Ασφαλές AI-Driven Edge Computing για Δίκτυα 6G – Προκλήσεις και Λύσεις Κυβερνοασφάλειας

Contents

Λίστα Εικόνων

Λιστα Πινάκων

ΠΕΡΙΛΗΨΗ

Η εξέλιξη των ασύρματων τηλεπικοινωνιών έχει οδηγήσει στην ανάπτυξη της έκτης γενιάς δικτύων (6G), η οποία στοχεύει στην παροχή ταχυτήτων άνω του 1 Tbps, καθυστέρησης κάτω των 0,1 ms και μαζικής συνδεσιμότητας. Η ενσωμάτωση τεχνολογιών όπως το Edge Computing και η Τεχνητή Νοημοσύνη (AI) διαδραματίζει καθοριστικό ρόλο στην επίτευξη αυτών των χαρακτηριστικών. Το Edge Computing, σε αντίθεση με το παραδοσιακό Cloud Computing, επεξεργάζεται τα δεδομένα τοπικά, μειώνοντας τον χρόνο απόκρισης και τον φόρτο του δικτύου.

Ωστόσο, η υιοθέτηση αυτής της προσέγγισης εισάγει σοβαρές προκλήσεις κυβερνοασφάλειας, συμπεριλαμβανομένης της έλλειψης κεντρικοποιημένων μηχανισμών ελέγχου, της διευρυμένης επιφάνειας επίθεσης και, κυρίως, της προστασίας της ιδιωτικότητας των δεδομένων.

Στην παρούσα πτυχιακή εργασία αναλύονται οι βασικότερες απειλές κυβερνοασφάλειας σε AI-driven Edge περιβάλλοντα δικτύων 6G. Παρουσιάζονται σύγχρονες τεχνικές ανίχνευσης και πρόληψης απειλών με την προσθήκη της τεχνητής νοημοσύνης. Επιπλέον, προτείνονται αρχιτεκτονικές ασφαλείας και βέλτιστες πρακτικές που έχουν αναδειχθεί μέσα από τη βιβλιογραφία καθώς και πραγματικές εφαρμογές.

ABSTRACT

The evolution of wireless communications has led to the development of new network generations, reaching the sixth generation (6G). 6G is expected to offer users, extremely high data rates combined with low latency and massive connectivity. The integration of technologies such as Edge Computing and Artificial Intelligence (AI) have a significant role in achieving it. Edge Computing, in contrast to traditional Cloud Computing technology, is more efficient in processing data. Major features of it, is the improving of the response time and the reducing of network congestion. The key characteristic is the decentralized data process instead of the centralized aspect of the cloud. The edge is not going to remove all the usage of Cloud. Cloud will continue to co-exist with edge. Each technology will be used where it is optimal according to its features.

AI will be embedded to 6G and Edge environments. This addition will enhance the network and will provide new applications. However, this adoption has many challenges. More specifically it introduces major cybersecurity challenges, including the lack of centralized control mechanisms, increased attack surfaces, and, the need to ensure data privacy.

This thesis analyzes the main cybersecurity threats in AI-driven edge environments for 6G networks. It presents modern detection and prevention techniques against cyber threats. It emphasizes through the case study in Federated Learning Environment, the use of a certain defense algorithm which is Krum, to prevent certain category of cyber-attacks, which is Data Poisoning. Additionally, it demonstrates security architectures and best practices that have emerged from the recent literature.

Κεφάλαιο 1 – Εισαγωγή

1.1 Πλαίσιο και Σημασία του Θέματος

Η εξέλιξη στις τηλεπικοινωνίες ξεκινώντας από το 1G μέχρι και το 5G έχει επαναπροσδιορίσει τη φύση που οι άνθρωποι όχι απλά επικοινωνούν μεταξύ τους, αλλά ακόμα και τον τρόπο που εργάζονται, αλληλεπιδρούν, ψυχαγωγούνται και μαθαίνουν. Οι μελλοντικές τάσεις της τεχνολογικής βιομηχανίας όπως: το metaverse και εικονική πραγματικότητα, τα οχήματα που δεν χρειάζονται οδηγό και η βιομηχανία 5.0, απαιτούν τεχνολογική υποδομή με ακόμα υψηλότερες ταχύτητες, εξαιρετικά χαμηλή καθυστέρηση και μαζική συνδεσιμότητα. Κάτω από αυτές τις νέες απαιτήσεις το 6G καθίσταται ικανό να πετύχει ταχύτητες άνω του 1 Tbps και απόκριση μικρότερη των 0,1 ms, δηλαδή ανώτερες των προκατόχων του (Hu *et al*., 2021).

Ταυτόχρονα η τεχνολογία ονόματι Edge Computing είναι άρρηκτα συνδεδεμένη με το 6G, φέρνοντας την απαραίτητη υπολογιστική ισχύ πιο κοντά στις συσκευές και εξαλείφει την ανάγκη επικοινωνίας των συσκευών με απομακρυσμένους servers που βρίσκονται στο εκάστοτε datacenter. Αυτό όχι μόνο ελαχιστοποιεί την καθυστέρηση που υπήρχε, αλλά και ενισχύει την ιδιωτικότητα και ζητήματα που προκύπταν καθώς έτσι βελτιώνει και την ασφάλεια των δεδομένων (Zhou et al., 2019). Στο νέο αυτό περιβάλλον που δημιουργείται η τεχνητή νοημοσύνη αποκτά κρίσιμο ρόλο. αλγόριθμοι μηχανικής μάθησης (machine Learning) και βαθιάς μάθησης (Deep Learning) προσφέρουν δυνατότητες πρόβλεψης, αυτοματοποίησης και δυναμικής διαχείρισης πόρων είτε αυτές αφορούν υπολογιστική ισχύ, είτε μεταφορά δεδομένων (Letaief et al., 2021).

Η σύγκλιση Edge–6G–AI, αν και είναι ικανή να δώσει μοναδικές ευκαιρίες στην κοινωνία, δημιουργεί και νέες προκλήσεις που οφείλουν να εξεταστούν στον τομέα της κυβερνοασφάλειας. Η κατανεμημένη φύση του Edge αυξάνει τα διαθέσιμα σημεία επίθεσης, ενώ η πολυπλοκότητα των δεδομένων και η εξάρτηση από έξυπνα μοντέλα καθιστούν απαραίτητη την ανάπτυξη νέων λύσεων λειτουργίας και άμυνας (Suomalainen et al., 2025). Η εργασία έχει σκοπό να εξετάσει το θεωρητικό και τεχνολογικό υπόβαθρο, αναλύει τον ρόλο της AI και του Edge στα δίκτυα 6G, και παρουσιάζονται προτάσεις για την ενίσχυση

που αφορούν θέματα σχετικά με την ασφάλεια των χρηστών και την αντιμετώπιση νέων κινδύνων.

1.2 Στόχοι της Πτυχιακής Εργασίας

Η παρούσα πτυχιακή εργασία έχει τους ακόλουθους σκοπούς:

- Την παρουσίαση των νέων γενιών δικτύων 6G και της λειτουργίας του Edge Computing καθώς και των προκατόχων τους.
- Την καταγραφή και ταξινόμηση των βασικών απειλών κυβερνοασφάλειας στα συστήματα αυτά.
- Την ανάλυση της σύγκλισης της τεχνητής νοημοσύνης του Edge computing και των δικτύων 6G.
- Την παρουσίαση μεθόδων άμυνας απέναντι στις νέες απειλές που προκύπτουν από τη σύγκλιση του Edge Computing, των δικτύων 6G και της Τεχνητής Νοημοσύνης.
- Την παρουσίαση αρχιτεκτονικών και καλών πρακτικών ασφαλείας με βάση τη βιβλιογραφία, στη νέα γενια κυβερνοασφάλειας.

1.3 Δομή της Εργασίας

Η εργασία οργανώνεται ως εξής:

- Στο Κεφάλαιο 2 παρουσιάζονται οι βασικές τεχνολογίες του Edge Computing και του 6G.
- Στο Κεφάλαιο 3 αναλύεται η αξιοποίηση της τεχνητής νοημοσύνης στο Edge και περιγράφεται το Federated Learning όπου θα χρησιμοποιηθεί για την μελέτη περίπτωσης
- Στο Κεφάλαιο 4 εντοπίζονται οι κυριότερες απειλές κυβερνοασφάλειας και η παρουσίαση της ανάγκης για την κυβερνοασφάλεια ως αρχιτεκτονική προσέγγιση.
- Στο Κεφάλαιο 5 προτείνονται λύσεις όπως τεχνικές πρόληψης και ανίχνευσης βασισμένες στην AI.
- Στο Κεφάλαιο 6 περιγράφεται μία μελέτη περίπτωσης Model Poisoning επίθεσης σε περιβάλλον Federated Learning και αξιολογείται η αποτελεσματικότητα του αλγορίθμου Krum.
- Στο Κεφάλαιο 7 παρατίθενται συμπεράσματα και προτάσεις για μελλοντική έρευνα.
- Στο Κεφάλαιο 8 παρουσιάζεται η Βιβλιογραφία.

Κεφάλαιο 2 – Τεχνολογίες Edge Computing και 6G

2.1 Εισαγωγή

Η πρόοδος στον κλάδο της επικοινωνίας είναι άρρηκτα συνδεδεμένη με τα πιο κρίσιμα τεχνολογικά άλματα, και ταυτόχρονα αποτελεί με την σειρά της και τα θεμέλια για πληθώρα άλλων κλαδών. Αυτό καθώς, ανακατασκευάζει τον τρόπο όπου οι άνθρωποι όχι μόνο επικοινωνούν μεταξύ τους αλλά εργάζονται και αλληλοεπιδρούν σε κάθε πτυχή της ανθρώπινης δραστηριότητας. Από τα πρώτα αναλογικά σήματα στα τέλη του 20ου αιώνα και πιο συγκεκριμένα κοντά στην δεκαετία του 1980 έως και τα τωρινά επιτεύγματα της ταχύτητας στα δίκτυα και τις μελλοντικές υποδομές του 6G, κάθε νέα γενιά κινητής τεχνολογίας συντέλεσε με τον δικό της μοναδικό τρόπο ως προς την πορεία μίας πιο καθολικής συνδεσιμότητας και της ψηφιακής ολοκλήρωσης που διακατέχει το σήμερα.
Κάθε γενιά κινητής τηλεφωνίας διαφοροποιείται κυρίως ως προς δύο πυλώνες. Πρώτον, ως προς τον τρόπο που διαμορφώνεται το σήμα και δεύτερον τον τρόπο που επιτρέπει την πολλαπλή πρόσβαση των χρηστών στο δίκτυο.

Από το 1980 περίπου, η πρώτη γενιά ή αλλιώς ονόματι 1G κινητών επικοινωνιών έκανε την εμφάνισή της, και εισήγαγε για πρώτη φορά αυτό που αποκαλούμε "ασύρματη φωνητική επικοινωνία". Η τεχνολογία 1G είναι βασισμένη στα λεγόμενα αναλογικά σήματα. Η εξάρτησή της όμως από αυτά ερχόταν μαζί περιορισμούς ως προς την χωρητικότητα πολλαπλής πρόσβασης των χρηστών, καθώς και την ποιότητα της επικοινωνίας. Η απουσία μηχανισμών κρυπτογράφησης καθιστούσε τις συνομιλίες ευάλωτες σε οποιαδήποτε ευπάθεια, ενώ η ποιότητα του ήχου ήταν το κύριο πρόβλημα καθώς ήταν χαμηλής ποιότητας με παρεμβολές και θόρυβο ενώ οι συνεχείς διακοπές την καθιστούσαν προβληματική. Η πρωτεύων τεχνολογία εκείνης του 1980 χρησιμοποιούσε συστήματα όπως το AMPS (Advanced Mobile Phone System), το οποίο όμως αποτέλεσε τα θεμέλια για την ανάπτυξη των κινητών δικτύων (Sauter, 2021; Gupta & Kumar, 2015).
Η δεύτερη γενιά (2G) που εισήχθη στις αρχές του 1990, ήταν στην ουσία και το πρώτο τεχνολογικό άλμα με κρίσιμο αποτύπωμα, και αυτό γιατί εισήγαγε την ψηφιοποίηση των τηλεπικοινωνιών, αντικαθιστώντας τα αναλογικά συστήματα μετάδοσης που επικρατούσαν προηγουμένως. Η ποιότητα της φωνής βελτιώθηκε αισθητά ενώ οι παρεμβολές, οι διακοπές

και παράσιτα που δημιουργούνταν κατά την διάρκεια των επικοινωνιών είχαν μειωθεί σε ουσιώδη βαθμό αντίστοιχα. Η τεχνολογική αλλαγή αυτή σύστησε νέες υπηρεσίες όπως το SMS ή αλλιώς το Short Message Service κάτι καινοτόμο δεδομένο της εποχής του. Αυτό και οι υπηρεσίες MMS ή αλλιώς το Multimedia Messaging Service μετέτρεψαν σε καθολικό βαθμό τις παγκόσμιες επικοινωνίες ενώ ταυτόχρονα πάνω σε αυτές βασίστηκαν οι σύγχρονες εφαρμογές ανταλλαγής πολυμέσων όπως εικόνες, βίντεο και άλλων αρχείων.

Το πρώτο διεθνές πρότυπο που χρησιμοποιούσε η τεχνολογία των 2G δικτύων ήταν το GSM (Global System for Mobile Communications), που κύριο ανταγωνιστικό του πλεονέκτημα, ήταν η ευρεία κάλυψη. Παράλληλα εκείνη την εποχή έγιναν προσπάθειες πάνω σε νέες τεχνολογίες και πρότυπα αλλά δεν απορροφήθηκαν εν τέλη. Συμπληρωματικά ενσωματώθηκαν στο 2G τεχνολογίες όπως GPRS (General Packet Radio Service) και αργότερα του EDGE (Enhanced Data Rates for GSM Evolution) οι οποίες εισήγαγαν τη μεταγωγή πακέτων και κατέστησαν δυνατή την πρώιμη πρόσβαση στο διαδίκτυο, θέτοντας τις βάσεις για την ανάπτυξη αυτού που σήμερα αποκαλούμε κινητή διαδικτυακή επικοινωνία.

Η επόμενη γενιά, η τρίτη γενιά δικτύων (3G) καθιέρωσε την ευρυζωνική κινητή πρόσβαση στο διαδίκτυο, δηλαδή οι χρήστες μπορούσαν πλέον να χρησιμοποιούν το διαδίκτυο μέσω των φορητών τους συσκευών για διάφορες υπηρεσίες. Με την εξέλιξη της τεχνολογίας και την καθιέρωση τεχνολογικών προτύπων όπως το WCDMA (Wideband Code Division Multiple Access) και ύστερα το HSPA (High Speed Packet Access), οι οποίες αξιοποιούν τεχνικές πολλαπλής πρόσβασης και διαμοιρασμού φάσματος. Μέσω των τεχνολογιών αυτό επιτεύχθηκαν μεγαλύτεροι ρυθμοί μετάδοσης δεδομένων και βελτιωμένη αποδοτικότητα φάσματος, κάτι το οποίο συντέλεσε καθολικά στην ανάπτυξη κρίσιμων εργαλείων και υπηρεσιών που χρησιμοποιούνταν από πληθώρα ανθρώπων όπως ενδεικτικά οι βιντεοκλήσεις (Ghosh et al., 2010; Dahlman et al., 2014). Η 3G εν τέλη ήταν το σημείο καμπής όπου το κινητό τηλέφωνο μετατράπηκε από εργαλείο επικοινωνίας σε έξυπνη συσκευή κάνοντας το απαραίτητο αναπόσπαστο εξάρτημα από της σύγχρονης κοινωνίας.

Η επόμενη γενιά που ακολούθησε ήταν η τέταρτη γενιά (4G), βασισμένη στην τεχνολογία LTE (Long Term Evolution), όπου επέκτεινε και εδραίωσε την πλέον απαραίτητη ευρυζωνική κινητή επικοινωνία. Οι ταχύτητες βελτιώθηκαν σε καθοριστικό βαθμό ξεκλειδώνοντας νέες δυνατότητες στην επικοινωνία και το διαδίκτυο ενώ ταυτόχρονα περιστατικά χαμηλή καθυστέρησης εξαλείφθηκαν αισθητά. Τα δίκτυα 4G έκαναν τους χρήστες να έχουν ομαλή αναπαραγωγή περιεχομένου με ευκρίνεια και καλή ανάλυση, την αποθήκευση καθώς και επεξεργασία δεδομένων στο υπολογιστικό νέφος δίνοντας τους μία πιο ολοκληρωμένη εμπειρία στο διαδίκτυο (Ahmadpanah *et al*., 2016).

Η τωρινή γενιά σε εμπορικό επίπεδο, η πέμπτη γενιά (5G) αποτελεί την πιο ώριμη έκδοση της τεχνολογικής κινητής επικοινωνίας έως σήμερα. Βασίζεται σε υψηλότερες συχνότητες σε σχέση με τους προκατόχους του και προηγμένες τεχνικές κεραιών, η τεχνολογία 5G καταφέρνει ταχύτητες έως και 10 Gbps ανά δευτερόλεπτο, κάτι το οποίο επιτρέπει στους χρήστες σε εμπορικό επίπεδο να παρατηρούν συνήθως ταχύτητες ως 100 Mbps κάτι το οποίο ποικίλει καθώς εξαρτάται από διάφορους παράγοντες πχ ο πάροχος, εμπόδια και απόσταση κεραίας και δέκτη καθώς και πολλά ακόμη. Πλέον με την τεχνολογία της πέμπτης γενιάς (5G) εφαρμογές και εργαλεία εικονικής και επαυξημένης πραγματικότητας (VR/AR) και cloud gaming, ζωντανή μετάδοση είναι εφικτές σε εμπορικό επίπεδο με την εμπειρία των χρηστών να είναι πάντα το επίκεντρο. Η καθυστέρηση (latency) που λειτουργούσε αρνητικά στην εμπειρία των χρηστών σε προηγούμενες γενιές μειώνεται δραματικά έως και το 1 ms, στην ουσία δεν είναι αισθητή στις περισσότερες περιπτώσεις, επιτρέποντας στην τεχνολογία να αναπτυχθεί και να χρησιμοποιηθεί σε πληθώρα κλάδων όπως η οδήγηση χωρίς οδηγό, δηλαδή αυτόνομη οδήγηση με αισθητήρες ή ακόμα και στην ιατρική με χειρουργία εξ αποστάσεως να υλοποιούνται. Μία ακόμα χρήση του 5G καθοριστικής σημασίας για την τωρινή ανθρώπινη δραστηριότητα είναι η δυνατότητα πολλών συνδεδεμένων συσκευών με τη χρήση του Internet of Things (IoT), κάνοντας εφικτή την ανάπτυξη έξυπνων σπιτιών, πόλεων αλλά και ποικίλες χρήσεις σε βιομηχανικό επίπεδο. Δυστυχώς, όλη αυτή η επαναστατική τεχνολογία συνοδεύεται από ορισμένα προβλήματα και ζητήματα, ενδεικτικό παράδειγμα είναι η μικρότερη εμβέλεια λόγω των υψηλών συχνοτήτων και η ανάγκη για πυκνότερη τοποθέτηση κεραιών και υποδομών (Alkhazaali *et al*., 2017). Τέλος δεν όπως και στις προηγούμενες γενιές οφείλουμε να ερμηνεύουμε το 5G όχι ως μία απλή αναβάθμιση των υπηρεσιών επικοινωνίας και πρόσβασης διαδικτύου αλλά ως την τεχνολογική αρχιτεκτονική που καλείται η επόμενη γεννιά να εξελίξει την λεγόμενη 6G (Khan *et al*., 2019).

Η προαναφερθείσα γεννιά 6G, η οποία βρίσκεται για την ώρα σε προχωρημένο στάδιο έρευνας και ανάπτυξης της τυποποίησής της, με βάση τις πληροφορίες που μας παρέχονται ως τώρα, αναμένεται να αλλάξει σε ολιστικό και καθολικό βαθμό το οικοσύστημα των τηλεπικοινωνιών. Στοχεύει στην αξιοποίηση συχνοτήτων THz, επιτυγχάνοντας σε θεωρητικό επίπεδο ταχύτητες μετάδοσης έως 1 Tbps, δηλαδή έως και εκατό φορές μεγαλύτερες από το 5G που χρησιμοποιούμε ως τώρα. Η καθυστέρηση προβλέπεται να μειωθεί σε επίπεδα κάτω των 0.1 ms, δηλαδή θα οδηγήσει στην βελτίωση της λειτουργίας εφαρμογών που θεωρούνται κρίσιμης απόκρισης σε πραγματικό χρόνο όπως αυτές που αναφέραμε προηγουμένως

(Οδήγηση αυτόνομη, χειρουργεία εξ αποστάσεως) αλλά και πολλών ακόμα. Κύριο στοιχείο του 6G θα είναι η ενσωμάτωση της Τεχνητής Νοημοσύνης (ΤΝ) στα δίκτυα, σε όλα τα επίπεδα, κάτι το οποίο θα κάνει τα συστήματα να αυτοβελτιστοποιούνται, εφικτή την πρόβλεψη συμφόρησης του δικτύου με βάση ιστορικά δεδομένα, συμπεριφορά χρηστών και πρόληψη βλαβών, καθώς και την αποδοτική διαχείριση των υπολογιστικών πόρων. Επιπλέον, αναμένεται να υποστηρίζει εφαρμογές που είναι ανερχόμενες αυτή την στιγμή όπως οι ολογραφικές επικοινωνίες, εκτεταμένη πραγματικότητα (XR), αυτόνομα συστήματα και διαστημικές επικοινωνίες, προσφέροντας παγκόσμια κάλυψη. Η αξιοποίηση τέτοιων τεχνολογιών όπως το holographic beamforming δηλαδή την κατεύθυνση ασύρματων σημάτων με επαναστατικό τρόπο, το blockchain για ενίσχυση της ασφάλειας και οι ευφυείς μεταεπιφάνειες (intelligent metasurfaces) που είναι απαραίτητες για να επιτευχθεί ο νέος αυτός τρόπος μετάδοσης, αναμένεται να αποτελούν κρίσιμους πυλώνες για την κατασκευή και εδραίωση της νέας αυτής γενιάς (Chowdhury et al., 2019; Strinati et al., 2021).

Μια από τις πιο υποσχόμενες τεχνολογίες του 6G είναι οι Reconfigurable Intelligent Surfaces (RIS), γνωστές και ως Intelligent Reflecting Surfaces (IRS). Πρόκειται για επιφάνειες αποτελούμενες από εκατοντάδες μικροσκοπικά παθητικά στοιχεία που μπορούν να που αλλάζουν δυναμικά ανάλογα τα ηλεκτρομαγνητικά σήματα που λαμβάνουν, ανακλώντας το προς την τοποθεσία του δέκτη. Σε πειράματα που έχουν γίνει, η χρήση RIS με 100 στοιχεία έχει αποδείξει βελτίωση του SNR (Signal-to-Noise Ratio) κατά 20-30 dB σε σχέση με παραδοσιακές κεραίες, ενώ παράλληλα καταναλώνει έως και 90% λιγότερη ενέργεια σε σύγκριση με ενεργά συστήματα μετάδοσης (Basar et al., 2019).

Συμπληρωματικά, η τεχνολογία Massive MIMO (Multiple Input Multiple Output) αποτελεί άλλον επαναστατικό χαρακτηριστικό που θα αναπτυχθεί μέσω της τεχνολογίας του 6G. Σε αντίθεση με τα κλασικά MIMO συστήματα που χρησιμοποιούν 4-8 κεραίες, το Massive MIMO μπορεί να χρησιμοποιήσει την ίδια στιγμή από 64 μέχρι και 256 κεραίες, κάτι το οποίο επιτρέπει πλήθος χρηστών να εξυπηρετούνται ταυτόχρονα, σε αυτό το σημείο να τονιστεί πως οι κεραίες δεν λειτουργούν μόνο για ένα άτομο την φορά αλλά για πολλά ταυτόχρονα απλώς σε διαφορετικές δέσμες μέσω της τεχνικής spatial multiplexing. Αυτό οδηγεί σε αύξηση της φασματικής απόδοσης κατά 10x συγκριτικά με το 4G LTE (Larsson et al., 2014). Ο συνδυασμός RIS και Massive MIMO στο 6G που προκύπτει επιτρέπει ακόμα και την να επιτρέψει την εξυπηρέτηση περιοχών χωρίς γραμμή ορατότητας δηλαδή σημεία

όπου παρεμβάλλονται εμπόδια (Non-Line-of-Sight, NLOS), αντιμετωπίζοντας έτσι έναν από τους βασικά προβλήματα των THz συχνοτήτων.

2.2 Σύγκριση των δικτύων από 1G έως 6G

Ο Παρακάτω πίνακας 1 και η εικόνα 1 παρουσιάζει τις διαφορές από το 1G έως 6G δίκτυα:

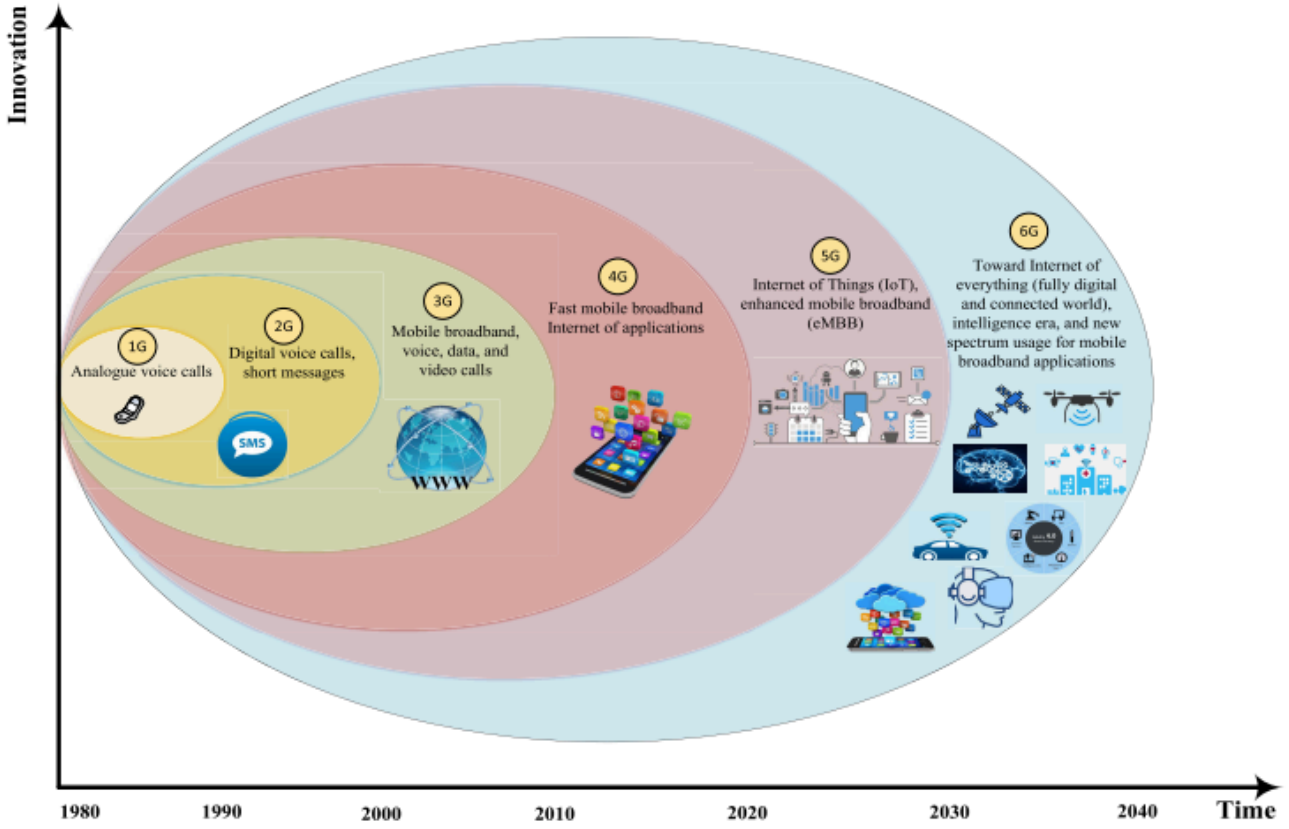
Πίνακας 1 Σύγκριση Δικτύων

Service and Support	1G	2G	3G	4G	5G	6G
Υπηρεσίες	Φωνή	Φωνή, SMS	Φωνή, SMS, Διαδίκτυο	Φωνή, Video, Cloud, Διαδυκτιακές εφαρμογές	IoT, XR (VR,AR)	Holography, Tactile Internet
Τεχνολογίες	AMPS, TACS	GSM	WCDMA	LTE, WiMAX	Massive MIMO	Ultra-Massive MIMO
Latency	>1000 ms	~600–750 ms	~100–500 ms	<100 ms	<10 ms	1 ms
Bandwidth	2 kbps	14.4–64 kbps	2 Mbps	2000 Mbps έως 1Gbps	>10 Gbps	1 Tbps
Frequency	30 KHz	1.8 GHz	1.8–2.4 GHz	2–8 GHz	30–90 GHz	THz Band
Τύπος Μετάδοσης	Αναλογική	Ψηφιακή	Ψηφιακή	Ψηφιακή (IP)	Ψηφιακή (AI-based)	AI-Native, THz

Μέγ. Ταχύτητα	~2.4 kbps	~64 kbps	~2 Mbps	~1 Gbps	~10 Gbps	>1 Tbps

Προσαρμοσμένο από το άρθρο «Key determinants of online impulse buying behavior», Ngo et al. (2025)

Εικόνα 1 Χρονική αναδρομή από το 1G έως 6G δίκτυα.



Χρονική αναδρομή από το 1G έως 6G δίκτυα. Αναδημοσιεύτηκε από Alsabah et al. (2021)

2.3 Εισαγωγή στο Edge Computing

Η κοινωνία μας παράγει ολοένα και περισσότερα δεδομένα που σε μεγάλο βαθμό είναι λογική εκροή της συνεχόμενης τεχνολογικής εξέλιξης. Οι άνθρωποι πλέον χρησιμοποιούν διαφόρων ειδών συσκευές για επικοινωνία και εργασία όπως κινητά τηλέφωνα, ταυτόχρονα χρησιμοποιούν «έξυπνους» αισθητήρες για να διευκολύνουν την καθημερινότητα τους στο σπίτι αλλά και σε βιομηχανικό επίπεδο για ταχύτητα, ενώ φορητές συσκευές συντροφεύουν αδιάκοπα πληθώρα ανθρώπων. Όλες αυτές οι συσκευές παράγουν δεδομένα μεγάλων όγκων και συνεχώς, έτσι δημιουργούνται Big Data περιβάλλοντα (Τα Big Data αναφέρονται σε δεδομένα που ποικίλουν ως προς την μορφή τους, έχουν μεγάλους όγκους και παράγονται συνεχώς). Τα δεδομένα με την σειρά τους, χρειάζονται είτε αποθήκευση είτε επεξεργασία και πολλές φορές άμεση αξιοποίηση, προκειμένου να ληφθεί κάποια απόφαση που πρόκυπτε συχνά από την τεχνική ανάλυσή τους. Το πρόβλημα αυτό είχε λυθεί σε κάποιο βαθμό με την τεχνολογία ονόματι Cloud Computing. Το τελευταίο επέτρεπε στους χρήστες του λύσεις για αυτήν την αποθήκευση, επεξεργασία, πρόσβαση με συγκεντρωτικές δομές, δηλαδή οι Servers που είχαν αυτά τα δεδομένα βρίσκονταν σε μεγάλα κέντρα δεδομένων (Data Centers). Η εξάρτηση της κοινωνίας από το cloud computing σύντομα δημιούργησε περιορισμούς και προβλήματα με βασικό θέμα, αυτό της μετάδοσης δεδομένων μέσω του δικτύου (network data transmission) να προκαλεί αυξημένη καθυστέρηση (latency) και κακή εμπειρία στον εκάστοτε χρήση αλλά και τις επιχειρήσεις οι οποίες απαιτούσαν και απαιτούν ταχύτητα για εξοικονόμηση χρόνου και κατά επέκταση κόστους. Αυτό το πρόβλημα σε συνδυασμό με το γεγονός ότι ο εκάστοτε πάροχος διαδικτύου δεν προσέφερε απαραίτητα αδιάκοπα σταθερή σύνδεση στο διαδίκτυο έντεινε περισσότερο την δυσχέρεια του. Τέλος προέκυψαν και ζητήματα που αφορούσαν την ασφάλεια των δεδομένων. Η λύση δόθηκε από την τεχνολογία του edge computing, που επαναπροσδιορίζει το πώς επεξεργάζονται τα δεδομένα, συγκεκριμένα αυτό που έκανε διαφορετικά είναι η μεταφορά της επεξεργασίας των πληροφοριών σε πιο κοντινό σημείο σε σχέση με το σημείο παραγωγής τους, μειώνοντας έτσι την καθυστέρηση (latency) και την εξάρτηση από κεντρικοποιημένες υποδομές. Για παράδειγμα, αυτό το κοντινό σημείο μπορεί να είναι στο ίδιο το κινητό, σε έναν τοπικό υπολογιστή ή σε έναν μικρό server μέσα στην επιχείρηση.

Δηλαδή ο τρόπος λειτουργίας του edge computing υποστηρίζει ένα σύστημα όπου τα δεδομένα επεξεργάζονται τοπικά, δηλαδή δεν αποστέλλονται σε απομακρυσμένους servers όπως το cloud, έτσι ελαχιστοποιούνται οι απαιτούμενοι πόροι. Αυτά τα κοντινά σημεία που αποστέλλονται τα δεδομένα αποκαλούνται ¨κόμβοι¨ και η όλη επεξεργασία αρχίζει και τελειώνει σε αυτά. Λόγω της κοντινής απόστασης επιτυγχάνεται μειωμένη καθυστέρηση (latency) και άμεση απόκριση γεγονός που βελτιώνει την εμπειρία του χρήστη αισθητά. Λόγω της εγγύτητας της επεξεργασίας των δεδομένων η εξάλειψη των μεταφορών των μεγάλων όγκων δεδομένων σε συνδυασμό με την απαλοιφή της καθυστέρησης παρέχει αυτόματα υψηλή ασφάλεια και ταυτόχρονα επιτυγχάνεται και ουσιώδης βελτίωση σε διάφορες πτυχές της ανθρώπινης δραστηριότητας. Παράλληλα, ένα έμμεσο ακόμα θετικό χαρακτηριστικό είναι πως τα δίκτυα αποφορτίζονται καθώς μόνο τα σημαντικά προωθούνται, μειώνοντας έτσι την συμφόρηση τους. Κάτι ακόμα άξιο αναφοράς είναι πως ακόμα και σε περιόδους χαμηλής ή μηδενικής ποιότητας σύνδεσης οι τοπικές συσκευές που λειτουργούν ως κόμβοι συνεχίζουν να λειτουργούν αυτόνομα καθώς η επεξεργασία των δεδομένων δεν εξαρτάται από τη σύνδεση στο διαδίκτυο. Παρότι το Edge Computing παρουσιάζεται να έχει ποικίλα πλεονεκτήματα, αντιμετωπίζει με την σειρά του ορισμένα κρίσιμα ζητήματα που οφείλουν λύση. Ένα σημαντικό μειονέκτημα είναι το κόστος εγκατάστασης που είναι αρκετά υψηλό, γιατί οι κόμβοι οφείλουν να λειτουργούν με ισχυρούς επεξεργαστές και επαρκή αποθηκευτικό χώρο. Είτε cloud computing, είτε edge υπάρχει ένας κόστος διαχείρισης του εκάστοτε συστήματος και στην δεύτερη περίπτωση είναι αρκετά περισσότερο καθώς υπάρχουν περισσότερες δομές – κόμβοι σε σχέση με το cloud που λειτουργεί με πιο συγκεντρωτικές υποδομές και μπορεί να βασιστεί περισσότερο σε οικονομίες κλίμακας και καταφέρνει να μειώσει το κόστος ανα μονάδα. Ταυτόχρονα, η διαχείριση ενός συστήματος με πολλές συσκευές - κόμβους είναι πιο δύσκολη από ένα απλό, κεντρικό cloud. Επιπροσθέτως, ένα ακόμη μειονέκτημα αποτελεί και στην προκειμένη τεχνολογία το ζήτημα της ασφάλειας. Ενώ δεν χρειάζεται να γίνει σε απομακρυσμένα data centers όπως με το cloud αυτό δεν σημαίνει πως οι κοντινές συσκευές - κόμβοι που λαμβάνουν τα δεδομένα είναι απόλυτα ασφαλής καθώς μπορούν να αποτελέσουν και οι ίδιες στόχους κακόβουλων κυβερνοεπιθέσεων. Τέλος, στα ήδη υπάρχοντα μεονεκτήματα έρχεται να προστεθεί αυτό του προμηθευτή των συσκευών κόμβων. Σε αυτή την τεχνολογική εποχή ολοένα και περισσότεροι κατασκευαστές προμηθεύουν την αγορά με τέτοιες συσκευές οι οποίες δεν είναι συμβατές μεταξύ τους καθώς χρησιμοποιούν διαφορετικά πρότυπα επικοινωνίας και συνδεσιμότητας. (Rikalovic et al., 2019)

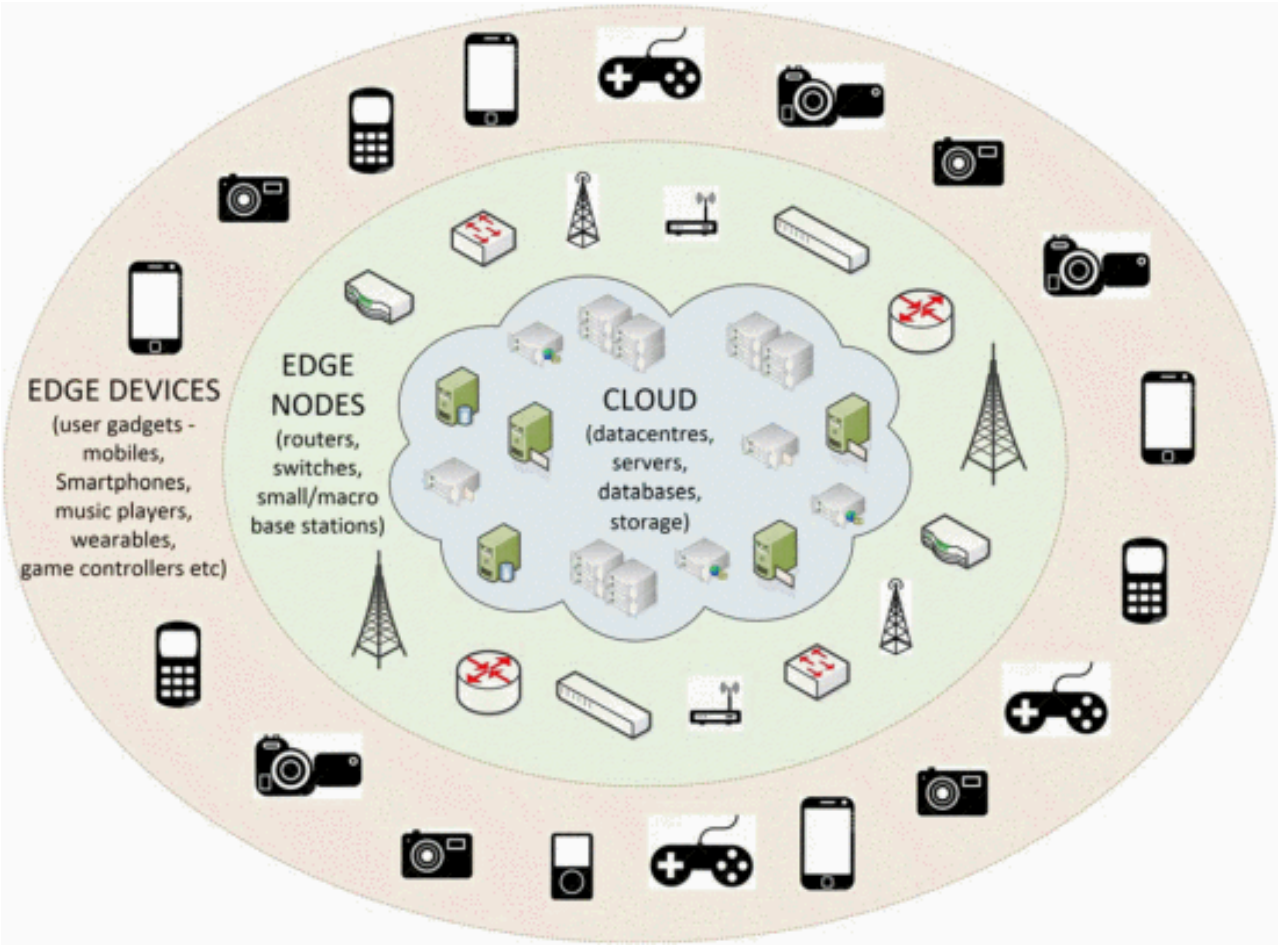
Ακολουθεί ο πίνακας 2 που οπτικοποιεί την σύγκριση μεταξύ edge computing και cloud computing

Πίνακας 2 Διισφορές του Edge & Cloud Computing

Χαρακτηριστικό	**Edge computing**	**Cloud computing**
Ποσότητα αποθήκευσης δεδομένων	Μικρή αποθήκευση δεδομένων	Μεγάλη αποθήκευση δεδομένων
Ποσότητα επεξεργασίας δεδομένων	Μικρός όγκος δεδομένων	Μεγάλος όγκος δεδομένων
Υπολογιστική ισχύς	Λιγότερο ισχυρό	Πιο ισχυρό
Χρόνος επεξεργασίας και απόκρισης	Γρήγορος	Πιο αργός
Ασφάλεια δικτύου/δεδομένων	Πιο ασφαλές (τοπική επεξεργασία)	Λιγότερο ασφαλές (μεταφορά δεδομένων)
Κόστος μεταφοράς/ανάλυσης	Χαμηλό ή μηδενικό	Υψηλότερο λόγω μεταφοράς δεδομένων

(Rikalovic et al., 2019)

Εικόνα 2 Σχέση μεταξύ των Edge κόμβων (Nodes) και του Cloud.



Πηγή: Edge devices and edge nodes in relation to the cloud. Source: Varghese, B., & Buyya, R. (2018). *Next generation cloud computing: New trends and research directions*. Future Generation Computer Systems, 79, 849–861. IEEE Xplore.

2.4 Εφαρμογές και Χρήσεις

Όπως αναφέρθηκε και προηγουμένως, η νέα τεχνολογία του Edge Computing φέρνει στην κοινωνία του σήμερα την επεξεργασία των δεδομένων πιο κοντά στο σημείο που αυτά παράγονται, κάποιες φορές ακόμα και στον ίδιο τον επεξεργαστή πχ όπως ένα έξυπνο ρολόι χειρός, μειώνοντας σημαντικά τον χρόνο απόκρισης και την εξάρτηση τους, από το cloud (Παπαδόπουλος, 2023). Έχει αρχίσει να αλλάζει ριζικά πολλούς τομείς λόγω της μικρής καθυστέρησης (latency) που είναι χαρακτηριστικό της. Τα αυτόνομα αυτοκίνητα λειτουργούν με έξυπνους αισθητήρες οι οποίοι χρειάζεται, να αναλύουν και να υπολογίζουν αμέσως το περιβάλλον κατά την διάρκεια της οδήγησης, προκειμένου να προσαρμοστούν στην κίνηση αλλά ακόμα και σε απρόοπτα εμπόδια. Τα δεδομένα αυτά επεξεργάζονται σε κόμβο μέσα στο ίδιο το αμάξι, ώστε το σύστημα να μπορεί να επιβραδύνει, να επιταχύνει ή να σταματά άμεσα χωρίς να την οποιαδήποτε καθυστέρηση από το διαδίκτυο. Θέτοντας την ασφάλεια ως ύψιστης σημασίας προτεραιότητα, η άμεση επεξεργασία καθίσταται απαραίτητη για το προϊόν της αυτόνομη οδήγησης (Khan κ.ά., 2022). Ήδη σε διάφορες χώρες του κόσμου κατασκευάζονται υποδομές για αυτόνομη οδήγηση. Εξαιρετικό παράδειγμα τέτοιας περίπτωσης, αποτελεί η Γερμανία, η οποία επενδύει σημαντικά σε τέτοιους αυτοκινητοδρόμους και στην επικοινωνία V2X (Vehicle-to-Everything) δηλαδή στην επικοινωνία του οχήματος όχι μόνο με άλλα οχήματα που ονομάζεται V2V ή Vehicle-to-Vehicle, αλλα και φανάρια , το ίδιο το δίκτυο ακόμα και με τους πεζούς μέσω των κινητών τους. (Weiß, 2011)

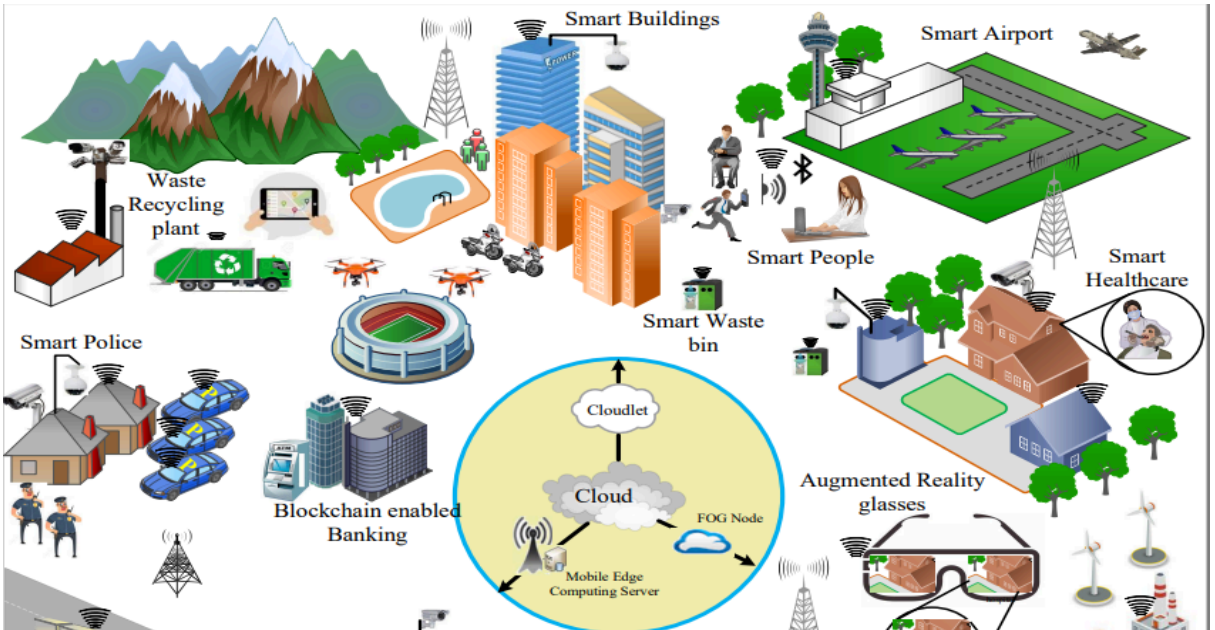
Το edge computing πέρα από τον κλάδο της αυτόνομης οδήγησης παρουσιάζει ποικίλες εφαρμογές και στον χώρο της σύγχρονης βιομηχανίας, καθώς δίνει την δυνατότητα στα μηχανήματα των βιομηχανικών μονάδων και εργοστασίων να λαμβάνουν καθοριστικής σημασίας δεδομένα σε πραγματικό χρόνο να τα επεξεργάζονται και να λειτουργούν ανάλογα με αυτά, ορισμένα παραδείγματα θα μπορούσε να είναι ή καταγραφή κραδασμών ή περιστατικά υπερθέρμανσης και αντίστοιχα το σύστημα να προειδοποιεί εγκαίρως

προκειμένου να αποφευχθούν οι επικείμενες βλάβες, μειώνοντας έτσι οι διακοπές παραγωγής και βελτιώνοντας την αποδοτικότητα και κατά επέκταση την κερδοφορία των επιχειρήσεων (Rikalovic *et al.*, 2019; Manis, 2022). Ένα παράδειγμα τέτοιας περίπτωσης είναι η πολυεθνική TITAN Cement που δραστηριοποιείται στον χώρο της παραγωγής τσιμέντου. Η συγκεκριμένη εταιρία έχει υιοθετήσει τέτοιες τεχνολογίες όπως η συλλογή δεδομένων από αισθητήρες στα μηχανήματα παραγωγής του τσιμέντου προκειμένου να εντοπίζει ενδείξεις ανωμαλίας όπως αλλαγή της θεμοκρασίας, δονήσεις, πίεση σε σωληνώσεις, και να προβαίνει σε προγνωστικές συντηρήσεις στα μηχανήματα της, πρωτού προκύψουν βλάβες (Manis, 2022).

Μία ακόμη εφαρμογή του edge θα είναι στις έξυπνες πόλεις. Οι πόλεις μετασχηματίζονται σε έξυπνες προκειμένου να προσκομίσουν ποικίλα οφέλη στους κατοίκους και τους επισκέπτες τους. Εφαρμογές όπως ο δυναμικός έλεγχος φωτεινών σηματοδοτών, η ανίχνευση κυκλοφοριακής συμφόρησης, η παρακολούθηση ποιότητας αέρα και η έξυπνη διαχείριση ενέργειας ή ύδρευσης είναι προβλήματα και ζητήματα που απασχολούν τις σύγχρονες κοινωνίες. Με τοπική ανάλυση δεδομένων, οι δημοτικές υπηρεσίες μπορούν να αντιδρούν άμεσα, χωρίς να αναμένουν επεξεργασία από κεντρικά συστήματα. Πόλεις όπως η Βαρκελώνη, Τόκιο, Νέα Υόρκη έχουν ήδη ενσωματώσει τέτοια συστήματα αναφέροντας την βελτίωση της κυκλοφορίας την μείωση της σπατάλης νερού και ενέργειας ενώ ταυτόχρονα και προβλήματα που πρέπει να αντιμετωπιστούν όπως έλλειψη σαφών κανονισμών & νόμων από το κράτος, το υψηλό κόστος, η κυβερνοασφάλεια και η δυσλειτουργικότητα. (Vangibhurathachhi, 2025)

Παρακάτω η εικόνα 3 δείχνει μία επισκόπηση από εφαρμογές του edge σε μία έξυπνη πόλη

Εικόνα 3 Οπτικοποίηση Εφαρμογών του edge σε μία έξυπνη πόλη



Πηγή: Edge computing architecture for smart cities (Khan *et al.*, 2019).

Στην υγειονομική περίθαλψη, οι φορητές συσκευές και τα “wearables” συλλέγουν μετρήσεις όπως καρδιακούς παλμούς, πίεση και οξυγόνο στο αίμα. Μέσω edge επεξεργασίας, οι κρίσιμες αλλαγές εντοπίζονται άμεσα και αποστέλλεται ειδοποίηση σε γιατρούς ή συγγενείς, κάτι που έχει αποδειχθεί σωτήριο σε χρόνιες παθήσεις ή σε ηλικιωμένους ασθενείς (Li & Chen, 2024). Ένα ρεαλιστικό παράδειγμα τέτοιας εταιρίας αποτελεί μία από τις θυγατρικές της Google η Fitbit η οποία δραστηριοποιείται στον κλάδο των έξυπνων ρολογιών και λοιπών έξυπνων φορέσιμων συσκευών (wearables), συλλέγοντας δεδομένα από τους φορείς των συσκευών όπως καρδιακοί παλμοί, την ποιότητα ύπνου, οξυγόνο στο αίμα ενώ ταυτόχρονα μπορεί να ειδοποιήσει πέρα από τον χρήστη και τον ιατρό αν χρησιμοποιηθεί κάποια τρίτη ιατρική πλατφόρμα. Αυτές οι ειδοποιήσεις είναι εφικτές άμεσα καθώς η επεξεργασία των δεδομένων υγείας γίνεται τοπικά. (Ringeval et al., 2020) (Gómez-González *et al.*, 2020)

Ένας ακόμα κλάδος που χρησιμεύει το Edge είναι η γεωργία ακριβείας, όπου αισθητήρες στο χωράφι αναλύουν τοπικά την υγρασία και τη θερμοκρασία του εδάφους για να ρυθμίζουν αυτόματα την άρδευση, εξοικονομώντας νερό και ενέργεια (Martínez, 2023). Καθώς αυξάνεται η διάδοση του 5G και προετοιμάζεται το 6G, το Edge Computing θα συνδυάζεται με περισσότερη εγγύτητα με την τεχνητή νοημοσύνη και το cloud, δημιουργώντας ένα ευφυές περιβάλλον όπου η άμεση απόφαση λαμβάνεται τοπικά, ενώ η βαθύτερη ανάλυση γίνεται κεντρικά. Έτσι, αναμένεται να γίνει ο «αφανής ήρωας» πίσω από τεχνολογίες που σύντομα θα θεωρούμε αυτονόητες: από αυτόνομα δίκτυα, ρομπότ, αλλά και πολλές ακόμα ευφυής υπηρεσίες που θα λειτουργούν διακριτικά στην καθημερινότητα.

Κεφάλαιο 3 – Τεχνητή Νοημοσύνη, 6G και Edge Computing

3.1 Εισαγωγή στο 6G

Τα δίκτυα έκτης γενιάς, ή αλλιώς 6G, θα είναι το επόμενο άλμα στον κλάδο των τηλεπικοινωνιών και αναμφίβολα θα αλλάξουν ουσιαστικά τον τρόπο που συνδεόμαστε και επικοινωνούμε. Αυτή τη στιγμή βρίσκεται σε ερευνητικό επίπεδο όχι μόνο από την ακαδημαϊκή κοινότητα, αλλά και από τεχνολογικούς κολοσσούς.

Δύο από τους κύριους στόχους του, είναι οι πολύ υψηλές ταχύτητες μετάδοσης δεδομένων που φτάνουν το επίπεδο των terabit ανά δευτερόλεπτο (σε αντίθεση με τις τωρινές ταχύτητες που υπό κατάλληλες συνθήκες, αγγίζουν μερικά Gbps), και η άμεση απόκριση με σχεδόν μηδενική καθυστέρηση (ultra-low latency), που υπολογίζεται έως 1ms (σε αντίθεση με τις τωρινές καθυστερήσεις που υπολογίζονται από 1 έως 10ms). Επιπλέον το σύστημα θα υποστηρίζει το "massive device connectivity" δηλαδή τη δυνατότητα σύνδεσης τεράστιου αριθμού συσκευών την ίδια χρονική στιγμή ακόμα και σε συνθήκες με υψηλή πυκνότητα συσκευών (High device density) κάτι το οποίο το καθιστά ιδανικό για IoT μεγάλης κλίμακας. Ακόμη, το 6G θα αξιοποιεί καλύτερα το διαθέσιμο φάσμα (spectral efficiency) αυξάνοντας το τωρινό throughput μετάδοσης χωρίς να χρειάζεται περισσότερη ζώνη εύρους.

Για να είναι εφικτά και ουσιαστικά όλα αυτά, το δίκυο θα είναι ευφυές, η Τεχνητή Νοημοσύνη (AI) θα είναι απαραίτητη στην ενσωμάτωση του δικτύου. Δεν θα είναι απλά ως ένα βοηθητικό εργαλείο ανάλυσης, αλλά θα είναι μία πλήρως ενσωματωμένη τεχνολογία που θα υπάρχει στη δομή του ίδιου του δικτύου (Strinati et al., 2021· Zhang et al., 2019). Οι αλγόριθμοι της θα μπορούν να προβλέπουν με προγνωστική ανάλυση πότε υπάρχει ανάγκη για αυξημένη κίνηση, και επιτρέποντας την κατανομή των πόρων να γίνεται δυναμικά (dynamic resource allocation) και να επιτυγχάνεται η βελτιστοποίηση του δικτύου σε πραγματικό χρόνο. Έτσι βελτιώνεται η αποδοτικότητα του φάσματος (spectral efficiency) και η αποδοτικότερη αξιοποίηση της υποδομής. Αυτές οι διεργασίες μειώνουν την σπατάλη των πόρων και πετυχαίνετε χαμηλότερο κόστος ανά bit μετάδοσης οδηγώντας σε πιο βιώσιμα μοντέλα (Tataria et al., 2021).

Βασικές φασματικές συχνότητες που θα αξιοποιεί η γενιά 6G είναι οι συχνότητες τεραχέρτζ (THz). Αυτές επιτρέπουν τη μετάδοση τεράστιου όγκου δεδομένων μέσα σε ελάχιστο χρόνο, λόγω του υψηλού εύρους ζώνης (large bandwidth) που διαθέτουν. Ωστόσο έχουν περιορισμένη εμβέλεια (limited propagation range) και αυξημένη εξασθένηση σήματος (high path loss) παράλληλα με ευαισθησία σε εμπόδια (blockage sensitivity). Σε συνδυασμό όμως με τεχνικές όπως το Massive MIMO (Massive Multiple-Input Multiple-Output) δηλαδή με πολλές κεραίες να εξυπηρετούν τους χρήστες θα βελτιωθούν πολλές παράμετροι των δικτύων. Χαρακτηριστικά όπως η χωρητικότητα (capacity) του δικτύου θα αυξηθεί, η ισχύς του σήματος και η κάλυψη (signal quality & coverage) μέσω του beamforming. Το beamforming αποτελεί έναν μηχανισμό του συστήματος, όπου το σήμα μεταδίδεται ταυτόχρονα σε έναν χρήστη ή κατεύθυνση από πολλές κεραίες αντί να μοιράζεται με τον ίδιο τρόπο σε όλους τους δέκτες. Η τεχνική του Massive MIMO (Massive Multiple-Input Multiple-Output) θα δίνει τη δυνατότητα για καλύτερη αποδοτικότητα φάσματος (spectral efficiency) καθώς θα εκμεταλλεύεται περισσότερο τις χωρικές ροές δηλαδή θα μεταδίδονται περισσότερα bits ανά Hz. Επιπλέον λόγω της φύση του συστήματος οι πολλαπλές κεραίες του επιτρέπουν θα μειωθούν οι παρεμβολές των σημάτων καθώς σχηματίζονται δέσμες σήματος (beams) που επιτρέπουν στα δεδομένα να μεταφέρονται με περισσότερη ακρίβεια. Οι προηγούμενες τεχνικές οδηγούν συμπερασματικά στη σημαντική βελτίωση της αξιοπιστίας της σύνδεσης.

Η Τεχνητή Νοημοσύνη θα είναι παρούσα στη νέα γενιά με ποικίλους τρόπους. Για παράδειγμα η τεχνητή Νοημοσυνή θα χρησιμοποιείται από τον ίδιο τον Πυρήνα δικτύου (core network) δηλαδή από το κεντρικό σύστημα ενός τηλεπικοινωνιακού δικτύου για την πρόβλεψη φόρτου στο δίκτυο, την κατανομή των πόρων καθώς και τον προγνωστικό εντοπισμό. Επιπλέον, στα άκρα του δικτύου, όπως οι κεραίες και οι servers, θα την ενσωματώνουν στις διεργασίες τους επιτρέποντας πιο ομαλή και αποδοτική λειτουργία, παραδείγματα σε αυτό το σημείο μπορούν να αποτελέσουν η αποδοτικότερη, λήψη αποφάσεων και κατανομή πόρων και ταχύτερη επεξεργασία δεδομένων. Παράλληλα, ανερχόμενες τεχνολογίες όπως αυτή της κβαντικής επικοινωνίας και του blockchain θα ενισχύσουν κυρίως την ασφάλεια και τη ακεραιότητα πληροφοριών. Οι επιμέρους συμβολές του θα εξεταστούν αναλυτικότερα στις επόμενες ενότητες.

3.2 Machine Learning και Deep Learing

Δύο σημαντικές υποκατηγορίες λειτουργίας της τεχνητής νοημοσύνης που είναι άξιες αναφοράς, είναι η "Μηχανική Μάθηση" και η "Βαθιά Μάθηση¨. Η "Μηχανική Μάθηση" ή αλλιώς Machine Learning (ML) και η "Βαθιά Μάθηση¨ ή αλλιώς το Deep Learning (DL) είναι δυο έννοιες που θα χρησιμοποιηθούν εξίσου στο νέο αυτό περιβάλλον. Αν και μοιάζουν αρκετά μεταξύ τους, έχουν σημαντικές διαφορές. Η τεχνολογία ML βασίζεται στην κύρια ιδέα ότι ο υπολογιστής μπορεί να μαθαίνει και να εκπαιδεύεται από τους όγκους δεδομένων που το τροφοδοτούμε, δηλαδή χωρίς να του λέμε επακριβώς τι να κάνει σε κάθε φάση επεξεργασίας της πληροφορίας. Δηλαδή, κατανοεί πρότυπα και μοτίβα μέσα στα δεδομένα και με τον καιρό γίνεται ολοένα και καλύτερο στις προβλέψεις του. Θα χρησιμοποιείται όταν τα δεδομένα θα είναι πιο μετρήσιμα όπως η πρόβλεψη κίνησης των δικτύων ή η βασική ανίχνευση βλαβών. Από την άλλη πλευρά, το Deep Learning είναι κάπως πιο πολυσύνθετο. Είναι ένα είδος Machine Learning, αλλά πιο «βαθύ». Χρησιμοποιεί νευρωνικά δίκτυα με πολλά επίπεδα (layers), τα οποία λειτουργούν παρόμοια με τον ανθρώπινο εγκέφαλο, για να αντιληφθεί πιο περίπλοκες πληροφορίες, όπως εικόνες, φωνή ή άλλα πολυμέσα. Τα πρώτα επίπεδα εντοπίζουν τις άκρες, γραμμές συχνότητες, ενώ τα μεσαία επίπεδα χτίζουν πάνω στα προηγούμενα σχήματα και μοτίβα. Τα τελικά επίπεδα χτίζοντας με την σειρά τους στα προηγούμενα επεξεργάζονται πιο σύνθετες έννοιες, χαρακτηριστικά και αναπαραστάσεις. Επειδή έχει αυτή τη δομή, μπορεί να διαχειρίζεται τεράστιο όγκο δεδομένων με μεγάλη ακρίβεια, κάτι που το ML δεν τα καταφέρνει πάντα το στον ίδιο βαθμό. Καταλήγοντας το ML θα χρησιμοποιείται για πιο μονοδιάστατες περιπτώσεις συγκριτικά, ενώ το DL είναι για πιο πολυσύνθετες. Παρακάτω ακολουθεί ένας πίνακας με τις βασικές συγκρίσεις μεταξύ των δύο μοντέλων.

Παρακάτω ο Πίνακας 3 όπου γίνεται σύγκριση Machine Learning και Deep Learning στο Edge Computing.

Πίνακας 3 Σύγκριση Machine & Deap Learning

Χαρακτηριστικό	Machine Learning (ML)	Deep Learning (DL)
Υπολογιστική πολυπλοκότητα	Χαμηλότερη	Υψηλή
Αρχιτεκτονική πολυπλοκότητα Μοντέλου	Απλούστερη	Πολυεπίπεδα νευρωνικά δίκτυα
Όγκος Δεδομένων	Μικρότεροι όγκοι	Τεράστιοι όγκοι
Πολυπλοκότητα δεδομένων	Κυρίως δομημένα δεδομένα	Δομημένα και μη δομημένα (εικόνα, ήχος, σήμα)
Εφαρμογές	Χρησιμοποιείται σε προβλέψεις κίνησης δικτύου, βελτιστοποίηση πόρων, βασική ανίχνευση βλαβών και ασφάλεια	Χρησιμοποιείται σε ανάλυση σύνθετων σημάτων, real-time βελτιστοποίηση δικτύου, προηγμένη ασφάλεια και επεξεργασία φωνής/εικόνας

Πηγή: Ιδία επεξεργασία, βασισμένη σε Mao et al. (2017); Goodfellow et al. (2016).

Να τονιστεί σε αυτό το σημείο πως, δεν είναι ότι το ML δεν είναι εφικτό να επεξεργαστεί εικόνα/ήχο. Είναι ότι συνήθως χρειάζεται περισσότερη προεπεξεργασία, ενώ το DL την ενσωματώνει μέσα στο ίδιο το μοντέλο λειτουργίας του.

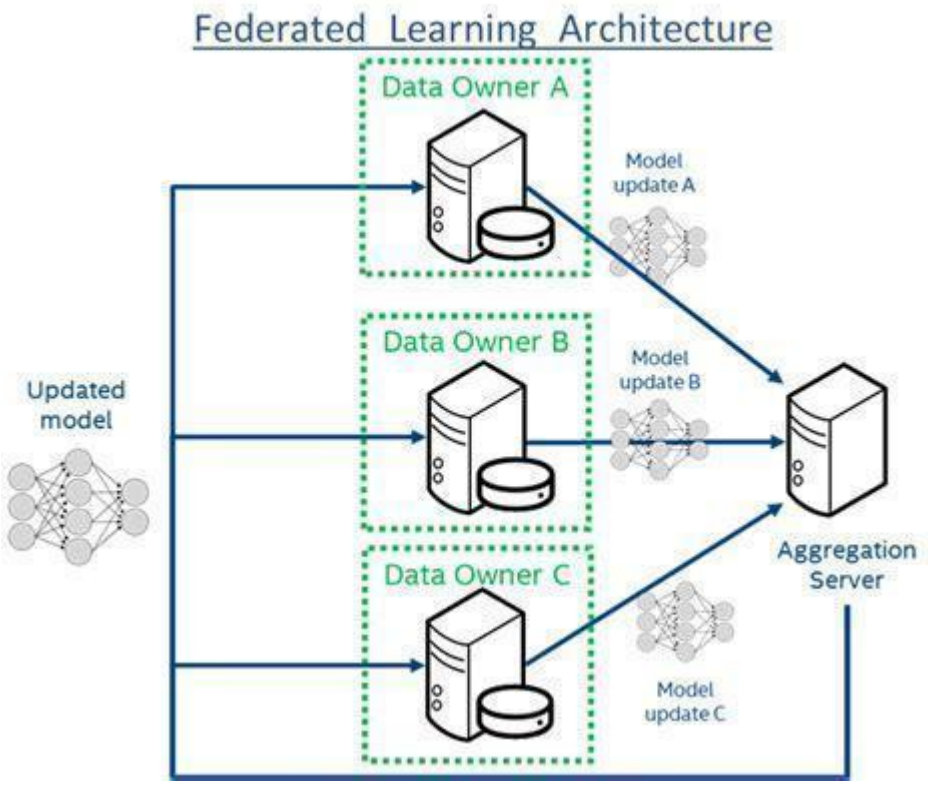
3.3 Federated Learning

Μία ακόμα νέα τεχνολογία είναι το Federated Learning (FL) είναι μια σχετικά νέα ιδέα στη μηχανική μάθηση και έχει παρόμοια φιλοσοφία με το edge computing. Πιο συγκεκριμένα το Federated Learning (FL) κατανέμει την εκπαίδευση σε τοπικές συσκευές (edge devices) και ένας κεντρικός server συντονίζει τις διαδικασίες. Σε αυτόν τον κεντρικό server αποστέλλονται μόνο οι ενημερώσεις του μοντέλου (model updates) που είναι εκροή της επεξεργασίας των δεδομένων τοπικά. Ο κεντρικός αυτός Server έχει δύο κύριες λειτουργείες τις συγχωνεύσεις (aggregation) αυτών των ενημερώσεων, προκειμένου να ενημερώσει το παγκόσμιο μοντέλο και τον συντονισμό (coordination) της διαδικασίας εκπαίδευσης. Οι κύριες κατηγορίες ενημερώσεων του μοντέλου (model updates) είναι οι παράμετροι (Model weights) και τα Gradients (κλίσεις). Οι παράμετροι (Model weights) καθορίζουν την βαρύτητα που επηρεάζει η εκάστοτε είσοδος (input) το τελικό αποτέλεσμα του μοντέλου (output). Ενώ τα Gradients (κλίσεις) δείχνουν το κατά πόσο πρέπει να τροποποιηθούν αυτά τα weights.

Το Federated Learning (FL) προστατεύει την ιδιωτικότητα, καθώς δεν αποστέλλει τα δεδομένα σε κάποια κεντρική υποδομή. Ταυτόχρονα η εκπαίδευση των μοντέλων συνεχίζεται σε τοπικά επίπεδα. χωρίς να σταματά η πρόοδος της μάθησης. Το Federated Learning (FL) παρότι παρουσιάζεται ως απλή έννοια ο συντονισμός του μοντέλου και η ισορροπία μεταξύ απόδοσης – προστασίας των δεδομένων αποτελεί σημαντική πρόκληση

Στην Εικόνα 4 παρακάτω, απεικονίζεται η βασική αρχιτεκτονική του FL, όπου οι τοπικά εκπαιδευμένοι παράμετροι συγχωνεύονται σε έναν κεντρικό κόμβο για τη δημιουργία ενός βελτιωμένου παγκόσμιου μοντέλου.

Εικόνα 4 Αρχιτεκτονική Federated Learning



Πηγή: Li et al. (2020)

Όπως φαίνεται, το Federated Learning επιτυγχάνει ισορροπία μεταξύ μάθησης και ιδιωτικότητας, τα δεδομένα παραμένουν στις συσκευές, ενώ μόνο τα μοντέλα ή οι παράμετροι μοιράζονται.

Κεφάλαιο 4 – Κυβερνοασφάλεια στα Δίκτυα Edge και 6G

4.1 Εισαγωγή στην Ασφάλεια των Δικτύων Επόμενης Γενιάς

Στο κομμάτι της κυβερνοασφάλειας, η μετάβαση που έγινε από τα κλασικά δίκτυα, στα δίκτυα επόμενης γενιάς (5G και 6G) επιφέρει σημαντικές προκλήσεις. Το Internet of Things έχει οδηγήσει στην ραγδαία αύξηση των “έξυπνων” συσκευών. Άρα οι κόμβοι (ή αλλιώς nodes) που συνδέονται στο δίκτυο έχουν πολλαπλασιαστεί. Κατά επέκταση, κυρίως λόγο του Internet of Things, έχουν αυξηθεί και τα endpoints δηλαδή ένα υποσύνολο των κόμβων που αναφέρεται στις τελικές συσκευές που συνδέονται στο δίκτυο. Ο κάθε ένας κόμβος αποτελεί πιθανό στόχο επίθεσης λόγω πιθανών ευπαθειών (Nguyen et al., 2021).

Καθώς η πολυπλοκότητα της αρχιτεκτονικής γίνεται πιο σύνθετη και προστίθενται περισσότεροι κόμβοι (nodes), τόσο αυξάνεται και η επιφάνεια της επίθεσης (attack surface). Ο όρος επιφάνεια επίθεσης ή attack surface αναφέρεται στο σύνολο των πιθανών σημείων (entry points) όπου ένας κακόβουλος παράγοντας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Οι κακόβουλες αυτές επιθέσεις έχουν χωριστεί σε κατηγορίες με βάση κάποια κριτήρια που τις διαχωρίζουν. Ένα συχνό είδος επιθέσεων που παρατηρείται είναι οι Distributed Denial of Service ή DDos. Στόχος του συγκεκριμένου είδους είναι να διακόψουν την διαθεσιμότητα κάποιου συστήματος προς τους χρήστες. Το πετυχαίνουν αυτό, δημιουργώντας πληθώρα αιτημάτων στον server, προκειμένου αυτός να μην μπορεί να ανταποκριθεί στα νόμιμα αιτήματα.

Ένα άλλο συχνό είδος κυβερνοεπιθέσεων είναι οι επιθέσεις Man-in-the-Middle (MitM). Στην προκειμένη περίπτωση ο επιτιθέμενος προσπαθεί να παρεμβληθεί μεταξύ της επικοινωνίας μεταξύ δύο κόμβων (nodes) χωρίς να γίνει αντιληπτός. Συνήθως στόχος του συγκεκριμένου είδους επίθεσης είναι η υποκλοπή των δεδομένων (eavesdropping) ενώ σε άλλες περιπτώσεις η αλλοίωσή τους (data tampering).

Επιπλέον ένα συχνό είδος κυβερνοεπιθέσεων είναι οι επιθέσεις Spoofing. Οι επιθέσεις spoofing έχουν να κάνουν με την παραποίηση της ταυτότητας του χρήστη και έχουν στόχο τη μη εξουσιοδοτημένη πρόσβαση στο σύστημα παρακάμπτοντας τους μηχανισμούς αυθεντικοποίησης του (authentication mechanisms). Η παραποίηση ή η πλαστογράφηση της ταυτότητας είναι εφικτό να επιτευχθεί σε πολλαπλά επίπεδα του δικτύου. Αναφέρονται μερικά ενδεικτικά με βάση τη σύγχρονη βιβλιογραφία: IP Spoofing, DNS Spoofing, email Spoofing (Tang et al., 2021).

Ένα ακόμα συχνό είδος κυβερνοεπιθέσεων ονομάζεται Side-Channel Attack. Στο συγκεκριμένο είδος επίθεσης ο επιτιθέμενος δεν επιτίθεται με την κλασική έννοια της κυβερνοεπίθεσης. Δηλαδή δεν προσπαθεί να παραβιάσει την πρόσβαση στα δεδομένα απευθείας. Στόχος της συγκεκριμένης επίθεσης είναι η παρατήρηση των φυσικών και λειτουργικών συμπεριφορών του συστήματος. Τέτοιες συμπεριφορές αφορούν την θερμοκρασία, την κατανάλωση ενέργειας, το χρόνο εκτέλεσης εργασιών και άλλα. Έπειτα η παρατήρηση αυτή επιτρέπει στους κακόβουλους χρήστες να συμπεράνουν τις διεργασίες που εκτελεί το σύστημα και στη συνέχεια να εξάγουν κρυπτογραφικά κλειδιά (cryptographic keys) και στη συνέχεια να χρησιμοποιηθούν για μη εξουσιοδοτημένη πρόσβαση ή για αποκρυπτογράφηση των δεδομένων. Η κρυπτογράφηση αποτελεί καίρια λειτουργία των συστημάτων τηλεπικοινωνίας. Στην ουσία όταν τα δεδομένα αποστέλλονται από τον έναν κόμβο σε άλλον το σύστημα μετατρέπει τα δεδομένα σε ciphertext δηλαδή χρησιμοποιεί την διαδικασία της κρυπτογράφησης προκειμένου να μπορούν να είναι αναγνώσιμα και να αποκωδικοποιηθούν μόνο από τον χρήστη που διαθέτει το σωστό κρυπτογραφικό κλειδί.

Ακολουθεί παρακάτω ο πίνακας 4 οπού δείχνει πιο ευδιάκριτα τα χαρακτηριστικά των ειδών κυβερνοεπίθεσης που αναφέρθηκαν.

Πίνακας 4 Κατηγορίες Κυβερνοεπιθέσεων

Τύπος Επίθεσης	Περιγραφή
Distributed Denial of Service ή DDos	Αποστολή μεγάλου όγκου αιτημάτων στο σύστημα προκειμένου αυτό να μην καθίσταται δυνατό να εξυπηρετήσει τα νόμιμα αιτήματα.
Man-in-the-Middle (MitM)	Ο επιτιθέμενος προσπαθεί να παρεμβληθεί μεταξύ της επικοινωνίας δύο κόμβων. Σκοπός η αλλοίωση (data tampering), η ανακατεύθυνση (redirection) ή την υποκλοπή (eavesdropping) των δεδομένων
Spoofing	Παραποίηση ταυτότητας με σκοπό τη μη εξουσιοδοτημένη πρόσβαση ή την παράκαμψη μηχανισμών αυθεντικοποίησης. Χωρίζεται σε τύπους ανάλογα το κανάλι-μέσο και επίπεδο που χρησιμοποιείται.
Side-channel	Παρατήρηση φυσικών και λειτουργικών χαρακτηριστικών του συστήματος όπως η θερμοκρασία και η κατανάλωση ενέργειας. Σκοπός, η εξαγωγή ευαίσθητων δεδομένων, όπως τα κρυπτογραφικά κλειδιά

Πηγή: Sicari et al. (2015); Zhou et al. (2019); Roman et al. (2018); Stojmenovic & Wen (2014).

Πέρα από την κρυπτογράφηση των δεδομένων όπου αναφέρθηκε προηγουμένως, υπάρχουν και άλλοι αμυντικοί μηχανισμοί που θεωρούνται θεμελιώδης στην κυβερνοασφάλεια, όπως ο έλεγχος ταυτότητας (authentication). Στη συγκεκριμένη μέθοδο το σύστημα ζητάει από το χρήστη ένα ή περισσότερα στοιχεία αυθεντικοποίησης, προκειμένου να επιβεβαιώσει και να του επιτρέψει την

πρόσβαση. Τέτοια στοιχεία αποτελούν κάποιο PIN, ένας κωδικός (password), δαχτυλικό αποτύπωμα και αρκετά ακόμη. (Rose *et al*., 2020).

Ακόμα ένας καίριος αμυντικός μηχανισμός που αξιοποιείται είναι τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS). Η λειτουργία του είναι ο εντοπισμός των κακόβουλων ενεργειών και όχι απαραίτητα η άμεση απόκορυση του εισβολέα. Αυτός ο εντοπισμός γίνεται με την παρατήρηση ανώμαλων συμπεριφορών του δικτύου. Δηλαδή παρατηρεί τις ανωμαλίες σε αυτό όπως τον ασυνήθιστο αριθμό αιτημάτων (requests) ή αποστολή μεγαλύτερων όγκων δεδομένων σε άγνωστους servers. Όταν το σύστημα όχι μόνο εντοπίζει την απειλή και πέρα από την ειδοποίηση των διαχειριστών προβαίνει και σε μηχανισμούς απόκρουσης, τότε ονομάζεται IPS (Intrusion Prevention Systems – IPS) (Sicari *et al*., 2015).

Με την συμβίωση πολλαπλών τεχνολογιών όπως το Internet of Things (IoT), Edge Computing, Cloud Computing, 5G, 6G, Τεχνητή Νοημοσύνη, Εικονική Πραγματικότητα και άλλες έχουν οδηγήσει στη κατασκευή μίας πολυσύνθετης αρχιτεκτονικής.
Σε συνδιασμό με την αύξηση της επιφάνειας της επίθεσης και την εισαγωγή πολλαπλών διαφορετικών συστημάτων επικοινωνίας από τους κατασκευαστές, οι παραδοσιακές τεχνικές άμυνας κακόβουλων κυβερνοεπιθέσεων έχουν καταστεί ανεπαρκείς. (Jiang *et al*., 2021) (Khan *et al*., 2019)

Παρότι διάφοροι προστατευτικοί μηχανισμοί όπως η διαδικασία της κρυπτογράφησης και του ελέγχου ταυτότητας παρέχουν μερική ασφάλεια στα συστήματα, δεν το προστατεύουν από κάθε πιθανή δίοδο ενός κακόβουλου χρήστη, δηλαδή δεν μπορούν να το θωρακίσουν από κάθε πιθανή ευπάθεια. (Hu *et al*., 2021)

Οι σύγχρονες απαιτήσεις έχουν οδηγήσει στη δημιουργία της Zero Trust μεθόδου, μία πιο δυναμική και αρχιτεκτονική προσέγγιση στα συστήματα κυβερνοασφάλειας, όπου θα αναλυθεί εκτενέστερα παρακάτω. (Rose *et al*., 2020)

4.2 Zero Trust Architecture (ZTA) στα Δίκτυα 6G

Η προσέγγιση αυτή δεν αντικαθιστά τους προηγούμενους αμυντικούς μηχανισμούς της κυβερνοασφάλειας, αλλά τους ενισχύει. Βασίζεται στην αρχή “never trust, always verify” σύμφωνα με αυτή ποτέ δεν εμπιστεύεται από πριν τον χρήστη, την συσκευή, τα endpoints και γενικότερα οτιδήποτε είναι τμήμα του δικτύου και όλα τα στοιχεία του υπόκεινται σε διαρκή επαλήθευση και έλεγχο πρόσβασης. Πιο συγκεκριμένα ελέγχει συνεχώς ποιος ζητάει της πρόσβαση, τι συσκευή χρησιμοποιείται, ποια δικαιώματα δίνονται καθώς και αν η δραστηριότητά του είναι ύποπτη.

Δεδομένης της πολυπλοκότητας των δικτύων 6G, των πολυεπίπεδων τεχνολογιών και συστημάτων που δημιουργούν το οικοσύστημα και των αμέτρητων συσκευών η Zero Trust Architecture (ZTA) λειτουργεί κάτω από θεμελιώδεις κανόνες προκειμένου να ενισχυθεί η αποτελεσματικότητά της. Ένας κύριος κανόνας είναι πως το κάθε σύστημα χρήστης ή συσκευή που ζητάει δικαιώματα πρόσβασης, δεν παίρνει πλήρης πρόσβαση παρά μόνο για την λειτουργία που θέλει να εκτελέσει. Ταυτόχρονα η πρόσβαση που του δίνεται είναι και χρονικά οριοθετημένη. Αυτή η αρχή ονομάζεται Least Privilege Access (Rose *et al.*, 2020).

Μία εξίσου θεμελιώδης αρχή αποτελεί η Continuous Authentication & Monitoring. Αυτή η περίπτωση αφορά την διαρκή ταυτοποίηση και τον έλεγχο. Η ταυτοποίηση της εκάστοτε οντότητας (χρήστη, συσκευή, σύστημα και άλλα) δεν γίνεται μόνο όταν στην αρχή αλλά του ζητείται εκ νέου επαλήθευση όταν τα μοτίβα συμπεριφοράς του θεωρηθούν ύποπτα. Ένα τέτοιο παράδειγμα θα αποτελούσε όταν αλλάξει τοποθεσία σύνδεσης. Αυτή η αρχή επικαλύπτεται σε κάποιο βαθμό από την αρχή Identity-centric Security (Ασφάλεια με επίκεντρο την ταυτότητα). Η διαφορά του είναι ότι η Continuous Authentication & Monitoring επικεντρώνεται στο επαληθεύει την ταυτότητα και τον συνεχή έλεγχο της συμπεριφοράς. Δηλαδή προσανατολίζεται στο κάθε πότε γίνεται ο έλεγχος της ταυτότητας, ενώ η Identity-centric Security επικεντρώνεται στο ποια είναι αυτή η ταυτότητα. Δηλαδή η ερώτηση που απαντά είναι με βάση τι αποφασίζεται η πρόσβαση; (Rose *et al.*, 2020)

Σε παλαιότερες όταν ένας κακόβουλος αποκτούσε πρόσβαση σε μία συσκευή τότε μπορούσε να κινηθεί και στα άλλα συστήματα του ίδιου συστήματος. Για αυτό το λόγο Zero Trust Architecture (ZTA) εφαρμόζει την αρχή της Micro-segmentation (Μικροτμηματοποίηση Δικτύου). Δηλαδή τμηματοποιεί το δίκτυο σε επιμέρους μικρότερα τμήματα ώστε όταν ο κακόβουλος χρήστης που θα αποκτήσει μη εξουσιοδοτημένη πρόσβαση να του ζητηθεί εκ νέου επαλήθευση των στοιχείων όταν αποφασίσει να κινηθεί στα υπόλοιπα τμήματα του δικτύου (Rose *et al.*, 2020).

Επιπλέον μία ακόμα θεμελιώδης αρχή της Zero Trust Architecture (ZTA) αποτελεί η Multi-Factor Authentication (MFA) (Πολυπαραγοντική Ταυτοποίηση). Δηλαδή το σύστημα ζητάει περισσότερο από ένα στοιχείο προκειμένου να επιτρέψει την πρόσβαση. Ένα παράδειγμα αποτελεί το γεγονός πως ορισμένα συστήματα απαιτούν πέρα από κάτι που γνωρίζει ο χρήστης (όπως ένας κωδικός ή pin) και κάτι που διαθέτει στην κατοχή του(όπως η συσκευή του ή αναγνώριση προσώπου) (Rose *et al.*, 2020).

Τον τελευταίο πυλώνα της Zero Trust Architecture (ZTA) καθιστά η Encryption & Secure Communication (Κρυπτογράφηση και Ασφαλής Επικοινωνία), ένας βασικός μηχανισμός κυβερνοασφάλειας που αναφέρθηκε και στην προηγούμενη ενότητα. Δηλαδή τα δεδομένα κρυπτογραφούνται στην μεταφορά τους αλλά και στην αποθήκευσή τους. Έτσι πληρούνται έννοιες που είναι άρρηκτα συνδεδεμένες με την κυβερνοασφάλεια όπως η ακεραιότητα καθώς και η εμπιστευτικότητα (Rose *et al.*, 2020).

Ο παρακάτω Πίνακας 5 περιγράφει πιο ευδιάκριτα τις θεμελιώδης αρχές όπου στηρίζεται η Zero Trust Architecture (ZTA). Ενώ ο Πίνακας 6 δείχνει πιο συγκεντρωτικά τον προσανατολισμό των αμυντικών τεχνολογιών συμπεριλαμβανομένης και της Zero Trust Architecture (ZTA). (Rose *et al.*, 2020)

Πίνακας 5 Θεμελιώδες Αρχές στην Κυβερνοασφάλεια

Θεμελιώδης Αρχή	**Περιγραφή**
Least Privilege Access	Παρέχει μόνο τα δικαιώματα που είναι απαραίτητα στην οντότητα και όχι παραπάνω
Continuous Authentication and Monitoring	Συνεχής επαλήθευση της ταυτότητας της οντότητας και έλεγχος της συμπεριφοράς της.
Identity-centric Security	Επικέντρωση στην ταυτότητα της οντότητας και όχι αν είναι ήδη συνδεδεμένη στο δίκτυο
Micro-segmentation	Χρήση πολλαπλών παραγόντων ταυτοποίησης της ταυτότητας
Encryption & Secure Communication	Κωδικοποίηση των δεδομένων και στην μεταφορά και στην αποθήκευσή τους

Πηγή: Προσαρμογή από Rose *et al*. (2020) και Sicari *et al*. (2015).

Πίνακας 6 Κατηγορίες Αμυντικών Μηχανισμών στην Κυβερνοασφάλεια

Μηχανισμός άμυνας	**Περιγραφή**
Κρυπτογράφηση	Κωδικοποίηση των δεδομένων και στην μεταφορά και στην αποθήκευσή τους
Έλεγχος ταυτότητας (authentication)	Επαλήθευση της ταυτότητας της οντότητας μέσω στοιχείων αυθεντικοποίησης
Intrusion Detection Systems (IDS)	Συστήματα ανίχνευσης εισβολών
Intrusion Prevention Systems (IPS)	Σύστημα που εντοπίζει και αποτρέπει κακόβουλες ενέργειες

Zero Trust Architecture (ZTA)	Αρχιτεκτονική προσέγγιση κυβερνοασφάλειας που βασίζεται στη συνεχή επαλήθευση της οντότητας

Πηγή: Προσαρμογή από Rose *et al*. (2020).

4.3 Επιπτώσεις από την Ενσωμάτωση AI στην Ασφάλεια

Η συνεχόμενη αύξηση της πολυπλοκότητας των δικτύων 6G και των Edge περιβαλλόντων έχει οδηγήσει στην ανάγκη για κατασκευή πιο ευφυών αμυντικών μηχανισμών. Με την ενσωμάτωση της τεχνητής νοημοσύνης στην κυβερνοασφάλεια αυτό καθίσταται εφικτό. Η τεχνητή νοημοσύνη έχει τη δυνατότητα να ενισχύσει λειτουργίες όπως τον εντοπισμό ανωμαλιών στο σύστημα (anomaly detection) και την ανίχνευση ύποπτης δραστηριότητας. Αυτό επιτυγχάνεται μέσω αλγορίθμων μηχανικής μάθησης, οι οποίοι χρησιμοποιούνται για την ανάλυση μεγάλων όγκων δεδομένων σε πραγματικό χρόνο. (Hu *et al*., 2021; Al-Ansi *et al*., 2021).

Αυτό θεωρείται ιδιαίτερα σημαντικό καθώς οι απατήσεις για σχεδόν μηδενικό latency είναι άρρηκτα συνδεδεμένο με τη λειτουργία των δικτύων 6G. Οι χρήσεις της τεχνητής νοημοσύνης που θα ενισχυθούν στην κυβερνοασφάλεια πληθαίνουν καθώς προστίθεται η ικανότητά της να εκπαιδεύεται από τον τεράστιο όγκο δεδομένων σε αντίθεση με τα παραδοσιακά μοντέλα που λειτουργούν με συγκεκριμένα μοτίβα και κανόνες. Τέτοια παραδείγματα ενίσχυσης της κυβερνοασφάλειας αποτελούν: ο εντοπισμός εισβολών (intrusion detection), η ανίχνευση εισβολών (Prevention detection), η πρόβλεψη πιθανών απειλών (predictive analysis) και η η δυναμική προσαρμογή των μηχανισμών ασφάλειας (adaptive security) (Hu *et al*., 2021).
Ακόμα μπορεί να επιφέρει ενίσχυση και στη Zero Trust αρχιτεκτονική. Η Zero Trust παρότι αποτελεί μία αποδοτικότερη προσέγγιση από τα παραδοσιακά μοντέλα στην κυβερνοασφάλεια, η αύξηση της πολυπλοκότητας καθιστά απαραίτητη την ενσωμάτωση της τεχνητής νοημοσύνης στην κυβερνοασφάλεια. Η τεχνητή νοημοσύνη καθίσταται εφικτή να χρησιμοποιηθεί με ποικίλες χρησιμότητες σε αυτήν. Με την χρήση της τα μεγάλη μεγέθη δεδομένων που προκύπτουν από την συνεχή επαλήθευση και έλεγχο καθώς και από άλλες δράσεις θα είναι εφικτό να αναλυθούν και να παρέχουν σε πραγματικό χρόνο αποφάσεις. Η απαίτηση για σχεδόν μηδενικό

Latency είναι απαραίτητη στα edge περιβάλλοντα.

Παρότι η ενίσχυση των αμυντικών μηχανισμών είναι εμφανής με την ενσωμάτωση της τεχνητής νοημοσύνης, παρουσιάζονται και μειονεκτήματα. Αυτό επιτυγχάνεται καθώς τα ίδια τα δεδομένα εκπαίδευσης των μηχανικών συστημάτων εκμάθησης και η διαδικασία λήψης αποφάσεων αποτελούν τους στόχους εξιδεικευμένων κυβερνοπιθέσεων.

Μία από τις κύριες κατηγορίες επιθέσεων αποτελούν οι adversarial ή evasion attacks. Στις συγκεκριμένες τύπου κυβερνοεπιθέσεων, ο κακόβουλος χρήστης έχει σκοπό να παραπλανήσει το σύστημα τεχνητής νοημοσύνης στο να το κατευθύνει σε κάποια εσφαλμένη απόφαση (Hu *et al.*, 2021; Blanchard *et al.*, 2017).

Τέτοιες αποφάσεις περιλαμβάνουν την εσφαλμένη ταξινόμηση ή τη λάθος πρόβλεψη. Αυτό το πετυχαίνουν παραμετροποιώντας και αλλοιώνοντας τα δεδομένα εισόδου (input) που λαμβάνει το σύστημα τεχνητής νοημοσύνης. Τέτοιες περιπτώσεις αποτελούν καίριο πρόβλημα σε πολλές εφαρμογές των 6G, όπως η αυτόνομη οδήγηση, οπού οι συνέπειες θα μπορούσαν να καθίστανται σοβαρές.

Παρόμοια λογική ακολουθούν και οι επιθέσεις Data Poisoning. Έτσι και σε αυτές σκοπός είναι να οδηγηθεί το σύστημα σε εσφαλμένες αποφάσεις. Αυτό που την διαφοροποιεί είναι ο τρόπος που γίνεται η επίθεση καθώς και το σημείο που στοχεύει. Πιο συγκεκριμένα δεν αλλοιώνει τα δεδομένα εισόδου (input) αλλά στοχεύει τα δεδομένα εκπαίδευσης του μοντέλου. Έτσι το μοντέλο εκπαιδεύεται με λανθασμένα δεδομένα, γεγονός που καθιστά τις αποφάσεις του αναξιόπιστες.

Μία ακόμα σημαντική κατηγορία επιθέσεων αποτελεί η model extraction attack. Στην προκειμένη κατηγορία επιθέσεων ο κακόβουλος χρήστης προσπαθεί να εξάγει πληροφορίες για το μοντέλο τεχνητής νοημοσύνης. Ο επιτιθέμενος αλληλοεπιδρά με το μοντέλο με μεγάλους όγκους ερωτήσεων (queries) και αναλύει τις αποκρίσεις του σε αυτές. Σταδιακά αποκωδικοποιεί τη συμπεριφορά του και τη λογική λειτουργίας ή ακόμα και τις παραμέτρους του. Έτσι καθίσταται εφικτή η ανακατασκευή ή η αντιγραφή του, γεγονός που μπορεί να οδηγήσει σε εντοπισμών ευπαθειών, αδυναμιών και αποκάλυψη ευαίσθητων δεδομένων που μπορούν να αξιοποιηθούν σε μεταγενέστερες επιθέσεις.

Στο παρακάτω πίνακα 5 αναφέρονται πιο ευδιάκριτα οι κατηγορίες των επιθέσεων που αναφέρθηκαν καθώς και οι στόχοι και τα πιθανά αποτελέσματα τους (Hu *et al.*, 2021; Blanchard *et al.*, 2017).

Πίνακας 7 Οπτικοποίηση Κατηγοριών Κυβερνοεπιθέσεων

Κατηγορία Επίθεσης	Στόχος	Πιθανό αποτέλεσμα
Adversarial / Evasion Attacks	Τα δεδομένα εισόδου που λαμβάνει το AI σύστημα κατά τη λειτουργία του	Λανθασμένη ταξινόμηση ή εσφαλμένες προβλέψεις
Data Poisoning Attacks	Τα δεδομένα εκπαίδευσης του μοντέλου	Εκπαίδευση του μοντέλου με λανθασμένα δεδομένα και μειωμένη αξιοπιστία
Model Extraction Attacks	Τη λειτουργία και τη λογική του μοντέλου AI	Ανακατασκευή ή αντιγραφή του μοντέλου και εντοπισμός ευπαθειών

Για την αντιμετώπιση των νέων τύπων επιθέσεων αναπτύσσονται νέες τεχνικές κυβερνοασφάλειας. Μία από αυτές τις τεχνικές άμυνας αποτελεί το adversarial training. Στη συγκεκριμένη τεχνική το μοντέλο αντί να εκπαιδεύεται μόνο με φυσιολογικά δεδομένα, εκπαιδεύεται και με κακόβουλα δεδομένα προκειμένου να αναπτύξει ανθεκτικότητα σε επιθέσεις τύπου adversarial και evasion Attacks (Hu *et al.*, 2021; Blanchard *et al.*, 2017). Ταυτόχρονα σημαντικό ρόλο διαδραματίζουν και οι privacy-preserving τεχνικές, όπως το Differential Privacy και το Homomorphic Encryption. Το Differential Privacy προσθέτει στατιστικό θόρυβο στα δεδομένα δηλαδή τα αλλοιώνει με ελεγχόμενο τρόπο προσθέτοντας τυχαίες μεταβολές στα δεδομένα ή στα αποτελέσματα. Έτσι ο κακόβουλος χρήστης δεν καθίσταται ικανός

να εξάγει εύκολα ευαίσθητα δεδομένα για συγκεκριμένα άτομα (Truex *et al.*, 2019). Αντίστοιχα, το Homomorphic Encryption επιτρέπει την επεξεργασία δεδομένων ενώ αυτά παραμένουν κρυπτογραφημένα. Με αυτόν τον τρόπο βελτιώνεται σημαντικά η ασφάλεια η προστασία των πληροφοριών κατά την εκπαίδευση και λειτουργία των μοντέλων τεχνητής νοημοσύνης. (Li *et al.*, 2020).

Ακολουθεί ο πίνακας 6 που δείχνει περισσότερο ευδιάκριτα τις κατηγορίες κυβερνοασφάλειας καθώς και την λειτουργία και τους στόχους τους.

Πίνακας 8 Κατηγορίες Αμυντικών Μηχανισμών Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια των Δικτύων 6G

Τεχνική Άμυνας	Τρόπος λειτουργίας	Στόχος
Adversarial Training	Το μοντέλο εκπαιδεύεται με φυσιολογικά αλλά και κακόβουλα/αλλοιωμένα δεδομένα	Αύξηση ανθεκτικότητας απέναντι σε επιθέσεις τύπου adversarial και evasion attacks
Differential Privacy	Προσθήκη ελεγχόμενου στατιστικού θορύβου στα δεδομένα ή στα αποτελέσματα του συστήματος	Προστασία ιδιωτικότητας και περιορισμός αποκάλυψης ευαίσθητων πληροφοριών
Homomorphic Encryption	Επεξεργασία δεδομένων ενώ αυτά παραμένουν κρυπτογραφημένα	Προστασία δεδομένων κατά την αποθήκευση και επεξεργασία τους

Πηγή: Προσαρμογή από Hu *et al.* (2021), Truex *et al.* (2019) και Li *et al.* (2020).

Συνεπώς από τα παραπάνω γίνεται αντιληπτή η ανάγκη πως η κυβερνοασφάλεια δεν αρκεί να αποτελεί μια μεταγενέστερη προσθήκη στα συστήματα, αλλά καθίσταται

απαραίτητο, οι αλγόριθμοι και τα μοντέλα να χτιστούν γύρω από αυτήν ακόμα και σε επίπεδο σχεδιασμού και υποδομών.

Κεφάλαιο 6 – Μελέτη Περίπτωσης (Case Study)

6.1 Ορισμός και Κατηγορίες Model Poisoning

Το Model Poisoning που θα χρησιμοποιηθεί για τη μελέτη περίπτωσης αποτελεί μία από τις πιο κρίσιμες κατηγορίες κυβερνοεπιθέσεων σε περιβάλλοντα Federated Learning. Η κύρια διαφορά του με άλλες γνωστές κατηγορίες επιθέσεων όπως οι adversarial attacks είναι πως δεν πραγματοποιείται κατά τη λειτουργία του μοντέλου τεχνητής νοημοσύνης (inference time). Το Model Poisoning στοχεύει τις ενημερώσεις παραμέτρων του μοντέλου (gradients ή weights) που αποστέλλονται κατά τη διαδικασία εκπαίδευσης. Πιο συγκεκριμένα επιδιώκεται να αλλιώσουν τα gradients ή τα weights, που αποστέλλονται από τους clients προς τον κεντρικό server κατά τη διαδικασία εκπαίδευσης. Το global model ενημερώνεται μέσω aggregation (συνάθροιση) των gradients όλων των clients. Έστω και ένας μικρός αριθμός κακόβουλων clients είναι αρκετός προκειμένου να επηρεαστεί η συνολική συμπεριφορά του μοντέλου. Στις Data poisoning ο επιτιθέμενος στοχεύει τα δεδομένα εκπαίδευσης ώστε να επηρεάσει έμμεσα τη διαδικασία μάθησης ενώ στο Model Poisoning παρεμβαίνει πιο άμεσα αλλοιώνοντας τις ενημερώσεις των παραμέτρων (gradients ή weights) που αποστέλλονται προς το παγκόσμιο μοντέλο μέσω του κεντρικού server.

Όπως αναφέρθηκε και στην υποενότητα 4.3, οι τύπου poisoning επιθέσεις που αποσκοπούν να αλλοιώσουν τη διαδικασία εκπαίδευσης προκειμένου να μειώσουν την αξιοπιστία και απόδοση του μοντέλου (Biggio & Roli, 2018).

Σε περιβάλλοντα Federated learning όπως αναφέρθηκε και στην ενότητα 3.3, οι τύπου Poisoning επιθέσεις είναι δυσκολότερο να ανιχνευθούν εξαιτίας της

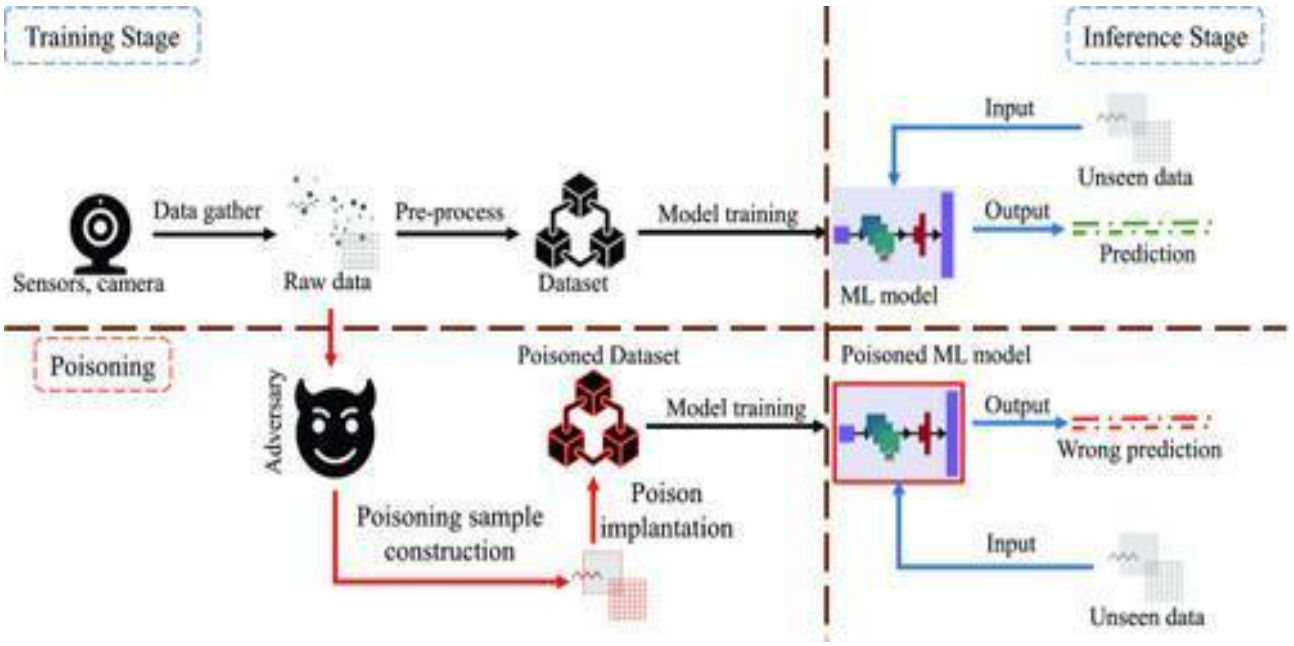
αποκεντρωμένης εκπαίδευσης. Σε τέτοια περιβάλλοντα όπου η εκπαίδευση γίνεται αποκεντρωμένα σε τοπικές υποδομές και συσκευές, ο κεντρικός server δεν έχει άμεση πρόσβαση στα τοπικά δεδομένα εκπαίδευσης των συμμετεχόντων. Έτσι ο επιτιθέμενος μπορεί να αποστείλει αλλοιωμένες ενημερώσεις παραμέτρων (gradients) χωρίς να εντοπιστεί εύκολα από το σύστημα. Η δυνατότητα αυτή αυξάνει σημαντικά την επιφάνεια επίθεσης (attack surface) των distributed AI συστημάτων που έχουν στη διάθεσή τους οι κακόβουλοι χρήστες. Προκύπτει η ανάγκη για να καθιστούν πιο ανθεκτικοί μηχανισμοί aggregation και ανίχνευσης κακόβουλων ενημερώσεων.
Αυτή η συμπεριφορά εντάσσεται στη κατηγορία Byzantine faults. Τέτοιες περιπτώσεις δημιουργούνται όταν ένας συμμετέχων του συστήματος δεν ακολουθεί το προβλεπόμενο πρωτόκολλο και αποστέλλει αυθαίρετες ή κακόβουλες ενημερώσεις προς το δίκτυο (Blanchard et al., 2017).

Οι επιθέσεις Model Poisoning στο Federated Learning διακρίνονται σε δύο βασικές κατηγορίες. Στην πρώτη κατηγορία ανήκουν οι επιθέσεις αλλοίωσης απόδοσης (untargeted attacks). Οι επιθέσεις αυτές αποσκοπούν στη μείωση της συνολικής ακρίβειας του global model, οδηγώντας το σύστημα σε αυξημένο ποσοστό λανθασμένων προβλέψεων.

Στη δεύτερη κατηγορία ανήκουν οι στοχευμένες επιθέσεις (targeted/backdoor attacks). Κατά τις επιθέσεις αυτές, ο κακόβουλος χρήστης επιδιώκει το μοντέλο να λειτουργεί φυσιολογικά για το μεγαλύτερο μέρος των δεδομένων εισόδου. Ωστόσο, όταν εμφανίζονται συγκεκριμένα μοτίβα ή δεδομένα εισόδου, το μοντέλο οδηγείται σκόπιμα σε μια προκαθορισμένη και λανθασμένη απόφαση (Gu et al., 2019).

Ακολουθεί η εικόνα 6 οπου διακρίνονται οι δύο φάσεις του μοντέλου εκπαίδευσης υπό συνθήκες επιθέσεων τύπου Poisoning. Αριστερά βλέπουμε την φάση εκπαίδευσης (training stage) και δεξιά από τις κάθετες διακεκομμένες γραμμές την φάση λειτουργίας (inference stage) του μοντέλου. Ταυτόχρονα διακρίνονται από τις οριζόντιες διακεκομμένες γραμμές η ομαλή λειτουργία του μοντέλου από την πάνω πλευρά και η λειτουργία του μοντέλου αφού έχει υποστεί Poisoning attack από την κάτω πλευρά

Εικόνα 5 Poison Attack Αρχιτεκτονική



Πηγή: (Tian et al., 2022)

6.2 Ο Αλγόριθμος Krum: Θεωρητική Ανάλυση

Για την αντιμετώπιση τέτοιων επιθέσεων έχουν προταθεί Byzantine-robust aggregation τεχνικές όπως ο Krum. Ο αλγόριθμος Krum προτάθηκε από τους Blanchard et al. (2017) και ήταν από τους πρώτους aggregation algorithms που σχεδιάστηκαν ειδικά ώστε να συνεχίζουν να λειτουργούν σωστά ακόμη και όταν κάποιοι συμμετέχοντες του συστήματος είναι κακόβουλοι ή στέλνουν λανθασμένα ενημερώσεις (updates). Οι aggregation algorithms χρησιμοποιούνται σε περιβάλλοντα Federated Learning για τη συγκέντρωση των gradients ή ενημέρωση παραγόντων (parameter updates) που αποστέλλονται από τους συμμετέχοντες clients. Στη συνέχεια, ο κεντρικός server συνδυάζει τις συγκεκριμένες ενημερώσεις παραμέτρων με στόχο τη δημιουργία του νέου global model. Πριν την ανάπτυξη του Krum, ένας από τους πιο συχνά χρησιμοποιούμενους aggregation algorithms στο Federated Learning ήταν ο FedAvg. Ο Krum διαφοροποιείται καθώς δεν υπολογίζει τον μέσο όρο αλλά επιλέγει το update που παρουσιάζει τη μικρότερη απόκλιση από τα περισσότερα υπόλοιπα updates. Αυτό καθώς θεωρεί ότι τα κακόβουλα gradients εμφανίζουν σημαντικά μεγαλύτερη απόκλιση από τα gradients των αξιόπιστων συμμετεχόντων (clients).

Η διαδικασία επιλογής του πιο αξιόπιστου update πραγματοποιείται μέσω του παρακάτω μηχανισμού βαθμολόγησης. Έστω n clients οι οποίοι αποστέλλουν τα updates g_1, g_2, ..., g_n προς τον κεντρικό server, ενώ f αντιπροσωπεύει τον αριθμό των κακόβουλων (Byzantine) clients του συστήματος. ο Krum υπολογίζει για κάθε client i ένα βαθμολόγιο (score) ως εξής: για κάθε update g_i υπολογίζονται οι

τετραγωνικές απόστάσεις από όλα τα υπόλοιπα updates, και στη συνέχεια το score του συγκεκριμένου client ορίζεται ως το άθροισμα των (n - f - 2) μικρότερων απόστάσεων. Το update με το χαμηλότερο score, δηλαδή εκείνο που παρουσιάζει τη μικρότερη συνολική απόκλιση από τα υπόλοιπα updates, επιλέγεται για την ενημέρωση του παγκόσμιου μοντέλου (global model).

Μαθηματικά, αν ορίσουμε το N(i) ως το σύνολο των (n - f - 2) πλησιέστερων updates στο g_i (εξαιρουμένου του ίδιου), τότε το score του i είναι: $s(i) = \Sigma_{□ \in N(i)} ||g_i - g_□||^2$. Ο Krum επιστρέφει το update g_{i^*} όπου $i^* = \text{argmin } s(i)$. Το κρίσιμο θεωρητικό αποτέλεσμα των Blanchard et al. (2017) αποδεικνύει ότι εφόσον $n \geq 2f + 3$, ο Krum εγγυάται Byzantine resilience δηλαδή ανθεκτικότητα υπό ορισμένες συνθήκες στην κατανομή των δεδομένων.

Ένας περιορισμός του Krum είναι ότι χρησιμοποιεί μόνο ένα update σε κάθε γύρο εκπαίδευσης. Αυτό επιβραδύνει τη σύγκλιση του παγκόσμιου μοντέλου (global model) προς τη βέλτιστη απόδοση συγκριτικά με τον FedAvg. Αυτό το μειονέκτημα έχει οδηγήσει στην πρόταση παραλλαγών του, όπως ο Multi-Krum.Ο συγκεκριμένος αλγόριθμος επιλέγει τα m “καλύτερα” updates και υπολογίζει τον μέσο τους, εξισορροπώντας ανθεκτικότητα και ταχύτητα σύγκλισης (Blanchard et al., 2017). Στην παρούσα προσομοίωση χρησιμοποιείται η βασική μορφή του Krum (single best), ώστε να αξιολογηθεί η ανθεκτικότητά του υπό ακραίες συνθήκες επίθεσης.

6.3 Παραμετροποίηση Αλγορίθμου και Αιτιολόγηση Επιλογών

Στη παρούσα μελέτη θα εξεταστεί η untargeted επίθεση τύπου sign-flip. Κατά την επίθεση αυτή, ο κακόβουλος client αντιστρέφει το πρόσημο των gradients που αποστέλλει προς τον κεντρικό server. Έτσι επηρεάζει τη διαδικασία βελτιστοποίησης του παγκόσμιου μοντέλου (global model), οδηγώντας το σύστημα σε μειωμένη απόδοση και αυξημένο ποσοστό λανθασμένων προβλέψεων. Η επιλογή του συγκεκριμένου τύπου επίθεσης γίνεται εσκεμμένα καθώς αποτελεί χαρακτηριστικό παράδειγμα Byzantine συμπεριφοράς σε περιβάλλον Federated Learning. Παράλληλα, επιτρέπει την αποτελεσματική αξιολόγηση του αλγορίθμου Krum, ο οποίος έχει σχεδιαστεί για την ανίχνευση και αντιμετώπιση κακόβουλων ενημερώσεων παραμέτρων που αποστέλλονται από Byzantine clients.

Ο σχεδιασμός της προσομοίωσης βασίστηκε σε συγκεκριμένες επιλογές παραμέτρων που αντικατοπτρίζουν ρεαλιστικά σενάρια ανάπτυξης Federated Learning σε περιβάλλοντα Edge Computing. Ταυτόχρονα ελαχιστοποιούν τον υπολογιστικό φόρτο για σκοπούς επαναληψιμότητας. Ο πίνακας που ακολουθεί συνοψίζει τις επιλεγείσες τιμές και την αιτιολόγησή τους.

Ο αριθμός των clients ορίστηκε σε n = 12, ώστε να αναπαρασταθεί ένα μεσαίου μεγέθους Federated Learning δίκτυο, συγκρίσιμο με σενάρια edge deployments όπου πολλαπλοί κόμβοι (IoT συσκευές, base stations) συνεργάζονται για εκπαίδευση ενός κοινού μοντέλου ανίχνευσης ανωμαλιών. Ο αριθμός αυτός ικανοποιεί τη θεωρητική απαίτηση $n \geq 2f + 3$ για Byzantine resilience, εφόσον $f = 3$ (δηλαδή, $12 \geq 9$).

Το ποσοστό κακόβουλων clients ορίστηκε σε f = 3 (25% του συνόλου). Η επιλογή αυτή είναι σκόπιμα “επιθετική”: η βιβλιογραφία συνήθως εξετάζει σενάρια με 10-30% κακόβουλους συμμετέχοντες (Fung et al., 2020), ενώ το 25% αντιπροσωπεύει ένα σενάριο υψηλής πίεσης που επιτρέπει σαφή αξιολόγηση της αντοχής του Krum.

Ο αριθμός των γύρων επικοινωνίας ορίστηκε σε rounds = 40. Αυτός ο αριθμός είναι αρκετός για να παρατηρηθεί τόσο η αρχική φάση σύγκλισης όσο και η σταθεροποίηση της ακρίβειας, χωρίς υπερβολική εκτέλεση. Τα τοπικά βήματα εκπαίδευσης ορίστηκαν σε local_steps = 3 ανά γύρο, μια τιμή που ισορροπεί μεταξύ επαρκούς τοπικής πληροφόρησης και αποφυγής υπερβολικής τοπικής απομάκρυνσης (client drift), φαινομένου που μπορεί να επηρεάσει αρνητικά τη σύγκλιση σε κατανεμημένα περιβάλλοντα (Karimireddy et al., 2020).

Το τοπικό learning rate ορίστηκε σε local_lr = 0.05, τιμή που εξασφαλίζει σταθερή σύγκλιση χωρίς ταλαντώσεις, ενώ το global learning rate global_lr = 1.0 εφαρμόζει την επιλεγείσα ενημέρωση αυτούσια στο global model, ώστε να αξιολογείται άμεσα η επίδραση της συγκέντρωσης Krum χωρίς πρόσθετη κλιμάκωση.

Η διάσταση του μοντέλου ορίστηκε σε dim = 30, αντιπροσωπεύοντας ένα απλό γραμμικό ταξινομητή (logistic regression) σε χώρο χαρακτηριστικών 30 διαστάσεων. Αυτή η επιλογή επιτρέπει τον γρήγορο υπολογισμό των αποστάσεων Euclid που απαιτεί ο Krum, ενώ παράλληλα παρέχει επαρκή στατιστική πολυπλοκότητα για να αξιολογηθεί ο αντίκτυπος της επίθεσης. Τέλος, ο συντελεστής ενίσχυσης της επίθεσης malicious_scale = 2.0 εξασφαλίζει ότι τα κακόβουλα updates έχουν επαρκή “ενέργεια” ώστε να προκαλέσουν παραμόρφωση αν δεν φιλτραριστούν, χωρίς να καθίστανται τετριμμένα αναγνωρίσιμα λόγω υπερβολικής κλίμακας.

6.4 Υλοποίηση Αλγορίθμου σε Python

Ακολουθεί ο πλήρης κώδικας Python που υλοποιεί την προσομοίωση Federated Learning με Krum aggregation και sign-flip Model Poisoning Attack. Ο κώδικας χρησιμοποιεί απόκλειστικά τη βιβλιοθήκη NumPy, εξασφαλίζοντας πλήρη επαναληψιμότητα και διαφάνεια της υλοποίησης.

```
import numpy as np

#Παραμετροποίηση
SEED          = 42      # Σπόρος τυχαιότητας για αναπαραγωγιμότητα
np.random.seed(SEED)
n_clients     = 12     # Σύνολο clients
f_malicious   = 3      # Κακόβουλοι clients (25%)
rounds        = 40     # Γύροι επικοινωνίας
local_steps   = 3      # Τοπικά βήματα SGD ανά γύρο
local_lr      = 0.05   # Τοπικό learning rate
global_lr     = 1.0    # Global learning rate
dim           = 30     # Διάσταση παραμέτρων μοντέλου
n_per_client  = 250    # Δείγματα ανά client
test_size     = 2500   # Μέγεθος test set
malicious_scale = 2.0  # Συντελεστής ενίσχυσης επίθεσης

if n_clients - f_malicious - 2 < 1:
    raise ValueError("Απαιτείται n - f - 2 >= 1 για Krum.")

# ── Συνθετικά δεδομένα (γραμμικά διαχωρίσιμα) ──────────────────
w_true = np.random.randn(dim)
```

```
def gen_data(n):
    X = np.random.randn(n, dim)
    logits = X.dot(w_true) + 0.1 * np.random.randn(n)
    y = (logits > 0).astype(int)
    return X, y

clients_data = []
for i in range(n_clients):
    X, y = gen_data(n_per_client)
    shift = 0.15 * (np.random.rand(dim) - 0.5)  # Non-IID μετατόπιση
    clients_data.append((X + shift, y))
X_test, y_test = gen_data(test_size)

# ─── Βοηθητικές συναρτήσεις ──────────────────────────────────────
def sigmoid(z):
    return 1.0 / (1.0 + np.exp(-z))

def compute_accuracy(w, X, y):
    return np.mean((sigmoid(X.dot(w)) >= 0.5).astype(int) == y)

def logistic_grad(w, X, y):
    p = sigmoid(X.dot(w))
    return X.T.dot(p - y) / X.shape[0]

# ─── Υλοποίηση Krum ──────────────────────────────────────────────
def krum_aggregation(updates, f):
    updates = np.asarray(updates, dtype=np.float64)
    n = updates.shape[0]
    if n - f - 2 < 1:
        return np.mean(updates, axis=0)
    diffs   = updates[:, None, :] - updates[None, :, :]
    sqdists = np.sum(diffs ** 2, axis=2)
    np.fill_diagonal(sqdists, 1e18)
    m = n - f - 2
    scores = np.array([np.sum(np.partition(sqdists[i], m)[:m])
                       for i in range(n)])
    return updates[int(np.argmin(scores))]
```

```
# ── Αρχικοποίηση και επιλογή κακόβουλων clients ──────────────────
w_global = np.zeros(dim)
malicious_set = {2, 5, 9}  # σταθερό για όλα τα σενάρια
history = {"round": [], "acc_test": [], "mean_update_norm": []}

# ── Κύριος βρόχος προσομοίωσης ───────────────────────────────────
for r in range(1, rounds + 1):
    updates, norms = [], []
    for i in range(n_clients):
        X_i, y_i = clients_data[i]
        w_local  = w_global.copy()
        for _ in range(local_steps):
            w_local -= local_lr * logistic_grad(w_local, X_i, y_i)
        update = w_local - w_global
        if i in malicious_set:
            update = -malicious_scale * update  # sign-flip + scaling
        updates.append(update)
        norms.append(np.linalg.norm(update))
    chosen = krum_aggregation(np.vstack(updates), f=f_malicious)
    w_global += global_lr * chosen
    acc = compute_accuracy(w_global, X_test, y_test)
    history["round"].append(r)
    history["acc_test"].append(acc)
    history["mean_update_norm"].append(np.mean(norms))

# history περιέχει την πορεία ακρίβειας ανά γύρο
```

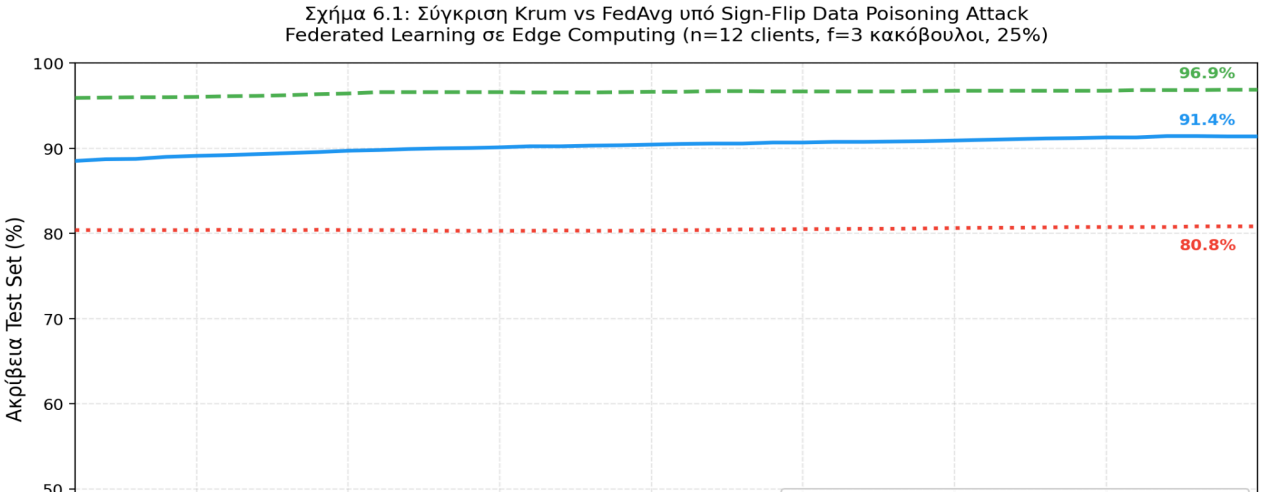
6.5 απότελέσματα Προσομοίωσης και Αξιολόγηση

Η εκτέλεση της προσομοίωσης για 40 γύρους με τις παραμέτρους που περιεγράφηκαν παραπάνω αποδεικνύει την αποτελεσματικότητα του Krum ως μηχανισμός άμυνας έναντι της sign-flip Model Poisoning επίθεσης. Το global model συγκλίνει ομαλά παρά την παρουσία 25% κακόβουλων clients, με την ακρίβεια στο test set να φτάνει το 91.4%, έναντι 96.9% του baseline (FedAvg χωρίς επίθεση) και 80.8% του FedAvg υπό την ίδια επίθεση. Διαφορά +10.6% υπέρ του Krum.

Η ανθεκτικότητα του Krum απέναντι στην επίθεση βασίζεται στον τρόπο αξιολόγησης των gradients που αποστέλλονται από τους clients. Τα sign-flipped updates των κακόβουλων clients βρίσκονται εμφανίζουν αντίθετη κατεύθυνση από τα “έγκυρα” updates των υπόλοιπων clients. Άρα έχουν μεγάλες αποκλίσεις από αυτά. Το βαθμολόγιο Krum τους απόδίδει υψηλή τιμή, οδηγώντας το μοντέλο να αγνοεί αυτόματα τις κακόβουλες ενημερώσεις. Το update με το χαμηλότερο score, που επιλέγεται τελικά, ανήκει σε έναν από τους έγκυρους clients, εξασφαλίζοντας ότι το global model κινείται σε σωστή κατεύθυνση.

Παρακάτω η εικόνα 5 την Σύγκριση Krum με FedAvg υπό Sign-Flip Model Poisoning Attack

Εικόνα 6 Σύγκριση Krum με FedAvg υπό Sign-Flip Model Poisoning Attack



Αυτό που παρατηρείται είναι πως η μέση τιμή μεγέθους των ενημερώσεων (mean update norm) σταθεροποιείται σχετικά γρήγορα κατά τη διαδικασία εκπαίδευσης. Το γεγονός αυτό υποδηλώνει τη σταθερότητα του παγκόσμιου μοντέλου (global model) έπειτα από μερικούς γύρους εκπαίδευσης. Βέβαια η τελική του σύγκλιση για την βέλτιστη απόδοση καθυστερεί λίγο περισσότερο, λόγω του τρόπου λειτουργίας του αλγορίθμου. Η συγκεκριμένη συμπεριφορά γίνεται εμφανής μέσω της σύγκρισης με έναν κλασικό FedAvg αλγόριθμο σε περιβάλλον χωρίς κακόβουλους χρήστες.

Συνολικά, η προσομοίωση επιβεβαιώνει εμπειρικά το θεωρητικό αποτέλεσμα των Blanchard et al. (2017). Ο Krum παρέχει αποδεδειγμένη ανθεκτικότητα σε Byzantine επιθέσεις, καθιστώντας τον κατάλληλο για ανάπτυξη σε edge περιβάλλοντα 6G όπου δεν είναι δυνατή η πλήρης εμπιστοσύνη σε όλους τους συμμετέχοντες (clients).

Κεφάλαιο 7 – Συμπεράσματα και Μελλοντικές Κατευθύνσεις

7.1 Συνοπτική Παρουσίαση Συμβολής της Εργασίας

Η παρούσα πτυχιακή εργασία είχε ως βασικό αντικείμενο τη διερεύνηση της σχέσης ανάμεσα στο Edge Computing, στα δίκτυα 6G και στην Τεχνητή Νοημοσύνη (AI), με ιδιαίτερη έμφαση στις προκλήσεις που αφορούν την κυβερνοασφάλεια.

Η εργασία αυτή ξεκίνησε οριοθετώντας τα θεμέλια των τηλεπικοινωνιών και την εξέλιξή τους, με την πάροδο του χρόνου. Αρχικά παρουσιάστηκαν τα βασικά χαρακτηριστικά και οι τεχνολογικές απαιτήσεις των δικτύων επόμενης γενιάς. Παρουσιάστηκε και αναλύθηκε η έννοια του Edge Computing, καθώς και η συμβολή του σε κατανεμημένες υποδομές προσφέροντας κατανεμημένη επεξεργασία δεδομένων πιο κοντά στις πηγές τους, αντιμετωπίζοντας περιορισμούς των

παραδοσιακών cloud υποδομών (Shi et al., 2016). Έτσι επιτυγχάνονται σημαντικές βελτιώσεις στη ταχύτητα και μείωση των καθυστερήσεων (latency).

Στη συνέχεια αναφέρθηκαν τεχνικές μηχανικής μάθησης (Machine Learning και Deep Learning) και η προσέγγιση Federated Learning σε περιβάλλοντα επόμενης γενιάς και 6G.
Έπειτα εισήχθη η νέα γενιά δικτύων 6G που αναμένεται να καθιερωθεί σε εμπορικό επίπεδο τα επόμενα χρόνια καθώς τα πλεονεκτήματα του όπως η αποδοτικότερη διαχείριση των πόρων, η ελάχιστη καθυστέρηση και ο μεγάλος όγκος συσκευών που μπορεί να υποστηρίξει (Strinati et al., 2021; Zhang et al., 2019).

Τα χαρακτηριστικά των δικτύων 6G συμβάλλουν σημαντικά σε κομβικά θέματα όπως στη μείωση της καθυστέρησης, στην καλύτερη διαχείριση των πόρων, και στην υποστήριξη μεγάλου αριθμού συσκευών σε πραγματικό χρόνο. Επιπροσθέτως αναφέρθηκαν οι σύγχρονες απαιτήσεις κυβερνοασφάλειας των δικτύων επόμενης γενιάς και παρουσιάστηκε η Zero Trust αρχιτεκτονική ως ένα πιο δυναμικό και αυστηρό μοντέλο προστασίας των κατανεμημένων υποδομών.

Καίρια θέση σε αυτή τη μετάβαση της νέας γενιάς αποτελεί η Τεχνητή Νοημοσύνη. Η οποία δεν αντιμετωπίζεται πλέον ως ένα βοηθητικό εργαλείο, αλλά ως αναπόσπαστο μέρος της λειτουργίας και διαχείρισης των δικτύων (Sun et al., 2019). Αναπόφευκτα, η ενσωμάτωση της AI επηρεάζει σημαντικά και τον τομέα της κυβερνοασφάλειας, καθώς δημιουργεί νέες δυνατότητες ανίχνευσης και αντιμετώπισης απειλών, αλλά ταυτόχρονα εισάγει και νέες κατηγορίες επιθέσεων που στοχεύουν τα ίδια τα AI συστήματα.

Η εργασία ανέδειξε ότι η σύγκλιση Edge – 6G – AI δεν αποτελεί απλώς μελλοντικό σενάριο, αλλά ήδη διαμορφώνει την κατεύθυνση της έρευνας και της βιομηχανικής ανάπτυξης (Tataria et al., 2021). Οι τρεις τεχνολογίες, σε συνδυασμό, δημιουργούν τις προϋποθέσεις για νέες υπηρεσίες μεγάλης κλίμακας, όπως αυτόνομα συστήματα μεταφορών, προηγμένες εφαρμογές τηλεϊατρικής, έξυπνες πόλεις και βιομηχανική αυτοματοποίηση. Ωστόσο, η ίδια αυτή πρόοδος συνοδεύεται από προκλήσεις ασφάλειας, αφού η αυξημένη πολυπλοκότητα και κατανεμημένη φύση των συστημάτων διευρύνουν τα σημεία πιθανής επίθεσης (Roman et al., 2018).

Πραγματοποιήθηκε μελέτη περίπτωσης επιθέσεων τύπου Model Poisoning σε περιβάλλον Federated Learning καθώς και αξιολογήθηκε η αποτελεσματικότητα του αλγορίθμου Krum ως μηχανισμός άμυνας.

Η συμβολή της εργασίας εντοπίζεται τόσο στη θεωρητική τεκμηρίωση όσο και στην πρακτική ανάδειξη των κυριότερων προκλήσεων και ευκαιριών που αναμένεται να διαμορφώσουν την επόμενη δεκαετία.

7.2 Κύρια Συμπεράσματα για AI + Edge + 6G

Από την ανάλυση που προηγήθηκε προκύπτουν ορισμένα βασικά συμπεράσματα που αναδεικνύουν τη σημασία της συνεργασίας μεταξύ Edge Computing, 6G και Τεχνητής Νοημοσύνης.

Το edge computing με τα χαρακτηριστικά του, μειώνει την καθυστέρηση και ενισχύει την αποκεντρωμένη επεξεργασία δεδομένων. Τα δίκτυα 6G αναμένεται να προσφέρουν αυξημένες ταχύτητες, βελτιωμένη διαχείριση πόρων και δυνατότητα υποστήριξης μεγάλου αριθμού συσκευών. Ταυτόχρονα καθίσταται απαραίτητη η ανάγκη ενσωμάτωσης της τεχνητής νοημοσύνης για αυτοματοποιήσεις και βελτιστοποιήσεις των δικτύων.

Αυτή η ενσωμάτωση όμως σε περιβάλλοντα 6G και Edge, ελλοχεύει προκλήσεις για την κυβερνοασφάλεια. Η επιφάνεια επίθεσης αυξάνεται όπως και η πολυπλοκότητα των υποδομών. Ταυτόχρονα εμφανίζονται νέες κατηγορίες επιθέσεων που στοχεύουν τα ίδια τα συστήματα τεχνητής νοημοσύνης. Έτσι αναδεικνύεται η σημασία προσεγγίσεων όπως Federated Learning και αμυντικών μηχανισμών που είναι ανθεκτικοί σε Byzantine fault, οι οποίοι χρησιμοποιήθηκαν και στη μελέτη

περίπτωσης αλλά και η ανάπτυξη αρκετών ακόμα που προστατεύουν το σύστημα από διαφορετικές μορφές επιθέσεων.

7.3 Μελλοντικές Τεχνολογικές Τάσεις

Αν και το αντικείμενο της εργασίας επικεντρώνεται στο Edge Computing, τα δίκτυα 6G, την Τεχνητή Νοημοσύνη και την κυβερνοασφάλεια, δεν μπορεί να αγνοηθεί η συνεχής εξέλιξη του τοπίου των επικοινωνιών και οι τεχνολογικές κατευθύνσεις που διαφαίνονται για το μέλλον. Ορισμένες από τις σημαντικότερες τάσεις που θα κατευθύνουν τις κοινωνίες είναι οι παρακάτω.

Δίκτυα 7G και πέραν αυτών: Η έρευνα για τα δίκτυα έβδομης γενιάς (7G) και πέραν αυτών στοχεύει στην πλήρη ενοποίηση των επίγειων, εναέριων και διαστημικών επικοινωνιών. Η συγκεκριμένη κατεύθυνση στοχεύει να αξιοποιήσει νέες μορφές φάσματος όπως τα sub-THz καθώς και τα οπτικά φάσματα. Σκοπό αποτελεί η παγκόσμια συνδεσιμότητα σε καθολικό επίπεδο. Θα εξαλείψει πλήρως γεωγραφικούς περιορισμούς, είτε αυτοί πρόκειται για υπερπυκνοκατοικοιμένες περιοχές είτε απομακρυσμένες αγροτικές. (Giordani et al., 2020).

Ακόμα μία σημαντική έννοια θα αποτελέσει η κβαντική επικοινωνία. Η αξιοποίηση αρχών της κβαντικής φυσικής, όπως η κβαντική διεμπλοκή και η κβαντική κρυπτογραφία θα κατέχουν κρίσιμο ρόλο ιδιαίτερα στις πτυχές τις κυβερνοασφάλειας. Σύμφωνα με την θεωρία της κβαντικής φυσικής θα είναι εφικτό να επιτευχθεί η κβαντική διανομή κλειδιών (QKD). Αυτή η λύση θα προσφέρει θεωρητικά απόλυτη ασφάλεια στη μετάδοση δεδομένων, καθιστώντας αδύνατη την υποκλοπή χωρίς ανίχνευση. Έτσι θα μπορούσαν να επιτευχθεί η μέγιστη κυβερνοασφάλεια (Pirandola et al., 2020).

Η πράσινη ανάπτυξη θα είναι άρρηκτα συνδεδεμένη με τις επικοινωνίες. Τα πράσινα ζητήματα ήδη απασχολούν τις κοινωνίες του σήμερα και οι τεχνολογικοί κολοσσοί όπως και τα κράτη έχουν δεσμευτεί με χρονικά περιθώρια για την πράσινη μετάβασή τους. Ζητήματα όπως η χαμηλή κατανάλωση, τα χαμηλά αποτυπώματα άνθρακα, οι ανανεώσιμες πηγές ενέργειας και η μείωση του περιβαλλοντικού φορτίου θα είναι το επίκεντρο. (Zhang et al., 2020).

Ακόμα οι Νευρομορφικοί υπολογιστές (neuromorphic computing) αποτελούν νέες αρχιτεκτονικές υπολογισμού που μιμούνται τη λειτουργία του ανθρώπινου εγκεφάλου και αναμένεται να επιτύχουν καίρια βελτίωση στην επεξεργασία δεδομένων, ιδιαίτερα στο Edge. (Indiveri & Liu, 2015).

Καταλήγοντας, η πορεία των δικτύων δεν θα περιοριστεί στα κλασσικά επιτεύγματα όπως τη βελτίωση της ταχύτητας και της χωρητικότητας, αλλά θα στοχεύει την ολική ενοποίηση των επικοινωνιών, την ενδυνάμωση της ασφάλεια, την ενεργειακή βιωσιμότητα αλλά και θα ασπαστεί νέα υπολογιστικά συστήματα

7.4 Κλείσιμο

Φτάνοντας στο τέλος της εργασίας είναι εύκολα αντιληπτό πως η σύγκλιση του AI, Edge, 6G δεν αποτελεί απλά μια τάση, αλλά αποτελεί τα θεμέλια για την επόμενη ψηφιακή εποχή. Η Τεχνητή Νοημοσύνη, επιτρέπει στα δίκτυα να αναλύουν δεδομένα, να προσαρμόζονται δυναμικά και να λαμβάνουν αυτόνομες αποφάσεις. Το Edge Computing μειώνει δραστικά τις καθυστερήσεις, φέρνοντας την επεξεργασία πιο κοντά στην πηγή των δεδομένων. Έτσι πετυχαίνεται η άμεση απόκριση ακόμη και σε εφαρμογές που απαιτούν αποφάσεις σε πραγματικό χρόνο. Τέλος, το 6G δημιουργεί το αναγκαίο πλαίσιο για παγκόσμια, αξιόπιστη και ακόμα πιο γρήγορη συνδεσιμότητα, θέτοντας τα θεμέλια για την καθολική δικτύωση ανθρώπων, συσκευών και υποδομών (Strinati et al., 2021; Shi et al., 2016).

Από τη μία πλευρά, η ενοποίηση αυτών των τεχνολογιών υπόσχεται νέες υπηρεσίες πολλά υποσχόμενων. Όπως την τηλεϊατρική και την εκπαίδευση εξ αποστάσεως, ως τα αυτόνομα οχήματα και τις έξυπνες πόλεις. Ωστόσο, παραμένουν ζητήματα που σχετίζονται με την ασφάλεια, την προστασία της ιδιωτικότητας, το ρυθμιστικό πλαίσιο και την κοινωνική αποδοχή των νέων τεχνολογιών.

Παρά τις προκλήσεις, είναι βέβαιο ότι η σύγκλιση του AI – Edge – 6G θα αποτελέσει τον ακρογωνιαίο λίθο της ψηφιακής κοινωνίας των επόμενων δεκαετιών επηρεάζοντας τον τρόπο λειτουργίας της καθημερινότητας και οδηγώντας την κοινωνία στην εποχή την ολικής συνδεσιμότητας

Κεφάλαιο 8 – ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ngo, T. T. A., et al. (2025). *Key determinants of online impulse buying behavior*. Journal Name, Volume(Issue). https://doi.org/10.xxxx
- Alsabah, M., Abdulrazzaq Naser, M., Mahmood, B. M., Abdulhussain, S. H., Eissa, M. R., Al-Baidhani, A., Noordin, N. K., Sait, S. M., Al-Utaibi, K. A., & Hashim, F. (2021). *6G wireless communications networks: A comprehensive survey*. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3124812
- Vangibhurathachhi, S. K. (2025). *Edge computing in IoT for smart cities*. International Journal of Multidisciplinary Research and Growth Evaluation, 6(4), 620–624.
- Ringeval, M., Wagner, G., Denford, S., Paré, G., & Kitsiou, S. (2020). *Fitbit-based interventions for healthy lifestyle outcomes: A systematic review and meta-analysis*. Journal of Medical Internet Research, 22(10), e23968. https://doi.org/10.2196/23968
- Akyildiz, I.F., Gutierrez-Estevez, D.M. & Reyes, E.C. (2010) 'The evolution to 4G cellular systems: LTE-Advanced', Physical Communication, 3(4), pp. 217–244.

- Toorani, M. and Beheshti, S.A.A. (2008) ‘Solutions to the GSM Security Weaknesses’, in *Proceedings of the Second International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2008)*. Cardiff, UK: IEEE, pp. 576–581. Available at: https://doi.org/10.1109/NGMAST.2008.88 (Accessed: 22 May 2026).
- Chowdhury, M.Z., Shahjalal, M., Hasan, M.K. & Jang, Y.M. (2019) ‘6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions’, IEEE Open Journal of the Communications Society, 1, pp. 957–975.
- Dahlman, E., Parkvall, S. & Skold, J. (2014) 4G: LTE/LTE-Advanced for Mobile Broadband. Academic Press.
- Alkhazaali, N.H., Aljiznawi, R.A., Jabbar, S.Q. and Kadhim, D.J. (2017) ‘Mobile Communication through 5G Technology (Challenges and Requirements)’, *International Journal of Communications, Network and System Sciences*, 10(5B), pp. 202–207. Available at: https://doi.org/10.4236/ijcns.2017.105B020 (Accessed: 22 May 2026).
- Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N. & Thomas, T. (2010) ‘LTE-advanced: next-generation wireless broadband technology’, IEEE Wireless Communications, 17(3), pp. 10–22.
- Eluwole, O.T., Jamaludin, M.Z.B., Ndzi, D.L. and Khan, I. (2018) ‘From 1G to 5G, What Next?’, *IAENG International Journal of Computer Science*, 45(3), pp. 339–347. Available at: https://www.iaeng.org/IJCS/issues_v45/issue_3/IJCS_45_3_06.pdf (Accessed: 22 May 2026).
- Parvez, I., Rahmati, A., Guvenc, I., Sarwat, A.I. & Dai, H. (2018) ‘A survey on low latency towards 5G: RAN, core network and caching solutions’, IEEE Communications Surveys & Tutorials, 20(4), pp. 3098–3130.
- Sauter, M. (2021) From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband. Wiley.
- Ahmadpanah, S.H., Chashmi, A.J. and Yadollahi, M. (2016) ‘4G Mobile Communication Systems: Key Technology and Evolution’, *arXiv preprint arXiv:1606.05477*. Available at: https://arxiv.org/abs/1606.05477 (Accessed: 22 May 2026).
- Strinati, E.C., Barbarossa, S., Gonzalez-Jimenez, J.L., Ktenas, D., Cassiau, N., Maret, L. and Dehos, C. (2019) ‘6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication’, *IEEE Vehicular Technology Magazine*, 14(3), pp. 42–50. Available at: https://doi.org/10.1109/MVT.2019.2921162 (Accessed: 22 May 2026).

- Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G.K. and Fan, P. (2019) '6G wireless networks: Vision, requirements, architecture, and key technologies', *IEEE Vehicular Technology Magazine*, 14(3), pp. 28–41. Available at: https://doi.org/10.1109/MVT.2019.2921208 (Accessed: 22 May 2026).
- Chen, J. and Ran, X. (2019) 'Deep learning with edge computing: A review', *Proceedings of the IEEE*, 107(8), pp. 1655–1674. Available at: https://doi.org/10.1109/JPROC.2019.2921977 (Accessed: 22 May 2026)
- Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R. *et al.* (2021) 'Advances and open problems in federated learning', *Foundations and Trends in Machine Learning*, 14(1–2), pp. 1–210. Available at: https://doi.org/10.1561/2200000083 (Accessed: 22 May 2026).
- Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y. and Shi, W. (2019) 'Edge Computing for Autonomous Driving: Opportunities and Challenges', *Proceedings of the IEEE*, 107(8), pp. 1697–1716. Available at: https://doi.org/10.1109/JPROC.2019.2915983 (Accessed: 22 May 2026).
- Mao, Y., You, C., Zhang, J., Huang, K. and Letaief, K.B. (2017) 'A survey on mobile edge computing: The communication perspective', *IEEE Communications Surveys & Tutorials*, 19(4), pp. 2322–2358. Available at: https://doi.org/10.1109/COMST.2017.2745201 (Accessed: 22 May 2026).
- Gómez-González, E., Gomez, E., Márquez-Rivas, J., Guerrero-Claro, M., Fernández-Lizaranzu, I., Relimpio-López, M.I., Dorado, M.E., Mayorga-Buiza, M.J., Izquierdo-Ayuso, G. and Capitán-Morales, L. (2020) 'Artificial intelligence in medicine and healthcare: a review and classification of current and near-future applications and their ethical and social impact', *arXiv preprint arXiv:2001.09778*. Available at: https://arxiv.org/abs/2001.09778 (Accessed: 22 May 2026)
- Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016) 'Edge Computing: Vision and Challenges', *IEEE Internet of Things Journal*, 3(5), pp. 637–646. Available at: https://doi.org/10.1109/JIOT.2016.2579198 (Accessed: 22 May 2026).
- Tataria, H., Shafi, M., Molisch, A.F., Dohler, M., Sjöland, H. and Tufvesson, F. (2021) '6G wireless systems: Vision, requirements, challenges, insights, and opportunities', *Proceedings of the IEEE*, 109(7), pp. 1166–1199. Available at: https://doi.org/10.1109/JPROC.2021.3061701 (Accessed: 22 May 2026).
- Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R. and Zhou, Y. (2019) 'A Hybrid Approach to Privacy-Preserving Federated Learning', *Proceedings of*

the 12th ACM Workshop on Artificial Intelligence and Security (AISec '19), pp. 1–11. Available at: https://doi.org/10.1145/3338501.3357370 (Accessed: 22 May 2026).

- Pham, Q.V., Fang, F., Ha, V.N., Piran, M.J., Le, M., Le, L.B. and Hwang, W.J. (2020) 'A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art', *IEEE Access*, 8, pp. 116974–117017. Available at: https://doi.org/10.1109/ACCESS.2020.3001277 (Accessed: 22 May 2026).
- Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G.K. and Fan, P. (2019) '6G wireless networks: Vision, requirements, architecture, and key technologies', *IEEE Vehicular Technology Magazine*, 14(3), pp. 28–41. Available at: https://doi.org/10.1109/MVT.2019.2921208 (Accessed: 22 May 2026).
- Khan, L.U., Yaqoob, I., Tran, N.H., Kazmi, S.M.A., Dang, T.N. and Hong, C.S. (2019) 'Edge-Computing-Enabled Smart Cities: A Comprehensive Survey', *arXiv preprint arXiv:1909.08747*. Available at: https://arxiv.org/abs/1909.08747 (Accessed: 22 May 2026).
- Zhou, J. et al. (2019) 'Predictive maintenance in smart factories: From machine learning to artificial intelligence', *IEEE Access*, 7, pp. 129398–129412.
- Apruzzese, G. et al. (2018) 'Machine learning for cybersecurity: a survey', *IEEE Communications Surveys & Tutorials*, 21(3), pp. 3036–3070.
- Biggio, B. & Roli, F. (2018) 'Wild patterns: Ten years after the rise of adversarial machine learning', *Pattern Recognition*, 84, pp. 317–331.
- Dai, Y. et al. (2020) 'Privacy-enhancing technologies for 6G: Opportunities and challenges', *IEEE Network*, 34(6), pp. 72–79.
- Goodfellow, I., Shlens, J. & Szegedy, C. (2015) 'Explaining and harnessing adversarial examples', *International Conference on Learning Representations (ICLR)*.
- Nguyen, T.T. et al. (2021) 'Blockchain for 5G and beyond networks: A state of the art survey', *Journal of Network and Computer Applications*, 190, 103–128.
- Papernot, N. et al. (2016) 'The limitations of deep learning in adversarial settings', *IEEE European Symposium on Security and Privacy*, pp. 372–387.
- Pitropakis, N. et al. (2019) 'A taxonomy and survey of attacks against machine learning', *Computer Science Review*, 34, 100199.
- Roman, R., Lopez, J. & Mambo, M. (2018) 'Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges', *Future Generation Computer Systems*, 78, pp. 680–698.
- Hu, Y., Mirsky, Y., Dolan-Gavitt, B., Macedo, D., Mullins, B., Oliveira, R. and Shmatikov, V. (2021) 'Artificial Intelligence Security: Threats and Countermeasures', *ACM*

Computing Surveys, 55(1), pp. 1–36. Available at: https://doi.org/10.1145/3487890 (Accessed: 22 May 2026).

- Sicari, S. et al. (2015) 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks*, 76, pp. 146–164.
- Stojmenovic, I. & Wen, S. (2014) 'The fog computing paradigm: Scenarios and security issues', *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, pp. 1–8.
- Tang, F. et al. (2021) 'Security challenges in 6G wireless communications', *IEEE Wireless Communications*, 28(6), pp. 142–149.
- Tramèr, F. et al. (2016) 'Stealing machine learning models via prediction APIs', *USENIX Security Symposium*, pp. 601–618.
- Zhou, Y. et al. (2019) 'Side-channel attacks in edge computing: Threats and defenses', *IEEE Internet of Things Journal*, 6(3), pp. 4729–4742.
- Giordani, M., Polese, M., Mezzavilla, M., Rangan, S. & Zorzi, M. (2020) 'Toward 6G networks: Use cases and technologies', *IEEE Communications Magazine*, 58(3), pp. 55–61.
- Indiveri, G. & Liu, S.-C. (2015) 'Memory and information processing in neuromorphic systems', *Proceedings of the IEEE*, 103(8), pp. 1379–1397.
- Kairouz, P. et al. (2021) 'Advances and open problems in federated learning', *Foundations and Trends in Machine Learning*, 14(1), pp. 1–210.
- Liu, L. et al. (2020) 'Edge computing for autonomous driving: Opportunities and challenges', *Proceedings of the IEEE*, 108(2), pp. 242–260.
- Mao, Y. et al. (2017) 'A survey on mobile edge computing: The communication perspective', *IEEE Communications Surveys & Tutorials*, 19(4), pp. 2322–2358.
- Nguyen, T.T. et al. (2021) 'Blockchain for 5G and beyond networks: A state of the art survey', *Journal of Network and Computer Applications*, 190, 103–128.
- Pirandola, S. et al. (2020) 'Advances in quantum cryptography', *Advances in Optics and Photonics*, 12(4), pp. 1012–1236.
- Roman, R., Lopez, J. & Mambo, M. (2018) 'Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges', *Future Generation Computer Systems*, 78, pp. 680–698.
- Shi, W. et al. (2016) 'Edge computing: Vision and challenges', *IEEE Internet of Things Journal*, 3(5), pp. 637–646.
- Strinati, E.C. et al. (2021) '6G: The next frontier', *IEEE Vehicular Technology Magazine*, 16(3), pp. 38–47.

- Sun, Y. et al. (2019) ‘Application of machine learning in wireless networks: Key techniques and open issues’, *IEEE Communications Surveys & Tutorials*, 21(4), pp. 3072–3108.
- Zhang, Z. et al. (2019) ‘6G wireless networks: Vision, requirements, architecture, and key technologies’, *IEEE Vehicular Technology Magazine*, 14(3), pp. 28–41.
- Khan, L.U., Yaqoob, I., Tran, N.H., Kazmi, S.M.A., Dang, T.N. and Hong, C.S. (2019) ‘Edge-Computing-Enabled Smart Cities: A Comprehensive Survey’, *arXiv preprint arXiv:1909.08747*. Available at: https://arxiv.org/abs/1909.08747 (Accessed: 22 May 2026).
- Abbas, N., Zhang, Y., Taherkordi, A. and Skeie, T. (2018) ‘Mobile Edge Computing: A Survey’, *IEEE Internet of Things Journal*, 5(1), pp. 450–465. Available at: https://doi.org/10.1109/JIOT.2017.2750180 (Accessed: 22 May 2026).
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y. (2017) ‘Understanding the Mirai Botnet’, *Proceedings of the 26th USENIX Security Symposium*, pp. 1093–1110. Available at: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (Accessed: 22 May 2026).
- Li, T., Sahu, A.K., Talwalkar, A. and Smith, V. (2020) ‘Federated learning: Challenges, methods, and future directions’, *IEEE Signal Processing Magazine*, 37(3), pp. 50–60. Available at: https://doi.org/10.1109/MSP.2020.2975749 (Accessed: 22 May 2026).
- Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) *Zero Trust Architecture (NIST Special Publication 800-207)*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-207 (Accessed: 22 May 2026).
- Sharma, R., Popli, S., Singh, D., & Nain, P. K. (2024). *A Survey on Smart Cities Enabled by 6G and Edge Computing.* Available at: https://www.researchgate.net/publication/383196392
- Li, T., Sahu, A.K., Talwalkar, A. and Smith, V. (2020) ‘Federated Learning: Challenges, Methods, and Future Directions’, *IEEE Signal Processing Magazine*, 37(3), pp. 50–60. Available at: https://doi.org/10.1109/MSP.2020.2975749 (Accessed: 22 May 2026).
- Jiang, W., Han, B., Habibi, M.A. and Schotten, H.D. (2021) ‘The road towards 6G: A comprehensive survey’, *IEEE Open Journal of the Communications Society*, 2, pp.

334–366. Available at: https://doi.org/10.1109/OJCOMS.2021.3057679 (Accessed: 22 May 2026).

- Al-Ansi, A., Al-Ansi, A.M., Muthanna, A., Elgendy, I.A. and Koucheryavy, A. (2021) ‘Survey on Intelligence Edge Computing in 6G: Characteristics, Challenges, Potential Use Cases, and Market Drivers’, *Future Internet*, 13(5), p. 118. Available at: https://doi.org/10.3390/fi13050118 (Accessed: 22 May 2026).

- Blanchard, P., El Mhamdi, E.M., Guerraoui, R. and Stainer, J. (2017) ‘Machine learning with adversaries: Byzantine tolerant gradient descent’, *Advances in Neural Information Processing Systems (NeurIPS)*, 30, pp. 119–129. Available at: https://proceedings.neurips.cc/paper/2017/hash/f4b9ec30ad9f68f89b29639786cb62ef-Abstract.html (Accessed: 22 May 2026).

- Tataria, H., Shafi, M., Molisch, A.F., Dohler, M., Sjöland, H. and Tufvesson, F. (2021) ‘6G wireless systems: Vision, requirements, challenges, insights, and opportunities’, *Proceedings of the IEEE*, 109(7), pp. 1166–1199. Available at: https://doi.org/10.1109/JPROC.2021.3061701 (Accessed: 22 May 2026).

- Basar, E., Di Renzo, M., De Rosny, J., Debbah, M., Alouini, M.S. and Zhang, R. (2019) ‘Wireless communications through reconfigurable intelligent surfaces’, *IEEE Access*, 7, pp. 116753–116773. Available at: https://doi.org/10.1109/ACCESS.2019.2935192 (Accessed: 22 May 2026)

- Larsson, E.G., Edfors, O., Tufvesson, F. and Marzetta, T.L. (2014) ‘Massive MIMO for next generation wireless systems’, *IEEE Communications Magazine*, 52(2), pp. 186–195. Available at: https://doi.org/10.1109/MCOM.2014.6736761 (Accessed: 22 May 2026).

- Weiß, C. (2011) ‘V2X communication in Europe – From research projects to standardization and field tests’, *Computer Networks*, 55(14), pp. 3103–3119. Available at: https://doi.org/10.1016/j.comnet.2011.03.016 (Accessed: 22 May 2026).

- Akyildiz, I.F., Han, C., Hu, Z., Nie, S. and Jornet, J.M. (2022) ‘Terahertz Band Communication: An Old Problem Revisited and Research Directions for the Next Decade’, *IEEE Transactions on Communications*, 70(6), pp. 4250–4285. Available at: https://doi.org/10.1109/TCOMM.2022.3171800 (Accessed: 22 May 2026).

- Bajic, B., Cosic, I., Katalinic, B., Moraca, S., Lazarevic, M. and Rikalovic, A. (2019) ‘Edge Computing vs. Cloud Computing: Challenges and Opportunities in Industry 4.0’, in Katalinic, B. (ed.) *Proceedings of the 30th DAAAM International Symposium on Intelligent Manufacturing and Automation*. Vienna: DAAAM International, pp. 864–871. Available at: https://doi.org/10.2507/30th.daaam.proceedings.120 (Accessed: 22 May 2026).

- Varghese, B. and Buyya, R. (2018) ‘Next generation cloud computing: New trends and research directions’, *Future Generation Computer Systems*, 79, pp. 849–861. Available at: https://doi.org/10.1016/j.future.2017.09.020 (Accessed: 22 May 2026).

- Manis, O. (2022) *Digital Transformation at Titan Group*. Smart Factory Conference 2022. TITAN Cement Company S.A. Available at: https://presentations.boussiasevents.gr/files/_boussias_conferences_content/presentations/smart_factory/2022/Manis_SmartFactory2022.pdf (Accessed: 22 May 2026).

- Khan, L.U., Yaqoob, I., Tran, N.H., Kazmi, S.M.A., Dang, T.N. and Hong, C.S. (2019) ‘Edge-Computing-Enabled Smart Cities: A Comprehensive Survey’, *arXiv preprint arXiv:1909.08747*. Available at: https://arxiv.org/abs/1909.08747 (Accessed: 22 May 2026).

- Tian, Z., Cui, L., Liang, J., & Yu, S. (2022). *A comprehensive survey on poisoning attacks and countermeasures in machine learning*. ACM Computing Surveys, 55(8), Article 166, 1–35. https://doi.org/10.1145/3551636