, Rastin Pries, Mu He και Wolfgang Kellerer. *Investigating Inter-NF Dependencies in Cloud-Native 5G Core Networks. Proceedings of the 2021 17th International Conference on Network and Service Management: Smart Management for Future Networks and Services, CNSM 2021*, σελίδες 370–374, Izmir, 2021. Institute of Electrical and Electronics Engineers Inc.

[10] Balazs Bertenyi, Richard Burbidge, Gino Masini, Sasha Sirotkin και Yin Gao. *NG Radio Access Network (NG-RAN). Journal of ICT Standardization*, 6(1):59–76, 2018.

[11] Christos Bouras, Anastasia Kollia και Andreas Papazois. *SDN & NFV in 5G: Advancements and Challenges. 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, Paris, 2017. IEEE.

[12] Alejandro Llorens-Carrodeguas, Cristina Cervello-Pastor, Irian Leyva-Pupo, Juan Manuel Lopez-Soler, Jorge Navarro-Ortiz και Jose Angel Exposito-Arenas. *An Architecture for the 5G Control Plane based on }SDN and Data Distribution Service. 2018 Fourth International Conference on Software Defined Systems (SDS)*, Barcelona, 2018. IEEE.

[13] Michal Lom, Ondrej Pribyl και Miroslav Svitek. *Industry 4.0 as a Part of Smart Cities. 2016 Smart Cities Symposium Prague (SCSP)*, Prague, 2016. IEEE.

[14] Sakshi Painuly, Priya Kohli, Priya Matta και Sachin Sharma. *Advance applications and future challenges of 5G IoT. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, σελίδες 1381–1384, Thoothukudi, 2020. Institute of Electrical and Electronics Engineers Inc.

[15] Maria A. Lema, Andrés Laya, Toktam Mahmoodi, Maria Cuevas, Joachim Sachs, Jan Markendahl και Mischa Dohler. *Business Case and Technology Analysis for 5G Low Latency Applications. IEEE Access*, 5:5917–5935, 2017.

[16] Jose Ordonez-Lucena, Pablo Ameigeiras, DIego Lopez, Juan J. Ramos-Munoz, Javier Lorca και Jesus Folgueira. *Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. IEEE Communications Magazine*, 55(5):80–87, 2017.

[17] Petar Popovski, Kasper Floe Trillingsgaard, Osvaldo Simeone και Giuseppe Durisi. *5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view. IEEE Access*, 6:55765–55779, 2018.

[18] Liming Fang, Bo Zhao, Yang Li, Zhe Liu, Chunpeng Ge και Weizhi Meng. *Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances. IEEE Network*, 34(6):54–61, 2020.

[19] Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran και Imran Razzak. *Machine learning for 5G security: Architecture, recent advances, and challenges. Ad Hoc Networks*, 123, 2021.

[20] Yi Shi και Yalin E. Sagduyu. *Adversarial Machine Learning for Flooding Attacks on 5G Radio Access Network Slicing. 2021 IEEE International Conference on Communications Workshops, ICC Workshops 2021 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., 2021.

[21] Nikhil Tripathi και Neminath Hubballi. *Slow rate denial of service attacks against HTTP/2 and detection. Computers and Security*, 72:255–272, 2018.

[22] Cong Wu, Rong Shi και Ke Deng. *Reconnaissance and Experiment on 5G-SA Communication Terminal Capability and Identity Information. 2021 9th International Conference on Intelligent Computing and Wireless Optical Communications, ICWOC 2021*, σελίδες 16–22. Institute of Electrical and Electronics Engineers Inc., 2021.

[23] Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski και Piotr Zórawski. *SDN-based mitigation of scanning aacks for the 5G internet of radio light system. ACM International Conference Proceeding Series*. Association for Computing Machinery, 2018.

[24] Piyush Goyal και Anurag Goyal. *Comparative Study of two Most Popular Packet Sniffing Tools-Tcpdump and Wireshark. 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, Girne, 2017.

[25] Miroslav Mitev, Arsenia Chorti, E. Veronica Belmega και Martin Reed. *Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation. 2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019.

[26] Bharat Bhushan, G Sahoo και Amit Kumar Rai. *Man-In-The-Middle Attack in Wireless and Computer Networking-A review. 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, 2017.

[27] Yaoqi Yang, Xianglin Wei, Renhui Xu, Laixian Peng, Lei Zhang και Lin Ge. *Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency. IEEE Access*, 8:103860–103874, 2020.

[28] Eungha Kim και Young-il Choi. *Traffic monitoring system for 5G core network. 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, Zagreb, Croatia, 2019. IEEE.

[29] Keshav Sood, Mohammad Reza Nosouhi, Dinh Duc Nha Nguyen, Frank Jiang, Morshed Chowdhury και Robin Doss. *Intrusion Detection Scheme With Dimensionality Reduction in Next Generation Networks. IEEE Transactions on Information Forensics and Security*, 18:965–979, 2023.

[30] Ziadoon Kamil Maseer, Robiah Yusof, Nazrulazhar Bahaman, Salama A. Mostafa και Cik Feresa Mohd Foozy. *Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset. IEEE Access*, 9:22351–22370, 2021.

[31] Ming Liu, Zhi Xue, Xianghua Xu, Changmin Zhong και Jinjun Chen. *Host-based intrusion detection system with system calls: Review and future trends*, 2019.

[32] Tom M Mitchell. *Does Machine Learning Really Work?* Τεχνική Αναφορά με αριθμό, 1997.

[33] Isabella Castiglioni, Leonardo Rundo, Marina Codari, Giovanni Di Leo, Christian Salvatore, Matteo Interlenghi, Francesca Gallivanone, Andrea Cozzi, Natascha Claudia D'Amico και Francesco Sardanelli. *AI applications to medical images: From machine learning to deep learning*, 2021.

[34] A. T.D. Perera, P. U. Wickramasinghe, Vahid M. Nik και Jean Louis Scartezzini. *Machine learning methods to assist energy system optimization. Applied Energy*, 243:191–205, 2019.

[35] Hussam N. Fakhouri, Sadi Alawadi, Feras M. Awaysheh, Imad Bani Hani, Mohannad Alkhalaileh και Faten Hamad. *A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. Electronics (Switzerland)*, 12(22), 2023.

[36] WANG Hua, ZHOU Lijuan και MA Cuiqin. *2009 International Conference on Information Engineering and Computer Science. 2009 International Conference on Information Engineering and Computer Science*, Wuhan, China, 2009. I E E E.

[37] Nandish Chattopadhyay, Anupam Chattopadhyay, Sourav Sen Gupta και Michael Kasper. *Curse of Dimensionality in Adversarial Examples. 2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, 2019.

[38] Ganesh R. Naik, Suviseshamuthu Easter Selvan, Massimiliano Gobbo, Amit Acharyya και Hung T. Nguyen. *Principal Component Analysis Applied to Surface Electromyography: A Comprehensive Review*, 2016.

[39] Hemant Kumar Gianey και Rishabh Choudhary. *Comprehensive Review On Supervised Machine Learning Algorithms. Proceedings - 2017 International Conference on Machine Learning and Data Science, MLDS 2017*, τόμος 2018-January, σελίδες 38–43. Institute of Electrical and Electronics Engineers Inc., 2017.

[40] Amanpreet Singh, Narina Thakur και Aakanksha Sharma. *A Review of Supervised Machine Learning
}Algorithms (16th-18th March, 2016) : INDIA Com-2016. Proceedings of the 10th INDIACom ; 2016 3rd International Conference on Computing for Sustainable Global Development*. Bharati Vidyapeeth's Institute of Computer Applications and Management, 2016.

[41] Fabian-Robert St¨oter, Soumitro Chakrabarty, Bernd Edler και Emanu¨el A. P. Habets. *CLASSIFICATION VS. REGRESSION IN SUPERVISED LEARNING
}FOR SINGLE CHANNEL SPEAKER COUNT ESTIMATION. 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, σελίδα 465. Institute of Electrical and Electronics Engineers, 2018.

[42] Happiness Ugochi Dike, Yimin Zhou, Kranthi Kumar Deveerasetty και Qingtian Wu. *Unsupervised Learning Based On Artificial Neural
}Network: A Review. IEEE-CBS 2018 : 2018 IEEE International Conference on Cyborg and Bionic Systems*, Shenzhen, China, 2018. IEEE.

[43] Jingjing Cui, Zhiguo Ding, Pingzhi Fan και Naofal Al-Dhahir. *Unsupervised machine learning-based user clustering in millimeter-Wave-NOMA systems. IEEE Transactions on Wireless Communications*, 17(11):7425–7440, 2018.

[44] Mohsin Munir, Shoaib Ahmed Siddiqui, Andreas Dengel και Sheraz Ahmed. *DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. IEEE Access*, 7:1991–2005, 2019.

[45] G. Thippa Reddy, M. Praveen Kumar Reddy, Kuruva Lakshmanna, Rajesh Kaluri, Dharmendra Singh Rajput, Gautam Srivastava και Thar Baker. *Analysis of Dimensionality Reduction Techniques on Big Data. IEEE Access*, 8:54776–54788, 2020.

[46] Wang Qiang και Zhan Zhongli. *Reinforcement Learning Model,Algorithms }and Its Application. Proceedings 2011 International Conference on Mechatronic Science, Electric Engineering, and Computer*, Jilin, China, 2011. IEEE.

[47] A Jović, K Brkić και N Bogunović. *A review of feature selection methods with applications. 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, 2015.

[48] Cosmin Lazar, Jonatan Taminau, Stijn Meganck, David Steenhoff, Alain Coletta, Colin Molter, Virginie De Schaetzen, Robin Duque, Hugues Bersini και Ann Nowé. *A survey on filter techniques for feature selection in gene expression microarray analysis. IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 9(4):1106–1119, 2012.

[49] Naoual El aboudi και Laila Benhlima. *Review on Wrapper Feature Selection Approaches. 2016 International Conference on Engineering and MIS (ICEMIS)*, Agadir, 2016. IEEE.

[50] Haoyue Liu, Mengchu Zhou και Qing Liu. *An embedded feature selection method for imbalanced data classification. IEEE/CAA Journal of Automatica Sinica*, 6(3):703–715, 2019.

[51] Susmita Ray. *A Quick Review of Machine Learning Algorithms. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, 2019. [IEEE].

[52] Madan Somvanshi και Pranjali Chavan. *A Review of Machine Learning Techniques using Decision Tree and Support Vector Machine. 2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, Pune, 2016.

[53] Ashir Javeed, Shijie Zhou, Liao Yongjian, Iqbal Qasim, Adeeb Noor και Redhwan Nour. *An Intelligent Learning System Based on Random Search Algorithm and Optimized Random Forest Model for Improved Heart Disease Detection. IEEE Access*, 7:180235–180243, 2019.

[54] Yaping Chang, Wei Li και Zhongming Yang. *Network intrusion detection based on random forest and support vector machine. Proceedings - 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017*, τόμος 1, σελίδες 635–638, Guangzhou, 2017. Institute of Electrical and Electronics Engineers Inc.

[55] Sarah Naiem, Ayman E. Khedr, Amira M. Idrees και Mohamed I. Marie. *Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing. IEEE Access*, 11:124597–124608, 2023.

[56] Shemim Begum, Debasis Chakraborty και Ram Sarkar. *Data Classification Using Feature Selection and kNN Machine Learning Approach. Proceedings - 2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015*, σελίδες 811–814, Jabalpur, 2016. Institute of Electrical and Electronics Engineers Inc.

[57] Libo Zhang, Tiejian Luo, Fei Zhang και Yanjun Wu. *A Recommendation Model Based on Deep Neural Network. IEEE Access*, 6:9454–9463, 2018.

[58] Rob G.J. Wijnhoven και Peter H.N. De With. *Fast training of object detection using stochastic gradient descent. Proceedings - International Conference on Pattern Recognition*, σελίδες 424–427, Istanbul, 2010.

[59] Sebastian Bock και Martin Weiß. *A Proof of Local Convergence for the Adam Optimizer. 2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, 2019.

[60] Ali Rospawan, Ching Chih Tsai και Chi Chih Hung. *Two-layer Intelligent Learning Control Using Output Recurrent Fuzzy Neural LSTM-BLS with RMSprop. IEEE Access*, 13:34334–34349, 2025.

[61] Ali Yadavar Nikravesh, Samuel A. Ajila, Chung Horng Lung και Wayne Ding. *Mobile network traffic prediction using MLP, MLPWD, and SVM. Proceedings - 2016 IEEE International Congress on Big Data, BigData Congress 2016*, σελίδες 402–409. Institute of Electrical and Electronics Engineers Inc., 2016.

[62] Manjunath Jogin, Mohana, Madhulika M S, Divya G D, Meghana R K και Apoorva S. *Feature Extraction using Convolution Neural }Networks (CNN) and Deep Learning. 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2018. IEEE.

[63] Chuanlong Yin, Yuefei Zhu, Jinlong Fei και Xinzheng He. *A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access*, 5:21954–21961, 2017.

[64] Areeba Ishtiaq, Kashif Munir, Ali Raza, Nagwan Abdel Samee, Mona M. Jamjoom και Zahid Ullah. *Product Helpfulness Detection With Novel Transformer Based BERT Embedding and Class Probability Features. IEEE Access*, 12:55905–55917, 2024.

[65] Alec Radford, Karthik Narasimhan, Tim Salimans και Ilya Sutskever. *Improving Language Understanding by Generative Pre-Training.* Τεχνική Αναφορά με αριθμό, 2018.

[66] Zhijin Qin, Geoffrey Ye Li και Hao Ye. *Federated Learning and Wireless Communications. IEEE Wireless Communications*, 28(5):134–140, 2021.

[67] Ehsan Hallaji, Roozbeh Razavi-Far, Mehrdad Saif, Boyu Wang και Qiang Yang. *Decentralized Federated Learning: A Survey on Security and Privacy. IEEE Transactions on Big Data*, 10(2):194–213, 2024.

[68] Di Cao, Shan Chang, Zhijian Lin, Guohua Liu και Donghong Sun. *Understanding distributed poisoning attack in federated learning. Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, τόμος 2019-December, σελίδες 233–239, Tianjin, 2019. IEEE Computer Society.

[69] Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li και H. Vincent Poor. *Federated Learning for Internet of Things: A Comprehensive Survey*, 2021.

[70] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li και Yuan Gao. *A survey on federated learning. Knowledge-Based Systems*, 216, 2021.

[71] Elena Fedorchenko, Evgenia Novikova και Anton Shulepov. *Comparative Review of the Intrusion Detection Systems Based on Federated Learning: Advantages and Open Challenges*, 2022.

[72] Anna Bogdanova, Nii Attoh-Okine και Tetsuya Sakurai. *Risk and Advantages of Federated Learning for Health Care Data Collaboration. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 6(3), 2020.

[73] Jingwen Zhang, Jiale Zhang, Junjun Chen και Shui Yu. *GAN Enhanced Membership Inference: A Passive
}Local Attack in Federated Learning. 2020 IEEE International Conference on Communications : proceedings : Dublin, Ireland, 7-11 June 2020*, Dublin, 2020. IEEE.

[74] Mohammed Aledhari, Rehma Razzak, Reza M. Parizi και Fahad Saeed. *Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications*, 2020.

[75] Tuo Zhang, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari και A. Salman Avestimehr. *Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. IEEE Internet of Things Magazine*, 5(1):24–29, 2022.

[76] Marta Samper Hernández. *Decentralized Federated Learning: Fundamentals,
}State of the Art, Frameworks, Trends,
}and Challenges. Lenguas Modernas*, (62):183–209, 2023.

[77] Sawsan Abdulrahman, Hanine Tout, Hakima Ould-Slimane, Azzam Mourad, Chamseddine Talhi και Mohsen Guizani. *A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal*, 8(7):5476–5497, 2021.

[78] Liangqi Yuan, Ziran Wang, Lichao Sun, Philip S. Yu και Christopher G. Brinton. *Decentralized Federated Learning: A Survey and Perspective. IEEE Internet of Things Journal*, 2024.

[79] Christos Papadopoulos, Konstantinos Filippos Kollias και George F. Fragulis. *Recent Advancements in Federated Learning: State of the Art, Fundamentals, Principles, IoT Applications and Future Trends*, 2024.

[80] Wei Huang, Tianrui Li, Dexian Wang, Shengdong Du, Junbo Zhang και Tianqiang Huang. *Fairness and accuracy in horizontal federated learning. Information Sciences*, 589:170–185, 2022.

[81] Yang Liu, Yan Kang, Tianyuan Zou, Yanhong Pu, Yuanqin He, Xiaozhou Ye, Ye Ouyang, Ya Qin Zhang και Qiang Yang. *Vertical Federated Learning: Concepts, Advances, and Challenges. IEEE Transactions on Knowledge and Data Engineering*, 36(7):3615–3634, 2024.

[82] Yang Liu, Yan Kang, Chaoping Xing, Tianjian Chen και Qiang Yang. *A Secure Federated Transfer Learning Framework. IEEE Intelligent Systems*, 35(4):70–82, 2020.

[83] Hao Wang, Zakhary Kaplan, Di Niu και Baochun Li. *Optimizing Federated Learning on Non-IID Data with Reinforcement Learning. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2024.

[84] Zhuoning Guo, Duanyi Yao, Qiang Yang και Hao Liu. *HiFGL: A Hierarchical Framework for Cross-silo Cross-device Federated Graph Learning. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, σελίδες 968–979. Association for Computing Machinery, 2024.

[85] Chao Huang, Jianwei Huang και Xin Liu. *Cross-Silo Federated Learning: Challenges and Opportunities. IEEE COMMUNICATIONS MAGAZINE*, 2022.

[86] Muhammad Habibur Rehman, Ahmed Mukhtar Dirir, Khaled Salah, Ernesto Damiani και Davor Svetinovic. *TrustFed: A Framework for Fair and Trustworthy Cross-Device Federated Learning in IIoT. IEEE Transactions on Industrial Informatics*, 17(12):8485–8494, 2021.

[87] Ahmed El Ouadrhiri και Ahmed Abdelhadi. *Differential Privacy for Deep and Federated Learning: A Survey. IEEE Access*, 10:22359–22380, 2022.

[88] Ian Zhou, Farzad Tofigh, Massimo Piccardi, Mehran Abolhasan, Daniel Franklin και Justin Lipman. *Secure Multi-Party Computation for Machine Learning: A Survey. IEEE Access*, 12:53881–53899, 2024.

[89] Arpan Jain, Ammar Ahmad Awan, Quentin Anthony, Hari Subramoni και Dhableswar K. DK Panda. *2019 IEEE International Conference on Cluster Computing (CLUSTER) : proceedings : September 23-26, 2019, Albuquerque, New Mexico USA.*

*2019 IEEE International Conference on Cluster Computing (CLUSTER) : proceedings : September 23-26, 2019, Albuquerque, New Mexico USA*, Albuquerque, 2019. IEEE.

[90] Andrius Budrionis, Magda Miara, Piotr Miara, Szymon Wilk και Johan Gustav Bellika. *Benchmarking PySyft Federated Learning Framework on MIMIC-III Dataset. IEEE Access*, 9:116869–116878, 2021.

[91] Fabian Pedregosa FABIANPEDREGOSA, Vincent Michel, Olivier Grisel OLIVIERGRISEL, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Jake Vanderplas, David Cournapeau, Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Bertrand Thirion, Olivier Grisel, Vincent Dubourg, Alexandre Passos, Matthieu Brucher, Matthieu Perrot andÉdouardand, andÉdouard Duchesnay και FRÉdouard Duchesnay EDOUARDDUCHESNAY. *Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research*, 12:2825–2830, 2011.

[92] Aiden Gigi Samuel, Sia Viji Puthusseri, Edryn Shajan Eazhakadan και Monali Shetty. *Detecting Malicious Blockchain Attacks through Flower using Horizontal Federated Learning: An Investigation of Federated Approaches. 2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, Delhi, 2023. Institute of Electrical and Electronics Engineers Inc.

[93] Jakub Michalek, Vladislav Skorpil και Vaclav Oujezsky. *Federated Learning on Android-Highlights from Recent Developments. International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, τόμος 2022-October, σελίδες 27–30, Valencia, 2022. IEEE Computer Society.

[94] Syed Shariyar Murtaza, Paris Lak, Ayse Bener και Armen Pischdotchian. *How to effectively train IBM watson: classroom experience. Proceedings of the Annual Hawaii International Conference on System Sciences*, τόμος 2016-March, σελίδες 1663–1670, Koloa, 2016. IEEE Computer Society.

[95] K. R. Jayaram, Vinod Muthusamy, Gegi Thomas, Ashish Verma και Mark Purcell. *Adaptive Aggregation For Federated Learning. Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022*, σελίδες 180–185, Osaka, 2022. Institute of Electrical and Electronics Engineers Inc.

[96] Fan Zhang, Chong Chen, Xian Sheng Hua και Xiao Luo. *FATE: Learning Effective Binary Descriptors With Group Fairness. IEEE Transactions on Image Processing*, 33:3648–3661, 2024.

[97] Pian Qi, Diletta Chiaro, Antonella Guzzo, Michele Ianni, Giancarlo Fortino και Francesco Piccialli. *Model aggregation techniques in federated learning: A comprehensive survey*, 2024.

[98] Shiva Mehta και Aseem Aneja. *Securing Data Privacy in Machine Learning: The FedAvg of Federated Learning Approach. 2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, σελίδες 1–5, Pimari Chinchwad, 2024. IEEE.

[99] Wei Bin Kou, Qingfeng Lin, Ming Tang, Shuai Wang, Guangxu Zhu και Yik Chung Wu. *FedRC: A Rapid-Converged Hierarchical Federated Learning Framework in Street Scene Semantic Understanding. IEEE International Conference on Intelligent Robots and Systems*, σελίδες 2578–2585, Abu Dhabi, 2024. Institute of Electrical and Electronics Engineers Inc.

[100] Li Ju, Tianru Zhang, Salman Toor και Andreas Hellander. *Accelerating Fair Federated Learning: Adaptive Federated Adam. IEEE Transactions on Machine Learning in Communications and Networking*, 2:1017–1032, 2024.

[101] Hibatallah Kabbaj, Rachid El-Azouzi και Abdellatif Kobbane. *Robust Federated Learning via Weighted Median Aggregation*. 2024 2nd International Conference on Federated Learning Technologies and Applications (FLTA)*, σελίδες 298–303, Valencia, 2024. IEEE.

[102] Xiumin Li, Mi Wen, Siying He, Rongxing Lu και Liangliang Wang. *A Scheme for Robust Federated Learning with Privacy-preserving Based on Krum AGR. 2023 IEEE/CIC International Conference on Communications in China, ICCC 2023*, Dalian, 2023. Institute of Electrical and Electronics Engineers Inc.

[103] Tianxiang Wang, Zhonglong Zheng και Feilong Lin. *Federated learning framework based on trimmed mean aggregation rules*, 2025.

[104] Nour Moustafa. *A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society*, 72, 2021.

[105] Guojun. Wang. *Federated TON IoT Windows Datasets for Evaluating }AI-based Security Applications. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE Computer Society, Conference Publishing Services, 2021.

[106] Enrique Mármol Campos, Pablo Fernández Saura, Aurora González-Vidal, José L. Hernández-Ramos, Jorge Bernal Bernabé, Gianmarco Baldini και Antonio Skarmeta. *Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks*, 203, 2022.

[107] Othmane Belarbi, Theodoros Spyridopoulos, Eirini Anthi, Ioannis Mavromatis, Pietro Carnelli και Aftab Khan. *Federated Deep Learning for Intrusion Detection in IoT Networks. Proceedings - IEEE Global Communications Conference, GLOBECOM*, σελίδες 237–242. Institute of Electrical and Electronics Engineers Inc., 2023.

[108] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova και Benjamin Turnbull. *Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems*, 100:779–796, 2019.

[109] Segun I. Popoola, Ruth Ande, Bamidele Adebisi, Guan Gui, Mohammad Hammoudeh και Olamide Jogunola. *Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices. IEEE Internet of Things Journal*, 9(5):3930–3944, 2022.

[110] Francisco Lopesde Caldas Filho, Samuel Carlos Meneses Soares, Elder Oroski, Robsonde Oliveira Albuquerque, Rafael Zerbini Alvesda Mata, Fábio Lúcio Lopesde Mendonça και Rafael Timóteode Sousa Júnior. *Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning. Sensors*, 23(14), 2023.

[111] Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras και Helge Janicke. *Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access*, 10:40281–40306, 2022.

[112] Md Mamunur Rashid, Shahriar Usman Khan, Fariha Eusufzai, Md Azharuddin Redwan, Saifur Rahman Sabuj και Mahmoud Elsharief. *A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. Network*, 3(1):158–179, 2023.

[113] Danish Javeed, Muhammad Shahid Saeed, Muhammad Adil, Prabhat Kumar και Alireza Jolfaei. *A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc Networks*, 162, 2024.

[114] Arpan Jain, Ammar Ahmad Awan, Quentin Anthony, Hari Subramoni και Dhableswar K. DK Panda. *Performance Characterization of DNN Training }using TensorFlow and PyTorch on Modern Clusters. 2019 IEEE International Conference on Cluster Computing (CLUSTER)*, Albuquerque, 2019. IEEE.

[115] Xue Ying. *An Overview of Overfitting and its Solutions. Journal of Physics: Conference Series*, τόμος 1168. Institute of Physics Publishing, 2019.

# Συντομογραφίες - Αρκτικόλεξα - Ακρωνύμια

| | |
|---|---|
| βλ. | βλέπε |
| κ.α. | και άλλα |
| κ.λπ. | και λοιπά |
| κ.ο.κ | και ούτω καθεξής |
| π.χ. | παραδείγματος χάριν |
| 1G | First Generation |
| 2G | Second Generation |
| 3G | Third Generation |
| 4G | Fourth Generation |
| 5G | Fifth Generation |
| 5GC | 5G Core |
| ACK | Acknowledge |
| AI | Artificial Intelligence |
| AMF | Access and Mobility Management Function |
| APIs | Application Programming Interfaces |
| ARP | Address Resolution Protocol |
| AR/VR | Augmented Reality / Virtual Reality |
| AUSF | Authentication Server Function |
| BPSO | Binary Particle Swarm Optimization |

| | |
|---|---|
| CDFL | Cross-Device Federated Learning |
| CFL | Centralized Federated Learning |
| CLI | Command Line Interface |
| CNNs | Convolutional Neural Networks |
| CSFL | Cross-Silo Federated Learning |
| DBN | Deep Belief Networks |
| DFL | Decentralized Federated Learning |
| DNS | Domain Name System |
| DoS/DDoS | Denial of Service / Distributed Denial of Service |
| DP | Differential Privacy |
| EPC | Evolved Packet Core |
| FedAdam | Federated Adam |
| FedAvg | Federated Averaging |
| FedAvgM | Federated Averaging with Momentum |
| FedMedian | Federated Median |
| FIN | Finish |
| FL | Federated Learning |
| FLKD | Federated Knowledge Distillation |
| FN | False Negatives |
| FP | False Positives |
| FTP | File Transfer Protocol |

| | |
|---|---|
| FRL | Federated Reinforcement Learning |
| FTL | Federated Transfer Learning |
| GA | Genetic Algorithms |
| GDPR | General Data Protection Regulation |
| gNB | Next Generation NodeB |
| GRU | Gated Recurrent Units |
| HD | High Definition |
| HFL | Horizontal Federated Learning |
| HIDPS | Host-based Intrusion Detection and Prevention System |
| Host-based IDS | Host-based Intrusion Detection System |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IoT | Internet of Things |
| IQR | Interquartile Range |
| K-De | Kernel Density Estimation |
| K-Means | K-Means Clustering Algorithm |
| LSTM | Long Short-Term Memory |
| LTE | Long Term Evolution |
| MAC | Media Access Control |

| | |
|---|---|
| MitM | Man-in-the-Middle |
| ML | Machine Learning |
| MLPs | Multi-Layer Perceptrons |
| NG | Next Generation interface |
| NG-RAN | Next Generation Radio Access Network |
| NIDS | Network Intrusion Detection System |
| NEF | Network Exposure Function |
| NFV | Network Functions Virtualization |
| NG-RAN | Next Generation Radio Access Network |
| NNs | Neural Networks |
| NR | New Radio |
| NRF | Network Repository Function |
| NSA | Non-Standalone |
| PCA | Principal Component Analysis |
| PCF | Policy Control Function |
| PFCP | Packet Forwarding Control Protocol |
| PV | Photovoltaics |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RNNs | Recurrent Neural Networks |
| SA | Standalone |

| | |
|---|---|
| SBA | Service-Based Architecture |
| SDN | Software-Defined Networking |
| SGD | Stochastic Gradient Descent |
| SML | Support Machine Learning |
| SMF | Session Management Function |
| SMPC | Secure Multi-Party Computation |
| SMS | Short Message Service |
| SVMs | Support Vector Machines |
| TEEs | Trusted Execution Environments |
| TCP | Transmission Control Protocol |
| TFF | TensorFlow Federated |
| TLS | Transport Layer Security |
| TN | True Negatives |
| ToN IoT | Telecommunications and Network Internet of Things |
| TP | True Positives |
| UDP | User Datagram Protocol |
| UDM | Unified Data Management |
| UE | User Equipment |
| UPF | User Plane Function |
| URLLC | Ultra-Reliable Low-Latency Communications |
| VNFs | Virtual Network Functions |
| xGB | Extreme Gradient Boosting |

# Απόδοση ξενόγλωσσων όρων

| Απόδοση | Ξενόγλωσσος όρος |
|---|---|
| μηχανική μάθηση | machine learning |
| βαθιά μάθηση | deep learning |
| εκπαίδευση | training |
| εξαγωγή συμπερασμάτων | inference |
| χαρακτηριστικά | features |
| διάνυσμα | vector |
| Συστήματα Ανίχνευσης Εισβολών | Intrusion Detection Systems |