Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ :"Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών
(MSc in Climate Crisis and Information and Communication Technologies)"

«Κυβερνοασφάλεια και Προστασία Δεδομένων σε Smart Grids: Προοπτικές και Προκλήσεις στην Εποχή των 6G Δικτύων»

Ονοματεπώνυμο: Κωνσταντίνα – Θεοδώρα Πανάγου

Α.Μ.: MKK2412

Επιβλέπων καθηγητής :

Γκρίτζαλης Στέφανος

Συνεπιβλέπων καθηγητής :

Μανιάτης Ιωάννης

Μεταπτυχιακή Διπλωματική Εργασία

Πειραιάς,2026

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας, αισθάνομαι την ανάγκη να ευχαριστήσω δημόσια τους ανθρώπους που συνέβαλαν, ο καθένας με τον δικό του τρόπο, στην πραγμάτωση αυτού του στόχου. Αρχικά, ευχαριστώ θερμά τους καθηγητές μου τον κύριο Γκρίτζαλη Στέφανο και τον κύριο Μανιάτη Ιωάννη για την επιστημονική τους κατάρτιση και την αρωγή τους, η οποία υπήρξε καθοριστική για την εξέλιξη της έρευνάς μου.

Ένα μεγάλο ευχαριστώ ανήκει στους γονείς μου. Η παρουσία τους ως το απόλυτο στήριγμα στη ζωή μου, η αδιάκοπη ενθάρρυνση και οι θυσίες τους, ήταν τα θεμέλια πάνω στα οποία στηρίχθηκα για να ολοκληρώσω τις σπουδές μου. Η αγάπη τους είναι η δύναμη που με ωθεί να εξελίσσομαι συνεχώς.

Το πιο βαθύ και ειλικρινές «ευχαριστώ», όμως, το χρωστάω στον παππού μου. Είναι ο άνθρωπος που μου εμφύσησε τις αξίες και τα ιδανικά που με ορίζουν. Από εκείνον έμαθα τι σημαίνει να είσαι αγωνιστής: με δίδαξε να αντιμετωπίζω κάθε δυσκολία με σθένος και να μην εγκαταλείπω ποτέ τις μάχες της ζωής. Τον αγαπώ βαθιά και του αφιερώνω αυτή την προσπάθεια, ως ελάχιστο φόρο τιμής για όλα όσα μου έχει προσφέρει.

Περίληψη

Η παρούσα εργασία εξετάζει το κρίσιμο ζήτημα της κυβερνοασφάλειας και της προστασίας των δεδομένων στα Έξυπνα Δίκτυα (Smart Grids), εστιάζοντας στις προκλήσεις και τις προοπτικές που αναδύονται με την έλευση των δικτύων 6G. Η μετάβαση προς ένα πιο ψηφιοποιημένο και αποκεντρωμένο ενεργειακό μοντέλο, αν και προσφέρει σημαντικά οφέλη στην ενεργειακή απόδοση και τη διαχείριση των πόρων, εισάγει ταυτόχρονα νέες ευπάθειες. Η ευρεία χρήση συσκευών IoT και έξυπνων μετρητών διευρύνει την επιφάνεια επίθεσης, καθιστώντας τις κρίσιμες υποδομές ευάλωτες σε κακόβουλες ενέργειες, όπως οι επιθέσεις εισαγωγής ψευδών δεδομένων (FDIA) και τα δίκτυα botnet.

Στο πλαίσιο αυτό, η μελέτη αναλύει προηγμένες τεχνολογικές λύσεις για τη θωράκιση του δικτύου. Εξετάζεται ο ρόλος της τεχνολογίας Blockchain και των αλγορίθμων συναίνεσης (όπως ο PBFT) στη διασφάλιση της ακεραιότητας των ενεργειακών συναλλαγών σε microgrids. Ιδιαίτερη έμφαση δίνεται στις τεχνικές ομομορφικής κρυπτογράφησης (PHE και TFHE), οι οποίες επιτρέπουν την ανάλυση

δεδομένων κατανάλωσης και την ανίχνευση ανωμαλιών χωρίς να παραβιάζεται η ιδιωτικότητα των χρηστών.

Επιπλέον, η εργασία διερευνά τη συμβολή της Τεχνητής Νοημοσύνης (AI) και του Edge Intelligence στην ανάπτυξη μηχανισμών προληπτικής ασφάλειας και ανθεκτικότητας. Μέσω της βιβλιογραφικής ανασκόπησης σύγχρονων ερευνητικών δεδομένων, αναδεικνύεται η ανάγκη για μετάβαση σε κβαντικά ασφαλείς λύσεις (quantum-safe solutions) και την υιοθέτηση αρχιτεκτονικών «Μηδενικής Εμπιστοσύνης» (Zero Trust). Συμπερασματικά, η εργασία υπογραμμίζει ότι η ασφάλεια των Smart Grids απαιτεί μια ολιστική προσέγγιση, η οποία θα συνδυάζει την τεχνολογική καινοτομία με αυστηρά διεθνή πρότυπα και πολιτικές προστασίας, διασφαλίζοντας τη σταθερότητα και την εμπιστοσύνη στο ενεργειακό σύστημα του μέλλοντος.

Λέξεις-κλειδιά: *Smart Grids, Κυβερνοασφάλεια, Δίκτυα 6G, Blockchain, Ομομορφική Κρυπτογράφηση, Ιδιωτικότητα Δεδομένων, Τεχνητή Νοημοσύνη.*

Abstract

This paper examines the critical issue of cybersecurity and data protection in Smart Grids, focusing on the challenges and prospects emerging with the advent of 6G networks. The transition towards a more digitized and decentralized energy model, while offering significant benefits in energy efficiency and resource management, simultaneously introduces new vulnerabilities. The widespread use of IoT devices and smart meters expands the attack surface, making critical infrastructure susceptible to malicious activities, such as False Data Injection Attacks (FDIA) and botnet networks.

In this context, the study analyzes advanced technological solutions for network hardening. The role of Blockchain technology and consensus algorithms (such as PBFT) in ensuring the integrity of energy transactions in microgrids is examined. Particular emphasis is placed on homomorphic encryption techniques (PHE and TFHE), which allow for the analysis of consumption data and anomaly detection without compromising user privacy.

Furthermore, the paper explores the contribution of Artificial Intelligence (AI) and Edge Intelligence in developing proactive security and resilience mechanisms. Through a literature review of modern research data, the need for transitioning to

quantum-safe solutions and the adoption of "Zero Trust" architectures is highlighted. In conclusion, the paper emphasizes that Smart Grid security requires a holistic approach, combining technological innovation with strict international standards and protection policies, ensuring stability and trust in the energy system of the future.

Keywords: *Smart Grids, Cybersecurity, 6G Networks, Blockchain, Homomorphic Encryption, Data Privacy, Artificial Intelligence.*

Περιεχόμενα

Πίνακας περιεχομένων εικόνων:

Κεφάλαιο 1: Εισαγωγή

Η ραγδαία εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών έχει οδηγήσει στον ριζικό μετασχηματισμό των παραδοσιακών ηλεκτρικών δικτύων σε «Έξυπνα Δίκτυα» (Smart Grids). Η μετάβαση αυτή δεν αποτελεί απλώς μια τεχνολογική αναβάθμιση, αλλά μια κρίσιμη αλλαγή παραδείγματος που επιτρέπει την αμφίδρομη ροή πληροφορίας και ενέργειας, τη δυναμική ενσωμάτωση ανανεώσιμων πηγών και την ενεργή συμμετοχή των καταναλωτών μέσω έξυπνων μετρητών. Στην εποχή της ψηφιοποίησης, τα Smart Grids αποτελούν τη ραχοκοκαλιά των σύγχρονων κοινωνιών, προσφέροντας βελτιωμένη ενεργειακή απόδοση, αξιοπιστία και βιωσιμότητα.

Ωστόσο, η αυξανόμενη πολυπλοκότητα αυτών των συστημάτων, η οποία εντείνεται από τη μαζική υιοθέτηση συσκευών Internet of Things (IoT) και την επικείμενη έλευση των δικτύων 6G, διευρύνει σημαντικά την επιφάνεια επίθεσης. Η διασύνδεση κρίσιμων υποδομών με το δημόσιο διαδίκτυο καθιστά τα ενεργειακά δίκτυα ευάλωτα σε εξελιγμένες κυβερνοαπειλές, όπως οι επιθέσεις έγχυσης ψευδών δεδομένων (FDIA), οι επιθέσεις άρνησης υπηρεσίας (DDoS) και η κατασκοπεία δεδομένων. Η διασφάλιση της κυβερνοασφάλειας και η προστασία της ιδιωτικότητας των καταναλωτών δεν αποτελούν πλέον προαιρετικά χαρακτηριστικά, αλλά θεμελιώδεις προϋποθέσεις για τη σταθερότητα και την κοινωνική αποδοχή των έξυπνων υποδομών.

Στο πλαίσιο των δικτύων επόμενης γενιάς (6G), οι προκλήσεις γίνονται ακόμη πιο σύνθετες. Ενώ το 6G υπόσχεται σχεδόν μηδενική καθυστέρηση και τεράστιο εύρος ζώνης, εισάγει επίσης νέες παραμέτρους επικινδυνότητας λόγω της ακραίας αποκέντρωσης και της ευρείας χρήσης ευφυΐας στο άκρο του δικτύου (edge intelligence). Η ανάγκη για προηγμένους μηχανισμούς προστασίας, όπως η ομομορφική κρυπτογράφηση, οι αρχιτεκτονικές μηδενικής εμπιστοσύνης (Zero Trust) και η τεχνολογία Blockchain, καθίσταται επιτακτική για την αντιμετώπιση απειλών που εξελίσσονται με ταχύτητες πέρα από τις δυνατότητες των παραδοσιακών συστημάτων ασφαλείας.

Η παρούσα εργασία εξετάζει διεξοδικά το τοπίο της κυβερνοασφάλειας στα Smart Grids, αναλύοντας τις σύγχρονες απειλές και τις τεχνολογίες αιχμής που

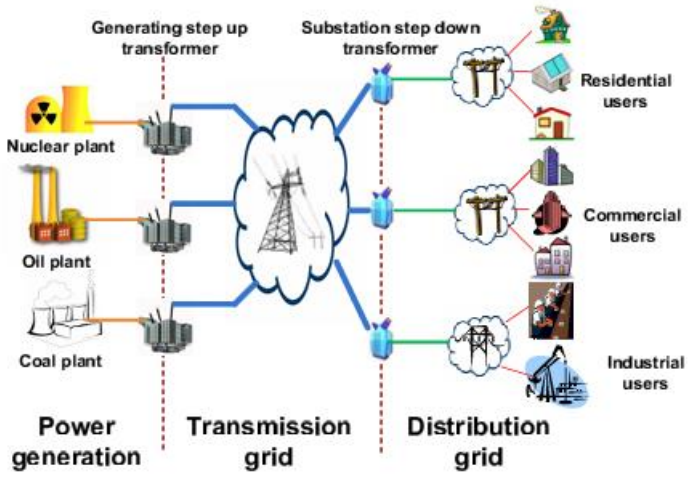
επιστρατεύονται για την αντιμετώπισή τους. Ιδιαίτερη έμφαση δίνεται στην προστασία των προσωπικών δεδομένων και στις προοπτικές που ανοίγονται με την ενσωμάτωση του 6G, προσφέροντας μια ολιστική προσέγγιση που συνδέει την τεχνική αρτιότητα με την επιχειρησιακή συνέχεια και την ασφάλεια του πολίτη. Στόχος είναι η ανάδειξη των βέλτιστων στρατηγικών που θα επιτρέψουν τη δημιουργία ενός ανθεκτικού, ασφαλούς και ιδιωτικού ενεργειακού μέλλοντος.

1.1. Αντικείμενο και σημασία

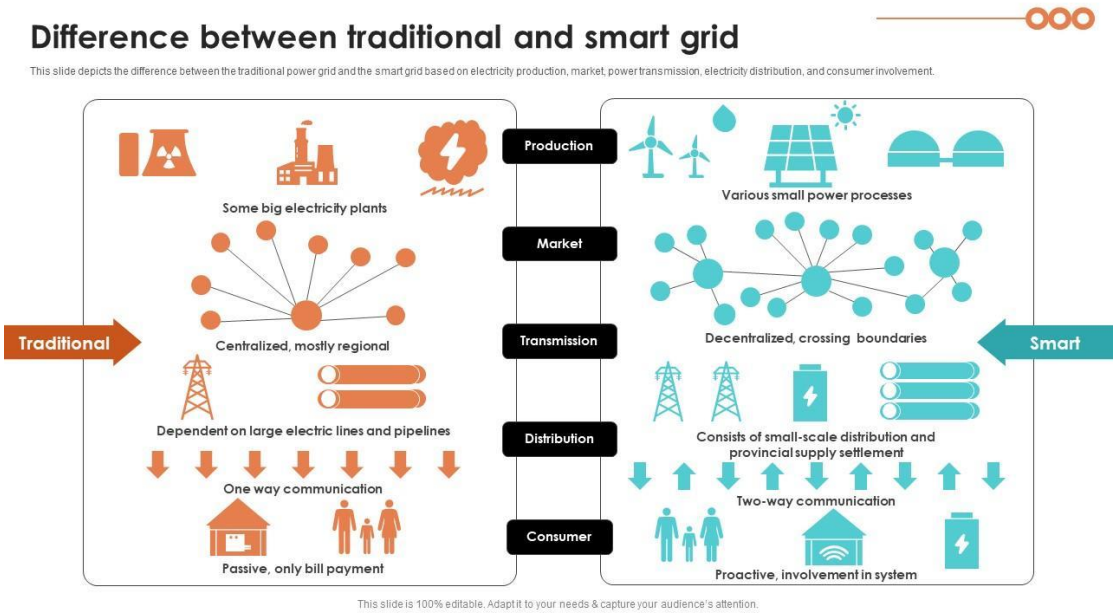
1.1.1. **Ορισμός Smart Grids:** βασικά χαρακτηριστικά, διαφορές από συμβατικά δίκτυα, λειτουργία

Το Έξυπνο Δίκτυο (Smart Grid) ορίζεται ως η επόμενη γενιά των συστημάτων ηλεκτρικής ενέργειας, η οποία χρησιμοποιεί αμφίδρομες ροές ηλεκτρισμού και πληροφοριών για τη δημιουργία ενός ευρέως διεσπαρμένου και αυτοματοποιημένου δικτύου παράδοσης ενέργειας (Fang et al., 2012). Σύμφωνα με τον Wissner (2011), ο όρος αυτός περιγράφει την αναβάθμιση και τον εκσυγχρονισμό του υπάρχοντος συστήματος μέσω της ενσωμάτωσης των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ICT), επιτρέποντας την έξυπνη ενσωμάτωση των ενεργειών όλων των χρηστών που είναι συνδεδεμένοι σε αυτό,παραγωγών, καταναλωτών και εκείνων που εκτελούν και τους δύο ρόλους ταυτόχρονα.

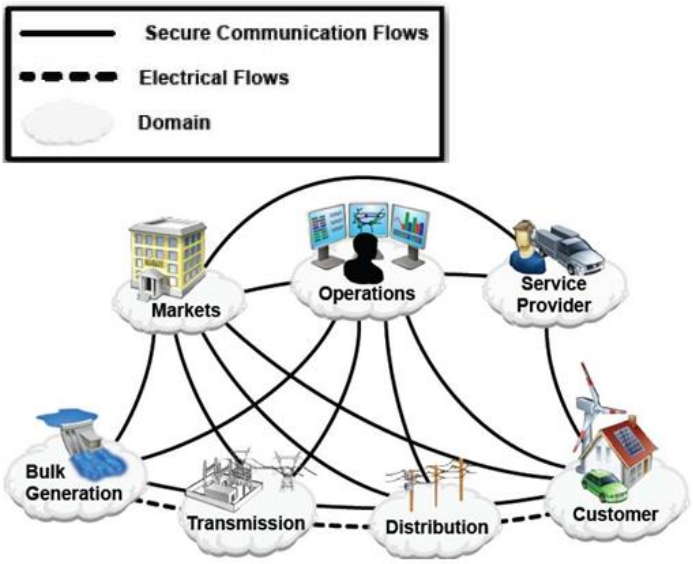
Η κύρια διαφορά ανάμεσα στα συμβατικά και τα έξυπνα δίκτυα εντοπίζεται στον τρόπο με τον οποίο διακινείται η ενέργεια και η πληροφορία. Ενώ τα παραδοσιακά δίκτυα χαρακτηρίζονται από μια κεντρική και μονόδρομη ροή από τους μεγάλους σταθμούς παραγωγής προς τους παθητικούς καταναλωτές, το έξυπνο δίκτυο εισάγει μια αλληλεπιδραστική σχέση όπου η πληροφορία ρέει παράλληλα με την ηλεκτρική ενέργεια (Fang et al., 2012). Αυτή η αλλαγή επιτρέπει στο δίκτυο να μην είναι πλέον μια άκαμπτη υποδομή, αλλά ένα δυναμικό σύστημα που μπορεί να παρακολουθείται και να ελέγχεται σε πραγματικό χρόνο.



Εικόνα 1:Ένα παράδειγμα του παραδοσιακού δικτύου ηλεκτρικής ενέργειας (Πηγή:Fang et al., 2012).



Εικόνα 2:Διαφορές παραδοσιακού με smart grid (Πηγή: SlideGeeks, n.d)



Εικόνα 3:Το εννοιολογικό μοντέλο αναφοράς του έξυπνου δικτύου σύμφωνα με το NIST(National Institute of Standards and Technology - Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ) (Πηγή: Fang et al., 2012).

Επιπλέον, η δομή των έξυπνων δικτύων διευκολύνει τη μετάβαση από το μοντέλο της κεντρικής παραγωγής προς τη Διεσπαρμένη Παραγωγή (Distributed Generation). Όπως επισημαίνει ο Wissner (2011), τα συμβατικά δίκτυα αντιμετωπίζουν σοβαρές δυσκολίες στην ενσωμάτωση πτητικών ανανεώσιμων πηγών ενέργειας (ΑΠΕ), όπως η αιολική και η ηλιακή, λόγω της έλλειψης ευελιξίας τους. Το έξυπνο δίκτυο, ωστόσο, προσφέρει τις απαραίτητες δυνατότητες παρακολούθησης για να εξισορροπεί την παραγωγή από ΑΠΕ με τη ζήτηση, διασφαλίζοντας τη σταθερότητα του συστήματος (Wissner, 2011).

Λειτουργικά, το έξυπνο δίκτυο οργανώνεται σε τρία κρίσιμα συστήματα: το έξυπνο σύστημα υποδομής, το σύστημα διαχείρισης και το σύστημα προστασίας (Fang et al., 2012). Το σύστημα υποδομής περιλαμβάνει τα υποσυστήματα ενέργειας, πληροφοριών και επικοινωνιών, τα οποία αποτελούν τη βάση για όλες τις προηγμένες λειτουργίες. Αυτή η πολυεπίπεδη αρχιτεκτονική επιτρέπει τη μετατροπή των φυσικών γραμμών μεταφοράς σε ένα «έξυπνο» δίκτυο που μπορεί να αναλύει δεδομένα και να λαμβάνει αποφάσεις αυτόνομα (Fang et al., 2012).

Σημαντικό ρόλο στη νέα αυτή λειτουργία παίζει η Προηγμένη Υποδομή Μέτρησης (Advanced Metering Infrastructure - AMI), η οποία επιτρέπει τη συλλογή δεδομένων κατανάλωσης σε πολύ μικρά χρονικά διαστήματα. Σύμφωνα με τους Fang et al.

(2012), οι έξυπνοι μετρητές αποτελούν το βασικό εργαλείο αλληλεπίδρασης, δίνοντας στους καταναλωτές τη δυνατότητα να έχουν πλήρη επίγνωση της χρήσης ενέργειας. Αυτό οδηγεί στην εφαρμογή προγραμμάτων «απόκρισης ζήτησης» (demand response), όπου η κατανάλωση μετατοπίζεται από τις ώρες αιχμής σε ώρες χαμηλότερου κόστους, βελτιστοποιώντας τη χρήση των πόρων.

Ένα ακόμη βασικό χαρακτηριστικό που διαφοροποιεί το έξυπνο δίκτυο είναι η ικανότητα «αυτοΐασης» (self-healing) και η ενισχυμένη αξιοπιστία του. Ενώ στα παλαιότερα συστήματα η αποκατάσταση βλαβών βασιζόταν σε χειροκίνητες διαδικασίες και είχε περιορισμένη επίγνωση της κατάστασης, τα έξυπνα δίκτυα χρησιμοποιούν αυτοματοποιημένο έλεγχο και προηγμένους αλγόριθμους για την αυτόματη ανίχνευση και απομόνωση σφαλμάτων (Wissner, 2011). Αυτή η ικανότητα μειώνει σημαντικά τη διάρκεια των διακοπών ρεύματος και προστατεύει το δίκτυο από εκτεταμένες καταρρεύσεις (blackouts).

Παράλληλα, το έξυπνο σύστημα διαχείρισης στοχεύει στη βελτίωση της ενεργειακής απόδοσης και στη μείωση του λειτουργικού κόστους. Όπως αναλύουν οι Fang et al. (2012), μέσω της χρήσης τεχνολογιών επικοινωνίας και ανάλυσης δεδομένων, οι πάροχοι μπορούν να προβλέπουν τη ζήτηση με μεγαλύτερη ακρίβεια και να διαχειρίζονται τα φορτία πιο αποτελεσματικά. Αυτό επιτυγχάνεται με τη χρήση μεθόδων όπως η δυναμική τιμολόγηση, η οποία ευθυγραμμίζει τα οικονομικά κίνητρα των χρηστών με τις τεχνικές ανάγκες του δικτύου (Fang et al., 2012).

Συμπερασματικά, η μετάβαση στο έξυπνο δίκτυο αποτελεί τον ακρογωνιαίο λίθο για ένα βιώσιμο ενεργειακό μέλλον, συμφιλιώνοντας την ασφάλεια εφοδιασμού με την περιβαλλοντική προστασία. Σύμφωνα με τον Wissner (2011), ο μετασχηματισμός αυτός μέσω των τεχνολογιών ICT είναι απαραίτητος για τον εκσυγχρονισμό των αγορών ηλεκτρικής ενέργειας και την υποστήριξη της πράσινης ανάπτυξης. Το έξυπνο δίκτυο δεν είναι απλώς μια τεχνική βελτίωση, αλλά μια ριζική αλλαγή παραδείγματος που μετατρέπει τους παθητικούς καταναλωτές σε ενεργούς συμμετέχοντες (Wissner, 2011).

1.1.2. **Σχέση με ψηφιοποίηση και IoT:** ενσωμάτωση αισθητήρων, IoT συσκευών, διαχείριση ενεργειακών δεδομένων

Στη σύγχρονη εποχή, ο τομέας της ενέργειας βιώνει έναν ριζικό μετασχηματισμό που καθοδηγείται από την ψηφιοποίηση, η οποία επιτρέπει τη χρήση προηγμένων δεδομένων για την ενίσχυση της αποδοτικότητας και της ανθεκτικότητας των υποδομών (Kharbouch et al., 2025). Η ψηφιοποίηση δεν αποτελεί απλώς μια τεχνική αναβάθμιση, αλλά τη βάση για τη μετάβαση από τα παραδοσιακά δίκτυα στα Έξυπνα Δίκτυα (Smart Grids), όπου η πληροφορία ρέει αμφίδρομα μεταξύ παραγωγού και καταναλωτή (Eltamaly & Elghaffar, 2021).

Κεντρικό ρόλο σε αυτή τη διαδικασία παίζει το Διαδίκτυο των Πραγμάτων (IoT), το οποίο μέσω ενός εκτεταμένου δικτύου αισθητήρων επιτρέπει τη συλλογή δεδομένων σε πραγματικό χρόνο από κάθε σημείο του δικτύου (Kharbouch et al., 2025). Η ενσωμάτωση των τεχνολογιών πληροφορικής και επικοινωνιών είναι απαραίτητη για τον εκσυγχρονισμό του ηλεκτρικού δικτύου, καθώς επιτρέπει τη βελτίωση της παροχής ισχύος και την καθιστά πιο φιλική προς το περιβάλλον (Eltamaly & Elghaffar, 2021).

Η υλοποίηση αυτών των τεχνολογιών βασίζεται στην εγκατάσταση συσκευών IoT και έξυπνων μετρητών, οι οποίοι αποτελούν τα δομικά στοιχεία για την παραγωγή και επεξεργασία πληροφοριών (Kharbouch et al., 2025). Οι έξυπνοι μετρητές παρέχουν στους καταναλωτές καλύτερες επιλογές παροχής και πληροφόρησης, επιτρέποντάς τους να διαδραματίζουν ενεργό ρόλο στη βελτιστοποίηση της λειτουργίας του συστήματος (Eltamaly & Elghaffar, 2021).

Μέσω της Προηγμένης Υποδομής Μέτρησης (Advanced Metering Infrastructure - AMI), η διαχείριση των ενεργειακών δεδομένων γίνεται πιο ακριβής, επιτρέποντας την άμεση ανίχνευση διακοπών και την απομόνωση σφαλμάτων (Kharbouch et al., 2025). Αυτή η συνεχή ροή δεδομένων υποστηρίζει τη Διαχείριση Πλευράς Ζήτησης (Demand Side Management-DSM), δίνοντας κίνητρα στους καταναλωτές να αναθεωρήσουν τα πρότυπα κατανάλωσής τους για τη βελτίωση της συνολικής απόδοσης (Eltamaly & Elghaffar, 2021).

Η ενσωμάτωση αισθητήρων επιτρέπει επίσης τη δημιουργία Ψηφιακών Διδύμων (Digital Twins), τα οποία αποτελούν εικονικές αναπαραστάσεις των φυσικών συστημάτων για την παρακολούθηση και προσομοίωση της λειτουργίας τους σε πραγματικό χρόνο (Kharbouch et al., 2025). Η χρήση τέτοιων ψηφιακών μοντέλων,

σε συνδυασμό με έξυπνες συσκευές, διευκολύνει τον έλεγχο του εξοπλισμού και την αυτοματοποίηση των υποσταθμών και των γραμμών διανομής (Eltamaly & Elghaffar, 2021).

Επιπλέον, η έλευση των δικτύων 6G υπόσχεται υπερ-αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης, οι οποίες είναι κρίσιμες για τη μεταφορά του τεράστιου όγκου δεδομένων που παράγουν οι αισθητήρες IoT (Kharbouch et al., 2025). Η τεχνολογία αυτή είναι απαραίτητη για την ενσωμάτωση μικροπαραγωγής και συστημάτων αποθήκευσης ενέργειας, τα οποία απαιτούν ακριβή συντονισμό για τη διατήρηση της ισορροπίας του δικτύου (Eltamaly & Elghaffar, 2021).

Η χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης πάνω στα δεδομένα του IoT επιτρέπει την προληπτική συντήρηση και την πρόβλεψη της ζήτησης με υψηλή ακρίβεια (Kharbouch et al., 2025). Αυτό βοηθά στην αντιμετώπιση των περιορισμών του συστήματος ισχύος, καθώς οι πάροχοι μπορούν να προσαρμόζουν τη λειτουργία τους βάσει των πληροφοριών που λαμβάνουν για τις τιμές και τη χρήση ενέργειας (Eltamaly & Elghaffar, 2021).

Ωστόσο, η εκτεταμένη ψηφιοποίηση και η σύνδεση δισεκατομμυρίων συσκευών IoT ενέχει κινδύνους για την κυβερνοασφάλεια και την προστασία των προσωπικών δεδομένων των χρηστών (Kharbouch et al., 2025). Παρά τις προκλήσεις, η εφαρμογή έξυπνων τεχνολογιών σε κτίρια και οικιακούς αυτοματισμούς παραμένει ο βασικός πυλώνας για την επίτευξη ενός πιο πράσινου και βιώσιμου ενεργειακού μέλλοντος (Eltamaly & Elghaffar, 2021).

Συμπερασματικά, η συνέργεια μεταξύ IoT, αισθητήρων και ψηφιακών διδύμων αναβαθμίζει το δίκτυο σε ένα ευφυές οικοσύστημα που μπορεί να αυτο-θεραπεύεται και να βελτιστοποιείται δυναμικά (Kharbouch et al., 2025). Η σημασία αυτής της ενσωμάτωσης έγκειται στην ικανότητά της να μετατρέπει τα ακατέργαστα δεδομένα σε αξιοποιήσιμη γνώση, διασφαλίζοντας την ενεργειακή ασφάλεια και την αποδοτικότητα (Eltamaly & Elghaffar, 2021).

1.1.3. Σημασία κυβερνοασφάλειας και προστασίας δεδομένων

Η μετάβαση από τα παραδοσιακά δίκτυα ηλεκτρικής ενέργειας προς τα Έξυπνα Δίκτυα (Smart Grids) αποτελεί μία από τις πιο κρίσιμες εφαρμογές του κυβερνοφυσικού Διαδικτύου των Πραγμάτων (IoT). Αυτή η εξέλιξη βασίζεται στην ενσωμάτωση τεχνολογιών πληροφορικής και επικοινωνιών στην υπάρχουσα υποδομή, επιτρέποντας την αμφίδρομη ροή ενέργειας και δεδομένων (Alomari et al., 2025). Ωστόσο, η εκτεταμένη χρήση αισθητήρων και έξυπνων συσκευών, ενώ βελτιώνει την αποδοτικότητα, διευρύνει σημαντικά την επιφάνεια επίθεσης, καθιστώντας την κυβερνοασφάλεια τον μεγαλύτερο σύγχρονο προκλητικό παράγοντα για τον ενεργειακό τομέα (Unsal et al., 2021).

Το τοπίο των απειλών στα Έξυπνα Δίκτυα είναι εξαιρετικά σύνθετο, περιλαμβάνοντας επιθέσεις που στοχεύουν στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. Οι απειλές κυμαίνονται από παραδοσιακές επιθέσεις άρνησης εξυπηρέτησης (DoS- Denial of Service) έως εξειδικευμένες επιθέσεις, όπως η έγχυση ψευδών δεδομένων (False Data Injection Attacks - FDIA), οι οποίες στοχεύουν στην παραπλάνηση των συστημάτων ελέγχου (Unsal et al., 2021). Ιδιαίτερα οι επιθέσεις FDIA θεωρούνται από τις πιο επικίνδυνες, καθώς μπορούν να παρακάμψουν τους παραδοσιακούς μηχανισμούς ανίχνευσης σφαλμάτων (Alomari et al., 2025).

Οι επιπτώσεις αυτών των απειλών στις κρίσιμες υποδομές μπορούν να είναι καταστροφικές, οδηγώντας σε εκτεταμένες διακοπές ρεύματος ή ακόμη και φυσική καταστροφή του εξοπλισμού. Χαρακτηριστικό παράδειγμα αποτελεί η επίθεση "Aurora", η οποία απέδειξε ότι ένας εισβολέας μπορεί να προκαλέσει σοβαρή βλάβη σε γεννήτριες μέσω του ελέγχου των διακοπτών (Unsal et al., 2021). Επιπλέον, ιστορικά περιστατικά, όπως η επίθεση στο δίκτυο της Ουκρανίας το 2015, αναδεικνύουν πώς η χρήση κακόβουλου λογισμικού μπορεί να αφήσει εκατοντάδες χιλιάδες καταναλωτές χωρίς παροχή ενέργειας (Alomari et al., 2025).

Πέρα από τις μεγάλες υποδομές, οι καταναλωτές επηρεάζονται άμεσα από την παραβίαση της προστασίας των δεδομένων τους μέσω των έξυπνων μετρητών. Η συλλογή ευαίσθητων πληροφοριών σχετικά με τις καταναλωτικές συνήθειες, αν εκτεθεί, παραβιάζει την ιδιωτικότητα του χρήστη και επιτρέπει την παρακολούθηση

των δραστηριοτήτων εντός της οικίας (Unsal et al., 2021). Επιθέσεις όπως το "sniffing" (παθητική επίθεση όπου ο εισβολέας «ακούει» και καταγράφει τα πακέτα δεδομένων που διακινούνται στο δίκτυο) και το "spoofing" (ενεργή επίθεση όπου ο κυβερνοεγκληματίας προσποιείται ότι είναι μια νόμιμη ή έμπιστη πηγή) σε υποδομές AMI επιτρέπουν σε μη εξουσιοδοτημένους χρήστες να υποκλέπτουν δεδομένα ή να προβαίνουν σε κλοπή ενέργειας, προκαλώντας οικονομικές απώλειες (Alomari et al., 2025).

Η κριτική σημασία της κυβερνοασφάλειας για την αξιοπιστία του δικτύου συνδέεται άρρηκτα με την ικανότητα του συστήματος να λαμβάνει ακριβείς αποφάσεις σε πραγματικό χρόνο.(Unsal et al., 2021). Μια επιτυχής κυβερνοεπίθεση μπορεί να χειραγωγήσει τις εντολές ελέγχου, προκαλώντας αστάθεια στη συχνότητα και την τάση, θέτοντας σε κίνδυνο τη συνολική λειτουργία της ηλεκτρικής υποδομής (Alomari et al., 2025).

Για την ενίσχυση της ανθεκτικότητας, οι νέες κατευθύνσεις στρέφονται προς την ενσωμάτωση της Τεχνητής Νοημοσύνης και του Blockchain. Το Blockchain μπορεί να διασφαλίσει την ακεραιότητα των δεδομένων μέσω αποκεντρωμένων καθολικών, ενώ η Μηχανική Μάθηση προσφέρει προηγμένες δυνατότητες ανίχνευσης ανωμαλιών σε πραγματικό χρόνο (Alomari et al., 2025). Αυτές οι τεχνολογίες επιτρέπουν στο δίκτυο να αναγνωρίζει "ύποπτα" πρότυπα επικοινωνίας και να ενεργοποιεί αυτόματες άμυνες πριν την εκδήλωση μιας σοβαρής βλάβης (Unsal et al., 2021).

Επιπρόσθετα, η χρήση Ψηφιακών Διδύμων (Digital Twins) και προηγμένων εργαλείων προσομοίωσης επιτρέπει την αξιολόγηση της ασφάλειας σε εικονικό περιβάλλον (Alomari et al., 2025). Με αυτόν τον τρόπο, οι διαχειριστές μπορούν να δοκιμάζουν την απόκριση του δικτύου σε σενάρια επιθέσεων FDIA ή DoS χωρίς να διακινδυνεύουν τη φυσική υποδομή (Unsal et al., 2021). Η ικανότητα του δικτύου να παραμένει λειτουργικό ακόμη και υπό συνθήκες επίθεσης (cyber-resilience) αποτελεί πλέον τον κεντρικό στόχο του σχεδιασμού.

Συμπερασματικά, η προστασία των δεδομένων και η κυβερνοασφάλεια δεν είναι απλώς τεχνικές προσθήκες, αλλά θεμελιώδη στοιχεία για την επιβίωση του σύγχρονου ενεργειακού συστήματος. Η εξάρτηση της κοινωνίας από την ηλεκτρική

ενέργεια καθιστά κάθε παραβίαση στο Έξυπνο Δίκτυο ζήτημα εθνικής ασφάλειας (Alomari et al., 2025). Η συνεχής έρευνα για τον εντοπισμό νέων τρωτών σημείων και η ανάπτυξη προσαρμοσμένων λύσεων είναι απαραίτητη για τη διασφάλιση ενός αξιόπιστου και βιώσιμου ψηφιακού μέλλοντος (Unsal et al., 2021).

1.2.Σκοποί και ερευνητικά ερωτήματα

Ο κύριος σκοπός της παρούσας εργασίας είναι η διεξοδική ανάλυση των προκλήσεων κυβερνοασφάλειας και της προστασίας δεδομένων που ανακύπτουν στα Σύγχρονα Έξυπνα Δίκτυα (Smart Grids), με ιδιαίτερη έμφαση στις νέες τεχνολογικές παραδείγματα που εισάγει η εποχή των 6G δικτύων. Η μελέτη στοχεύει στην αξιολόγηση και πρόταση προηγμένων τεχνικών λύσεων που διασφαλίζουν την ακεραιότητα του δικτύου και την ιδιωτικότητα των καταναλωτών σε ένα περιβάλλον αυξανόμενης ψηφιοποίησης και διασυνδεσιμότητας.

Ειδικότερα, η εργασία επιδιώκει να αναδείξει πώς η μετάβαση από κεντρικές σε αποκεντρωμένες αρχιτεκτονικές, σε συνδυασμό με την ευφυΐα στο άκρο του δικτύου (edge intelligence), μπορεί να θωρακίσει τις κρίσιμες ενεργειακές υποδομές AMI και SCADA απέναντι σε εξελιγμένες κυβερνοεπιθέσεις.

Για την επίτευξη του παραπάνω σκοπού, η έρευνα επικεντρώνεται στην απάντηση των ακόλουθων ερευνητικών ερωτημάτων:

1. **Ποιες είναι οι κρίσιμες ευπάθειες** και τα νέα διανύσματα επιθέσεων που προκύπτουν στα Smart Grids από την ενσωμάτωση των δικτύων 6G και των συσκευών IoT;
2. **Με ποιο τρόπο η ομομορφική κρυπτογράφηση** (σχήματα PHE και TFHE) μπορεί να επιτρέψει την ανίχνευση ανωμαλιών και τη συγκέντρωση δεδομένων χωρίς να παραβιάζεται το απόρρητο της κατανάλωσης των χρηστών;
3. **Πώς μπορεί η τεχνολογία Blockchain**, μέσω αλγορίθμων συναίνεσης όπως ο PBFT, να διασφαλίσει την ακεραιότητα των ενεργειακών συναλλαγών και να αποτρέψει την έγχυση ψευδών δεδομένων (FDIA);

4. **Ποιες στρατηγικές πρόληψης και διαχείρισης περιστατικών** (π.χ. Moving Target Defense, Zero Trust) είναι οι πλέον αποτελεσματικές για την αντιμετώπιση επιθέσεων τύπου IoT botnet;
5. **Ποιες είναι οι μελλοντικές προοπτικές** για την ενσωμάτωση της Τεχνητής Νοημοσύνης (AI-based resilience) και την ανάπτυξη κβαντικά ασφαλών (quantum-safe) λύσεων στα δίκτυα επόμενης γενιάς;

1.3 Μεθοδολογία

Η παρούσα εργασία βασίζεται στη μεθοδολογία της δευτερογενούς ποιοτικής έρευνας μέσω της συστηματικής βιβλιογραφικής ανασκόπησης. Στόχος είναι η σύνθεση και η κριτική ανάλυση υφιστάμενων επιστημονικών δεδομένων που αφορούν την κυβερνοασφάλεια στα Έξυπνα Δίκτυα, με έμφαση στις τεχνολογίες αιχμής που αναπτύχθηκαν την τελευταία πενταετία.

Για τη συλλογή του απαραίτητου υλικού πραγματοποιήθηκε εκτενής αναζήτηση σε διεθνείς ακαδημαϊκές βάσεις δεδομένων, όπως οι **IEEE Xplore**, **ScienceDirect**, **SpringerLink** και **Google Scholar**.

Τα κριτήρια επιλογής των πηγών επικεντρώθηκαν στα εξής:

- **Χρονική εγγύτητα:** Δόθηκε προτεραιότητα σε άρθρα που δημοσιεύθηκαν μετά το 2020, προκειμένου να συμπεριληφθούν οι πλέον πρόσφατες εξελίξεις στα δίκτυα 6G και την κβαντική ασφάλεια.
- **Επιστημονική εγκυρότητα:** Επιλέχθηκαν μελέτες από έγκριτα περιοδικά με σύστημα κριτών (peer-reviewed journals) και πρακτικά διεθνών συνεδρίων.
- **Θεματική συνάφεια:** Συμπεριλήφθηκαν πηγές που καλύπτουν τόσο το θεωρητικό πλαίσιο των απειλών όσο και τις πρακτικές λύσεις κρυπτογράφησης και αποκεντρωμένης διαχείρισης.

Η ανάλυση των δεδομένων ακολουθεί μια δομημένη πορεία, ξεκινώντας από την περιγραφή της αρχιτεκτονικής των Smart Grids και των ευπαθειών τους, προχωρώντας στην εξέταση εξειδικευμένων τεχνολογιών προστασίας (Blockchain, Ομομορφική Κρυπτογράφηση) και καταλήγοντας στη διατύπωση στρατηγικών προτάσεων και μελλοντικών ερευνητικών κατευθύνσεων. Η προσέγγιση αυτή

επιτρέπει τη σφαιρική κατανόηση του προβλήματος και την εξαγωγή τεκμηριωμένων συμπερασμάτων για τη θωράκιση των σύγχρονων ενεργειακών υποδομών.

Κεφάλαιο 2: Smart Grids και Ψηφιακός Μετασχηματισμός

2.1. Αρχιτεκτονική και λειτουργικά επίπεδα

Η μετάβαση από το παραδοσιακό ηλεκτρικό δίκτυο στο Έξυπνο Δίκτυο (Smart Grid) αντιπροσωπεύει μια θεμελιώδη αλλαγή παραδείγματος, όπου η φυσική υποδομή ενσωματώνεται πλήρως με προηγμένες τεχνολογίες πληροφορικής και επικοινωνιών. Η αρχιτεκτονική ενός Smart Grid δεν είναι μια απλή μονοδιάστατη δομή, αλλά ένα σύνθετο οικοσύστημα που επιτρέπει την αμφίδρομη ροή τόσο της ενέργειας όσο και της πληροφορίας. Αυτή η πολυεπίπεδη οργάνωση είναι απαραίτητη για τη διαχείριση της πολυπλοκότητας που εισάγουν οι νέες τεχνολογίες και οι απαιτήσεις για ενεργειακή απόδοση (Nafi et al., 2016).

Κεντρικό ρόλο στην τυποποίηση αυτής της δομής παίζει το Μοντέλο Αρχιτεκτονικής Έξυπνου Δικτύου (Smart Grid Architecture Model - SGAM), το οποίο παρέχει ένα ολιστικό πλαίσιο για την οπτικοποίηση των αλληλεπιδράσεων στο δίκτυο. Το SGAM δομείται σε πέντε επίπεδα διαλειτουργότητας: το επιχειρηματικό, το λειτουργικό, το επίπεδο πληροφορίας, το επίπεδο επικοινωνίας και το επίπεδο των φυσικών στοιχείων. Αυτή η προσέγγιση επιτρέπει στους μηχανικούς να σχεδιάζουν συστήματα που είναι διαλειτουργικά, διασφαλίζοντας ότι διαφορετικές συσκευές από διαφορετικούς κατασκευαστές μπορούν να συνεργάζονται αρμονικά (Panda & Das, 2021).

Πέρα από το SGAM, μια άλλη σημαντική προσέγγιση είναι η Πολυεπίπεδη Αρχιτεκτονική Έξυπνου Δικτύου (Layered Smart Grid - LSG), η οποία δίνει έμφαση στην αυτονομία και την ιεραρχική οργάνωση των στοιχείων του δικτύου. Σύμφωνα με αυτή την αρχιτεκτονική, το δίκτυο χωρίζεται σε διακριτά επίπεδα όπως το επίπεδο ισχύος, το επίπεδο ελέγχου και το επίπεδο εφαρμογών. Αυτός ο διαχωρισμός επιτρέπει την ευκολότερη διαχείριση των σφαλμάτων και την αναβάθμιση μεμονωμένων τμημάτων του συστήματος χωρίς να επηρεάζεται η συνολική λειτουργία (Batista et al., 2014).

Το φυσικό επίπεδο ή επίπεδο εξαρτημάτων (Component Layer) αποτελεί τη βάση της αρχιτεκτονικής και περιλαμβάνει όλη την υλική υποδομή, από τις γεννήτριες και τους υποσταθμούς έως τους έξυπνους μετρητές στις κατοικίες. Σε αυτό το επίπεδο, η ενσωμάτωση Διεσπαρμένων Ενεργειακών Πόρων (DER), όπως τα φωτοβολταϊκά και

οι ανεμογεννήτριες, απαιτεί προηγμένους αισθητήρες για την παρακολούθηση της κατάστασης του δικτύου σε πραγματικό χρόνο. Η ακρίβεια των δεδομένων που συλλέγονται εδώ είναι κρίσιμη για όλες τις ανώτερες λειτουργίες (Panda & Das, 2021).

Συνεχίζοντας την ιεραρχία, το επίπεδο επικοινωνίας (Communication Layer) λειτουργεί ως ο συνδετικός κρίκος που μεταφέρει τα δεδομένα από το φυσικό επίπεδο στα συστήματα ελέγχου. Η χρήση τεχνολογιών όπως το ZigBee για τοπικά δίκτυα (HAN/NAN) και το WAN για επικοινωνίες μεγάλων αποστάσεων είναι καθοριστική. Η επιλογή του κατάλληλου πρωτοκόλλου επικοινωνίας επηρεάζει άμεσα την καθυστέρηση (latency) και την αξιοπιστία της μεταφοράς πληροφοριών, στοιχεία απαραίτητα για την απόκριση του δικτύου σε κρίσιμα συμβάντα (Batista et al., 2014).

Πάνω από την επικοινωνία βρίσκεται το επίπεδο πληροφορίας (Information Layer), το οποίο αναλαμβάνει τη σημασιολογική οργάνωση των δεδομένων. Σε αυτό το επίπεδο, τα ακατέργαστα δεδομένα μετατρέπονται σε αξιοποιήσιμη πληροφορία μέσω κοινών μοντέλων πληροφοριών (CIM). Η διαχείριση του τεράστιου όγκου δεδομένων (Big Data) που παράγεται από τα Smart Grids απαιτεί προηγμένες τεχνικές ανάλυσης, ώστε να επιτυγχάνεται ακριβής πρόβλεψη της ζήτησης και βελτιστοποίηση της παραγωγής (Panda & Das, 2021).

Το λειτουργικό επίπεδο (Function Layer) είναι εκεί όπου εκτελούνται οι λογικές διεργασίες και οι εφαρμογές ελέγχου του δικτύου. Εδώ περιλαμβάνονται λειτουργίες όπως η αυτοθεραπεία (self-healing), η διαχείριση της τάσης και ο έλεγχος των μικροδικτύων. Η ικανότητα του δικτύου να αναγνωρίζει αυτόματα ένα σφάλμα και να αναδιατάσσεται για την ελαχιστοποίηση της διακοπής ρεύματος είναι μία από τις πιο σημαντικές λειτουργικές βελτιώσεις σε σχέση με τα παραδοσιακά δίκτυα (Nafi et al., 2016).

Στην κορυφή της πυραμίδας βρίσκεται το επιχειρηματικό επίπεδο (Business Layer), το οποίο διασυνδέει τις λειτουργίες του δικτύου με την αγορά ενέργειας και τις στρατηγικές αποφάσεις. Σε αυτό το επίπεδο λαμβάνονται αποφάσεις για την τιμολόγηση, τη διαχείριση της ζήτησης (Demand Response) και τις επενδύσεις σε νέες υποδομές. Η αρχιτεκτονική πρέπει να υποστηρίζει νέα επιχειρηματικά μοντέλα,

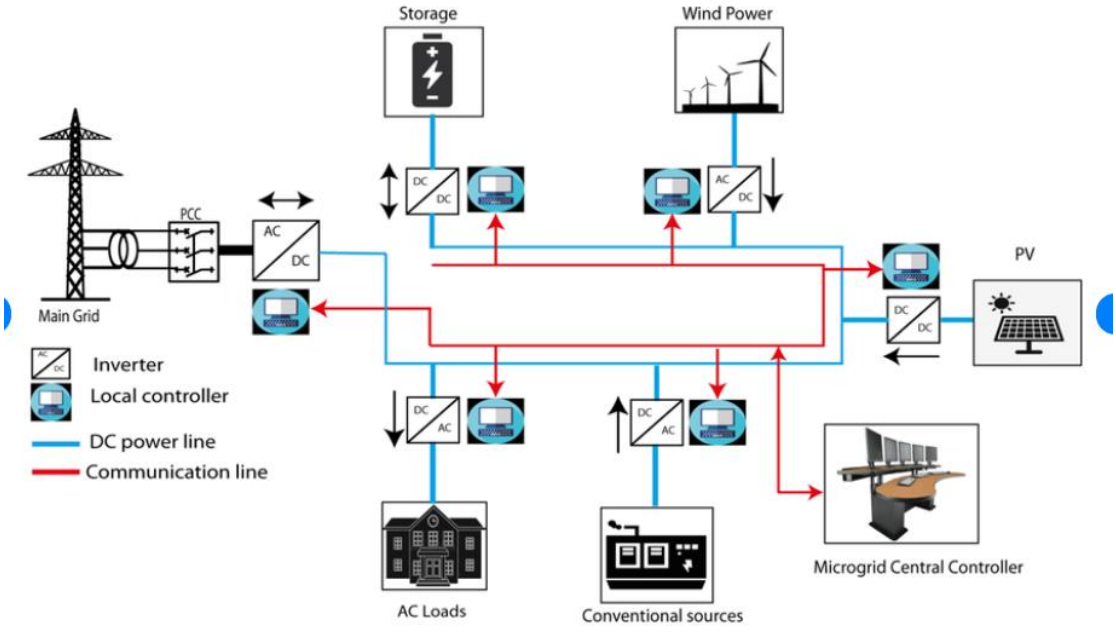
όπου ο καταναλωτής μπορεί να είναι ταυτόχρονα και παραγωγός (prosumer), πουλώντας ενέργεια πίσω στο δίκτυο (Nafi et al., 2016).

Συμπερασματικά, η πολυεπίπεδη αρχιτεκτονική των Smart Grids εξασφαλίζει ότι το σύστημα παραμένει ευέλικτο και ασφαλές απέναντι σε κυβερνοεπιθέσεις και φυσικές καταστροφές. Η στενή συνεργασία μεταξύ των λειτουργικών επιπέδων, από το φυσικό εξάρτημα έως την επιχειρηματική στρατηγική, είναι αυτή που επιτρέπει τον ψηφιακό μετασχηματισμό της ενέργειας. Μόνο μέσω μιας τέτοιας δομημένης αρχιτεκτονικής μπορεί να επιτευχθεί ο στόχος για ένα βιώσιμο και περιβαλλοντικά φιλικό ενεργειακό μέλλον (Panda & Das, 2021).

2.1.1 Κεντρικά vs αποκεντρωμένα συστήματα.

Η παραδοσιακή δομή των ηλεκτρικών δικτύων βασίστηκε επί δεκαετίες σε ένα κεντρικοποιημένο μοντέλο, όπου η παραγωγή ενέργειας συγκεντρώνεται σε μεγάλους σταθμούς και μεταφέρεται μονοδρομικά προς τους τελικούς καταναλωτές. Ωστόσο, ο ψηφιακός μετασχηματισμός και η ανάγκη για ενσωμάτωση ανανεώσιμων πηγών ενέργειας επιβάλλουν την επανεξέταση αυτής της δομής. Η κύρια διαφορά μεταξύ των κεντρικών και των αποκεντρωμένων συστημάτων έγκειται στον τρόπο λήψης αποφάσεων και στη διαχείριση των ενεργειακών πόρων, με τα αποκεντρωμένα συστήματα να κερδίζουν έδαφος λόγω της ευελιξίας τους (Khavari et al., 2017).

Σε ένα κεντρικό σύστημα διαχείρισης, ένας κεντρικός ελεγκτής συλλέγει πληροφορίες από όλα τα στοιχεία του δικτύου και λαμβάνει αποφάσεις για τη βέλτιστη κατανομή της ισχύος. Το μοντέλο αυτό προσφέρει το πλεονέκτημα του καθολικού ελέγχου και της επίτευξης του απόλυτου μαθηματικού βελτίστου για ολόκληρο το δίκτυο, καθώς ο ελεγκτής έχει πλήρη εικόνα των παραμέτρων λειτουργίας. Παρόλα αυτά, η υπολογιστική πολυπλοκότητα αυξάνεται εκθετικά όσο προστίθενται νέοι χρήστες και διεσπαρμένοι πόροι, καθιστώντας την κεντρική επεξεργασία αργή και δυσκίνητη (Fragkos et al., 2022).



Εικόνα 4:Αρχιτεκτονική κεντρικού ελέγχου(Πηγή: Albarakati et al., 2022).

Αντιθέτως, η αποκεντρωμένη αρχιτεκτονική βασίζεται στη διαίρεση του δικτύου σε μικρότερες, αυτόνομες μονάδες, όπως τα μικροδίκτυα (microgrids), όπου η λήψη αποφάσεων γίνεται τοπικά. Αυτή η προσέγγιση μειώνει δραστικά τον όγκο των δεδομένων που πρέπει να μεταφερθούν σε μεγάλες αποστάσεις και επιτρέπει την ταχύτερη απόκριση σε τοπικές διακυμάνσεις της ζήτησης ή της παραγωγής. Με τον τρόπο αυτό, το σύστημα γίνεται πιο ανθεκτικό, καθώς ένα σφάλμα σε μία μονάδα δεν προκαλεί απαραίτητα κατάρρευση ολόκληρου του δικτύου (Wu et al., 2022).

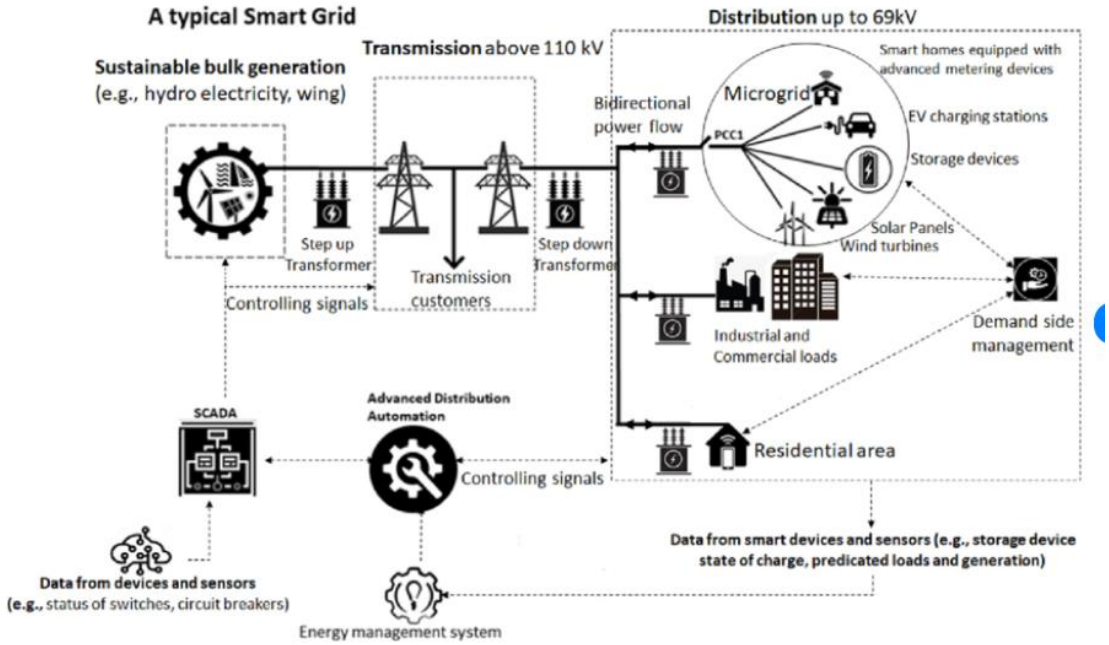
Η διαχείριση των Διεσπαρμένων Ενεργειακών Πόρων (DER) αποτελεί το πεδίο όπου η σύγκριση των δύο μοντέλων γίνεται πιο έντονη. Ενώ στα κεντρικά συστήματα οι πόροι αυτοί αντιμετωπίζονται ως παθητικά στοιχεία που πρέπει να συμμορφώνονται με τις εντολές του κέντρου, στα αποκεντρωμένα συστήματα οι DER συμμετέχουν ενεργά στη διαμόρφωση της τοπικής ενεργειακής ισορροπίας. Η αποκεντρωμένη διαχείριση επιτρέπει την αποτελεσματικότερη ενσωμάτωση φωτοβολταϊκών και ανεμογεννητριών, ελαχιστοποιώντας τις απώλειες μεταφοράς (Khavari et al., 2017).

Σημαντικό ρόλο στην επικράτηση των αποκεντρωμένων συστημάτων παίζει η τεχνολογία του blockchain και του edge computing, που επιτρέπουν την εκτέλεση συναλλαγών ενέργειας απευθείας μεταξύ των χρηστών (peer-to-peer). Στα συστήματα αυτά, η ασφάλεια και η διαφάνεια εξασφαλίζονται μέσω κρυπτογραφικών

πρωτοκόλλων, χωρίς την ανάγκη μιας κεντρικής αρχής ελέγχου. Αυτή η μετάβαση ενισχύει τον ρόλο του "prosumer" (παραγωγού-καταναλωτή), ο οποίος μπορεί να διαχειρίζεται αυτόνομα το ενεργειακό του προφίλ (Wu et al., 2022).

Παρά τα πλεονεκτήματα της αποκέντρωσης, η κυβερνοασφάλεια παραμένει μια πρόκληση που προσεγγίζεται διαφορετικά σε κάθε μοντέλο. Στα κεντρικά συστήματα, ο έλεγχος πρόσβασης είναι συγκεντρωμένος, γεγονός που διευκολύνει την επιτήρηση αλλά δημιουργεί ένα "μοναδικό σημείο αποτυχίας" (single point of failure). Αντίθετα, στα αποκεντρωμένα δίκτυα, η επιφάνεια επίθεσης είναι μεγαλύτερη λόγω του πλήθους των σημείων εισόδου, γεγονός που απαιτεί προηγμένες λύσεις κρυπτογράφησης και έξυπνα συμβόλαια για τη διασφάλιση της ακεραιότητας (Fragkos et al., 2022).

Μια άλλη κρίσιμη παράμετρος είναι η οικονομική αποδοτικότητα και ο χρόνος υπολογισμού των αλγορίθμων διαχείρισης. Μελέτες δείχνουν ότι ενώ τα κεντρικά μοντέλα μπορούν να επιτύχουν ελαφρώς υψηλότερα κέρδη για το συνολικό σύστημα κάτω από ιδανικές συνθήκες, τα αποκεντρωμένα μοντέλα υπερέχουν σε ταχύτητα επίλυσης προβλημάτων και είναι πιο κατάλληλα για εφαρμογές σε πραγματικό χρόνο. Αυτό τα καθιστά ιδανικά για το περιβάλλον της "αγοράς ενέργειας στην άκρη του δικτύου" (edge grid energy market), όπου οι αλλαγές είναι συνεχείς (Khavari et al., 2017).



Εικόνα 5:Ένα τυπικό Έξυπνο Δίκτυο που περιέχει Μικροδίκτυα και είναι εξοπλισμένο με SCADA, ADA και EMS (Πηγή:Norouzi et al.,2023).

Συμπερασματικά, η επιλογή μεταξύ κεντρικής και αποκεντρωμένης αρχιτεκτονικής δεν είναι απαραίτητα αμοιβαία αποκλειόμενη, καθώς το μέλλον των Smart Grids φαίνεται να κινείται προς υβριδικά μοντέλα. Η ικανότητα συνδυασμού της στρατηγικής εποπτείας ενός κεντρικού συστήματος με την τοπική αυτονομία και ταχύτητα των αποκεντρωμένων δομών θα αποτελέσει το κλειδί για την επιτυχία του ψηφιακού μετασχηματισμού. Η εξέλιξη των επικοινωνιακών πρωτοκόλλων θα συνεχίσει να γεφυρώνει το χάσμα μεταξύ αυτών των δύο προσεγγίσεων, διασφαλίζοντας ένα σταθερό και αποδοτικό δίκτυο (Fragkos et al., 2022).

2.1.2. Λειτουργικά επίπεδα: παραγωγή, μεταφορά, διανομή.

- **Λειτουργικός τομέας παραγωγής:**

Η παραγωγή ενέργειας στα έξυπνα δίκτυα υφίσταται μια θεμελιώδη μεταλλαγή, μεταβαίνοντας από μια συγκεντρωτική δομή παραγωγής σε μια πιο διασπαρμένη και αποκεντρωμένη μορφή. Αυτή η νέα προσέγγιση επιτρέπει τη μετατροπή των υπαρχουσών βιομηχανιών σε μια εποχή ενισχυμένων δικτύων που προσφέρουν ένα έξυπνο, ανταποκρίσιμο και αμφίδρομο σύστημα αυτόματης διαχείρισης. Σύμφωνα με τους Ohanu et al. (2024), η παραγωγή στα έξυπνα δίκτυα βασίζεται στην

ενσωμάτωση καθαρών και αποδοτικών φορτίων που προέρχονται από φυσικές πηγές, όπως η ηλιακή, η αιολική, η γεωθερμική, η πυρηνική και η βιοενέργεια (Ohanu et al.,2024)

Ένα κρίσιμο στοιχείο στη λειτουργία της παραγωγής είναι η χρήση των **Εικονικών Εργοστασίων Παραγωγής (Virtual Power Plants - VPP)**, τα οποία ορίζονται ως συλλογές διασπαρμένων ενεργειακών πόρων. Τα VPP ομαδοποιούν ανανεώσιμες πηγές, συστήματα αποθήκευσης, ελεγχόμενα φορτία και prosumers (χρήστες του ηλεκτρικού δικτύου που ταυτόχρονα καταναλώνουν και *παράγουν* ηλεκτρική ενέργεια)**.** σε μια ενιαία οντότητα, επιτρέποντας στο δίκτυο να λειτουργεί με αυτονομία και να βελτιστοποιεί την εμπορία ενέργειας. Αυτά τα συστήματα λειτουργούν ως ένας αποτελεσματικός μηχανισμός για την επίλυση των ζητημάτων ενέργειας των χρηστών, παρέχοντας βοηθητικές υπηρεσίες και εξασφαλίζοντας την οικονομική αξιοπιστία του συστήματος (Ohanu et al.,2024).

Λόγω της διαλείπουσας φύσης των ανανεώσιμων πηγών (όπως ο ήλιος και ο άνεμος), η παραγωγή στα έξυπνα δίκτυα εξαρτάται άμεσα από τις τεχνολογίες αποθήκευσης ενέργειας. Τα συστήματα αποθήκευσης μπαταριών (BESS - Battery Energy Storage Systems) και τα συστήματα αποθήκευσης ενέργειας (ESS-Energy Storage Systems) λειτουργούν ως εφεδρικές πηγές που μετριάζουν τις διακυμάνσεις της τάσης και την αστάθεια. Η σύνδεση αυτών των συσκευών αποθήκευσης με το δίκτυο καθιστά εφικτή τη βέλτιστη ροή ενέργειας, διασφαλίζοντας τη συνέχεια του φορτίου και τη σταθερότητα του δικτύου κάτω από οποιεσδήποτε συνθήκες (Ohanu et al.,2024).

Επιπλέον, ο τομέας της παραγωγής ενισχύεται από τη συμμετοχή των **"prosumers"**, δηλαδή των καταναλωτών που παράγουν ενέργεια στο οικιακό τους περιβάλλον. Αυτοί οι χρήστες έχουν τη δυνατότητα είτε να αποθηκεύουν το πλεόνασμα ενέργειας για μελλοντική χρήση, είτε να το πωλούν απευθείας στο δίκτυο ή σε άλλους καταναλωτές μέσω αποκεντρωμένων δικτύων. Η δυνατότητα αυτή της αμφίδρομης ροής ισχύος επιτρέπει τη συνεχή παρακολούθηση των προτιμήσεων των καταναλωτών από το σημείο της παραγωγής μέχρι το σημείο της παροχής(Ohanu et al.,2024).Η αποτελεσματική λειτουργία όλης αυτής της παραγωγικής αλυσίδας απαιτεί ένα **Σύστημα Διαχείρισης Ενέργειας (Energy Management System - EMS)**. Το EMS είναι απαραίτητο για τον συντονισμό των ανανεώσιμων πηγών και τη διασφάλιση της πλήρους αξιοποίησής τους, συμβάλλοντας ταυτόχρονα στην

ελαχιστοποίηση των αρμονικών και στη βελτίωση της αποδοτικότητας του δικτύου. Στα έξυπνα σπίτια, το EMS παρακολουθεί τη ζήτηση και την προσφορά σε πραγματικό χρόνο, εκτελώντας διορθωτικές ενέργειες βάσει των δεδομένων που λαμβάνει από τους έξυπνους αισθητήρες (Ohanu et al.,2024).

Συνοπτικά, η παραγωγή στα έξυπνα δίκτυα δεν είναι πλέον μια στατική διαδικασία, αλλά ένα δυναμικό σύστημα που βασίζεται στην προηγμένη επικοινωνία και τον αυτοματισμό. Σε αντίθεση με το παραδοσιακό δίκτυο όπου οι προμηθευτές έχουν μικρό έλεγχο, οι τεχνολογίες των έξυπνων δικτύων και οι αισθητήρες παρέχουν στις εταιρείες ενέργειας ανώτερο έλεγχο στη διανομή και την παραγωγή της ηλεκτρικής ενέργειας. Αυτό το μοντέλο μειώνει τον αριθμό των διακοπών ρεύματος και αυξάνει τη συνολική αποδοτικότητα, προσφέροντας στους πελάτες μεγαλύτερο λόγο στον τρόπο χρήσης της ενέργειας (Ohanu et al.,2024).

- **Λειτουργικός τομέας μεταφοράς:**

Σύμφωνα με άρθρο του Pacific Northwest National Laboratory (PNNL), ο λειτουργικός τομέας της Μεταφοράς (Transmission) στα έξυπνα δίκτυα αποτελεί τη ραχοκοκαλιά του συστήματος "bulk power", το οποίο μεταφέρει την ηλεκτρική ενέργεια από τους σταθμούς παραγωγής σε μεγάλες αποστάσεις προς τα κέντρα κατανάλωσης. Στο πλαίσιο του έξυπνου δικτύου, η μεταφορά εξελίσσεται από μια παθητική υποδομή σε ένα δυναμικό σύστημα που ενσωματώνει προηγμένους αισθητήρες, αυτοματισμούς και ψηφιακές τεχνολογίες επικοινωνίας (Pacific Northwest National Laboratory, n.d.).

Η λειτουργία της μεταφοράς στα έξυπνα δίκτυα περιλαμβάνει τα εξής βασικά σημεία:

Προηγμένη Επιτήρηση σε Πραγματικό Χρόνο: Με τη χρήση προηγμένων αισθητήρων, το δίκτυο μεταφοράς μπορεί να παρακολουθεί και να αναφέρει τις συνθήκες των γραμμών σε πραγματικό χρόνο. Αυτό επιτρέπει τη ροή περισσότερης ενέργειας μέσω των υπαρχουσών γραμμών, καθιστώντας το δίκτυο σημαντικά πιο αποδοτικό και μειώνοντας την ανάγκη για άμεση κατασκευή νέων υποδομών.

Αυξημένη Αξιοπιστία και Αυτονομία: Το έξυπνο δίκτυο μεταφοράς χαρακτηρίζεται ως "έξυπνο" επειδή είναι ικανό να ανιχνεύει υπερφορτώσεις στο σύστημα και να

αναδρομολογεί την ισχύ αυτόματα. Αυτή η αυτόνομη λειτουργία επιτρέπει την επίλυση προβλημάτων ταχύτερα από όσο μπορεί να ανταποκριθεί ο άνθρωπος, ελαχιστοποιώντας ή και προλαμβάνοντας πιθανές διακοπές ρεύματος (blackouts).

Ενσωμάτωση Ανανεώσιμων Πηγών Ενέργειας: Μία από τις μεγαλύτερες προκλήσεις της μεταφοράς είναι η ενσωμάτωση μεταβλητών πηγών, όπως η αιολική και η ηλιακή ενέργεια. Το έξυπνο δίκτυο, μέσω έξυπνα ελεγχόμενων τεχνολογιών αποθήκευσης ενέργειας μεγάλης κλίμακας, διευκολύνει την ομαλή ένταξη αυτών των πηγών στο σύστημα μεταφοράς, εξασφαλίζοντας σταθερότητα παρά τη διαλείπουσα φύση τους.

Μείωση Απωλειών και Νέες Τεχνολογίες: Η χρήση καινοτόμων υλικών, όπως τα υπεραγώγιμα καλώδια ισχύος, βοηθά στη δραστική μείωση των απωλειών κατά τη μεταφορά. Αυτά τα καλώδια μπορούν να μεταφέρουν εκθετικά περισσότερη ισχύ, ενισχύοντας τη δυνατότητα του συστήματος μεταφοράς να ανταποκρίνεται στην αυξανόμενη ζήτηση της ψηφιακής οικονομίας.

Ανθεκτικότητα και Ασφάλεια: Καθώς το σύστημα μεταφοράς γίνεται πιο αποκεντρωμένο και ενισχύεται με πρωτόκολλα ασφαλείας, καθίσταται πιο ανθεκτικό απέναντι σε φυσικές καταστροφές, ακραία καιρικά φαινόμενα και κυβερνοεπιθέσεις. Η ψηφιακή επικάλυψη (data overlay) στις υποδομές μεταφοράς επιτρέπει τη διατήρηση της ποιότητας της ισχύος χωρίς διακυμάνσεις ή διαταραχές.

Συντονισμός και Εποπτεία: Η διαχείριση του εθνικού συστήματος μεταφοράς τελεί υπό την εποπτεία ομοσπονδιακών και κρατικών φορέων (όπως η FERC στις ΗΠΑ), οι οποίοι επιβάλλουν πρότυπα αξιοπιστίας. Το έξυπνο δίκτυο παρέχει στους διαχειριστές τα απαραίτητα εργαλεία ανάλυσης (Grid Analytics) για την στιγμιαία εξισορρόπηση προσφοράς και ζήτησης, κάτι που είναι ζωτικής σημασίας για την εθνική ασφάλεια και τη δημόσια υγεία (Pacific Northwest National Laboratory, n.d.).

- **Λειτουργικός τομέας μεταφοράς διανομής:**

Το έξυπνο δίκτυο διανομής αποτελεί το κρίσιμο σημείο διασύνδεσης μεταξύ του συστήματος μεταφοράς και των τελικών καταναλωτών, ενσωματώνοντας προηγμένες τεχνολογίες πληροφορικής και επικοινωνιών. Σύμφωνα με τους Esmail et al. (2020),

η κύρια διαφορά από το παραδοσιακό δίκτυο έγκειται στην ικανότητα του συστήματος να διαχειρίζεται αμφίδρομες ροές ισχύος και πληροφοριών, επιτρέποντας την ενεργή συμμετοχή των καταναλωτών και την ενσωμάτωση διάσπαρτης παραγωγής (DG), όπως τα φωτοβολταϊκά και οι ανεμογεννήτριες, στο επίπεδο της χαμηλής και μέσης τάσης.

Η λειτουργία της διανομής στα έξυπνα δίκτυα βασίζεται σε τρεις κύριες στρατηγικές ελέγχου: την κεντρική (centralized), την αποκεντρωμένη (decentralized) και την αυτόνομη (autonomous) στρατηγική. Το άρθρο υπογραμμίζει ότι τα **Συστήματα Πολλαπλών Πρακτόρων (Multi-Agent Systems - MAS)** είναι καθοριστικά για τη σύγχρονη διανομή, καθώς επιτρέπουν σε ευφυείς "πράκτορες" (agents) να λαμβάνουν αποφάσεις τοπικά, εξασφαλίζοντας ταχύτητα και ευελιξία χωρίς την ανάγκη συνεχούς επικοινωνίας με ένα κεντρικό σύστημα ελέγχου (Esmail et al., 2020).

Ένα από τα σημαντικότερα χαρακτηριστικά του έξυπνου δικτύου διανομής είναι η **διαχείριση σφαλμάτων (fault management)**, η οποία χωρίζεται σε τρία στάδια: τον εντοπισμό του σφάλματος, την απομόνωση του ελαττωματικού τμήματος και την αποκατάσταση της παροχής (restoration). Μέσω της χρήσης "έξυπνων" διακοπτών και αισθητήρων, το δίκτυο μπορεί να αναγνωρίζει αυτόματα τη θέση μιας βλάβης και να αναδιαμορφώνει τη δομή του (reconfiguration), περιορίζοντας τη διακοπή ρεύματος μόνο στην ελάχιστη δυνατή περιοχή (Esmail et al., 2020).

Η έννοια της **"αυτο-ίασης" (self-healing)** αποτελεί τον πυρήνα της αξιοπιστίας στη διανομή. Όπως αναφέρεται στο άρθρο, το έξυπνο δίκτυο διανομής μπορεί να χωρίζεται σε "νησίδες" ή μικροδίκτυα (microgrids) που λειτουργούν αυτόνομα όταν το κύριο δίκτυο αντιμετωπίζει προβλήματα. Αυτή η ικανότητα διασφαλίζει ότι κρίσιμα φορτία, όπως νοσοκομεία ή δημόσιες υπηρεσίες, παραμένουν ηλεκτροδοτούμενα ακόμη και σε περιπτώσεις εκτεταμένων βλαβών στο σύστημα μεταφοράς (Esmail et al., 2020).

Επιπλέον, η διανομή στα έξυπνα δίκτυα βελτιστοποιεί την **ποιότητα ισχύος και τη διαχείριση της ζήτησης**. Η χρήση έξυπνων μετρητών επιτρέπει στις εταιρείες κοινής ωφέλειας να παρακολουθούν την κατανάλωση σε πραγματικό χρόνο και να εφαρμόζουν προγράμματα απόκρισης ζήτησης (demand response), ενθαρρύνοντας τους καταναλωτές να μεταφέρουν τη χρήση ενέργειας σε ώρες εκτός αιχμής. Αυτό

μειώνει την καταπόνηση των μετασχηματιστών διανομής και παρατείνει τη διάρκεια ζωής του εξοπλισμού του δικτύου (Esmail et al., 2020).

Τέλος, η αξιοπιστία του συστήματος διανομής μετριέται με δείκτες όπως ο SAIDI και ο SAIFI, οι οποίοι βελτιώνονται σημαντικά με την υιοθέτηση αποκεντρωμένων στρατηγικών ελέγχου. Οι Esmail et al. (2020) καταλήγουν ότι η μετάβαση σε ένα έξυπνο σύστημα διανομής δεν αυξάνει μόνο την αποδοτικότητα, αλλά δημιουργεί ένα ανθεκτικό δίκτυο ικανό να υποστηρίξει την ηλεκτροκίνηση και την πλήρη απανθρακοποίηση της ενέργειας στο επίπεδο της γειτονιάς.

2.1.3. Συστήματα ελέγχου και διαχείρισης ενέργειας.

Τα Συστήματα Διαχείρισης Ενέργειας (Energy Management Systems - EMS) αποτελούν τον «ακρογωνιαίο λίθο» της λειτουργίας των έξυπνων δικτύων, λειτουργώντας ως ο κεντρικός μηχανισμός που διασφαλίζει την ισορροπία μεταξύ προσφοράς και ζήτησης. Σύμφωνα με τον **Fang (2023)**, το EMS αξιοποιεί προηγμένες τεχνολογίες πληροφορικής και στρατηγικές ευφυούς ελέγχου για τον συντονισμό της παραγωγής, της μεταφοράς και της κατανάλωσης ενέργειας. Η κύρια αποστολή του είναι να μετατρέψει το παραδοσιακό ηλεκτρικό δίκτυο σε ένα σύστημα υψηλής απόδοσης, αξιοπιστίας και περιβαλλοντικής συνείδησης, ικανό να διαχειρίζεται την πολυπλοκότητα των σύγχρονων ενεργειακών αναγκών(Fang,2023).

Η ανάγκη για εξελιγμένα συστήματα EMS εντείνεται λόγω της αυξανόμενης διείσδυσης των Ανανεώσιμων Πηγών Ενέργειας (ΑΠΕ). Όπως επισημαίνεται στο άρθρο, οι ΑΠΕ χαρακτηρίζονται από εγγενή αστάθεια και διαλείπουσα λειτουργία, γεγονός που καθιστά τη σταθερότητα του δικτύου μια συνεχή πρόκληση. Το EMS παρεμβαίνει ως ο συνδετικός κρίκος που προσφέρει παρακολούθηση σε πραγματικό χρόνο και βελτιστοποίηση βάσει δεδομένων, διασφαλίζοντας ότι οι διακυμάνσεις στην παραγωγή (π.χ. από αιολικά ή ηλιακά πάρκα) δεν επηρεάζουν την ακεραιότητα του δικτύου(Fang,2023).

Ένα κρίσιμο υποσύστημα που αναλύει ο **Fang (2023)** είναι η **Διανεμημένη Αποθήκευση Ενέργειας (Distributed Energy Storage)**. Το EMS συντονίζει τη λειτουργία των συστημάτων αποθήκευσης, επιτρέποντας την «εξομάλυνση» της καμπύλης φορτίου. Αυτό επιτυγχάνεται με την αποθήκευση ενέργειας κατά τις ώρες

χαμηλής ζήτησης και την απελευθέρωσή της κατά τις ώρες αιχμής, μειώνοντας έτσι την καταπόνηση των υποδομών και βελτιώνοντας τη συνολική οικονομική αποδοτικότητα του συστήματος. Επιπλέον, η ενσωμάτωση της **ευφυούς διαχείρισης ηλεκτρικών οχημάτων (EVs)** αποτελεί βασική λειτουργία των σύγχρονων EMS. Το σύστημα ελέγχου δεν διαχειρίζεται απλώς τη φόρτιση των οχημάτων, αλλά μπορεί να τα αξιοποιήσει ως κινητές μονάδες αποθήκευσης που προσφέρουν ενέργεια πίσω στο δίκτυο όταν υπάρχει ανάγκη. Αυτός ο αμφίδρομος έλεγχος ενισχύει την ευελιξία του δικτύου και επιτρέπει την καλύτερη αξιοποίηση της διαθέσιμης καθαρής ενέργειας(Fang,2023).

Σημαντικό ρόλο παίζει επίσης η **ανίχνευση και διάγνωση σφαλμάτων (Fault Perception and Diagnosis)**. Το EMS στα έξυπνα δίκτυα διαθέτει την ικανότητα να αντιλαμβάνεται ανωμαλίες στη λειτουργία του εξοπλισμού πριν αυτές οδηγήσουν σε αστοχία. Μέσω της ανάλυσης μεγάλων δεδομένων (Big Data), το σύστημα μπορεί να προβαίνει σε προληπτική συντήρηση και αυτόματη απομόνωση προβληματικών τμημάτων, εξασφαλίζοντας την αδιάλειπτη παροχή ενέργειας στους καταναλωτές(Fang,2023).

Τέλος, το άρθρο υπογραμμίζει ότι το μέλλον των EMS συνδέεται άρρηκτα με την υιοθέτηση τεχνολογιών όπως το **Blockchain** για ασφαλείς συναλλαγές ενέργειας και τη χρήση **ευφυών αλγορίθμων δρομολόγησης (Intelligent Dispatching)**. Παρά τις προκλήσεις που αφορούν την κυβερνοασφάλεια και την ανάγκη για διεθνή τυποποίηση, η συνεχή εξέλιξη της τεχνολογίας EMS υπόσχεται μια βιώσιμη ενεργειακή μετάβαση, μειώνοντας το αποτύπωμα άνθρακα και προσφέροντας οικονομικότερα ενεργειακά μοντέλα για τις βιομηχανίες και τους οικιακούς χρήστες(Fang,2023).

2.2. IoT και αισθητήρες στο ενεργειακό δίκτυο

2.2.1 Ρόλος αισθητήρων και IoT συσκευών στη συλλογή δεδομένων.

Η ενσωμάτωση του Διαδικτύου των Πραγμάτων (IoT) στα έξυπνα δίκτυα αποτελεί τη βάση για τη μετάβαση από τα παραδοσιακά συστήματα ισχύος σε ευφυή, αυτοματοποιημένα δίκτυα. Οι αισθητήρες και οι συσκευές IoT λειτουργούν ως το «νευρικό σύστημα» του δικτύου, επιτρέποντας τη συνεχή και σε πραγματικό χρόνο

συλλογή δεδομένων από όλα τα σημεία της ενεργειακής αλυσίδας. Σύμφωνα με τους Kirmani κ.ά. (2023), αυτή η υποδομή είναι απαραίτητη για την παρακολούθηση της κατάστασης του εξοπλισμού, τη μέτρηση της κατανάλωσης και τη διασφάλιση της σταθερότητας του συστήματος, προσφέροντας πρωτοφανή ορατότητα στους διαχειριστές.

Οι συσκευές IoT στα έξυπνα δίκτυα αποτελούνται από αισθητήρες, ενεργοποιητές (actuators) και υπολογιστικές μονάδες που επιτρέπουν την αυτόνομη λήψη αποφάσεων. Όπως εξηγούν οι Sahu & Mahapatra (2020), το IoT συνδέει κάθε αντικείμενο του δικτύου με το Διαδίκτυο, επιτρέποντας την ανταλλαγή πληροφοριών μεταξύ των σταθμών παραγωγής, των γραμμών μεταφοράς και των τελικών χρηστών. Αυτή η διασυνδεσιμότητα επιτρέπει τη μετατροπή των δεδομένων σε χρήσιμη γνώση, διευκολύνοντας την αποτελεσματική συνεργασία μεταξύ των εναλλακτικών πηγών ενέργειας και των έξυπνων οχημάτων.

Στο επίπεδο της παραγωγής και της μεταφοράς, οι έξυπνοι αισθητήρες και οι μονάδες μέτρησης φάσης (PMUs) συλλέγουν κρίσιμες παραμέτρους, όπως η τάση και η συχνότητα. Οι συσκευές IoT επιτρέπουν την απομακρυσμένη παρακολούθηση των υποσταθμών, μειώνοντας την ανάγκη για φυσική επιθεώρηση και επιτρέποντας την αυτόματη ανίχνευση ανωμαλιών. Οι Kirmani κ.ά. (2023) επισημαίνουν ότι η έγκαιρη ανίχνευση βλαβών μέσω αυτών των αισθητήρων αποτρέπει την εξέλιξη μικρών προβλημάτων σε εκτεταμένες διακοπές ρεύματος.

Η συλλογή δεδομένων στο επίπεδο του καταναλωτή βασίζεται σε έξυπνους μετρητές και οικιακές συσκευές IoT που υποστηρίζουν την αμφίδρομη επικοινωνία. Σύμφωνα με τους Sahu & Mahapatra (2020), η χρήση τεχνολογιών όπως το Narrowband IoT (NB-IoT) παρέχει ευρεία κάλυψη και χαμηλή κατανάλωση ενέργειας, καθιστώντας το ιδανικό για την παρακολούθηση εκατομμυρίων συσκευών σε αστικά περιβάλλοντα. Αυτοί οι αισθητήρες «τελευταίου μέτρου» (last-meter) επιτρέπουν την ακριβή τιμολόγηση και τη βελτιστοποίηση της χρήσης ενέργειας σε επίπεδο νοικοκυριού.

Η αρχιτεκτονική αυτών των συστημάτων συλλογής δεδομένων οργανώνεται συνήθως σε τρία επίπεδα: το επίπεδο αντίληψης (perception layer), το επίπεδο δικτύου και το επίπεδο εφαρμογής. Το **επίπεδο αντίληψης** περιλαμβάνει τους φυσικούς αισθητήρες που συλλέγουν τις πληροφορίες, ενώ το **επίπεδο δικτύου** αναλαμβάνει την ασφαλή

μεταφορά και δρομολόγηση των δεδομένων προς το κέντρο ελέγχου μέσω τεχνολογιών όπως το 6G, το ZigBee ή το Wi-Fi. Στην κορυφή της πυραμίδας, το **επίπεδο εφαρμογής** επεξεργάζεται τις εισερχόμενες πληροφορίες για την παροχή εξειδικευμένων υπηρεσιών, όπως η παρακολούθηση της κατανάλωσης και η διαχείριση φορτίου. Οι Kirmani κ.ά. (2023) υπογραμμίζουν ότι η επιτυχία του δικτύου εξαρτάται από την ικανότητα αυτών των συσκευών να λειτουργούν αξιόπιστα σε ετερογενή περιβάλλοντα, παρά τους περιορισμούς στην επεξεργαστική τους ισχύ.

Ωστόσο, η μαζική ανάπτυξη αισθητήρων IoT αυξάνει την επιφάνεια επίθεσης του δικτύου, καθιστώντας την κυβερνοασφάλεια κρίσιμη προτεραιότητα. Οι Sahu & Mahapatra (2020) προειδοποιούν ότι οι παραβιασμένοι αισθητήρες μπορούν να στείλουν ψευδή δεδομένα στο κέντρο ελέγχου, προκαλώντας λανθασμένες ενέργειες που θέτουν σε κίνδυνο τη σταθερότητα του συστήματος. Η διασφάλιση της αυθεντικότητας και της ακεραιότητας των συλλεγόμενων δεδομένων είναι απαραίτητη προϋπόθεση για τη λειτουργία των έξυπνων πόλεων και των βιώσιμων ενεργειακών δικτύων του μέλλοντος (Kirmani et al., 2023· Sahu & Mahapatra, 2020).

Συμπερασματικά, ο συνδυασμός αισθητήρων και IoT συσκευών αποτελεί τον θεμέλιο λίθο για την ψηφιοποίηση των ηλεκτρικών δικτύων, προσφέροντας τη δυνατότητα για μια πιο πράσινη και αποδοτική ενεργειακή διαχείριση. Παρά τις προκλήσεις που αφορούν την πολυπλοκότητα των δικτύων επικοινωνίας και τους κινδύνους ασφαλείας, η συνεχής εξέλιξη των IoT τεχνολογιών υπόσχεται να βελτιώσει την ανθεκτικότητα των έξυπνων δικτύων, καθιστώντας τα ικανά να ανταποκριθούν στις απαιτήσεις της σύγχρονης κοινωνίας (Kirmani et al., 2023· Sahu & Mahapatra, 2020).

2.2.2. Παρακολούθηση, πρόβλεψη, αυτοματοποίηση λειτουργιών.

Η ενσωμάτωση του Διαδικτύου των Πραγμάτων (IoT) στα Έξυπνα Δίκτυα (Smart Grids) αποτελεί τον ακρογωνιαίο λίθο για τον μετασχηματισμό των παραδοσιακών συστημάτων ενέργειας σε δυναμικά, αμφίδρομα οικοσυστήματα. Η χρήση προηγμένων αισθητήρων επιτρέπει τη συνεχή **παρακολούθηση** των ηλεκτρικών παραμέτρων σε πραγματικό χρόνο, προσφέροντας στους διαχειριστές μια λεπτομερή εικόνα της κατάστασης του δικτύου από την παραγωγή έως την κατανάλωση (Qays et al., 2023). Η δυνατότητα αυτή εξαλείφει τα τυφλά σημεία των συμβατικών δικτύων,

επιτρέποντας την έγκαιρη ανίχνευση ανωμαλιών και τη βελτιστοποίηση της ροής ενέργειας.

Στο επίπεδο της **πρόβλεψης**, οι αισθητήρες IoT συλλέγουν τεράστιους όγκους δεδομένων που, μέσω αναλυτικών εργαλείων και αλγορίθμων μηχανικής μάθησης, επιτρέπουν την ακριβή εκτίμηση της ζήτησης φορτίου. Όπως επισημαίνει ο Khare (2024), η προγνωστική ανάλυση (predictive analytics) συμβάλλει καθοριστικά στην εξισορρόπηση προσφοράς και ζήτησης, μειώνοντας την ανάγκη για εφεδρικές μονάδες παραγωγής που συχνά είναι κοστοβόρες και περιβαλλοντικά επιβαρυντικές. Η πρόβλεψη επεκτείνεται και στην προληπτική συντήρηση του εξοπλισμού, καθώς οι αισθητήρες μπορούν να αναγνωρίσουν σημάδια φθοράς πριν αυτά οδηγήσουν σε αστοχία.

Η **αυτοματοποίηση των λειτουργιών** αποτελεί το επόμενο στάδιο αυτής της τεχνολογικής εξέλιξης. Η χρήση έξυπνων μετρητών (Smart Meters) και ενεργοποιητών (actuators) επιτρέπει στο δίκτυο να λαμβάνει αυτόνομες αποφάσεις για την αναδρομολόγηση της ενέργειας ή την απομόνωση σφαλμάτων χωρίς την ανάγκη ανθρώπινης παρέμβασης. Σύμφωνα με τους Qays et al. (2023), αυτή η ικανότητα «αυτο-ίασης» (self-healing) ενισχύει την αξιοπιστία του συστήματος, περιορίζοντας τη διάρκεια και την έκταση των διακοπών ρεύματος, ενώ ταυτόχρονα βελτιστοποιεί τη λειτουργία των ανανεώσιμων πηγών ενέργειας.

Επιπλέον, η αυτοματοποίηση μέσω IoT διευκολύνει τη διαχείριση της **απόκρισης ζήτησης** (demand response). Οι αισθητήρες επικοινωνούν με οικιακές ή βιομηχανικές συσκευές, ρυθμίζοντας την κατανάλωση σε ώρες αιχμής με βάση τη διαθεσιμότητα και το κόστος της ενέργειας. Αυτή η αμφίδρομη ροή πληροφοριών και ισχύος μετατρέπει τον καταναλωτή σε ενεργό συμμετέχοντα (prosumer), διασφαλίζοντας τη σταθερότητα της τάσης και τη συνολική αποδοτικότητα της υποδομής (Khare, 2024).

Τεχνικά, η υποδομή αυτή βασίζεται σε πολυεπίπεδα μοντέλα αρχιτεκτονικής, όπου το επίπεδο των αισθητήρων (perception layer) είναι υπεύθυνο για την απόκτηση των δεδομένων. Η χρήση πρωτοκόλλων χαμηλής κατανάλωσης ενέργειας διασφαλίζει ότι οι αισθητήρες μπορούν να λειτουργούν για μεγάλα διαστήματα σε απομακρυσμένες

τοποθεσίες, παρέχοντας κρίσιμα δεδομένα για τη θερμοκρασία των μετασχηματιστών ή την ποιότητα της ισχύος (Qays et al., 2023).

Ωστόσο, η αυξημένη αυτοματοποίηση και η εξάρτηση από τους αισθητήρες εισάγουν προκλήσεις που σχετίζονται με την κυβερνοασφάλεια και τη διαλειτουργικότητα των συστημάτων. Η ανάγκη για ενιαία πρότυπα επικοινωνίας είναι επιτακτική, ώστε τα δεδομένα από διαφορετικούς κατασκευαστές αισθητήρων να μπορούν να ενσωματωθούν απρόσκοπτα στα κεντρικά συστήματα ελέγχου (SCADA) (Khare, 2024).

Συμπερασματικά, η συνέργεια παρακολούθησης, πρόβλεψης και αυτοματοποίησης μέσω IoT προσδίδει στο ενεργειακό δίκτυο την απαραίτητη ευφυΐα για να ανταπεξέλθει στις απαιτήσεις της σύγχρονης εποχής. Η μετάβαση από την αντιδραστική (reactive) στην προληπτική (proactive) διαχείριση, όπως τεκμηριώνεται από τις σύγχρονες έρευνες, αποτελεί τη μοναδική βιώσιμη οδό για την επίτευξη ενεργειακής απόδοσης και περιβαλλοντικής αειφορίας.

2.2.3 Συνδεσιμότητα και επικοινωνιακά πρωτόκολλα

Η αποτελεσματική λειτουργία του Έξυπνου Δικτύου (Smart Grid) βασίζεται στην απρόσκοπτη συνδεσιμότητα εκατομμυρίων ετερογενών συσκευών και αισθητήρων. Η αρχιτεκτονική αυτή απαιτεί μια στιβαρή υποδομή επικοινωνιών που να υποστηρίζει την αμφίδρομη ροή δεδομένων μεταξύ του πεδίου παραγωγής/κατανάλωσης και των κέντρων ελέγχου. Όπως επισημαίνουν οι Ben Dhaou et al. (2020), η επιλογή των επικοινωνιακών τεχνολογιών καθορίζεται από τις απαιτήσεις του κάθε τομέα του δικτύου (HAN, NAN, WAN), με έμφαση στην αξιοπιστία και την κάλυψη.

Στο επίπεδο της τοπικής συνδεσιμότητας, οι τεχνολογίες χαμηλής κατανάλωσης ενέργειας και μικρής εμβέλειας παίζουν καθοριστικό ρόλο. Πρωτόκολλα όπως το ZigBee (IEEE 802.15.4) και το Bluetooth Low Energy (BLE) χρησιμοποιούνται ευρέως για τη διασύνδεση έξυπνων μετρητών και οικιακών συσκευών. Η χρήση του IPv6 πάνω από δίκτυα χαμηλής ισχύος (6LoWPAN) αποτελεί κρίσιμο κρίκο, καθώς επιτρέπει την απόδοση διευθύνσεων IP σε περιορισμένους πόρους αισθητήρων, διευκολύνοντας την ενσωμάτωσή τους στο ευρύτερο Διαδίκτυο (Tightiz & Yang, 2020).

Για τις επικοινωνίες ευρείας περιοχής (WAN), το Smart Grid αξιοποιεί τόσο ενσύρματες όσο και ασύρματες λύσεις. Οι οπτικές ίνες και οι τεχνολογίες Power Line Communication (PLC) προσφέρουν υψηλή ταχύτητα και αξιοπιστία, ενώ τα δίκτυα κινητής τηλεφωνίας (4G/5G) και οι τεχνολογίες LPWAN (όπως το LoRaWAN και το NB-IoT) παρέχουν την απαραίτητη γεωγραφική κάλυψη για απομακρυσμένους αισθητήρες. Η επιλογή εξαρτάται από το κρίσιμο μέγεθος της καθυστέρησης (latency), με το 5G να υπόσχεται σχεδόν πραγματικό χρόνο απόκρισης για κρίσιμες λειτουργίες ελέγχου (Ben Dhaou et al., 2020).

Στο επίπεδο των πρωτοκόλλων εφαρμογής, το Smart Grid καλείται να διαχειριστεί διαφορετικούς τύπους δεδομένων. Πρωτόκολλα όπως το MQTT (Message Queuing Telemetry Transport) και το CoAP (Constrained Application Protocol) κυριαρχούν λόγω του ελαφρύ σχεδιασμού τους, ο οποίος είναι ιδανικός για συσκευές IoT με περιορισμένη επεξεργαστική ισχύ. Το MQTT, βασισμένο στο μοντέλο publish/subscribe, προσφέρει υψηλή αποδοτικότητα σε δίκτυα με χαμηλό εύρος ζώνης, διασφαλίζοντας τη μεταφορά δεδομένων τηλεμετρίας (Tightiz & Yang, 2020).

Ιδιαίτερη σημασία έχει η συμμόρφωση με διεθνή πρότυπα όπως το IEC 61850, το οποίο ορίζει το πλαίσιο επικοινωνίας για την αυτοματοποίηση υποσταθμών. Σύμφωνα με τους Tightiz και Yang (2020), η χρήση πρωτοκόλλων όπως το MMS (Manufacturing Message Specification) και το XMPP (eXtensible Messaging and Presence Protocol) επιτρέπει τη διαλειτουργικότητα μεταξύ εξοπλισμού διαφορετικών κατασκευαστών, κάτι που αποτελεί μία από τις μεγαλύτερες προκλήσεις στη σύγχρονη ενεργειακή υποδομή.

Η διαλειτουργικότητα δεν αφορά μόνο τη σύνδεση, αλλά και τη σημασιολογική κατανόηση των δεδομένων. Η χρήση πρωτοκόλλων που υποστηρίζουν την ιεραρχική δομή δεδομένων επιτρέπει στο Smart Grid να αναγνωρίζει αυτόματα νέες συσκευές και να τις εντάσσει στο σύστημα ελέγχου. Αυτή η «plug-and-play» ικανότητα είναι ζωτικής σημασίας για την επέκταση των δικτύων IoT και την ενσωμάτωση ανανεώσιμων πηγών ενέργειας (Ben Dhaou et al., 2020).

Τέλος, η ασφάλεια των επικοινωνιακών πρωτοκόλλων παραμένει προτεραιότητα. Τα πρωτόκολλα IoT πρέπει να ενσωματώνουν ισχυρούς μηχανισμούς κρυπτογράφησης (π.χ. TLS/DTLS) για την προστασία των δεδομένων από κυβερνοεπιθέσεις. Η

πολυπλοκότητα της αρχιτεκτονικής του Smart Grid απαιτεί μια πολυεπίπεδη προσέγγιση ασφάλειας, όπου κάθε πρωτόκολλο επικοινωνίας συμβάλλει στη συνολική θωράκιση της υποδομής έναντι κακόβουλων παρεμβάσεων (Tightiz & Yang, 2020).

Συμπερασματικά, η συνδεσιμότητα στο IoT-assisted Smart Grid επιτυγχάνεται μέσα από ένα σύνθετο μωσαϊκό πρωτοκόλλων που εξισορροπούν την κατανάλωση ενέργειας, την ταχύτητα μετάδοσης και την ασφάλεια. Η εξέλιξη αυτών των προτύπων αποτελεί τη βάση για ένα πιο ευέλικτο και ανθεκτικό ενεργειακό μέλλον.

2.3. Δεδομένα και αυτοματοποίηση

2.3.1 Ανάλυση ενεργειακών δεδομένων και real-time monitoring.

Η ενσωμάτωση του Διαδικτύου των Πραγμάτων (IoT) στο σύγχρονο ενεργειακό δίκτυο έχει μεταβάλει ριζικά τον τρόπο συλλογής και επεξεργασίας πληροφοριών, επιτρέποντας την παρακολούθηση της υποδομής σε πραγματικό χρόνο. Οι έξυπνοι αισθητήρες και οι μετρητές αποτελούν πλέον τα «μάτια» του δικτύου, παράγοντας τεράστιους όγκους δεδομένων που αφορούν τόσο την κατανάλωση όσο και τη λειτουργική κατάσταση των κρίσιμων εξαρτημάτων. Σύμφωνα με τους Liu και Nielsen (2016), η ανάλυση αυτών των δεδομένων αποτελεί ένα σύνθετο πρόβλημα big data analytics, καθώς απαιτεί την ταυτόχρονη επεξεργασία παράλληλων ροών δεδομένων από εκατομμύρια σημεία μέτρησης.

Η παρακολούθηση σε πραγματικό χρόνο (real-time monitoring) δεν περιορίζεται μόνο στην καταγραφή της κατανάλωσης, αλλά επεκτείνεται και στη διάγνωση της κατάστασης του ηλεκτρομηχανολογικού εξοπλισμού. Όπως επισημαίνει η Bharathi (2024), η χρήση αισθητήρων με υποστήριξη IoT επιτρέπει τη διαρκή παρατήρηση κρίσιμων στοιχείων, όπως οι κινητήρες και οι μετασχηματιστές εντός του έξυπνου δικτύου. Αυτή η συνεχής εποπτεία καθιστά εφικτό τον εντοπισμό σφαλμάτων πριν αυτά εκδηλωθούν ως πλήρεις αστοχίες, προωθώντας τη στρατηγική της προληπτικής συντήρησης (predictive maintenance).

Μία από τις σημαντικότερες προκλήσεις στη διαχείριση αυτών των δεδομένων είναι η καθυστέρηση (latency) στη μετάδοση και την επεξεργασία. Η υιοθέτηση της

Τεχνητής Νοημοσύνης στις παρυφές του δικτύου (Edge AI) προσφέρει μια αποτελεσματική λύση σε αυτό το ζήτημα. Η Bharathi (2024) τεκμηριώνει ότι η επεξεργασία δεδομένων τοπικά στις συσκευές μπορεί να βελτιώσει την ταχύτητα της διαγνωστικής ανάλυσης κατά περισσότερο από 70%. Αυτή η αποκεντρωμένη προσέγγιση επιτρέπει την άμεση λήψη αποφάσεων, κάτι που είναι ζωτικής σημασίας για τη σταθερότητα του συστήματος σε περιπτώσεις απότομων διακυμάνσεων.

Στο επίπεδο της ανίχνευσης ανωμαλιών (anomaly detection), η ανάλυση δεδομένων επικεντρώνεται στον εντοπισμό προτύπων κατανάλωσης που αποκλίνουν από το αναμενόμενο. Οι Liu και Nielsen (2016) προτείνουν τη χρήση εποπτευόμενης μάθησης (supervised learning) και στατιστικών μεθόδων παλινδρόμησης για την αναγνώριση ασυνήθιστων συμπεριφορών. Αυτές οι τεχνικές επιτρέπουν στις εταιρείες κοινής ωφέλειας να εντοπίζουν έγκαιρα φαινόμενα όπως η ρευματοκλοπή ή οι βλάβες στη δικτυακή υποδομή, ενώ παράλληλα βοηθούν τους καταναλωτές να κατανοήσουν και να διορθώσουν σπατάλες ενέργειας.

Η αρχιτεκτονική που υποστηρίζει αυτή την ανάλυση συχνά βασίζεται σε υβριδικά μοντέλα, όπως η Lambda Architecture. Αυτό το πλαίσιο επιτρέπει τον συνδυασμό της επεξεργασίας ιστορικών δεδομένων (batch processing) με την ανάλυση ζωντανών ροών δεδομένων (stream processing). Σύμφωνα με τους Liu και Nielsen (2016), η χρήση εργαλείων όπως το Spark Streaming διασφαλίζει την κλιμακωσιμότητα του συστήματος, επιτρέποντας την ταυτόχρονη παρακολούθηση χιλιάδων έξυπνων μετρητών με υψηλή ακρίβεια και χαμηλό χρόνο απόκρισης.

Εκτός από την απόδοση, η προστασία της ιδιωτικότητας των δεδομένων αποτελεί κεντρικό πυλώνα του real-time monitoring. Η εφαρμογή τεχνικών όπως η Ομοσπονδιακή Μάθηση (Federated Learning) επιτρέπει την εκπαίδευση μοντέλων ανίχνευσης σφαλμάτων τοπικά στις συσκευές, χωρίς να απαιτείται η κοινή χρήση ευαίσθητων προσωπικών δεδομένων στο κεντρικό νέφος (Cloud). Η Bharathi (2024) υπογραμμίζει ότι αυτή η μέθοδος εγγυάται την ασφάλεια των πληροφοριών, επιτυγχάνοντας ταυτόχρονα ποσοστά αναγνώρισης σφαλμάτων που υπερβαίνουν το 94%.

Η συνέργεια μεταξύ των IoT αισθητήρων και των προηγμένων αναλυτικών μοντέλων δημιουργεί ένα οικοσύστημα «αυτο-ίασης» (self-healing) για το ενεργειακό δίκτυο. Η

ικανότητα του συστήματος να αναγνωρίζει αυτόνομα τις ανωμαλίες και να προσαρμόζει τη λειτουργία του σε πραγματικό χρόνο μειώνει το λειτουργικό κόστος και την ανάγκη για ανθρώπινη παρέμβαση. Αυτό οδηγεί σε μια πιο ανθεκτική υποδομή, ικανή να διαχειριστεί την πολυπλοκότητα των ανανεώσιμων πηγών ενέργειας και τις αυξημένες απαιτήσεις των σύγχρονων πόλεων (Bharathi, 2024).

Συμπερασματικά, η ανάλυση ενεργειακών δεδομένων και το real-time monitoring μέσω IoT αποτελούν τη βάση για τη μετάβαση σε ένα ευφυές ενεργειακό περιβάλλον. Η ενσωμάτωση τεχνολογιών αιχμής, όπως το Edge AI και η προηγμένη ανάλυση ροών δεδομένων, διασφαλίζει ότι το δίκτυο παραμένει αποδοτικό, ασφαλές και κλιμακώσιμο, ικανοποιώντας τις ανάγκες τόσο των παρόχων όσο και των τελικών χρηστών (Liu & Nielsen, 2016).

2.3.2. Big Data, edge & cloud computing.

Η μετάβαση προς το Έξυπνο Δίκτυο (Smart Grid) σηματοδοτεί τη μεταμόρφωση των παραδοσιακών ενεργειακών συστημάτων σε ένα εκτεταμένο δίκτυο παραγωγής δεδομένων, όπου η πληροφορία καθίσταται εξίσου κρίσιμη με την ίδια την ηλεκτρική ισχύ. Η ευρεία εγκατάσταση έξυπνων μετρητών και αισθητήρων IoT δημιουργεί έναν τεράστιο όγκο δεδομένων, τα οποία χαρακτηρίζονται από τις «5Vs» των **Big Data**: Όγκο (Volume), Ταχύτητα (Velocity), Ποικιλία (Variety), Αξιοπιστία (Veracity) και Αξία (Value). Σύμφωνα με τους Zhang κ.ά. (2018), η διαχείριση αυτών των δεδομένων απαιτεί προηγμένες αναλυτικές μεθόδους που υπερβαίνουν τις δυνατότητες των συμβατικών συστημάτων επεξεργασίας, αποτελώντας τη βάση για τη λήψη αποφάσεων σε πραγματικό χρόνο.

Η τεχνολογία του **Cloud Computing** αποτελεί την κεντρική υποδομή για την αποθήκευση και τη σύνθετη επεξεργασία αυτών των πληροφοριών. Το υπολογιστικό νέφος προσφέρει την απαραίτητη κλιμακωσιμότητα (scalability) και τους υπολογιστικούς πόρους για την εκπαίδευση εξελιγμένων μοντέλων Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης. Όπως επισημαίνουν οι Singh κ.ά. (2024), οι πλατφόρμες που ενσωματώνουν το Cloud, όπως η SC-CMP, επιτρέπουν τη συνεχή παρακολούθηση και τον προγνωστικό προγραμματισμό της ενεργειακής ζήτησης, διευκολύνοντας την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας και τη διαχείριση της φόρτισης ηλεκτρικών οχημάτων (EVs).

Παρά τα πλεονεκτήματα του Cloud, η ανάγκη για απόκριση σε πραγματικό χρόνο και η μείωση της καθυστέρησης (latency) οδήγησαν στην ανάδυση του **Edge Computing**. Η επεξεργασία των δεδομένων στις «παρυφές» του δικτύου, δηλαδή κοντά στην πηγή παραγωγής τους (αισθητήρες, τοπικοί ελεγκτές), επιτρέπει την ταχύτερη λήψη αποφάσεων χωρίς να επιβαρύνεται το κεντρικό δίκτυο επικοινωνιών. Οι Diamantoulakis κ.ά. (2015) τονίζουν ότι η αποκεντρωμένη αυτή προσέγγιση είναι ζωτικής σημασίας για τη δυναμική διαχείριση ενέργειας (DEM), καθώς επιτρέπει τον άμεσο μετριασμό προβλημάτων ευστάθειας πριν αυτά επηρεάσουν το ευρύτερο δίκτυο.

Η συνέργεια μεταξύ Cloud και Edge computing δημιουργεί μια ιεραρχική αρχιτεκτονική που βελτιστοποιεί την **αυτοματοποίηση των λειτουργιών**. Ενώ το Edge διαχειρίζεται κρίσιμες λειτουργίες που απαιτούν ακαριαία δράση (π.χ. απομόνωση σφάλματος), το Cloud αναλαμβάνει τη μακροπρόθεσμη ανάλυση και τη στρατηγική βελτιστοποίηση του συστήματος. Σύμφωνα με τους Singh κ.ά. (2024), αυτή η υβριδική προσέγγιση είναι απαραίτητη για την ανθεκτικότητα των μικροδικτύων (microgrids), επιτρέποντας την αυτόνομη λειτουργία τους και την αποτελεσματική εξισορρόπηση φορτίου σε περιβάλλοντα με υψηλή διείσδυση ηλεκτρικών οχημάτων.

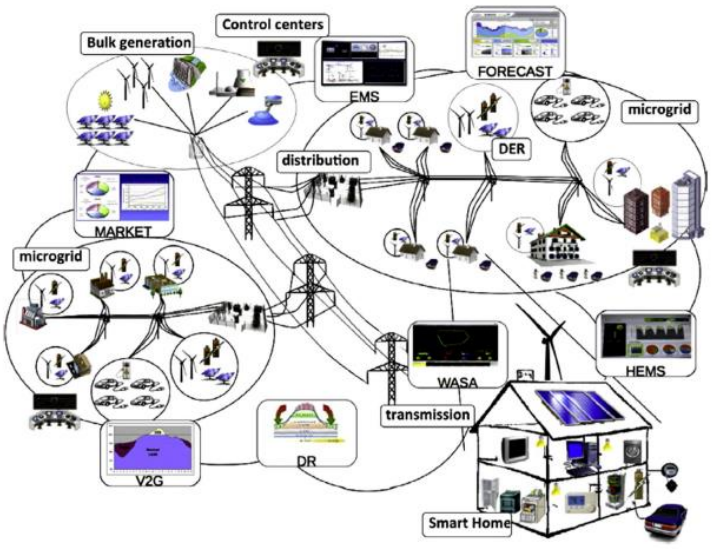
Στο πλαίσιο των Big Data, η **προγνωστική ανάλυση (predictive analytics)** παίζει καθοριστικό ρόλο στην πρόβλεψη της ζήτησης και της παραγωγής. Οι Zhang κ.ά. (2018) υποστηρίζουν ότι η αξιοποίηση δεδομένων από μετεωρολογικά συστήματα και γεωγραφικά πληροφοριακά συστήματα (GIS), σε συνδυασμό με τις μετρήσεις του δικτύου, επιτρέπει στις εταιρείες κοινής ωφέλειας να προβλέπουν τις ώρες αιχμής με μεγάλη ακρίβεια. Αυτό επιτρέπει την εφαρμογή προγραμμάτων απόκρισης ζήτησης (demand response), μειώνοντας το λειτουργικό κόστος και την ανάγκη για χρήση ρυπογόνων εφεδρικών μονάδων παραγωγής.

Η επεξεργασία των δεδομένων μέσω του **Fog Computing** (μιας ενδιάμεσης βαθμίδας μεταξύ Edge και Cloud) ενισχύει περαιτέρω την ασφάλεια και την προστασία της ιδιωτικότητας. Καθώς τα δεδομένα επεξεργάζονται τοπικά, μειώνεται η έκθεση ευαίσθητων πληροφοριών κατά τη μεταφορά τους στο διαδίκτυο. Οι Diamantoulakis κ.ά. (2015) αναφέρουν ότι η χρήση τέτοιων τεχνολογιών επιτρέπει στους καταναλωτές να συμμετέχουν ενεργά στην αγορά ενέργειας (ως "prosumers") χωρίς

να διακυβεύεται η ασφάλεια των δεδομένων τους, προάγοντας ένα πιο δημοκρατικό και αποκεντρωμένο ενεργειακό μοντέλο.

Τέλος, η ενσωμάτωση αυτών των τεχνολογιών υποστηρίζει την ανάπτυξη **αυτοματοποιημένων συστημάτων αυτο-ίασης (self-healing)**. Η ανάλυση ροών δεδομένων (stream processing) σε πραγματικό χρόνο επιτρέπει στο δίκτυο να αναγνωρίζει αυτόνομα τις ανωμαλίες και να προβαίνει σε διορθωτικές ενέργειες, όπως η αναδρομολόγηση της ισχύος. Η Singh κ.ά. (2024) τεκμηριώνουν ότι οι πλατφόρμες που βασίζονται στην Τεχνητή Νοημοσύνη μπορούν να βελτιστοποιήσουν τη χρήση των συστημάτων αποθήκευσης ενέργειας (μπαταρίες), διασφαλίζοντας την αδιάλειπτη παροχή ισχύος ακόμη και σε ακραίες συνθήκες.

Συμπερασματικά, ο συνδυασμός των Big Data, του Cloud και του Edge computing αποτελεί τη ραχοκοκαλιά της ψηφιακής μετάβασης των ενεργειακών δικτύων. Η ικανότητα επεξεργασίας και ανάλυσης δεδομένων σε διαφορετικά επίπεδα της υποδομής μετατρέπει το Smart Grid σε ένα ευφυές και προσαρμοστικό σύστημα, ικανό να ανταποκριθεί στις προκλήσεις της κλιματικής αλλαγής και της ενεργειακής αποδοτικότητας (Zhang et al., 2018).



Εικόνα 6:Η γενική διαδικασία των Big Data Analytics για τη Δυναμική Διαχείριση Ενέργειας (DEM) (Πηγή: Diamantoulakis et al., 2015)

2.3.3 Predictive analytics και ενεργειακή αποδοτικότητα

Η ψηφιοποίηση των ενεργειακών συστημάτων έχει οδηγήσει στην ανάδυση των Έξυπνων Δικτύων (Smart Grids), όπου η πληροφορία αποτελεί τον καταλύτη για τη βελτιστοποίηση της λειτουργίας τους. Σύμφωνα με τους Mahmood κ.ά. (2024), η ενσωμάτωση προηγμένων τεχνολογιών, όπως η Τεχνητή Νοημοσύνη (AI) και το Διαδίκτυο των Πραγμάτων (IoT), επιτρέπει τη μετάβαση από την απλή καταγραφή της κατανάλωσης στην προληπτική διαχείριση της ενέργειας, ενισχύοντας τη βιωσιμότητα των αποκεντρωμένων δικτύων.

Κεντρικό ρόλο στην προσπάθεια αυτή παίζουν τα **Predictive Analytics** (Προγνωστική Αναλυτική), τα οποία αξιοποιούν τον τεράστιο όγκο δεδομένων που παράγουν οι έξυπνοι μετρητές. Όπως επισημαίνουν οι Ma κ.ά. (2017), η εγκατάσταση εκατομμυρίων μετρητών παρέχει δεδομένα σε διαφορετικές χρονικές αναλύσεις, καθιστώντας αναγκαία τη χρήση αλγορίθμων μηχανικής μάθησης για την εξόρυξη πολύτιμης πληροφορίας που αφορά το προφίλ των καταναλωτών.

Η πρόβλεψη του φορτίου (load forecasting) αποτελεί τη βάση για την ενεργειακή αποδοτικότητα και την ευστάθεια του συστήματος. Οι Mahmood κ.ά. (2024) αναφέρουν ότι τεχνικές όπως η γραμμική παλινδρόμηση και η Παλινδρόμηση Διανυσμάτων Υποστήριξης (Support Vector Regression - SVR) χρησιμοποιούνται επιτυχώς για την πρόβλεψη της ζήτησης ισχύος, επιτρέποντας στους διαχειριστές να προσαρμόζουν την παραγωγή στις πραγματικές ανάγκες.

Στο πλαίσιο των ευφυών δικτύων, η ανάλυση δεδομένων επεκτείνεται και στην πρόβλεψη της παραγωγής από ανανεώσιμες πηγές ενέργειας. Σύμφωνα με τους Ma κ.ά. (2017), η ενσωμάτωση μετεωρολογικών δεδομένων και ιστορικών στοιχείων παραγωγής μέσω προγνωστικών μοντέλων είναι κρίσιμη για τη βελτιστοποίηση της έγχυσης πράσινης ενέργειας στο δίκτυο, μειώνοντας την εξάρτηση από τις ρυπογόνες μονάδες βάσης.

Η εφαρμογή στρατηγικών **Απόκρισης Ζήτησης (Demand Response - DR)** αποτελεί ένα ακόμη πεδίο όπου η προγνωστική αναλυτική επιφέρει σημαντικά οφέλη στην αποδοτικότητα. Οι Mahmood κ.ά. (2024) τονίζουν ότι η AI βελτιώνει τις στρατηγικές DR μέσω της αποτελεσματικής πρόβλεψης και διαχείρισης των φορτίων,

επιτρέποντας την αυτόματη προσαρμογή της κατανάλωσης σε ώρες αιχμής χωρίς να διακυβεύεται η άνεση των χρηστών.

Η συνέργεια του IoT με τα Συστήματα Διαχείρισης Ενέργειας (EMS) ενισχύει την ενεργειακή απόδοση μέσω του αυτοματισμού και της παρακολούθησης. Όπως σημειώνεται από τους Mahmood κ.ά. (2024), ο συνδυασμός αυτός προάγει την αειφορία, καθώς επιτρέπει τον εντοπισμό ενεργειακών απωλειών σε πραγματικό χρόνο και τη λήψη διορθωτικών μέτρων, βασισμένων σε προγνωστικά μοντέλα συμπεριφοράς.

Μια καινοτόμος προσέγγιση στην ενεργειακή αποδοτικότητα είναι η χρήση των **Ψηφιακών Διδύμων (Digital Twins)** για την προσομοίωση σεναρίων. Σύμφωνα με τους Mahmood κ.ά. (2024), τα Digital Twins βοηθούν στην ανάλυση της συμπεριφοράς του δικτύου υπό διαφορετικές συνθήκες, επιτρέποντας τη δοκιμή προγνωστικών στρατηγικών εξοικονόμησης ενέργειας πριν από την εφαρμογή τους στο πραγματικό περιβάλλον.

Η προγνωστική αναλυτική συμβάλλει επίσης καθοριστικά στη **διάγνωση και συντήρηση (predictive maintenance)** του δικτυακού εξοπλισμού. Οι Ma κ.ά. (2017) επισημαίνουν ότι ο έγκαιρος εντοπισμός ανωμαλιών και η πρόβλεψη αστοχιών μέσω της ανάλυσης δεδομένων μειώνει το λειτουργικό κόστος και διασφαλίζει την αδιάλειπτη και αποδοτική παροχή ενέργειας.

Παρά τα πλεονεκτήματα, η διαχείριση των Big Data στα ενεργειακά δίκτυα παρουσιάζει σημαντικές προκλήσεις κλιμακωσιμότητας. Οι Ma κ.ά. (2017) υπογραμμίζουν ότι οι υφιστάμενες μέθοδοι ανάλυσης συχνά αδυνατούν να ανταπεξέλθουν στην αυξανόμενη πολυπλοκότητα, απαιτώντας πιο εξελιγμένα εργαλεία στατιστικής ανάλυσης και εξόρυξης δεδομένων για την επίτευξη υψηλής ενεργειακής αποδοτικότητας.

Συμπερασματικά, ο συνδυασμός predictive analytics και αυτοματισμού αποτελεί τον μοναδικό δρόμο για τη διασφάλιση της ενεργειακής αποδοτικότητας σε ένα περιβάλλον αυξανόμενης ζήτησης. Όπως τεκμηριώνεται από τις σύγχρονες έρευνες, η ικανότητα πρόβλεψης και δυναμικής προσαρμογής είναι θεμελιώδης για τη

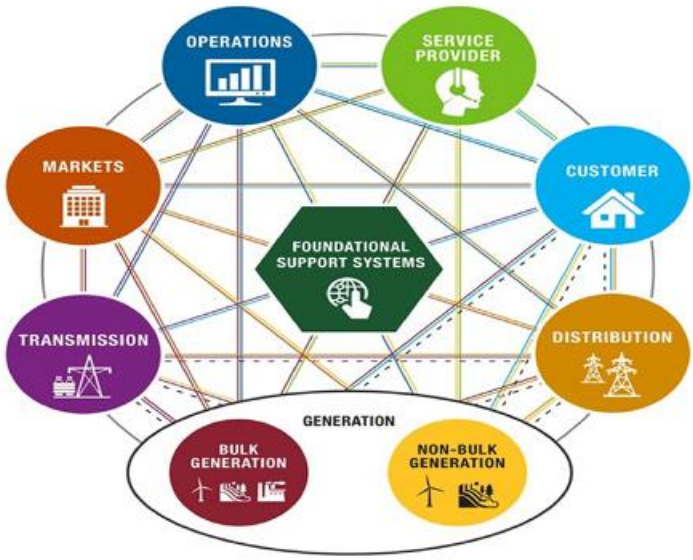
λειτουργία των έξυπνων ενεργειακών δικτύων (Mahmood et al., 2024; Ma et al., 2017).

Κεφάλαιο 3: Κυβερνοασφάλεια σε Smart Grids

3.1. Επιθέσεις σε SCADA και AMI

3.1.1 SCADA και AMI

Τα συστήματα Εποπτικού Ελέγχου και Συλλογής Δεδομένων (SCADA) αποτελούν τον πυρήνα της διαχείρισης των έξυπνων δικτύων, καθώς είναι υπεύθυνα για την παρακολούθηση και τον έλεγχο των φυσικών διεργασιών. Ωστόσο, η παραδοσιακή αρχιτεκτονική τους βασίστηκε συχνά στην απομόνωση, με αποτέλεσμα η σύγχρονη διασύνδεσή τους με το διαδίκτυο να τα εκθέτει σε σοβαρούς κινδύνους. Σύμφωνα με τους Mathas κ.ά. (2020), οι επιθέσεις σε συστήματα SCADA στοχεύουν συνήθως στην παρεμβολή των εντολών ελέγχου ή στην παραποίηση των δεδομένων τηλεμετρίας, γεγονός που μπορεί να οδηγήσει σε φυσική καταστροφή του εξοπλισμού ή σε γενικευμένες διακοπές ρεύματος.



Εικόνα 7:Περιβάλλον έξυπνου δικτύου (Πηγή:Mathas et al., 2020)

Μια ιδιαίτερα επικίνδυνη κατηγορία επιθέσεων στα συστήματα SCADA είναι οι **επιθέσεις παραπλάνησης (deception attacks)** που στοχεύουν στον εκτιμητή κατάστασης (state estimator). Όπως αναλύουν οι Teixeira κ.ά. (2010), οι επιθέσεις αυτές περιλαμβάνουν την έγχυση ψευδών δεδομένων (False Data Injection - FDI) στα

κανάλια επικοινωνίας. Ο στόχος είναι να τροποποιηθούν οι μετρήσεις με τέτοιο τρόπο ώστε το κέντρο ελέγχου να λάβει μια λανθασμένη εικόνα για την κατάσταση του δικτύου, ενώ η επίθεση παραμένει αόρατη από τους συμβατικούς μηχανισμούς ανίχνευσης κακών δεδομένων (Bad Data Detection).

Η πολυπλοκότητα των επιθέσεων FDI έγκειται στην ικανότητα του επιτιθέμενου να γνωρίζει τη συνδεσμολογία του δικτύου. Εάν ο εισβολέας κατέχει πληροφορίες για τη μήτρα τοπολογίας του συστήματος, μπορεί να κατασκευάσει «κρυφές» (stealthy) επιθέσεις που δεν προκαλούν υπολειμματικά σφάλματα στον εκτιμητή. Σύμφωνα με τους Teixeira κ.ά. (2010), αυτές οι επιθέσεις επιτρέπουν τη χειραγώγηση των ροών ισχύος και των τιμών ενέργειας, προκαλώντας οικονομική ζημία ή ακόμα και λειτουργική αστάθεια χωρίς να ηχήσει κανένας συναγερμός στο σύστημα διαχείρισης ενέργειας (EMS).

Παράλληλα, η Υποδομή Προηγμένης Μέτρησης (Advanced Metering Infrastructure - AMI) αποτελεί ένα κρίσιμο αλλά ευάλωτο σημείο εισόδου στο έξυπνο δίκτυο. Η AMI περιλαμβάνει εκατομμύρια έξυπνους μετρητές που επικοινωνούν αμφίδρομα με τον πάροχο, δημιουργώντας μια τεράστια επιφάνεια επίθεσης. Οι Mathas κ.ά. (2020) επισημαίνουν ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν φυσικές αδυναμίες των μετρητών ή κενά στα πρωτόκολλα ασύρματης επικοινωνίας για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, εκτελώντας επιθέσεις άρνησης υπηρεσίας (DoS) που παραλύουν τη συλλογή δεδομένων τιμολόγησης.

Μια συνηθισμένη απειλή για το AMI είναι οι επιθέσεις **επαναδιανομής φορτίου (load redistribution attacks)**. Σε αυτό το σενάριο, ο επιτιθέμενος παραβιάζει ένα σύνολο έξυπνων μετρητών και αναφέρει ψευδώς αυξημένη ή μειωμένη κατανάλωση σε συγκεκριμένες περιοχές. Όπως σημειώνουν οι Mathas κ.ά. (2020), η ψευδής αυτή πληροφόρηση μπορεί να αναγκάσει το σύστημα SCADA να λάβει λανθασμένες αποφάσεις αναδρομολόγησης της ενέργειας, οδηγώντας σε υπερφόρτωση γραμμών μεταφοράς και ενδεχομένως σε τοπικά blackouts.

Η χρήση μη κρυπτογραφημένων καναλιών επικοινωνίας στα παλαιότερα συστήματα SCADA επιτείνει το πρόβλημα. Οι Teixeira κ.ά. (2010) υπογραμμίζουν ότι η έλλειψη αυθεντικοποίησης επιτρέπει σε έναν εξελιγμένο επιτιθέμενο να εκτελέσει επιθέσεις τύπου man-in-the-middle, υποκλέπτοντας και τροποποιώντας τις μετρήσεις πριν

αυτές φτάσουν στον εκτιμητή κατάστασης. Η τρωτότητα αυτή καθιστά επιτακτική την υιοθέτηση ισχυρών πρωτοκόλλων ασφαλείας και την κρυπτογράφηση των δεδομένων από το σημείο μέτρησης έως το κέντρο ελέγχου.

Επιπλέον, οι επιθέσεις στο AMI μπορούν να χρησιμοποιηθούν ως εφαλτήριο για την κλιμάκωση της επίθεσης προς το κεντρικό δίκτυο. Η διασύνδεση των μετρητών με τα οικιακά δίκτυα (Home Area Networks - HAN) εισάγει επιπλέον κινδύνους, καθώς μια παραβιασμένη οικιακή συσκευή IoT μπορεί να χρησιμοποιηθεί για τη διάδοση κακόβουλου λογισμικού (malware) στο ευρύτερο δίκτυο AMI. Σύμφωνα με τους Mathas κ.ά. (2020), η έλλειψη ενιαίων προτύπων ασφαλείας στις συσκευές αυτές καθιστά την AMI την «αχίλλειο πτέρνα» της κυβερνοασφάλειας των έξυπνων δικτύων.

Η ανθεκτικότητα έναντι αυτών των επιθέσεων απαιτεί την ανάπτυξη προηγμένων συστημάτων ανίχνευσης εισβολών (IDS) που βασίζονται σε φυσικά μοντέλα του δικτύου. Οι Teixeira κ.ά. (2010) προτείνουν τη χρήση τεχνικών που αναλύουν τη συνέπεια των μετρήσεων με βάση τους νόμους του Kirchhoff, ώστε να εντοπίζονται FDI επιθέσεις που παρακάμπτουν τους στατιστικούς ελέγχους. Η συνδυασμένη ανάλυση δεδομένων από το SCADA και το AMI μπορεί να προσφέρει μια πιο ολιστική προσέγγιση στην ανίχνευση ανωμαλιών, θωρακίζοντας το δίκτυο από συντονισμένες κυβερνοεπιθέσεις.

Τέλος, η ανθρώπινη συνιστώσα και οι επιθέσεις κοινωνικής μηχανικής (social engineering) παραμένουν σημαντικοί παράγοντες κινδύνου για την ασφάλεια των συστημάτων ελέγχου. Η απόκτηση διαπιστευτηρίων πρόσβασης σε έναν σταθμό εργασίας SCADA μπορεί να επιτρέψει σε έναν επιτιθέμενο να παρακάμψει όλα τα τεχνικά μέτρα προστασίας. Οι Mathas κ.ά. (2020) τονίζουν ότι η κυβερνοασφάλεια των Smart Grids δεν είναι μόνο τεχνικό ζήτημα, αλλά απαιτεί τη συνεχή εκπαίδευση του προσωπικού και την αυστηρή τήρηση πολιτικών ασφαλείας σε όλα τα επίπεδα της ιεραρχίας του δικτύου.

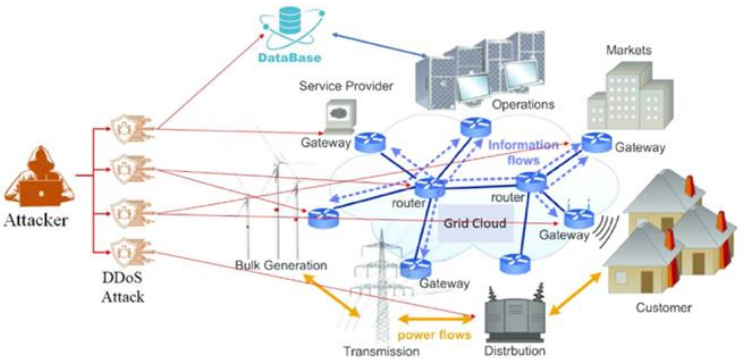
Συμπερασματικά, οι επιθέσεις σε SCADA και AMI αντιπροσωπεύουν μια υπαρξιακή απειλή για τη λειτουργία των έξυπνων δικτύων. Η κατανόηση των μηχανισμών επίθεσης, όπως οι FDI και DoS, είναι θεμελιώδης για τον σχεδιασμό ανθεκτικών

υποδομών που θα μπορούν να αντέξουν και να ανακάμψουν από εξελιγμένες κυβερνοαπειλές (Mathas et al., 2020; Teixeira et al., 2010).

3.1.2. Malware, ransomware, DoS/DDoS

Η σύγκλιση των λειτουργικών τεχνολογιών (OT) με τα δίκτυα πληροφορικής (IT) στα έξυπνα δίκτυα έχει αυξήσει σημαντικά την έκθεση των συστημάτων SCADA και των υποδομών AMI σε εξελιγμένες κυβερνοαπειλές, με τις επιθέσεις τύπου Malware, Ransomware και DoS/DDoS να αποτελούν τις σημαντικότερες απειλές για τη διαθεσιμότητα και την ακεραιότητα του δικτύου. Το κακόβουλο λογισμικό (Malware) και ειδικότερα το Ransomware στοχεύουν στον έλεγχο ή την κρυπτογράφηση κρίσιμων δεδομένων στα κέντρα ελέγχου, διεισδύοντας στα συστήματα SCADA μέσω μολυσμένων συσκευών ή phishing και στοχεύοντας σε πρωτόκολλα επικοινωνίας όπως το IEC 60870-5-104. Μόλις εγκατασταθούν, αυτές οι απειλές μπορούν να προκαλέσουν αλλοίωση των εντολών ελέγχου ή να «παγώσουν» τη λειτουργία του δικτύου απαιτώντας λύτρα (Dokku et al., 2025). Παράλληλα, στο επίπεδο της υποδομής AMI, το κακόβουλο λογισμικό μπορεί να μολύνει έξυπνους μετρητές, επιτρέποντας στους εισβολείς να αποκτούν μη εξουσιοδοτημένη πρόσβαση και να προκαλούν τοπικές διακοπές ή παραποίηση των δεδομένων χρέωσης (Ahmed et al., 2025).

Όσον αφορά τις επιθέσεις DoS και DDoS, αυτές στοχεύουν στην εξάντληση των πόρων του δικτύου επικοινωνίας, αποτελώντας σοβαρές απειλές κατά της διαθεσιμότητας των συστημάτων. Οι εισβολείς κατακλύζουν τους διακομιστές SCADA ή τους κόμβους AMI με τεράστιο όγκο αιτημάτων, εμποδίζοντας τη μεταφορά κρίσιμων μετρήσεων σε πραγματικό χρόνο, γεγονός που έχει ως αποτέλεσμα την απώλεια ορατότητας του δικτύου από τους χειριστές (Hasan et al., 2023). Λόγω της κρισιμότητας των χρόνων απόκρισης στα Smart Grids, μια επίθεση DoS μπορεί να καθυστερήσει τη λήψη αποφάσεων προστασίας, οδηγώντας σε αστάθεια ή ακόμα και σε ολική κατάρρευση μέσω ενός γενικευμένου blackout (Ahmed et al., 2025).



Εικόνα 8:Επίθεση DDoS σε έξυπνο δίκτυο(Πηγή:Hasan et al., 2023).

3.1.3. Ταξινόμηση και Αντιμετώπιση

Η αποτελεσματική αντιμετώπιση των σύγχρονων κυβερνοαπειλών στα έξυπνα δίκτυα επιβάλλει την υιοθέτηση μιας πολυεπίπεδης άμυνας, η οποία βασίζεται στον στρατηγικό συνδυασμό της κρυπτογράφησης και της τεχνητής νοημοσύνης. Στο πλαίσιο αυτό, η χρήση προηγμένων αλγορίθμων Μηχανικής Μάθησης (ML), όπως το Random Forest, ενσωματώνεται στα Συστήματα Ανίχνευσης Εισβολών (IDS) για τον εντοπισμό ανώμαλης κυκλοφορίας που υποδηλώνει την έναρξη μιας επίθεσης DDoS με εξαιρετική ακρίβεια (Dokku et al., 2025). Παράλληλα, η ενίσχυση της κρυπτογραφικής ανθεκτικότητας μέσω της εφαρμογής δυναμικών τεχνικών (όπως το πρότυπο AES-256 με χρήση κλειδιών BLAKE3), διασφαλίζει ότι ακόμα και σε περίπτωση που ένας εισβολέας αποκτήσει πρόσβαση στο κανάλι επικοινωνίας του συστήματος SCADA, δεν θα διαθέτει τη δυνατότητα να εισάγει κακόβουλο κώδικα ή να προβεί σε υποκλοπή δεδομένων (Dokku et al., 2025).

3.1.4. Απειλές στα συστήματα ελέγχου και μέτρησης

Η ενσωμάτωση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στα συστήματα ελέγχου SCADA και μέτρησης AMI έχει μετατρέψει το παραδοσιακό ηλεκτρικό δίκτυο σε ένα σύνθετο κυβερνο-φυσικό σύστημα, εκθέτοντάς το ταυτόχρονα σε πληθώρα νέων απειλών. Σύμφωνα με τους Szczepaniuk και Szczepaniuk (2025), η κύρια πρόκληση έγκειται στην ανάγκη εξισορρόπησης της διαθεσιμότητας του συστήματος με την ακεραιότητα των δεδομένων. Οι απειλές στα συστήματα αυτά δεν στοχεύουν πλέον μόνο στην κλοπή πληροφοριών, αλλά και στην άμεση παρέμβαση στις φυσικές διεργασίες παραγωγής και διανομής ενέργειας.

Οι επιθέσεις στα συστήματα **SCADA** επικεντρώνονται συχνά στην παραβίαση των πρωτοκόλλων επικοινωνίας μεταξύ των Κεντρικών Τερματικών Μονάδων (MTU) και των Απομακρυσμένων Μονάδων (RTU). Όπως επισημαίνουν οι Szczepaniuk και Szczepaniuk (2025), οι επιτιθέμενοι εκμεταλλεύονται την έλλειψη ισχυρής κρυπτογράφησης σε παλαιότερα βιομηχανικά πρωτόκολλα (όπως το Modbus), εκτελώντας επιθέσεις τύπου "Man-in-the-Middle" (MitM). Αυτό τους επιτρέπει να υποκλέπτουν εντολές ελέγχου ή να στέλνουν ψευδή σήματα απενεργοποίησης διακοπτών, προκαλώντας αστάθεια στο δίκτυο.

Μια ιδιαίτερα κρίσιμη απειλή είναι η **έγχυση ψευδών δεδομένων (False Data Injection - FDI)**, η οποία στοχεύει στην αλλοίωση των μετρήσεων που λαμβάνει ο εκτιμητής κατάστασης του δικτύου. Σύμφωνα με τους Nambundo κ.ά. (2025), αυτές οι επιθέσεις μπορούν να παραπλανήσουν τους διαχειριστές του συστήματος SCADA, κάνοντάς τους να πιστεύουν ότι το δίκτυο λειτουργεί εντός ασφαλών ορίων, ενώ στην πραγματικότητα βρίσκεται σε κατάσταση υπερφόρτωσης. Η πολυπλοκότητα αυτών των επιθέσεων καθιστά τον εντοπισμό τους εξαιρετικά δύσκολο από τους συμβατικούς μηχανισμούς ανίχνευσης σφαλμάτων.

Στο επίπεδο της υποδομής **AMI**, οι έξυπνοι μετρητές αποτελούν το πιο εκτεθειμένο σημείο του δικτύου. Οι Nambundo κ.ά. (2025) υπογραμμίζουν ότι οι μετρητές είναι ευάλωτοι σε επιθέσεις φυσικής πρόσβασης και παρεμβολής στο υλικολογισμικό τους (firmware manipulation). Μια παραβιασμένη συσκευή μέτρησης μπορεί να χρησιμοποιηθεί για την αναφορά ψευδών στοιχείων κατανάλωσης, οδηγώντας σε οικονομική απάτη ή σε λανθασμένο υπολογισμό του φορτίου αιχμής από το κέντρο ελέγχου.

Οι επιθέσεις **Άρνησης Υπηρεσίας (Distributed Denial of Service - DDoS)** αποτελούν μια συνεχή απειλή για τα δίκτυα μέτρησης. Όπως αναλύουν οι Szczepaniuk και Szczepaniuk (2025), ο κατακλυσμός των πυλών επικοινωνίας (gateways) του AMI με τεράστιο όγκο δεδομένων μπορεί να παραλύσει τη ροή πληροφοριών προς τον πάροχο. Αυτή η διακοπή στερεί από τους διαχειριστές την ορατότητα σε πραγματικό χρόνο, εμποδίζοντας την εφαρμογή κρίσιμων λειτουργιών όπως η απόκριση ζήτησης (demand response) και ο εντοπισμός σφαλμάτων.

Η εξάπλωση του **κακόβουλου λογισμικού (malware)** ειδικά σχεδιασμένου για βιομηχανικά συστήματα ελέγχου αποτελεί μια αυξανόμενη ανησυχία. Σύμφωνα με τους Szczepaniuk και Szczepaniuk (2025), απειλές όπως το ransomware μπορούν να κλειδώσουν την πρόσβαση σε κρίσιμες διεπαφές HMI (Human-Machine Interface), καθιστώντας αδύνατο τον έλεγχο των υποσταθμών από τους χειριστές. Η διασύνδεση των συστημάτων ελέγχου με τα εταιρικά δίκτυα IT αυξάνει την πιθανότητα διείσδυσης τέτοιων απειλών μέσω επιθέσεων ηλεκτρονικού ψαρέματος (phishing).

Επιπλέον, η υποδομή AMI αντιμετωπίζει απειλές που σχετίζονται με το **απόρρητο των δεδομένων**. Οι Nambundo κ.ά. (2025) επισημαίνουν ότι η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα κατανάλωσης των έξυπνων μετρητών μπορεί να αποκαλύψει προσωπικές συνήθειες και πρότυπα ζωής των χρηστών. Η απειλή αυτή απαιτεί την υιοθέτηση ισχυρών πρωτοκόλλων αυθεντικοποίησης και κρυπτογράφησης από άκρο σε άκρο (end-to-end encryption), προκειμένου να διασφαλιστεί η εμπιστευτικότητα των πληροφοριών.

Οι **απειλές εκ των έσω (insider threats)** παραμένουν ένας από τους πιο δύσκολα αντιμετωπίσιμους κινδύνους για τα συστήματα SCADA. Όπως αναφέρουν οι Szczepaniuk και Szczepaniuk (2025), άτομα με νόμιμη πρόσβαση στα συστήματα ελέγχου μπορούν να προκαλέσουν σκόπιμη βλάβη ή να εισάγουν κενά ασφαλείας χωρίς να γίνουν άμεσα αντιληπτά. Η αντιμετώπιση αυτής της απειλής απαιτεί αυστηρούς ελέγχους πρόσβασης και συνεχή παρακολούθηση της δραστηριότητας των χρηστών μέσω συστημάτων ανίχνευσης εισβολών (IDS).

Η σύγκλιση των δικτύων AMI και SCADA δημιουργεί επίσης τον κίνδυνο **αλυσιδωτών επιθέσεων**. Σύμφωνα με τους Nambundo κ.ά. (2025), μια παραβίαση στο επίπεδο των έξυπνων μετρητών μπορεί να χρησιμοποιηθεί ως σημείο εισόδου για την κλιμάκωση της επίθεσης προς το κεντρικό σύστημα διαχείρισης ενέργειας. Η έλλειψη επαρκούς κατάτμησης (segmentation) μεταξύ των διαφορετικών επιπέδων του δικτύου διευκολύνει την οριζόντια μετακίνηση των επιτιθέμενων εντός της υποδομής.

Συνοψίζοντας, οι απειλές στα συστήματα ελέγχου και μέτρησης είναι πολυδιάστατες και εξελίσσονται διαρκώς. Η προστασία των υποδομών SCADA και AMI απαιτεί μια ολιστική προσέγγιση κυβερνοασφάλειας που συνδυάζει προηγμένα τεχνικά μέτρα,

όπως η κρυπτογράφηση και η τεχνητή νοημοσύνη για την ανίχνευση ανωμαλιών, με ισχυρές πολιτικές ασφαλείας και εκπαίδευση του προσωπικού (Szczepaniuk & Szczepaniuk, 2025; Nambundo et al., 2025).

3.1.5. Επιπτώσεις σε λειτουργία και αξιοπιστία

Η ενσωμάτωση των συστημάτων SCADA και της υποδομής AMI αποτελεί τη ραχοκοκαλιά του Έξυπνου Δικτύου, ωστόσο η εξάρτηση από τις τεχνολογίες πληροφορικής και επικοινωνιών διευρύνει την επιφάνεια επίθεσης. Οι επιθέσεις σε αυτά τα κρίσιμα συστήματα δεν έχουν μόνο ψηφιακές προεκτάσεις, αλλά επηρεάζουν άμεσα τη φυσική λειτουργία και την αξιοπιστία της ενεργειακής παροχής. Σύμφωνα με τους Angara κ.ά. (2025), οι επιπτώσεις των κυβερνοεπιθέσεων είναι πολυεπίπεδες, περιλαμβάνοντας λειτουργικές διαταραχές, οικονομικές απώλειες και, σε ακραίες περιπτώσεις, μόνιμες ζημιές στις υποδομές.

Στο επιχειρησιακό επίπεδο, οι επιθέσεις σε συστήματα SCADA/AMI υπονομεύουν την ικανότητα του δικτύου να παρέχει κρίσιμες υπηρεσίες. Η μετάβαση προς ένα αποκεντρωμένο μοντέλο με αυξημένη χρήση ανανεώσιμων πηγών ενέργειας (DERs) καθιστά το δίκτυο πιο ευάλωτο σε προβλήματα ευστάθειας. Οι Angara κ.ά. (2025) επισημαίνουν ότι οποιαδήποτε κακόβουλη παρέμβαση στα συστήματα ελέγχου μπορεί να οδηγήσει σε απώλεια του συντονισμού των κατανεμημένων πόρων, θέτοντας σε κίνδυνο την ανθεκτικότητα του συνολικού συστήματος ισχύος.

Μια από τις πιο κρίσιμες επιπτώσεις στην αξιοπιστία αφορά τις επιθέσεις σε συστήματα κλειστού βρόχου (closed-loop controls). Σύμφωνα με τους Tan κ.ά. (2016), οι επιθέσεις ακεραιότητας που στοχεύουν στην τιμολόγηση πραγματικού χρόνου (Real-Time Pricing - RTP) μπορούν να αποσταθεροποιήσουν πλήρως το σύστημα. Η χειραγώγηση των σημάτων τιμής επηρεάζει τη συμπεριφορά των καταναλωτών και των αυτοματοποιημένων συστημάτων διαχείρισης φορτίου, δημιουργώντας μια επικίνδυνη ανατροφοδότηση που κλονίζει την ισορροπία προσφοράς και ζήτησης.

Η ανάλυση των Tan κ.ά. (2016) καταδεικνύει ότι επιθέσεις τύπου «scaling» και «delay» μπορούν να έχουν καταστροφικές συνέπειες. Μικρές, αλλά στοχευμένες τροποποιήσεις στα σήματα τιμολόγησης ενδέχεται να ενισχυθούν επαναληπτικά μέσω

του κλειστού βρόχου ελέγχου, οδηγώντας σε ακραίες διακυμάνσεις της ζήτησης. Αυτή η τεχνητή αστάθεια καθιστά τη λειτουργία του δικτύου μη προβλέψιμη, υποβαθμίζοντας την αξιοπιστία των παρεχόμενων υπηρεσιών προς τους τελικούς χρήστες.

Επιπλέον, η λειτουργική αναποτελεσματικότητα αποτελεί άμεσο επακόλουθο της παραβίασης της ακεραιότητας των δεδομένων. Όταν οι τιμές ενέργειας παραποιούνται κακόβουλα, οι καταναλωτές δεν έχουν τα κατάλληλα κίνητρα για τον περιορισμό της ζήτησης κατά τις ώρες αιχμής. Οι Tan κ.ά. (2016) σημειώνουν ότι αυτό οδηγεί σε υπερβολική καταπόνηση της υποδομής και αδικαιολόγητη αύξηση του λειτουργικού κόστους, καθώς το σύστημα αναγκάζεται να λειτουργεί κοντά στα όρια των δυνατοτήτων του χωρίς πραγματική ανάγκη.

Η πιο σοβαρή επίπτωση στην αξιοπιστία του δικτύου είναι η πρόκληση εκτεταμένων διακοπών ρεύματος (blackouts). Οι συντονισμένες επιθέσεις ακεραιότητας μπορούν να ωθήσουν το σύστημα σε καταστάσεις αστοχίας που υπερβαίνουν τους μηχανισμούς προστασίας. Όπως υπογραμμίζουν οι Tan κ.ά. (2016), η κακόβουλη ενίσχυση της ζήτησης μέσω παραπλανητικών σημάτων τιμής μπορεί να προκαλέσει υπερφόρτωση των γραμμών μεταφοράς, οδηγώντας σε αλυσιδωτές καταρρεύσεις της φυσικής υποδομής.

Στο επίπεδο της διανομής, η παραβίαση της υποδομής AMI επηρεάζει άμεσα τη διαχείριση του φορτίου και την ενσωμάτωση των DER. Οι Angara κ.ά. (2025) αναφέρουν ότι οι επιθέσεις σε έξυπνους μετρητές και ελεγκτές απόκρισης ζήτησης (demand response) διαταράσσουν την ορατότητα των διαχειριστών στο «τελευταίο μίλι» του δικτύου. Χωρίς ακριβή δεδομένα κατανάλωσης, η λήψη αποφάσεων για την αναδρομολόγηση της ισχύος γίνεται ανακριβής, αυξάνοντας την πιθανότητα τοπικών βλαβών.

Παράλληλα, οι επιθέσεις στα συστήματα SCADA στον τομέα των επιχειρήσεων (Operations domain) στερούν από τους χειριστές την απαραίτητη επίγνωση της κατάστασης (situational awareness). Η παραποίηση των δεδομένων τηλεμετρίας από μονάδες PMU ή RTU μπορεί να αποκρύψει ενεργά σφάλματα ή να υποδείξει ψευδείς ανωμαλίες. Αυτό έχει ως αποτέλεσμα την καθυστερημένη ή λανθασμένη

ανταπόκριση των διαχειριστών σε πραγματικά περιστατικά, υπονομεύοντας την επιχειρησιακή συνέχεια του οργανισμού (Angara et al., 2025).

Εκτός από τις τεχνικές αστοχίες, οι επιθέσεις στο AMI πλήττουν την εμπιστοσύνη των καταναλωτών μέσω της παραβίασης της ιδιωτικότητας και της ακρίβειας της τιμολόγησης. Σύμφωνα με τους Angara κ.ά. (2025), η απώλεια εμπιστοσύνης μπορεί να οδηγήσει σε μειωμένη συμμετοχή σε προγράμματα έξυπνης διαχείρισης, γεγονός που έμμεσα επηρεάζει τη μακροπρόθεσμη αξιοπιστία και την αποδοτικότητα του δικτύου. Η κυβερνοασφάλεια, συνεπώς, συνδέεται άρρηκτα με την κοινωνική αποδοχή των τεχνολογιών του Έξυπνου Δικτύου.

Συνοψίζοντας, οι επιπτώσεις των επιθέσεων σε SCADA και AMI είναι πολυδιάστατες και απειλούν τον πυρήνα της αποστολής των ενεργειακών δικτύων. Η διασφάλιση της αξιοπιστίας απαιτεί μια ολιστική προσέγγιση που να προστατεύει όχι μόνο τα δεδομένα, αλλά και τη δυναμική ευστάθεια των συστημάτων ελέγχου. Η κατανόηση αυτών των επιπτώσεων είναι θεμελιώδης για τον σχεδιασμό ανθεκτικών υποδομών ικανών να αντεπεξέλθουν σε εξελιγμένες κυβερνοαπειλές (Tan et al., 2016; Angara et al., 2025).

3.2.Επιθέσεις σε IoT συσκευές

3.2.1. Botnets, spoofing, unauthorized access

Η ραγδαία εξάπλωση των συσκευών του Διαδικτύου των Πραγμάτων (IoT) έχει δημιουργήσει ένα διευρυμένο πεδίο επιθέσεων, καθώς πολλές από αυτές τις συσκευές στερούνται ισχυρών μηχανισμών ασφαλείας λόγω περιορισμένης υπολογιστικής ισχύος και κόστους. Οι κυριότερες απειλές περιλαμβάνουν τη δημιουργία δικτύων botnets, τις επιθέσεις spoofing και τη μη εξουσιοδοτημένη πρόσβαση (Stojnic et al., 2025).

Τα botnets αποτελούν μία από τις πιο σοβαρές απειλές για το οικοσύστημα του Διαδικτύου των Πραγμάτων (IoT), καθώς αποτελούν δίκτυα μολυσμένων συσκευών (bots) που ελέγχονται εξ αποστάσεως από έναν επιτιθέμενο, γνωστό και ως botmaster. Ο μηχανισμός λειτουργίας τους βασίζεται στη μόλυνση των συσκευών IoT με κακόβουλο λογισμικό (malware), όπως τα διαβόητα Mirai και BASHLITE, τα

οποία έχουν την ικανότητα να σαρώνουν το διαδίκτυο για τον εντοπισμό συσκευών που διαθέτουν ακόμη τους εργοστασιακούς κωδικούς πρόσβασης ή άλλες γνωστές ευπάθειες (Meidan et al., 2018).

Μόλις σχηματιστεί το botnet, χρησιμοποιείται συνήθως για τη διεξαγωγή επιθέσεων κατανεμημένης άρνησης εξυπηρέτησης (Distributed Denial-of-Service - DDoS) μεγάλης κλίμακας, οι οποίες έχουν τη δύναμη να παραλύσουν κρίσιμες υποδομές ή υπηρεσίες (Gelgi et al., 2024). Λόγω του ότι η πολυπλοκότητα αυτών των επιθέσεων αυξάνεται συνεχώς, καθίσταται πλέον επιτακτική η ανάγκη για τη χρήση προηγμένων τεχνικών ανίχνευσης που βασίζονται στην τεχνητή νοημοσύνη, όπως οι Deep Autoencoders, οι οποίοι μπορούν να αναγνωρίζουν ύποπτα μοτίβα κίνησης στο δίκτυο (Meidan et al., 2018).

Επιθέσεις Spoofing

Το spoofing (πλαστογράφηση) αφορά την προσπάθεια ενός επιτιθέμενου να υποδυθεί μια έγκυρη συσκευή ή χρήστη στο δίκτυο για να αποκτήσει πρόσβαση σε δεδομένα ή να παρακάμψει ελέγχους ασφαλείας.

- **ARP Spoofing:** Μια κοινή τεχνική όπου ο επιτιθέμενος στέλνει ψευδή μηνύματα ARP στο τοπικό δίκτυο, συνδέοντας τη δική του διεύθυνση MAC με τη διεύθυνση IP μιας νόμιμης συσκευής. Αυτό επιτρέπει την υποκλοπή ή την τροποποίηση της κίνησης του δικτύου (Almousa et al., 2025).
- **IP/GPS Spoofing:** Ειδικότερα σε δορυφορικά δίκτυα IoT, οι επιθέσεις spoofing μπορούν να παραπλανήσουν τα συστήματα πλοήγησης ή συγχρονισμού, οδηγώντας σε εσφαλμένη λήψη αποφάσεων από τις αυτόνομες συσκευές (Stojnic et al., 2025).

Μη Εξουσιοδοτημένη Πρόσβαση (Unauthorized Access)

Η μη εξουσιοδοτημένη πρόσβαση αποτελεί το θεμέλιο για τις περισσότερες IoT επιθέσεις και προκύπτει από την αδυναμία των μηχανισμών ελέγχου πρόσβασης και ταυτοποίησης.

- **Αιτίες:** Η χρήση προκαθορισμένων (default) κωδικών πρόσβασης και η έλλειψη κρυπτογράφησης καθιστούν τις συσκευές ευάλωτες σε brute-force επιθέσεις ή σε μη εξουσιοδοτημένη είσοδο στο σύστημα (Jin et al., 2024).
- **Μοντελοποίηση Απειλών:** Το πλαίσιο **I3TM** (IoT Targeting-Threat Modeling) αναλύει τις τακτικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν αρχική πρόσβαση, να διατηρήσουν την παρουσία τους στο σύστημα και να κλιμακώσουν τα προνόμιά τους, υπογραμμίζοντας ότι η μη εξουσιοδοτημένη πρόσβαση είναι συχνά το πρώτο στάδιο μιας ευρύτερης επίθεσης botnet (Jin et al., 2024).

Η ανίχνευση επιθέσεων botnet και spoofing στο περιβάλλον του IoT απαιτεί εξελιγμένα εργαλεία, καθώς οι παραδοσιακές μέθοδοι που βασίζονται σε υπογραφές αποτυγχάνουν να εντοπίσουν νέες παραλλαγές κακόβουλου λογισμικού, καθιστώντας τη χρήση της Μηχανικής Μάθησης (ML) και της Βαθιάς Μάθησης (DL) την πλέον αποτελεσματική λύση. Συγκεκριμένα, μοντέλα όπως τα Convolutional Neural Networks (CNN) και οι Deep Autoencoders επιτρέπουν την ανάλυση στιγμιοτύπων συμπεριφοράς του δικτύου για τη διάκριση της κανονικής κίνησης από την ανώμαλη δραστηριότητα που προκαλείται από την εξάπλωση ενός botnet σε πραγματικό χρόνο, διευκολύνοντας την έγκαιρη απομόνωση των μολυσμένων συσκευών (Almousa et al., 2025; Meidan et al., 2018).

3.2.2. Επιπτώσεις σε δίκτυα και υπηρεσίες.

Η εκτεταμένη ενσωμάτωση των συσκευών του Διαδικτύου των Πραγμάτων (IoT) στην καθημερινότητα και στις κρίσιμες υποδομές έχει διευρύνει σημαντικά την **επιφάνεια επίθεσης** (attack surface). Λόγω των εγγενών περιορισμών στην υπολογιστική τους ισχύ και των ελλιπών μηχανισμών ασφαλείας, οι συσκευές αυτές καθίστανται ευάλωτες στην επιστράτευσή τους σε εκτενή δίκτυα **botnets**. Οι συνέπειες των επιθέσεων αυτών στα δίκτυα επικοινωνιών και στις παρεχόμενες υπηρεσίες είναι πολυδιάστατες, επηρεάζοντας τόσο την επιχειρησιακή αρτιότητα των συστημάτων όσο και την οικονομική τους βιωσιμότητα.

Συμφόρηση Δικτύου και Εξάντληση Πόρων

Η κυριότερη επίπτωση των IoT botnets εντοπίζεται στη διεξαγωγή επιθέσεων Κατανεμημένης Άρνησης Εξυπηρέτησης (DDoS). Οι επιθέσεις αυτές στοχεύουν στον κατακλυσμό των δικτυακών υποδομών με υπερβολικό όγκο κακόβουλης κίνησης, προκαλώντας κορεσμό του εύρους ζώνης (bandwidth).

Λειτουργική Κατάρρευση:Η ταυτόχρονη αποστολή αιτημάτων από χιλιάδες παραβιασμένες συσκευές προς έναν διακομιστή ή μια πύλη (gateway) παρεμποδίζει την πρόσβαση των νόμιμων χρηστών. Αυτή η «πλημμυρίδα» δεδομένων επιφέρει την εξάντληση των κεντρικών υπολογιστικών πόρων (CPU, μνήμη), οδηγώντας σε μη διαθεσιμότητα των υπηρεσιών (Gelgi et al., 2024).

Κλιμάκωση Επιπτώσεων: Σύμφωνα με τον Lernefalk (2021), ακόμη και μια περιορισμένη διείσδυση σε συσκευές ενός τοπικού ασύρματου δικτύου (WLAN) δύναται να υποβαθμίσει την Ποιότητα Υπηρεσίας (QoS), αυξάνοντας την καθυστέρηση (latency) και προκαλώντας απώλεια πακέτων για το σύνολο των συνδεδεμένων χρηστών.

Υποβάθμιση Κρίσιμων Υπηρεσιών και Αυτοματισμών

Στο πλαίσιο των έξυπνων δικτύων και των βιομηχανικών συστημάτων ελέγχου, η διαθεσιμότητα των υπηρεσιών συνδέεται άρρηκτα με την ασφάλεια και τη λειτουργική συνέχεια.

- **Διακοπή Επιχειρησιακής Λειτουργίας:** Οι επιθέσεις DoS/DDoS παρεμβάλλονται στη μετάδοση κρίσιμων μετρήσεων και εντολών σε πραγματικό χρόνο. Αυτό ενδέχεται να προκαλέσει αστάθεια σε υπηρεσίες κοινής ωφέλειας, καθώς οι διαχειριστές στερούνται την απαραίτητη ορατότητα και τον έλεγχο των απομακρυσμένων κόμβων (de Caldas Filho et al., 2023).
- **Συστημικές Αλυσιδωτές Αντιδράσεις:** Μια στοχευμένη επίθεση σε μια μεμονωμένη υπηρεσία IoT (π.χ. έξυπνη διαχείριση ενέργειας) μπορεί να επιφέρει κλυδωνισμούς σε ολόκληρη την εφοδιαστική αλυσίδα, προκαλώντας δυσλειτουργίες σε διασυνδεδεμένα συστήματα που βασίζονται στην ακεραιότητα και την έγκαιρη λήψη των δεδομένων (Gelgi et al., 2024).

Οικονομικές Προεκτάσεις και Διάβρωση της Εμπιστοσύνης

Οι συνέπειες υπερβαίνουν το τεχνικό επίπεδο, προκαλώντας σημαντική οικονομική επιβάρυνση και πλήττοντας την αξιοπιστία των τεχνολογιών.

- **Κόστος Αποκατάστασης:** Η διακοπή λειτουργίας μεταφράζεται σε άμεσες οικονομικές απώλειες, απορρέουσες από την απώλεια παραγωγικότητας και το υψηλό κόστος ανίχνευσης, μετριασμού (mitigation) και αποκατάστασης των πληγεισών υποδομών (Gelgi et al., 2024).
- **Φήμη και Αξιοπιστία:** Η συστηματική υποβάθμιση των υπηρεσιών κλονίζει την εμπιστοσύνη των καταναλωτών και των επιχειρήσεων στο οικοσύστημα του IoT. Η ανάγκη αυτή επιβάλλει την υιοθέτηση καινοτόμων μοντέλων προστασίας, όπως η **Ομοσπονδιακή Μάθηση (Federated Learning)**, η οποία επιτρέπει την αποκεντρωμένη ανίχνευση απειλών χωρίς την επιβάρυνση του κεντρικού δικτύου (de Caldas Filho et al., 2023).

Δικτυακή Αστάθεια και Μηχανισμοί Διάδοσης

Τα botnets χαρακτηρίζονται από την ικανότητα αυτο-αναπαραγωγής, καταναλώνοντας πόρους για τη σάρωση (scanning) και τη μόλυνση νέων στόχων. Αυτή η διαρκής δραστηριότητα σάρωσης δεσμεύει πολύτιμους πόρους της υποδομής ακόμη και σε περιόδους ύφεσης των επιθέσεων, μειώνοντας τη συνολική αποδοτικότητα και τη σταθερότητα του δικτύου (Lernefalk, 2021).

3.2.3 Παραδείγματα πραγματικών περιστατικών

Στην παρούσα υποενότητα επιχειρείται η επισκόπηση ορισμένων εκ των πλέον καθοριστικών επιθέσεων σε συσκευές του Διαδικτύου των Πραγμάτων (IoT). Τα περιστατικά αυτά λειτούργησαν ως καταλύτες για την ανάδειξη των δομικών τρωτοτήτων των σύγχρονων δικτύων, υπογραμμίζοντας παράλληλα την επιτακτική ανάγκη για την ανάπτυξη προηγμένων μεθοδολογιών ψηφιακής εγκληματολογίας (digital forensics). Η διαχρονική μελέτη των εν λόγω επιθέσεων προσφέρει μια σαφή εικόνα για την εξελικτική πορεία των απειλών: από τις πρωτόλειες μορφές μόλυνσης έως τα σύνθετα, κλιμακούμενα δίκτυα botnet που δύνανται να κλονίσουν την παγκόσμια ψηφιακή σταθερότητα.

Το Φαινόμενο Mirai (2016): Σημείο Καμπής για την Ασφάλεια του IoT

Η ανάδυση του botnet Mirai το 2016 συνιστά ορόσημο στην ιστορία της κυβερνοασφάλειας, καθώς εγκαινίασε μια νέα εποχή επιθέσεων μαζικής κλίμακας (Chee et al., 2025). Η επίθεση Κατανεμημένης Άρνησης Εξυπηρέτησης (DDoS) που εξαπολύθηκε στις 21 Οκτωβρίου 2016, προκάλεσε εκτεταμένες δυσλειτουργίες σε κρίσιμες υποδομές του Διαδικτύου, περιορίζοντας την πρόσβαση σε περισσότερους από 1.200 δημοφιλείς ιστοτόπους και υπηρεσίες (Zhang et al., 2020).

Η αποτελεσματικότητα του Mirai δεν βασίστηκε σε κάποια περίπλοκη τεχνική διείσδυσης, αλλά στην εκμετάλλευση εκατομμυρίων συσκευών χαμηλού κόστους (IP κάμερες, δρομολογητές), οι οποίες διέθεταν ασθενείς ή προεπιλεγμένες ρυθμίσεις ασφαλείας (default passwords). Το γεγονός αυτό κατέδειξε με εμφατικό τρόπο την επικινδυνότητα των ελλιπών πολιτικών ασφαλείας στην κατασκευή και διάθεση συσκευών IoT (Bock et al., 2023).

Εξελικτικές Παραλλαγές και Διάδοχα Σχήματα: Hajime και Mozi

Η δημοσιοποίηση του πηγαίου κώδικα του Mirai λειτούργησε ως υπόβαθρο για την ανάπτυξη νέων, πιο εξελιγμένων παραλλαγών, οι οποίες ενσωμάτωσαν προηγμένους μηχανισμούς αυτοπροστασίας και εκμετάλλευσης ευπαθειών (Bock et al., 2023):

- **Hajime:** Διαφοροποιείται μέσω της υιοθέτησης μιας αποκεντρωμένης αρχιτεκτονικής ομότιμων δικτύων (Peer-to-Peer - P2P). Η απουσία κεντρικού σημείου ελέγχου (Command and Control - C&C) καθιστά τον εντοπισμό και την εξάρθρωσή του εξαιρετικά δυσχερή για τις αρχές.
- **Mozi:** Αποτελεί μια πιο σύνθετη απειλή, η οποία παρουσιάζει προσαρμοστική συμπεριφορά βάσει γεωγραφικών και δικτυακών παραμέτρων. Η ύπαρξή του αποδεικνύει ότι τα botnets έχουν μετεξελιχθεί σε εξειδικευμένα εργαλεία κυβερνοεπίθεσης με δυνατότητα στόχευσης συγκεκριμένων υποδομών (Bock et al., 2023).

Bashlite/Gafgyt και η Στοχοποίηση του Πρωτοκόλλου Telnet

Παράλληλα με το Mirai, η οικογένεια κακόβουλου λογισμικού Bashlite (γνωστή και ως Gafgyt) υπήρξε πρωτοπόρος στην εκμετάλλευση του πρωτοκόλλου Telnet (Wu et al., 2020). Η στρατηγική του Bashlite βασίστηκε στην αυτοματοποιημένη σάρωση ανοικτών θυρών και τη χρήση τεχνικών brute-force. Δεδομένα από honeypots καταδεικνύουν ότι το συγκεκριμένο λογισμικό παραμένει ενεργό, ενσωματώνοντας διαρκώς νέα πρότυπα συμπεριφοράς που του επιτρέπουν να διαφεύγει των παραδοσιακών συστημάτων ανίχνευσης (Wu et al., 2020; Zhang et al., 2020).

Η συγκριτική ανάλυση των περιστατικών της περιόδου 2008-2021 αναδεικνύει μια σαφή μετατόπιση των επιτιθέμενων προς πιο εκλεπτυσμένες στρατηγικές, όπως η κλιμάκωση προνομίων (privilege escalation) και η αποφυγή ανίχνευσης (evasion techniques) (Chee et al., 2025). Εν κατακλείδι, η ασφάλεια του οικοσυστήματος IoT παύει να θεωρείται ένα στενά τεχνικό ζήτημα και αναδεικνύεται σε θεμελιώδη παράμετρο για τη θωράκιση των παγκόσμιων δικτύων και των κρίσιμων εθνικών υποδομών (Zhang et al., 2020).

3.3. Cross-layer επιθέσεις και cascading failures

Η αρχιτεκτονική του Έξυπνου Δικτύου (Smart Grid) χαρακτηρίζεται από μια βαθιά αλληλεξάρτηση μεταξύ του φυσικού επιπέδου ισχύος και του κυβερνοεπιπέδου επικοινωνιών. Αυτή η πολυπλοκότητα εισάγει την έννοια των **Cross-layer επιθέσεων (Διαστρωματικών επιθέσεων)**, οι οποίες εκμεταλλεύονται τις ευπάθειες σε περισσότερα από ένα επίπεδα του συστήματος (π.χ. φυσικό, δίκτυο, εφαρμογή) για την επίτευξη ενός καταστροφικού στόχου. Για παράδειγμα, μια επίθεση παρεμβολής (jamming) στο επίπεδο του δικτύου μπορεί να εμποδίσει τη διαβίβαση κρίσιμων μετρήσεων, επηρεάζοντας άμεσα τη λειτουργία των αλγορίθμων ελέγχου στο επίπεδο της εφαρμογής, γεγονός που οδηγεί σε φυσικές αστάθειες στο δίκτυο (Kurt et al., 2018).

Η πιο επικίνδυνη συνέπεια τέτοιων επιθέσεων είναι οι **Διαδοχικές Αστοχίες (Cascading Failures)**. Πρόκειται για μια αλυσιδωτή αντίδραση όπου μια αρχική βλάβη ή μια στοχευμένη κυβερνοεπίθεση σε ένα στοιχείο του δικτύου (π.χ. ένας υποσταθμός ή μια γραμμή μεταφοράς) προκαλεί την υπερφόρτωση και την επακόλουθη απόζευξη άλλων στοιχείων. Σύμφωνα με τους Bouslimani κ.ά. (2025),

επιθέσεις όπως το GPS spoofing σε μονάδες PMU μπορούν να αποσυγχρονίσουν τις μετρήσεις τάσης, οδηγώντας σε λανθασμένες ενέργειες των συστημάτων προστασίας που πυροδοτούν διαδοχικές αστοχίες και τελικά γενικευμένο blackout.

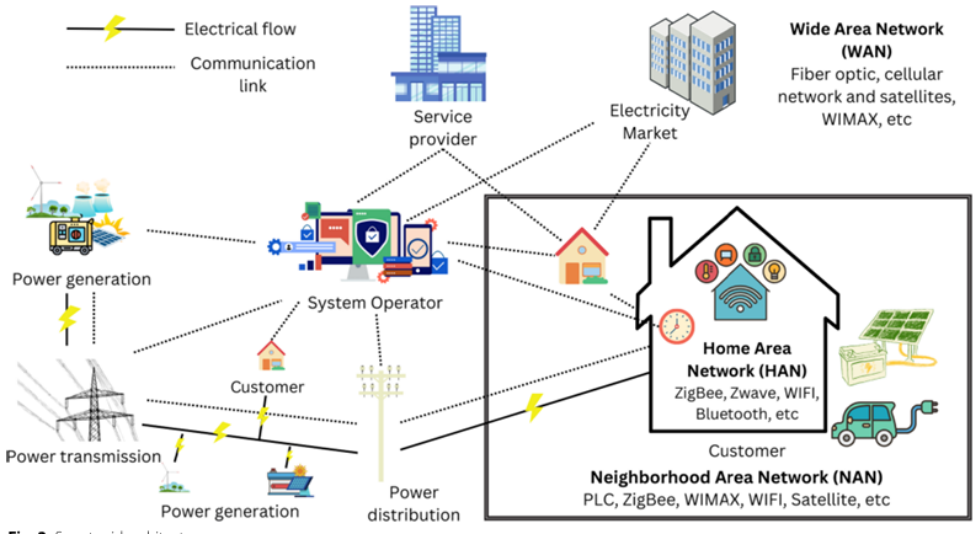
3.3.1. Συνδυασμένες επιθέσεις SCADA + AMI + IoT

Η σύγχρονη έρευνα υπογραμμίζει τον κίνδυνο των υβριδικών ή συνδυασμένων επιθέσεων που στοχεύουν ταυτόχρονα τα συστήματα SCADA, τις υποδομές AMI και τις συσκευές IoT, δημιουργώντας μια συνεργική απειλή που είναι εξαιρετικά δύσκολο να αντιμετωπιστεί:

1. **SCADA (Supervisory Control and Data Acquisition):** Αποτελεί τον στόχο υψηλού επιπέδου για τον έλεγχο της συχνότητας και της τάσης (AGC, LFC). Επιθέσεις έγχυσης ψευδών δεδομένων (FDIA) στο SCADA μπορούν να παραπλανήσουν τους χειριστές σχετικά με την πραγματική κατάσταση του δικτύου (Achaal et al., 2024).
2. **AMI (Advanced Metering Infrastructure):** Λειτουργεί ως το σημείο σύνδεσης με τον καταναλωτή. Η παραβίαση των έξυπνων μετρητών επιτρέπει τη χειραγώγηση της ζήτησης ή τη μαζική διακοπή παροχής, επηρεάζοντας την οικονομική ευστάθεια και τη σταθερότητα του φορτίου (Alshamasi & Ibrahim, 2025).
3. **IoT (Internet of Things):** Οι συσκευές IoT των καταναλωτών (π.χ. έξυπνοι φορτιστές EVs, HVAC) μπορούν να μετατραπούν σε botnets για την εκτέλεση επιθέσεων **Load Redistribution (Ανακατανομή Φορτίου)**. Συγχρονίζοντας την ενεργοποίηση ή απενεργοποίηση χιλιάδων τέτοιων συσκευών, ένας εισβολέας μπορεί να προκαλέσει απότομες αιχμές φορτίου που ξεπερνούν τα όρια αντοχής του δικτύου (Achaal et al., 2024; Bouslimani et al., 2025).
4. **Η Συνέργεια της Επίθεσης:** Η πραγματική ισχύς των συνδυασμένων επιθέσεων έγκειται στην ικανότητά τους να «τυφλώνουν» το σύστημα. Ενώ οι συσκευές IoT προκαλούν μια τεχνητή διαταραχή στο φορτίο, μια ταυτόχρονη επίθεση στο AMI και το SCADA μπορεί να αλλοιώσει τα δεδομένα των αισθητήρων, ώστε το κέντρο ελέγχου να μην αντιληφθεί την ανωμαλία εγκαίρως. Αυτός ο συντονισμός επιταχύνει τη μετάβαση από μια τοπική διαταραχή σε διαδοχικές αστοχίες (cascading failures), καθώς τα αυτόματα συστήματα προστασίας (π.χ. relays) αντιδρούν σε πραγματικές

υπερφορτώσεις που όμως παραμένουν αόρατες στα συστήματα επιτήρησης (Kurt et al., 2018).

Στο παρακάτω σχήμα απεικονίζονται τα πολλαπλά σημεία επίθεσης στο Έξυπνο Δίκτυο, αναδεικνύοντας πώς η διείσδυση σε διαφορετικά τμήματα (Generation, Transmission, Distribution, Customer) μπορεί να συνδυαστεί για την κατάρρευση του συστήματος.



Εικόνα 9:Έξυπνη αρχιτεκτονική δικτύων (Πηγή:Achaal et al., 2024)

3.3.2. Αλυσιδωτές αποτυχίες και κίνδυνοι για κρίσιμες υποδομές

Στο σύγχρονο περιβάλλον των Έξυπνων Δικτύων (Smart Grids), η φυσική υποδομή ισχύος είναι άρρηκτα συνδεδεμένη με το κυβερνοεπίπεδο επικοινωνιών. Αυτή η αλληλεξάρτηση, αν και προσφέρει βελτιστοποιημένη διαχείριση, εισάγει τον κίνδυνο των **αλυσιδωτών αποτυχιών (cascading failures)**. Ως αλυσιδωτή αποτυχία ορίζεται μια αλληλουχία γεγονότων όπου η αστοχία ενός στοιχείου του δικτύου προκαλεί διαδοχικές υπερφορτώσεις και αστοχίες σε άλλα στοιχεία, οδηγώντας τελικά σε ευρείας κλίμακας κατάρρευση του συστήματος (Islam et al., 2023).

Ο Μηχανισμός της Αλυσιδωτής Κατάρρευσης

Ο μηχανισμός της αλυσιδωτής κατάρρευσης στα Έξυπνα Δίκτυα αποτελεί μια σύνθετη διαδικασία που ξεκινά συνήθως με μια τοπική διαταραχή, η οποία μπορεί να

προκληθεί είτε από τυχαία σφάλματα είτε από στοχευμένες κυβερνοεπιθέσεις. Στο πλαίσιο των διαστρωματικών (cross-layer) επιθέσεων, ένας εισβολέας μπορεί να εκμεταλλευτεί το δίκτυο επικοινωνιών για να παραπλανήσει τους μηχανισμούς ελέγχου, προκαλώντας λανθασμένες αποκρίσεις του συστήματος.

Κεντρικό ρόλο σε αυτή τη διαδικασία παίζει η μεταφορά φορτίου, καθώς όταν μια γραμμή μεταφοράς τίθεται εκτός λειτουργίας λόγω επίθεσης ή υπερφόρτωσης, το φορτίο που μετέφερε αναδιανέμεται αυτόματα στις γειτονικές γραμμές. Εάν αυτές οι γραμμές λειτουργούν ήδη κοντά στα όριά τους, η επιπλέον επιβάρυνση μπορεί να προκαλέσει τη δική τους απόζευξη, δημιουργώντας ένα καταστροφικό φαινόμενο «ντόμινο» που εξαπλώνεται ταχύτατα στο δίκτυο (Ruj & Pal, 2022).

Παράλληλα, η κυβερνο-φυσική αλληλεξάρτηση επιτείνει το πρόβλημα, καθώς η αποτυχία στο επίπεδο της πληροφορίας, όπως για παράδειγμα η απώλεια ορατότητας λόγω μιας επίθεσης DoS, εμποδίζει τους διαχειριστές από το να λάβουν έγκαιρα διορθωτικά μέτρα. Αυτή η έλλειψη ελέγχου επιτρέπει στην αρχική τοπική αστοχία να κλιμακωθεί ανεξέλεγκτα και να εξελιχθεί σε ένα γενικευμένο blackout, καταδεικνύοντας την ανάγκη για ενισχυμένη ανθεκτικότητα σε όλα τα επίπεδα του συστήματος (Islam et al., 2023).

Επιθέσεις Τροποποίησης Φορτίου (Load-Altering Attacks - LAA)

Οι Επιθέσεις Τροποποίησης Φορτίου (Load-Altering Attacks - LAA) αποτελούν μια ιδιαίτερα επικίνδυνη μορφή κυβερνοαπειλής που μπορεί να προκαλέσει αλυσιδωτές αποτυχίες στο δίκτυο μέσω της εκμετάλλευσης συσκευών IoT. Η επικινδυνότητά τους έγκειται στη συντονισμένη δράση των εισβολέων, οι οποίοι παραβιάζοντας χιλιάδες συσκευές, όπως έξυπνους θερμοσίφωνες ή φορτιστές ηλεκτρικών οχημάτων, προκαλούν απότομες και μαζικές αλλαγές στη ζήτηση ενέργειας. Σύμφωνα με τους Goodridge κ.ά. (2023), οι στρατηγικά σχεδιασμένες επιθέσεις LAA στοχεύουν σε συγκεκριμένα σημεία του δικτύου που είναι πιο ευάλωτα σε δυναμικές αστάθειες, καθιστώντας τις αλυσιδωτές αποτυχίες αναπόφευκτες. Η απότομη αυτή διακύμανση του φορτίου μπορεί να παραβιάσει τα όρια ασφαλείας N-1, οδηγώντας σε κατάρρευση ακόμη και συστήματα που θεωρούνται ανθεκτικά (Goodridge et al., 2023).

Για την έγκαιρη ανίχνευση και αναχαίτιση τέτοιων απότομων διακυμάνσεων, η ενσωμάτωση των δικτύων 6G προσφέρει κρίσιμα πλεονεκτήματα μέσω της αρχιτεκτονικής Edge Intelligence και της επικοινωνίας εξαιρετικά χαμηλής καθυστέρησης (uRLLC). Η δυνατότητα επεξεργασίας τεράστιου όγκου δεδομένων σε πραγματικό χρόνο στο άκρο του δικτύου επιτρέπει την άμεση αναγνώριση μη φυσιολογικών προτύπων ζήτησης που υποδηλώνουν μια συντονισμένη επίθεση LAA προτού επέλθει η αποσταθεροποίηση της τάσης. Όπως επισημαίνουν οι Zhang et al. (2020), η χρήση Τεχνητής Νοημοσύνης στο άκρο των δικτύων επόμενης γενιάς επιτρέπει την αυτόματη απομόνωση των παραβιασμένων συσκευών IoT, περιορίζοντας τη μαζική επίδραση της επίθεσης και διασφαλίζοντας την ακεραιότητα των κρίσιμων υποδομών του έξυπνου δικτύου (Zhang et al., 2020).

Κίνδυνοι για τις Κρίσιμες Υποδομές

Οι κίνδυνοι για τις κρίσιμες υποδομές και οι αλυσιδωτές αποτυχίες (cascading failures) αποτελούν τη μεγαλύτερη απειλή για την εθνική ασφάλεια, δεδομένου ότι το έξυπνο δίκτυο λειτουργεί ως η βασική πηγή τροφοδοσίας για όλες τις υπόλοιπες κρίσιμες υποδομές. Όπως επισημαίνουν οι Islam et al. (2023), οι επιπτώσεις αυτών των αστοχιών είναι διατομεακές, καθώς μια ενδεχόμενη κατάρρευση του ηλεκτρικού δικτύου προκαλεί άμεση διαταραχή στην ύδρευση, τις τηλεπικοινωνίες, τις μεταφορές και τις υπηρεσίες υγείας. Επιπλέον, η έρευνα των Ruj και Pal (2022) αναδεικνύει τη σημαντική διαφορά μεταξύ στοχευμένων και τυχαίων επιθέσεων, αποδεικνύοντας ότι τα δίκτυα είναι εξαιρετικά ευάλωτα σε στοχευμένες ενέργειες που επικεντρώνονται σε κόμβους με υψηλό βαθμό διασυνδεσιμότητας (high-degree nodes).

Σε αυτές τις περιπτώσεις, η αλυσιδωτή κατάρρευση εξαπλώνεται πολύ ταχύτερα και απαιτεί σημαντικά μικρότερη προσπάθεια από την πλευρά του εισβολέα σε σύγκριση με την αντιμετώπιση τυχαίων βλαβών, καθιστώντας την προστασία αυτών των κεντρικών κόμβων ύψιστη προτεραιότητα για τη θωράκιση της εθνικής ασφάλειας.

Ενίσχυση της Ανθεκτικότητας

Για την προστασία των υποδομών, απαιτούνται προηγμένες λύσεις όπως το **Federated Learning (FL)**. Το FL επιτρέπει την ανίχνευση ανωμαλιών και επιθέσεων σε πραγματικό χρόνο στο «άκρο» του δικτύου (edge), προστατεύοντας ταυτόχρονα

την ιδιωτικότητα των δεδομένων και παρέχοντας έγκαιρη προειδοποίηση πριν μια τοπική διαταραχή εξελιχθεί σε αλυσιδωτή αποτυχία (Jithish et al., 2025).

3.3.3. Μέτρα πρόληψης και διαχείρισης κινδύνου

Η διασύνδεση των φυσικών συστημάτων ισχύος με τα δίκτυα επικοινωνιών δημιουργεί μια σύνθετη επιφάνεια επίθεσης όπου μια κυβερνοεπίθεση μπορεί να μεταφραστεί σε φυσική καταστροφή. Για την αποτελεσματική θωράκιση των έξυπνων δικτύων (Smart Grids) έναντι cross-layer επιθέσεων και την αποφυγή αλυσιδωτών αστοχιών (cascading failures), απαιτείται μια ολιστική προσέγγιση που καλύπτει όλο το φάσμα της κυβερνοασφάλειας.

Το Πλαίσιο NIST ως Στρατηγικός Οδηγός

Σύμφωνα με τους Achaal κ.ά. (2024), η διαχείριση κινδύνου δεν πρέπει να περιορίζεται μόνο στην αποτροπή, αλλά να ακολουθεί τις πέντε λειτουργίες του πλαισίου **NIST**: **Προσδιορισμός, Προστασία, Ανίχνευση, Απόκριση και Ανάκτηση**. Αυτή η κυκλική προσέγγιση διασφαλίζει ότι ακόμη και αν μια επίθεση παρακάμψει τα αρχικά μέτρα προστασίας, το σύστημα θα είναι σε θέση να την ανιχνεύσει έγκαιρα και να επανέλθει σε ασφαλή λειτουργία πριν προκληθεί γενικευμένο blackout.

Τεχνικές Ανίχνευσης και Μηχανική Μάθηση

Η πρόληψη των αλυσιδωτών αστοχιών βασίζεται σε μεγάλο βαθμό στην έγκαιρη ανίχνευση ανωμαλιών στα δεδομένα. Τα Συστήματα Ανίχνευσης Εισβολών (**IDS**) που χρησιμοποιούν αλγορίθμους Μηχανικής Μάθησης (π.χ. Random Forest, SVM) είναι κρίσιμα για τον εντοπισμό επιθέσεων έγχυσης ψευδών δεδομένων (FDI) ή επιθέσεων άρνησης υπηρεσίας (DoS). Όπως επισημαίνεται, η ικανότητα αυτών των συστημάτων να αναλύουν τεράστιους όγκους δεδομένων σε πραγματικό χρόνο επιτρέπει την απομόνωση του μολυσμένου τμήματος του δικτύου, αποτρέποντας την εξάπλωση της βλάβης από το ψηφιακό στο φυσικό επίπεδο (Achaal et al., 2024).

Κρυπτογράφηση και Έλεγχος Πρόσβασης

Για την προστασία των cross-layer επικοινωνιών, προτείνεται η εφαρμογή αυστηρών πρωτοκόλλων ασφαλείας, όπως το **IEC 62351**, το οποίο παρέχει μηχανισμούς

αυθεντικοποίησης και κρυπτογράφησης για τα βιομηχανικά πρωτόκολλα (π.χ. MODBUS, DNP3). Επιπλέον, ο έλεγχος πρόσβασης βάσει ρόλων (**RBAC**) περιορίζει τις δυνατότητες ενός επιτιθέμενου να κινηθεί οριζόντια μέσα στο δίκτυο, μειώνοντας την πιθανότητα να αποκτήσει έλεγχο κρίσιμων φυσικών διακοπτών (Achaal et al., 2024).

Στρατηγικές Ανθεκτικότητας (Resilience)

Η διαχείριση κινδύνου περιλαμβάνει επίσης τον σχεδιασμό «νησιδοποίησης» (islanding) του δικτύου. Σε περίπτωση που ανιχνευθεί μια κρίσιμη cross-layer επίθεση, το σύστημα μπορεί να αυτονομηθεί σε μικρότερα μικροδίκτυα (microgrids). Αυτό το μέτρο περιορίζει την επίδραση της επίθεσης και διασφαλίζει ότι η αλυσιδωτή αστοχία δεν θα επεκταθεί σε ολόκληρη την εθνική υποδομή(Achaal et al., 2024).

3.3.Διεθνείς Μελέτες Περίπτωσης και Πρακτικές Εφαρμογές Κυβερνοασφάλειας σε Έξυπνα Δίκτυα

Η πρακτική εφαρμογή των στρατηγικών κυβερνοασφάλειας σε παγκόσμιο επίπεδο αναδεικνύει την ανάγκη για μια πολυεπίπεδη προσέγγιση που συνδυάζει τεχνολογία, πρότυπα και ανθεκτικότητα. Στις Ηνωμένες Πολιτείες, η στρατηγική θωράκισης εστιάζει στις πρόσφατες κατευθυντήριες γραμμές του NIST (2024) για την προστασία των έξυπνων μετατροπέων σε οικιακά δίκτυα. Μια κρίσιμη εφαρμογή σε αυτό το πλαίσιο αφορά τη χρήση Ψηφιακών Διδύμων (Digital Twins), τα οποία επιτρέπουν την προσομοίωση κυβερνοεπιθέσεων σε περιβάλλον πραγματικού χρόνου, διασφαλίζοντας την ευστάθεια του συστήματος μέσω της χρήσης Μεγάλων Γλωσσικών Μοντέλων (LLMs) για την αυτόματη ανίχνευση ανωμαλιών (Ibrahim & Kashef, R., 2025). Παράλληλα, η Ευρωπαϊκή Ένωση προωθεί τη συνεργατική άμυνα μέσω του Κανονισμού 2024/1366 (European Commission, 2024), ο οποίος ρυθμίζει την ασφάλεια των διασυνοριακών ροών ενέργειας.

Στο πλαίσιο των τεχνολογιών επόμενης γενιάς, η υιοθέτηση του Edge Computing (Υπολογιστική Άκρων) σε ευρωπαϊκά και αμερικανικά δίκτυα προσφέρει μια νέα γραμμή άμυνας, επιτρέποντας την τοπική επεξεργασία δεδομένων και την άμεση αναγνώριση εισβολών (Intrusion Detection). Η αρχιτεκτονική αυτή μειώνει την ανάγκη μεταφοράς ευαίσθητων δεδομένων στο κεντρικό υπολογιστικό νέφος,

ελαχιστοποιώντας έτσι την επιφάνεια επίθεσης και τον κίνδυνο υποκλοπής πληροφοριών κατά τη μετάδοση, ενώ ταυτόχρονα υποστηρίζει την ανάγκη για απόκριση σε πραγματικό χρόνο που απαιτούν τα δίκτυα 6G (Bimpas et al.,2024).

Στην Ασία, η Κίνα ηγείται στην εφαρμογή της Κβαντικής Διανομής Κλειδιών (QKD), αναπτύσσοντας υποδομές που καθιστούν τις επικοινωνίες των γραμμών υψηλής τάσης απρόσβλητες από μελλοντικές κβαντικές απειλές (Lin et.al,2025), 2024). Η στρατηγική αυτή συμπληρώνεται από δορυφορικά-επίγειο δίκτυα νέας γενιάς που ενισχύουν το συνολικό πλαίσιο ασφαλείας (Huang et.al, 2025). Επιπλέον, η χρήση τεχνολογίας Blockchain για την ασφάλεια των συναλλαγών σε μικροδίκτυα (microgrids) στην Νοτιοανατολική Ασία έχει αποδείξει ότι μπορεί να αποτρέψει επιθέσεις αλλοίωσης δεδομένων (False Data Injection) σε συστήματα Peer-to-Peer εμπορίας ενέργειας, διασφαλίζοντας την ακεραιότητα των οικονομικών συναλλαγών χωρίς την ανάγκη κεντρικής αρχής (Yao et al., 2024).

Μια άλλη σημαντική εξέλιξη αφορά την ενσωμάτωση τεχνικών Ομομορφικής Κρυπτογράφησης (Homomorphic Encryption), η οποία επιτρέπει στους διαχειριστές να αναλύουν δεδομένα κατανάλωσης χωρίς να τα αποκρυπτογραφούν. Πρακτικές δοκιμές δείχνουν ότι αυτή η προσέγγιση "Privacy-by-Design" εξαλείφει τον κίνδυνο διαρροής προσωπικών δεδομένων σε περίπτωση παραβίασης της κεντρικής βάσης δεδομένων, ενισχύοντας την εμπιστοσύνη των καταναλωτών στο σύστημα (Xiao et al., 2025).

Τέλος, η εμπειρία από τις επιθέσεις στο ουκρανικό δίκτυο (BlackEnergy) προσφέρει, δέκα χρόνια μετά, θεμελιώδη διδάγματα για την ανθεκτικότητα των συστημάτων SCADA. Οι σύγχρονες αναλύσεις αυτών των περιστατικών οδηγούν στην ανάπτυξη προηγμένων συστημάτων "αυτοΐασης" (self-healing), τα οποία χρησιμοποιούν αλγορίθμους ενισχυτικής μάθησης (Reinforcement Learning) για να απομονώνουν αυτόματα τα τμήματα του δικτύου που δέχονται επίθεση, εξασφαλίζοντας τη συνεχή παροχή ενέργειας σε κρίσιμες υποδομές (Kordi et al., 2025). Η ενσωμάτωση αυτών των τεχνολογιών στο περιβάλλον 6G υπόσχεται χρόνο απόκρισης σε χιλιοστά του δευτερολέπτου, καθιστώντας τα δίκτυα του μέλλοντος κυβερνο-ανθεκτικά (cyber-resilient) έναντι σύνθετων απειλών (Ibrahim & Kashef, 2025).

Κεφάλαιο 4: Προστασία Δεδομένων και Ιδιωτικότητα

4.1. Χαρακτηριστικά ευαίσθητων δεδομένων

4.1.1. Προσωπικά δεδομένα καταναλωτών

Η μετάβαση προς τα έξυπνα δίκτυα (Smart Grids) αποτελεί μια από τις σημαντικότερες προκλήσεις του 21ου αιώνα για την ενεργειακή ασφάλεια και την αντιμετώπιση της κλιματικής αλλαγής. Κεντρικό ρόλο σε αυτή την εξέλιξη διαδραματίζουν οι έξυπνοι μετρητές, οι οποίοι καταγράφουν την ηλεκτρική κατανάλωση σε υψηλή συχνότητα, παρέχοντας κρίσιμα δεδομένα για τη διαχείριση του δικτύου. Ωστόσο, οι εν λόγω χρονοσειρές κατανάλωσης συνιστούν ευαίσθητα προσωπικά δεδομένα, καθώς η λεπτομερής φύση τους εμπίπτει σε αυστηρά νομικά πλαίσια προστασίας, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), λόγω των κινδύνων που ελλοχεύουν για την ιδιωτικότητα (Voyez et al., 2022).

Η ευαισθησία αυτή πηγάζει κυρίως από την ικανότητα εξαγωγής συμπερασμάτων για την ιδιωτική ζωή των ενοίκων μέσω προηγμένων αναλυτικών μεθόδων. Συγκεκριμένα, η εφαρμογή τεχνικών Μη Επεμβατικής Παρακολούθησης Φορτίου (NILM) επιτρέπει την αποδόμηση του συνολικού φορτίου και την ταυτοποίηση μεμονωμένων ηλεκτρικών συσκευών. Με αυτόν τον τρόπο, τρίτα μέρη μπορούν να αναγνωρίσουν με ακρίβεια τις καθημερινές συνήθειες ενός νοικοκυριού, όπως το πρόγραμμα ύπνου, τις ώρες γευμάτων ή τις περιόδους απουσίας, μετατρέποντας τις ενεργειακές μετρήσεις σε ένα μέσο παρακολούθησης της συμπεριφοράς (Armoogum & Bassoo, n.d.).

Ένα από τα πλέον ανησυχητικά χαρακτηριστικά των δεδομένων αυτών είναι η «μοναδικότητά» τους (uniqueness), η οποία λειτουργεί ως ψηφιακό δακτυλικό αποτύπωμα για κάθε νοικοκυριό. Η έρευνα έχει καταδείξει ότι η πλειονότητα των καταναλωτών μπορεί να ταυτοποιηθεί μοναδικά από ένα πολύ μικρό δείγμα μετρήσεων, γεγονός που καθιστά τις χρονοσειρές εξαιρετικά ευάλωτες σε επιθέσεις επαναταυτοποίησης. Η στατιστική πιθανότητα μοναδικότητας παραμένει υψηλή ακόμη και όταν εξετάζονται περιορισμένα χρονικά παράθυρα κατανάλωσης, υπογραμμίζοντας τη δυσκολία πλήρους ανωνυμοποίησης (Voyez et al., 2022).

Παρά τις προσπάθειες των διαχειριστών για προστασία μέσω της ψευδωνυμοποίησης, η απλή αφαίρεση των άμεσων αναγνωριστικών στοιχείων, όπως το όνομα, αποδεικνύεται συχνά ανεπαρκής. Λόγω του πληροφοριακού πλούτου των μετρήσεων, ένας εισβολέας με πρόσβαση σε δευτερεύουσες πηγές δεδομένων μπορεί να συσχετίσει μια «ανώνυμη» μέτρηση με ένα συγκεκριμένο άτομο. Αυτό το φαινόμενο της επαναταυτοποίησης (re-identification) καταδεικνύει ότι η ιδιωτικότητα δεν διασφαλίζεται μόνο με την απόκρυψη της ταυτότητας, αλλά απαιτεί βαθύτερες τεχνικές παρεμβάσεις (Voyez et al., 2022).

Πέρα από την παραβίαση της ιδιωτικότητας, η διαρροή τέτοιων δεδομένων ενέχει κινδύνους για τη φυσική ασφάλεια των καταναλωτών. Η ανάλυση των μοτίβων κατανάλωσης μπορεί να αποκαλύψει πότε μια κατοικία είναι άδεια, καθιστώντας την στόχο εγκληματικών ενεργειών. Επιπλέον, η ενσωμάτωση σύγχρονων τεχνολογιών, όπως τα ηλεκτρικά οχήματα, εισάγει πρόσθετες παραμέτρους επικινδυνότητας, καθώς τα δεδομένα φόρτισης μπορούν να προδώσουν τη γεωγραφική θέση και τις μετακινήσεις των χρηστών (Armoogum & Bassoo, n.d.).

Η συγκέντρωση αυτών των πληροφοριών σε κεντρικές υποδομές ή σε περιβάλλοντα υπολογιστικού νέφους (cloud) διευρύνει την επιφάνεια επίθεσης για κυβερνοεπιθέσεις. Οι πάροχοι υπηρεσιών συλλέγουν ένα ευρύ φάσμα δεδομένων που περιλαμβάνει τραπεζικές πληροφορίες και προσωπικά έγγραφα ταυτοποίησης, τα οποία συνδυάζονται με τα ενεργειακά προφίλ. Μια ενδεχόμενη παραβίαση σε αυτά τα συστήματα θα μπορούσε να οδηγήσει σε ταυτόχρονη αποκάλυψη ταυτότητας και προσωπικών χαρακτηριστικών, με σοβαρές επιπτώσεις για τον καταναλωτή (Armoogum & Bassoo, n.d.).

Η μεταβλητότητα της ευαισθησίας των δεδομένων εξαρτάται επίσης από τη χρονική ανάλυση και τις περιβαλλοντικές συνθήκες. Όσο πιο πυκνή είναι η δειγματοληψία των μετρήσεων, τόσο αυξάνεται η εντροπία και, κατά συνέπεια, η μοναδικότητα της πληροφορίας, καθιστώντας τα δεδομένα πιο αναγνωρίσιμα. Φαινόμενα όπως η εποχικότητα ή η αυξημένη ζήτηση κατά τις απογευματινές ώρες ενισχύουν τη διακριτότητα των μοτίβων κατανάλωσης, καθιστώντας ορισμένες χρονικές περιόδους πιο «επικίνδυνες» για την προστασία της ιδιωτικότητας (Voyez et al., 2022).

Για τον μετριασμό αυτών των κινδύνων, η σύγχρονη έρευνα προτείνει την υιοθέτηση προηγμένων κρυπτογραφικών και στατιστικών εργαλείων. Η Διαφορική Ιδιωτικότητα (Differential Privacy) και η ομομορφική κρυπτογράφηση αναδεικνύονται ως κορυφαίες λύσεις, επιτρέποντας την επεξεργασία των δεδομένων και την εξαγωγή χρήσιμων συμπερασμάτων χωρίς την αποκάλυψη του πραγματικού περιεχομένου των μετρήσεων. Οι τεχνικές αυτές στοχεύουν στην παρεμβολή ελεγχόμενου «θορύβου», ο οποίος προστατεύει το άτομο χωρίς να ακυρώνει τη χρησιμότητα της πληροφορίας για το δίκτυο (Armoogum & Bassoo, n.d.).

Συμπερασματικά, η διαχείριση των δεδομένων στα έξυπνα δίκτυα απαιτεί μια λεπτή ισορροπία μεταξύ της τεχνολογικής προόδου και των θεμελιωδών δικαιωμάτων των πολιτών. Η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων κατανάλωσης είναι προϋπόθεση για την κοινωνική αποδοχή των έξυπνων υποδομών. Η ολιστική προσέγγιση στην ασφάλεια, που συνδυάζει νομικά πλαίσια και προηγμένες τεχνικές προστασίας, είναι η μόνη οδός για την επιτυχή και ασφαλή λειτουργία των μελλοντικών ενεργειακών συστημάτων (Armoogum & Bassoo, n.d. · Voyez et al., 2022).

4.1.2. Ενεργειακά προφίλ και δεδομένα χρήσης

Η ενσωμάτωση των έξυπνων μετρητών στα σύγχρονα ενεργειακά δίκτυα επιτρέπει τη συλλογή δεδομένων κατανάλωσης σε εξαιρετικά υψηλή ανάλυση, συνήθως ανά διαστήματα 15 λεπτών. Σύμφωνα με τους Radovanovic κ.ά. (2022), αυτή η πυκνή ροή πληροφοριών επιτρέπει την εξαγωγή λεπτομερών προτύπων χρήσης, τα οποία αποτελούν τη βάση για τη δημιουργία των «ενεργειακών προφίλ» των καταναλωτών. Παρόλο που τα δεδομένα αυτά είναι ζωτικής σημασίας για τη βελτιστοποίηση του δικτύου, φέρουν εγγενή χαρακτηριστικά που τα καθιστούν εξαιρετικά ευαίσθητα από την άποψη της ιδιωτικότητας.

Ένα από τα κυριότερα χαρακτηριστικά αυτών των δεδομένων είναι η μοναδικότητά τους, η οποία επιτρέπει τη «δακτυλική αποτύπωση» (fingerprinting) των νοικοκυριών. Οι Radovanovic κ.ά. (2022) αποδεικνύουν ότι ακόμη και δεδομένα μίας μόνο εβδομάδας είναι επαρκή για να δημιουργηθεί ένα μοναδικό ενεργειακό αποτύπωμα. Η έρευνά τους δείχνει ότι ορισμένα νοικοκυριά παρουσιάζουν τόσο ιδιαίτερες συνήθειες, ώστε να μπορούν να ταυτοποιηθούν σχεδόν πάντα ανάμεσα σε

δεκάδες άλλα, καθιστώντας τα δεδομένα χρήσης ένα σταθερό αναγνωριστικό ταυτότητας.

Η ευαισθησία των δεδομένων ενισχύεται από τη δυνατότητα έμμεσης αποκάλυψης πληροφοριών για την καθημερινή ζωή των ενοίκων. Όπως επισημαίνουν οι Zhang κ.ά. (2022), τα ενεργειακά προφίλ δεν καταγράφουν απλώς την κατανάλωση, αλλά «προδίδουν» τις καθημερινές ρουτίνες, τις ώρες απουσίας από την κατοικία, ακόμη και τις συνήθειες ύπνου. Αυτά τα «δευτερεύοντα» δεδομένα μπορούν να εκμεταλλευτούν από κακόβουλους φορείς για την παρακολούθηση της φυσικής παρουσίας των ατόμων, θέτοντας σε κίνδυνο την ασφάλειά τους.

Επιπλέον, η ανάλυση των ενεργειακών προφίλ μέσω τεχνικών Μηχανικής Μάθησης επιτρέπει την ταυτοποίηση συγκεκριμένων χαρακτηριστικών των καταναλωτών. Σύμφωνα με τους Zhang κ.ά. (2022), μέσω της ανάλυσης των διακυμάνσεων του φορτίου, είναι εφικτή η αναγνώριση των τύπων των συσκευών που χρησιμοποιούνται στο σπίτι. Η πληροφορία αυτή μπορεί να οδηγήσει σε συμπεράσματα για το επίπεδο εισοδήματος, το μέγεθος της οικογένειας ή ακόμη και τις προσωπικές προτιμήσεις των καταναλωτών, στοιχεία που θεωρούνται αυστηρά προσωπικά.

Ένα άλλο κρίσιμο χαρακτηριστικό είναι η ανθεκτικότητα των δεδομένων αυτών απέναντι στις παραδοσιακές μεθόδους ανωνυμοποίησης. Οι Radovanovic κ.ά. (2022) τονίζουν ότι ακόμη και σύντομα αποσπάσματα δεδομένων (weekly snippets) επιτρέπουν σε έναν εισβολέα να διακρίνει ένα συγκεκριμένο σπίτι από μια ομάδα άλλων. Αυτό σημαίνει ότι η απλή αφαίρεση άμεσων αναγνωριστικών, όπως το όνομα ή η διεύθυνση, δεν επαρκεί για την προστασία του χρήστη, καθώς το ίδιο το μοτίβο κατανάλωσης λειτουργεί ως «υπογραφή».

Η χρήση προηγμένων αλγορίθμων Βαθιάς Μάθησης (Deep Learning) προσδίδει στα ενεργειακά δεδομένα μια νέα διάσταση επικινδυνότητας. Οι Zhang κ.ά. (2022) αναφέρουν ότι οι αλγόριθμοι αυτοί μπορούν να συσχετίσουν τα ενεργειακά προφίλ με εξωτερικές πηγές δεδομένων, οδηγώντας στην επανταυτοποίηση των χρηστών. Αυτή η ικανότητα των μοντέλων να «μαθαίνουν» και να προβλέπουν τη συμπεριφορά των καταναλωτών καθιστά τα δεδομένα χρήσης μια διαρκή απειλή για την ιδιωτικότητα, εάν δεν προστατευτούν επαρκώς.

Προς αντιμετώπιση αυτών των προκλήσεων, η σύγχρονη έρευνα προτείνει τη μετάβαση σε μοντέλα «Deep Learning με Προστασία Ιδιωτικότητας». Όπως εξηγούν οι Zhang κ.ά. (2022), η χρήση τεχνικών όπως η Ομομορφική Κρυπτογράφηση και ο Ασφαλής Πολυμερής Υπολογισμός επιτρέπει την ανάλυση των ευαίσθητων ενεργειακών προφίλ χωρίς την αποκάλυψη των ακατέργαστων δεδομένων. Αυτό το χαρακτηριστικό της «υπολογίσιμης κρυπτογράφησης» είναι απαραίτητο για να διατηρηθεί η χρησιμότητα των δεδομένων για το δίκτυο χωρίς να εκτίθεται ο καταναλωτής.

Συμπερασματικά, τα ενεργειακά προφίλ των έξυπνων δικτύων αποτελούν μια μοναδική κατηγορία ευαίσθητων δεδομένων που χαρακτηρίζονται από υψηλή ανάλυση, μοναδικότητα και πληροφοριακό πλούτο. Η ανάλυση των Radovanovic κ.ά. (2022) και των Zhang κ.ά. (2022) καταδεικνύει ότι η διαχείριση αυτών των δεδομένων απαιτεί κάτι περισσότερο από απλή ασφάλεια δικτύου· απαιτεί εξελιγμένες κρυπτογραφικές λύσεις που να αναγνωρίζουν τη φύση των δεδομένων χρήσης ως αναπόσπαστο κομμάτι της ψηφιακής και φυσικής ιδιωτικότητας του ατόμου.

4.1.3. Ευπάθειες και κίνδυνοι από μη εξουσιοδοτημένη πρόσβαση

Η αρχιτεκτονική των Έξυπνων Δικτύων εδράζεται στην αμφίδρομη και συνεχή ανταλλαγή πληροφοριών μεταξύ καταναλωτών και παρόχων, μια διαδικασία απαραίτητη για τη βελτιστοποίηση της ενεργειακής απόδοσης. Ωστόσο, αυτή η ροή δεδομένων μέσω δημόσιων ή ιδιωτικών δικτύων επικοινωνίας εισάγει κρίσιμες ευπάθειες, καθιστώντας το σύστημα εκτεθειμένο σε μη εξουσιοδοτημένη πρόσβαση. Τέτοιες παραβιάσεις δεν απειλούν μόνο την ιδιωτικότητα των χρηστών, αλλά δύνανται να υπονομεύσουν και την οικονομική σταθερότητα ολόκληρου του δικτύου.

Η κύρια ευπάθεια εντοπίζεται στη διαδικασία συλλογής των δεδομένων κατανάλωσης, όπου η πρόσβαση σε ακατέργαστες μετρήσεις επιτρέπει τη διενέργεια «εξόρυξης ιδιωτικότητας» (privacy mining). Λόγω της υψηλής ανάλυσης των δεδομένων, κακόβουλοι φορείς μπορούν να εξάγουν ακριβή συμπεράσματα για τις καθημερινές δραστηριότητες, τις συνήθειες διαβίωσης, ακόμη και την παρουσία ατόμων στην κατοικία (Wu et al., 2022). Αυτή η διείσδυση στην προσωπική ζωή των

καταναλωτών δημιουργεί σοβαρούς κινδύνους, μετατρέποντας τις ψηφιακές ευπάθειες σε απειλές για τη φυσική ασφάλεια των πολιτών.

Πέρα από την υποκλοπή πληροφοριών, η μη εξουσιοδοτημένη πρόσβαση επιτρέπει την κακόβουλη τροποποίηση δεδομένων, συχνά από τους ίδιους τους χρήστες. Η ύπαρξη «κακόβουλων καταναλωτών» αποτελεί μια σημαντική πρόκληση, καθώς η αποστολή ψευδών, μειωμένων μετρήσεων οδηγεί σε άμεση οικονομική ζημία για τους παρόχους (Ahadipour et al., 2019). Παράλληλα, η παροχή λανθασμένων πληροφοριών για τη ζήτηση ενέργειας παραπλανά τα συστήματα λήψης αποφάσεων, προκαλώντας επικίνδυνες ανισορροπίες στην ευστάθεια του συστήματος ισχύος.

Σημαντικές αδυναμίες παρατηρούνται επίσης στη διαδικασία της αθροιστικής συλλογής δεδομένων (data aggregation). Ενώ η ομαδοποίηση των μετρήσεων αποτελεί συνήθη πρακτική προστασίας, η έλλειψη ισχυρής κρυπτογράφησης στον αθροιστή (aggregator) μπορεί να αποβεί μοιραία. Χωρίς μηχανισμούς ανωνυμίας και καθορισμένων παραληπτών, ένας εισβολέας μπορεί να ανακτήσει τα ατομικά προφίλ κατανάλωσης, ακυρώνοντας κάθε προηγούμενο μέτρο προστασίας (Wu et al., 2022).

Για την αποτελεσματική αντιμετώπιση αυτών των κινδύνων, οι σύγχρονες προσεγγίσεις εστιάζουν σε δύο άξονες: την αυθεντικοποίηση και την ανίχνευση σφαλμάτων. Τα σχήματα ανώνυμης πιστοποίησης διασφαλίζουν ότι μόνο εξουσιοδοτημένοι μετρητές επικοινωνούν με το δίκτυο, διατηρώντας την ταυτότητα του χρήστη κρυφή (Wu et al., 2022). Ταυτόχρονα, η χρήση στατιστικών μεθόδων και συντελεστών συσχέτισης επιτρέπει τον εντοπισμό δόλιων μετρήσεων σε πραγματικό χρόνο, θωρακίζοντας το δίκτυο χωρίς να παραβιάζεται η ιδιωτικότητα των νομότυπων καταναλωτών (Ahadipour et al., 2019).

4.2.Privacy-preserving τεχνικές

4.2.1. Anonymization και pseudonymization

Η επιτακτική ανάγκη για επεξεργασία δεδομένων κατανάλωσης σε πραγματικό χρόνο, υπό το πρίσμα της διασφάλισης της ιδιωτικότητας των καταναλωτών, έχει οδηγήσει στην ανάπτυξη και υιοθέτηση προηγμένων κρυπτογραφικών λύσεων. Στο επίκεντρο αυτών των εξελίξεων βρίσκονται η Ομομορφική Κρυπτογράφηση

(Homomorphic Encryption - HE) και ο Ασφαλής Πολυμερής Υπολογισμός (Secure Multi-party Computation - SMC). Οι τεχνικές αυτές επιτρέπουν την εξαγωγή στατιστικών συμπερασμάτων και την ανάλυση κρυπτογραφημένων δεδομένων, διασφαλίζοντας παράλληλα ότι οι ευαίσθητες πληροφορίες παραμένουν απρόσιτες σε μη εξουσιοδοτημένες οντότητες (Bibi et al., 2025· Xiao et al., 2025).

Η Ομομορφική Κρυπτογράφηση (HE) αποτελεί μια πρωτοποριακή προσέγγιση που επιτρέπει την εκτέλεση μαθηματικών πράξεων απευθείας πάνω στα κρυπτογραφημένα δεδομένα. Το παραγόμενο αποτέλεσμα, μετά την αποκρυπτογράφησή του, ταυτίζεται με εκείνο που θα προέκυπτε αν οι πράξεις είχαν διενεργηθεί στα αρχικά δεδομένα. Στο πλαίσιο των Έξυπνων Δικτύων, η HE είναι καθοριστική για την προστασία της πληροφορίας κατά τη μετάδοση και την ανάλυση, καθώς αποτρέπει την επανταυτοποίηση των χρηστών μέσω της μελέτης των προτύπων κατανάλωσης (Adewole & Torra, 2022).

Ιδιαίτερο ενδιαφέρον παρουσιάζει το κρυπτοσύστημα Paillier, μια μερικώς ομομορφική τεχνική (PHE) που υποστηρίζει την πρόσθεση. Η εφαρμογή του είναι ιδανική για την άθροιση φορτίου και τον υπολογισμό Ευκλείδειων αποστάσεων για την επιλογή τιμολογίων, χωρίς να αποκαλύπτεται το αναλυτικό προφίλ φορτίου του χρήστη (Unterweger et al., 2016). Ωστόσο, η πολυπλοκότητα των σύγχρονων αναγκών έχει ωθήσει την έρευνα προς σχήματα όπως το TFHE (Fully Homomorphic Encryption over the Torus). Το TFHE επιτρέπει την εκτέλεση λογικών πυλών και μη γραμμικών πράξεων, οι οποίες είναι απαραίτητες για την έγκαιρη ανίχνευση ανωμαλιών στο δίκτυο (Xiao et al., 2025). Παρά τα πλεονεκτήματα αυτά, η HE αντιμετωπίζει προκλήσεις που σχετίζονται με το υψηλό υπολογιστικό κόστος και τον μεγάλο όγκο δεδομένων. Για τον μετριασμό αυτών των περιορισμών, προτείνονται υβριδικά μοντέλα που συνδυάζουν την αποδοτική άθροιση του Paillier με την αναλυτική ισχύ του TFHE, επιτυγχάνοντας ασφαλή ανίχνευση κυβερνοεπιθέσεων με βελτιστοποιημένη χρήση πόρων (Xiao et al., 2025).

Παράλληλα, ο Ασφαλής Πολυμερής Υπολογισμός (SMC) προσφέρει μια εναλλακτική μέθοδο συνεργατικής επεξεργασίας. Στο μοντέλο αυτό, διαφορετικές οντότητες —όπως καταναλωτές, προμηθευτές και έμπιστοι τρίτοι— συνεργάζονται για τον υπολογισμό μιας συνάρτησης χωρίς να αποκαλύπτει η μία στην άλλη τα δεδομένα εισόδου της. Η προσέγγιση αυτή είναι ιδιαίτερα αποτελεσματική σε

περιβάλλοντα περιορισμένης εμπιστοσύνης, καθώς διασφαλίζει ότι μόνο το τελικό αποτέλεσμα καθίσταται γνωστό (Unterweger et al., 2016).

Στα Έξυπνα Δίκτυα, ο SMC χρησιμοποιείται κυρίως για τον προσδιορισμό βέλτιστων τιμολογίων και την ανίχνευση κακόβουλων ενεργειών. Μέσω σχημάτων διαμοιρασμού μυστικού (secret sharing), προσφέρει υψηλή ακρίβεια και εξαλείφει τα μεμονωμένα σημείων αποτυχίας (single points of failure). Η επιτυχία του SMC βασίζεται στην αυστηρή τήρηση πρωτοκόλλων επικοινωνίας που εμποδίζουν τη διαρροή πληροφοριών μέσω των ενδιάμεσων υπολογιστικών σταδίων, καθιστώντας τον μια στιβαρή λύση για τη διασφάλιση της ιδιωτικότητας σε κρίσιμες υποδομές (Unterweger et al., 2016· Bibi et al., 2025).

4.2.2. Homomorphic encryption, secure multi-party computation

Η επιτακτική ανάγκη για επεξεργασία δεδομένων κατανάλωσης σε πραγματικό χρόνο, υπό το πρίσμα της διασφάλισης της ιδιωτικότητας των καταναλωτών, έχει οδηγήσει στην υιοθέτηση προηγμένων κρυπτογραφικών λύσεων. Στο επίκεντρο αυτών των εξελίξεων βρίσκονται η Ομομορφική Κρυπτογράφηση (Homomorphic Encryption - HE) και ο Ασφαλής Πολυμερής Υπολογισμός (Secure Multi-party Computation - SMC). Οι τεχνικές αυτές επιτρέπουν την εξαγωγή στατιστικών συμπερασμάτων και την ανάλυση κρυπτογραφημένων δεδομένων, διασφαλίζοντας παράλληλα ότι οι ευαίσθητες πληροφορίες παραμένουν απρόσιτες σε μη εξουσιοδοτημένες οντότητες (Bibi et al., 2025· Xiao et al., 2025).

Η Ομομορφική Κρυπτογράφηση (HE) αποτελεί μια πρωτοποριακή προσέγγιση που επιτρέπει την εκτέλεση μαθηματικών πράξεων απευθείας πάνω στα κρυπτογραφημένα δεδομένα. Το παραγόμενο αποτέλεσμα, μετά την αποκρυπτογράφησή του, ταυτίζεται με εκείνο που θα προέκυπτε αν οι πράξεις είχαν διενεργηθεί στα αρχικά δεδομένα. Στο πλαίσιο των Έξυπνων Δικτύων, η HE είναι καθοριστική για την προστασία της πληροφορίας κατά τη μετάδοση και την ανάλυση, καθώς αποτρέπει την επανταυτοποίηση των χρηστών μέσω της μελέτης των προτύπων κατανάλωσης (Adewole & Torra, 2022).

Ιδιαίτερο ενδιαφέρον παρουσιάζει το κρυπτοσύστημα Paillier, μια μερικώς ομομορφική τεχνική (PHE) που υποστηρίζει την πρόσθεση. Η εφαρμογή του είναι

ιδανική για την άθροιση φορτίου και τον υπολογισμό Ευκλείδειων αποστάσεων για την επιλογή τιμολογίων, χωρίς να αποκαλύπτεται το αναλυτικό προφίλ φορτίου του χρήστη (Unterweger et al., 2016). Ωστόσο, η πολυπλοκότητα των σύγχρονων αναγκών έχει ωθήσει την έρευνα προς σχήματα όπως το TFHE (Fully Homomorphic Encryption over the Torus). Το TFHE επιτρέπει την εκτέλεση λογικών πυλών και μη γραμμικών πράξεων, οι οποίες είναι απαραίτητες για την έγκαιρη ανίχνευση ανωμαλιών στο δίκτυο (Xiao et al., 2025). Παρά τα πλεονεκτήματα αυτά, η HE αντιμετωπίζει προκλήσεις που σχετίζονται με το υψηλό υπολογιστικό κόστος και τον μεγάλο όγκο δεδομένων. Για τον μετριασμό αυτών των περιορισμών, προτείνονται υβριδικά μοντέλα που συνδυάζουν την αποδοτική άθροιση του Paillier με την αναλυτική ισχύ του TFHE, επιτυγχάνοντας ασφαλή ανίχνευση κυβερνοεπιθέσεων με βελτιστοποιημένη χρήση πόρων (Xiao et al., 2025).

Παράλληλα, ο Ασφαλής Πολυμερής Υπολογισμός (SMC) προσφέρει μια εναλλακτική μέθοδο συνεργατικής επεξεργασίας. Στο μοντέλο αυτό, διαφορετικές οντότητες —όπως καταναλωτές, προμηθευτές και έμπιστοι τρίτοι— συνεργάζονται για τον υπολογισμό μιας συνάρτησης χωρίς να αποκαλύπτει η μία στην άλλη τα δεδομένα εισόδου της. Η προσέγγιση αυτή είναι ιδιαίτερα αποτελεσματική σε περιβάλλοντα περιορισμένης εμπιστοσύνης, καθώς διασφαλίζει ότι μόνο το τελικό αποτέλεσμα καθίσταται γνωστό (Unterweger et al., 2016).

Στα Έξυπνα Δίκτυα, ο SMC χρησιμοποιείται κυρίως για τον προσδιορισμό βέλτιστων τιμολογίων και την ανίχνευση κακόβουλων ενεργειών. Μέσω σχημάτων διαμοιρασμού μυστικού (secret sharing), προσφέρει υψηλή ακρίβεια και εξαλείφει τα μεμονωμένα σημεία αποτυχίας (single points of failure). Η επιτυχία του SMC βασίζεται στην αυστηρή τήρηση πρωτοκόλλων επικοινωνίας που εμποδίζουν τη διαρροή πληροφοριών μέσω των ενδιάμεσων υπολογιστικών σταδίων, καθιστώντας τον μια στιβαρή λύση για τη διασφάλιση της ιδιωτικότητας σε κρίσιμες υποδομές (Unterweger et al., 2016· Bibi et al., 2025).

4.2.3. Differential privacy και εφαρμογές σε Smart Grids

Η Διαφορική Ιδιωτικότητα (Differential Privacy - DP) αποτελεί ένα από τα πιο ισχυρά μαθηματικά πλαίσια για τη διασφάλιση της ιδιωτικότητας στα έξυπνα δίκτυα. Η βασική της αρχή έγκειται στην προσθήκη ελεγχόμενου στατιστικού θορύβου στα

δεδομένα κατανάλωσης, έτσι ώστε η παρουσία ή η απουσία ενός συγκεκριμένου χρήστη σε ένα σύνολο δεδομένων να μην επηρεάζει σημαντικά το αποτέλεσμα της ανάλυσης, καθιστώντας αδύνατη την επανταυτοποίησή του (Cao et al., 2018).

Η Πρόκληση του NILM και η Ανάγκη για DP

Μία από τις μεγαλύτερες απειλές για την ιδιωτικότητα των καταναλωτών είναι η Μη Παρεμβατική Παρακολούθηση Φορτίου (Non-Intrusive Load Monitoring - NILM). Μέσω του NILM, ένας εισβολέας μπορεί να αναλύσει τις λεπτομερείς μετρήσεις ενός έξυπνου μετρητή και να προσδιορίσει ποιες ηλεκτρικές συσκευές χρησιμοποιούνται και πότε, αποκαλύπτοντας ευαίσθητες καθημερινές δραστηριότητες των ενοίκων. Η Διαφορική Ιδιωτικότητα παρεμβαίνει σε αυτό το σημείο, «θορυβώνοντας» τις μετρήσεις με τέτοιο τρόπο ώστε να αποκρύπτονται οι υπογραφές των επιμέρους συσκευών, διατηρώντας παράλληλα τη συνολική χρηστικότητα των δεδομένων για τον πάροχο ενέργειας (Cao et al., 2018).

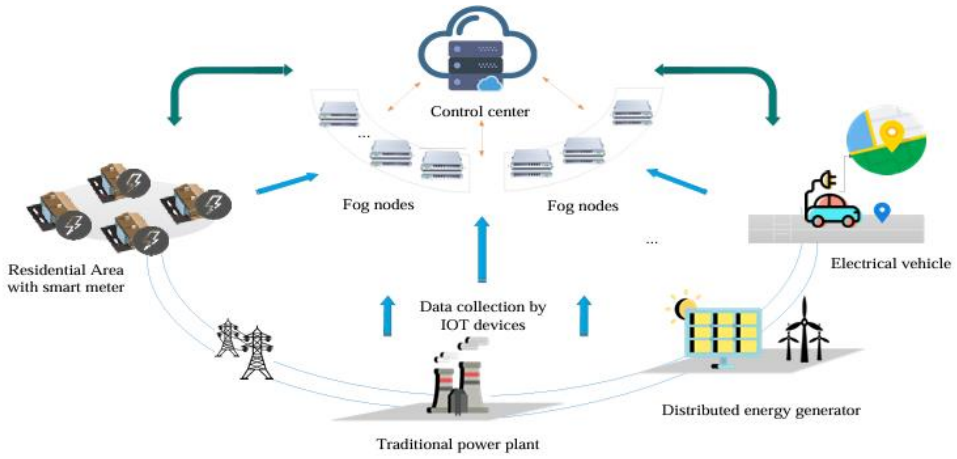
Τοπική Διαφορική Ιδιωτικότητα (Local Differential Privacy - LDP)

Μια εξελιγμένη μορφή της τεχνικής είναι η Τοπική Διαφορική Ιδιωτικότητα (LDP). Σε αντίθεση με την κλασική DP, όπου ο θόρυβος προστίθεται από έναν κεντρικό συλλέκτη δεδομένων, στην LDP ο θόρυβος προστίθεται απευθείας στον έξυπνο μετρητή του χρήστη πριν από τη μετάδοση. Όπως εξηγούν οι Gai κ.ά. (2022), αυτή η προσέγγιση εξαλείφει την ανάγκη για έναν «έμπιστο τρίτο», καθώς τα δεδομένα φεύγουν από το σπίτι του καταναλωτή ήδη προστατευμένα. Με τη χρήση μηχανισμών όπως η «Τυχαιοποιημένη Απόκριση» (Randomized Response), η LDP επιτρέπει στο κέντρο ελέγχου να εκτελεί στατιστικές αναλύσεις μεγάλης κλίμακας (π.χ. μέση κατανάλωση γειτονιάς) χωρίς να βλέπει ποτέ τις πραγματικές, ακατέργαστες μετρήσεις κανενός χρήστη.

Εφαρμογή μέσω Fog Computing

Για την αποτελεσματική υλοποίηση της DP στα έξυπνα δίκτυα, προτείνεται η χρήση αρχιτεκτονικών Fog Computing. Το επίπεδο "Fog" λειτουργεί ως ενδιάμεσος σταθμός κοντά στους χρήστες, ο οποίος αναλαμβάνει τη διαχείριση του θορύβου και τη συγκέντρωση των δεδομένων. Σύμφωνα με τους Cao κ.ά. (2018), η χρήση των Fog

nodes επιτρέπει τη διατήρηση της διαφορικής ιδιωτικότητας με πολύ χαμηλή υστέρηση (latency), γεγονός που είναι κρίσιμο για τις εφαρμογές πραγματικού χρόνου του έξυπνου δικτύου, όπως η απόκριση ζήτησης (demand response).



Εικόνα 10: Fog computing enabled data collection in smart grid (Πηγή:Cao et al., 2018)

Στη παραπάνω εικόνα υπάρχει η αρχιτεκτονική Fog Computing για το έξυπνο δίκτυο. Απεικονίζεται η διαστρωμάτωση μεταξύ των έξυπνων μετρητών, των κόμβων Fog (όπου εφαρμόζεται η επεξεργασία για τη διαφορική ιδιωτικότητα) και του κεντρικού νέφους ελέγχου.

Συμπεράσματα και Trade-offs

Η εφαρμογή της DP στα Smart Grids χαρακτηρίζεται από έναν συμβιβασμό μεταξύ της στάθμης ιδιωτικότητας (privacy budget ϵ) και της ακρίβειας των δεδομένων. Οι Gai κ.ά. (2022) τονίζουν ότι η βέλτιστη ρύθμιση του θορύβου επιτρέπει στο δίκτυο να λειτουργεί αποδοτικά (π.χ. για εξισορρόπηση φορτίου) διασφαλίζοντας ταυτόχρονα ότι οι προσωπικές συνήθειες των καταναλωτών παραμένουν μαθηματικά απρόσιτες σε οποιονδήποτε τρίτο.

4.3.Κανονιστικό πλαίσιο

4.3.1. Ρυθμιστικό Πλαίσιο, Διεθνή Πρότυπα και Βέλτιστες Πρακτικές Ασφαλείας (GDPR, NIS2, ENISA guidelines)

Η ενσωμάτωση προηγμένων ψηφιακών τεχνολογιών στα Έξυπνα Δίκτυα απαιτεί ένα ισχυρό θεσμικό πλαίσιο που να εξισορροπεί την ιδιωτικότητα του ατόμου με την

εθνική ενεργειακή ασφάλεια. Καθώς τα ενεργειακά συστήματα γίνονται όλο και πιο διασυνδεδεμένα, η συμμόρφωση με ολοκληρωμένους κανονισμούς, όπως ο **Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)** και η **Οδηγία NIS2**, καθίσταται επιτακτική. Σύμφωνα με τον GDPR, τα δεδομένα κατανάλωσης ενέργειας υψηλής ανάλυσης ταξινομούνται ως «δεδομένα προσωπικού χαρακτήρα», καθώς μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες για τις καθημερινές συνήθειες ή την κατάσταση υγείας ενός ενοίκου (EU Cyber Laws, 2024). Κατά συνέπεια, οι διαχειριστές του δικτύου πρέπει να τηρούν την αρχή της ελαχιστοποίησης των δεδομένων, συλλέγοντας μόνο ό,τι είναι απολύτως απαραίτητο για την επεξεργασία, διασφαλίζοντας παράλληλα ότι τα πρωτόκολλα για το «Δικαίωμα στη Λήθη» είναι ενσωματωμένα στα συστήματα διαχείρισης των βάσεων δεδομένων τους (Bibi et al., 2025).

Ενώ ο GDPR προστατεύει το άτομο, η **Οδηγία NIS2** επικεντρώνεται στη συλλογική ανθεκτικότητα των δικτύων και των συστημάτων πληροφοριών. Η NIS2 εισάγει αυστηρές υποχρεώσεις αναφοράς, απαιτώντας από τους φορείς εκμετάλλευσης να ειδοποιούν τις αρχές για σημαντικά περιστατικά ασφαλείας εντός 24 ωρών (ENISA, 2024b). Επιπλέον, αντιμετωπίζει την ασφάλεια της εφοδιαστικής αλυσίδας επιβάλλοντας στις εταιρείες ενέργειας να ελέγχουν τους προμηθευτές τους —όπως τους κατασκευαστές έξυπνων μετρητών— για να διασφαλίσουν την απουσία «πίσω πορτών» (backdoors) σε υλικό ή λογισμικό (Achaal et al., 2024). Για να γεφυρώσει το χάσμα μεταξύ αυτών των νομικών εντολών και της τεχνικής εφαρμογής, ο **Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)** παρέχει οδηγίες που ευνοούν τις **Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης (Zero Trust)**, όπου κάθε οντότητα του δικτύου επαληθεύεται συνεχώς, παράλληλα με τεχνικές όπως η Διαφορική Ιδιωτικότητα (Differential Privacy) για την ικανοποίηση των απαιτήσεων ανωνυμοποίησης (ENISA, 2024a).

Η διαχείριση της ιδιωτικότητας στα Έξυπνα Δίκτυα τυποποιείται περαιτέρω μέσω της υιοθέτησης διεθνώς αναγνωρισμένων πλαισίων, με κυριότερο το **ISO/IEC 27701**. Ως επέκταση του ISO/IEC 27001, το πρότυπο αυτό καθιερώνει ένα Σύστημα Διαχείρισης Πληροφοριών Ιδιωτικότητας (PIMS) που ορίζει σαφείς ρόλους διακυβέρνησης δεδομένων και επιβάλλει Εκτιμήσεις Αντικτύπου στην Προστασία Δεδομένων (DPIA) πριν από την εγκατάσταση νέων τεχνολογιών μέτρησης (ISO, 2024; Bibi et

al., 2025). Αυτό συχνά συμπληρώνεται από το **Πλαίσιο Κυβερνοασφάλειας του NIST**, το οποίο περιγράφει τις βασικές λειτουργίες Προσδιορισμού, Προστασίας, Ανίχνευσης, Απόκρισης και Ανάκαμψης, καθώς και από το πρότυπο **IEC 62351**, το οποίο θωρακίζει ειδικά τα πρωτόκολλα επικοινωνίας όπως τα DNP3 και IEC 61850 μέσω προηγμένης κρυπτογράφησης και αυθεντικοποίησης (Achaal et al., 2024).

Τελικά, η επίτευξη ασφάλειας υψηλού επιπέδου απαιτεί την καλλιέργεια μιας οργανωσιακής κουλτούρας που αντιμετωπίζει τη συμμόρφωση ως έναν κύκλο συνεχούς βελτίωσης και όχι ως μια στατική εργασία. Σύμφωνα με τον **ENISA (2025)**, οι βέλτιστες πρακτικές πρέπει να επικεντρώνονται στην τεχνική θωράκιση, όπως η **μικρο-κατάτμηση (micro-segmentation)** του δικτύου για την πρόληψη της οριζόντιας μετακίνησης των εισβολέων, και την εφαρμογή Αυθεντικοποίησης Πολλαπλών Παραγόντων (MFA) για όλα τα κρίσιμα συστήματα. Η επιχειρησιακή ανθεκτικότητα είναι εξίσου ζωτική· οι οργανισμοί θα πρέπει να διατηρούν αντίγραφα ασφαλείας "air-gapped" (φυσικά απομονωμένα) και να χρησιμοποιούν συστήματα **SIEM/SOAR** για την ανάλυση αρχείων καταγραφής (logs) σε πραγματικό χρόνο και την αυτοματοποιημένη απόκριση σε περιστατικά. Τέλος, επειδή ο ανθρώπινος παράγοντας παραμένει μια σημαντική ευπάθεια, η συνεχής εκπαίδευση σε θέματα phishing και κοινωνικής μηχανικής είναι απαραίτητη για να διασφαλιστεί ότι το προσωπικό σε όλα τα επίπεδα μπορεί να αμυνθεί έναντι των εξελισσόμενων κυβερνοαπειλών (ENISA, 2025).

Κεφάλαιο 5: 6G Δίκτυα και Ασφαλείς Αρχιτεκτονικές

5.1 Χαρακτηριστικά 6G και διαφορές με 5G

5.1.1. AI-native δίκτυα, terahertz spectrum, ultra-low latency

Η μετάβαση από το 5G στο 6G δεν αποτελεί μια απλή γραμμική αναβάθμιση, αλλά έναν ριζικό επανασχεδιασμό της αρχιτεκτονικής των δικτύων. Η σημαντικότερη διαφορά έγκειται στην έννοια του **AI-native** δικτύου. Ενώ το 5G χρησιμοποιεί την Τεχνητή Νοημοσύνη (AI) ως ένα εξωτερικό εργαλείο βελτιστοποίησης, το 6G ενσωματώνει τη νοημοσύνη ως δομικό στοιχείο (intrinsic element) σε κάθε επίπεδο της στοίβας επικοινωνίας. Αυτό επιτρέπει στο δίκτυο να λαμβάνει αυτόνομες αποφάσεις σε πραγματικό χρόνο, να αυτο-θεραπεύεται και να διαχειρίζεται την πολυπλοκότητα των πόρων με τρόπο που ήταν αδύνατος στις προηγούμενες γενιές (Omheni et al., 2025· Shome et al., 2025).

Ο δεύτερος πυλώνας του 6G είναι η αξιοποίηση του φάσματος **Terahertz (THz)**, το οποίο καταλαμβάνει τις συχνότητες μεταξύ 0,1 και 10 THz. Η χρήση αυτών των εξαιρετικά υψηλών συχνοτήτων προσφέρει τεράστιο εύρος ζώνης, επιτρέποντας ρυθμούς μετάδοσης δεδομένων που αγγίζουν το επίπεδο του Terabit ανά δευτερόλεπτο (Tbps). Σε σύγκριση με το 5G, το οποίο περιορίζεται στο φάσμα των mmWave (κάτω από 100 GHz), το 6G ξεκλειδώνει εφαρμογές όπως η ολογραφική τηλεπαρουσία και τα ψηφιακά δίδυμα (digital twins) υψηλής πιστότητας, που απαιτούν τεράστια χωρητικότητα δικτύου (Shome et al., 2025).

Ωστόσο, η χρήση του φάσματος THz εισάγει σημαντικές προκλήσεις, όπως οι ακραίες απώλειες διάδοσης και η ευαισθησία σε εμπόδια (blockage sensitivity). Για την αντιμετώπιση αυτών, το 6G εισάγει τις **Έξυπνες Ανακλαστικές Επιφάνειες (Intelligent Reflecting Surfaces - IRS)**. Αυτές οι επιφάνειες, ελεγχόμενες από αλγορίθμους AI, μπορούν να "καμπυλώνουν" και να ανακατευθύνουν τις δέσμες THz γύρω από εμπόδια, δημιουργώντας έξυπνα περιβάλλοντα επικοινωνίας. Αυτή η δυναμική διαμόρφωση του ασύρματου καναλιού αποτελεί μια θεμελιώδη διαφορά από το 5G, όπου το περιβάλλον θεωρούνταν στατικό και ανεξέλεγκτο (Balaji et al., 2025).

Η επίτευξη **εξαιρετικά χαμηλής υστέρησης (Ultra-low latency)** αποτελεί τον τρίτο κρίσιμο παράγοντα διαφοροποίησης. Ενώ το 5G στόχευε σε υστέρηση της τάξης του 1ms, το 6G στοχεύει σε επίπεδα κάτω από το 0,1ms (sub-millisecond). Αυτή η σχεδόν ακαριαία απόκριση είναι απαραίτητη για τον «Διαδίκτυο των Αισθήσεων» και την απομακρυσμένη χειρουργική ακριβείας. Η AI-native φύση του δικτύου επιτρέπει την πρόβλεψη της κίνησης και την προληπτική κατανομή πόρων, μειώνοντας δραματικά τους χρόνους αναμονής που παρατηρούνταν στο 5G (Shome et al., 2025· Omheni et al., 2025).

Για την υποστήριξη αυτής της χαμηλής υστέρησης, το 6G βασίζεται σε μια αποκεντρωμένη αρχιτεκτονική **Federated Edge AI**. Αντί τα δεδομένα να στέλνονται σε κεντρικούς διακομιστές (cloud), η επεξεργασία και η εκπαίδευση των μοντέλων AI συμβαίνουν τοπικά στους κόμβους άκρου (edge nodes). Αυτό όχι μόνο μειώνει την καθυστέρηση μετάδοσης, αλλά ενισχύει και την ιδιωτικότητα, καθώς τα ευαίσθητα δεδομένα των χρηστών δεν εγκαταλείπουν την τοπική υποδομή, μια σημαντική εξέλιξη σε σχέση με τις πιο συγκεντρωτικές προσεγγίσεις του 5G (Balaji et al., 2025).

Επιπλέον, το 6G εισάγει την τεχνολογία **Integrated Sensing and Communication (ISAC)**. Στο 6G, οι ίδιες οι κυματομορφές THz χρησιμοποιούνται ταυτόχρονα για τη μεταφορά δεδομένων και για την ανίχνευση του περιβάλλοντος (σαν ραντάρ). Αυτό επιτρέπει στο δίκτυο να «βλέπει» και να χαρτογραφεί τον φυσικό χώρο με ακρίβεια εκατοστού, προσφέροντας στην AI-native αρχιτεκτονική μια πρωτοφανή επίγνωση περιβάλλοντος (context awareness). Το 5G στερείται αυτής της εγγενούς δυνατότητας αίσθησης, παραμένοντας ένα καθαρά επικοινωνιακό μέσο (Omheni et al., 2025).

Η ασφάλεια σε ένα τόσο ευφυές και γρήγορο δίκτυο πρέπει επίσης να είναι αναβαθμισμένη. Το 6G ενσωματώνει **Κβαντική Κρυπτογραφία** και πρωτόκολλα Quantum Key Distribution (QKD) για την προστασία των THz links. Με τη βοήθεια της AI για τη διόρθωση σφαλμάτων σε κβαντικό επίπεδο, το 6G προσφέρει προστασία έναντι μελλοντικών κβαντικών απειλών, την ώρα που το 5G βασίζεται σε παραδοσιακές κρυπτογραφικές μεθόδους που ενδέχεται να καταστούν ευάλωτες τα επόμενα χρόνια (Balaji et al., 2025).

Τέλος, η διαχείριση της ενέργειας στα AI-native δίκτυα 6G γίνεται με τρόπο δυναμικό και "πράσινο". Η AI μπορεί να απενεργοποιεί τμήματα του δικτύου ή να ρυθμίζει την κατανάλωση των IRS σε πραγματικό χρόνο, ανάλογα με τη ζήτηση. Ενώ το 5G έκανε βήματα προς την ενεργειακή απόδοση, το 6G στοχεύει σε πλήρως βιώσιμα δίκτυα, όπου η ευφυΐα χρησιμοποιείται για την ελαχιστοποίηση του ανθρακικού αποτυπώματος των Terahertz επικοινωνιών (Omheni et al., 2025· Balaji et al., 2025).

5.1.2. Νέες δυνατότητες για Smart Grids και IoT integration

Η μετάβαση από το 5G στο 6G αντιπροσωπεύει κάτι πολύ περισσότερο από μια απλή αύξηση στις ταχύτητες μετάδοσης δεδομένων· σηματοδοτεί μια θεμελιώδη αλλαγή παραδείγματος προς μια «εγγενώς νοήμονα» (AI-native) αρχιτεκτονική δικτύου. Ενώ το 5G έθεσε τις αρχικές βάσεις για τη συνδεσιμότητα των Έξυπνων Δικτύων (Smart Grids), το 6G έχει σχεδιαστεί για να ξεπεράσει τους υφιστάμενους περιορισμούς όσον αφορά τη βαθιά ενσωμάτωση της Τεχνητής Νοημοσύνης (AI) και τη μαζική επεξεργασία δεδομένων στο άκρο του δικτύου (Khan, 2025). Με τη χρήση συχνοτήτων Terahertz (THz), το 6G προσφέρει σχεδόν μηδενική καθυστέρηση — κάτω από 0,1 ms— καθιστώντας το την οριστική υποδομή για κρίσιμες εφαρμογές IoT που απαιτούν ακρίβεια σε πραγματικό χρόνο και απόκριση κλασμάτων του δευτερολέπτου (Ullah et al., 2025).

Ένα καθοριστικό χαρακτηριστικό του οικοσυστήματος 6G-IoT είναι η ικανότητά του να υποστηρίζει μαζική πυκνότητα συσκευών, η οποία μπορεί να φτάσει έως και τα 10 εκατομμύρια αντικείμενα ανά τετραγωνικό χιλιόμετρο (Khan, 2025). Αυτή η επέκταση συνοδεύεται από την πρωτοποριακή ιδέα του "Zero-energy IoT", μια εξέλιξη που θα μπορούσε να φέρει επανάσταση στη συντήρηση των Smart Grids. Υπό αυτό το πλαίσιο, οι αισθητήρες μπορούν να λειτουργούν χωρίς παραδοσιακές μπαταρίες, συλλέγοντας ενέργεια από το περιβάλλον, όπως ραδιοκύματα ή ηλιακή ακτινοβολία. Αυτή η καινοτομία όχι μόνο μειώνει το λειτουργικό κόστος, αλλά ελαχιστοποιεί σημαντικά και το περιβαλλοντικό αποτύπωμα των ενεργειακών αναπτύξεων μεγάλης κλίμακας (Ullah et al., 2025).

Η εισαγωγή της Νοημοσύνης στο Άκρο (Edge Intelligence) εντός του πλαισίου του 6G ενισχύει περαιτέρω τα Έξυπνα Δίκτυα με πρωτοφανή αυτονομία. Επιτρέποντας τη

λήψη αποφάσεων τοπικά, το 6G εξαλείφει την ανάγκη για συνεχή μεταφορά δεδομένων σε κεντρικούς διακομιστές Cloud, κάτι που είναι απαραίτητο για την ταχεία ανίχνευση σφαλμάτων και τις δυνατότητες «αυτοθεραπείας» (self-healing). Έρευνες δείχνουν ότι τέτοιες αρχιτεκτονικές μπορούν να επιτύχουν ακρίβεια αυτοθεραπείας έως και 98% (Khan, 2025). Αυτή η τοπική νοημοσύνη είναι ιδιαίτερα ζωτική για την απρόσκοπτη ενσωμάτωση ανανεώσιμων πηγών ενέργειας, καθώς η στοχαστική και απρόβλεπτη φύση τους απαιτεί τους εξαιρετικά γρήγορους αλγορίθμους εξισορρόπησης που μόνο μια υποδομή 6G μπορεί να υποστηρίξει αξιόπιστα (Naja et al., 2023).

Επιπλέον, το 6G βελτιστοποιεί τη διαχείριση της ενέργειας μέσω εξελιγμένου Network Slicing και της ωρίμανσης της τεχνολογίας Vehicle-to-Grid (V2G). Σε ένα περιβάλλον 6G, το δίκτυο μπορεί να δημιουργήσει δυναμικά «λογικά κανάλια» που δίνουν προτεραιότητα στις ροές ενέργειας προς κρίσιμες υποδομές, όπως νοσοκομεία, κατά τη διάρκεια περιόδων αιχμής (Naja et al., 2023). Όταν συνδυάζονται με την τεχνολογία Blockchain, αυτές οι συναλλαγές γίνονται διαφανείς και αμετάβλητες, θωρακίζοντας το δίκτυο από κυβερνοεπιθέσεις που διαφορετικά θα μπορούσαν να απειλήσουν τη συστημική σταθερότητα (Ullah et al., 2025).

Τέλος, η σύγκλιση της «Ολοκληρωμένης Αίσθησης και Επικοινωνίας» (ISAC) επιτρέπει στα δίκτυα 6G να λειτουργούν ως ένα κατανεμημένο σύστημα ραντάρ, διευκολύνοντας τη δημιουργία «Ψηφιακών Διδύμων» (Digital Twins) ολόκληρης της ενεργειακής υποδομής σε πραγματικό χρόνο. Αυτά τα ψηφιακά αντίγραφα επιτρέπουν στους διαχειριστές να προσομοιώνουν σενάρια κρίσης και να βελτιστοποιούν την κατανομή φορτίου με εξαιρετική ακρίβεια. Ευθυγραμμίζοντας τη συμπεριφορά του δικτύου με τις πραγματικές ανάγκες κυκλοφορίας και ενέργειας των αστικών περιβαλλόντων, τα συστήματα αυτά μπορούν να επιτύχουν επίπεδα ενεργειακής αποδοτικότητας έως και 94% (Khan, 2025; Ullah et al., 2025).

5.2. Edge computing και AI-driven security

5.2.1. Αποκεντρωμένη επεξεργασία δεδομένων

Η μετάβαση προς την αποκεντρωμένη επεξεργασία δεδομένων στα Έξυπνα Δίκτυα (Smart Grids) αναδεικνύεται ως μια στρατηγική απάντηση στους εγγενείς

περιορισμούς της κεντρικής διαχείρισης. Στα παραδοσιακά μοντέλα, η μεταφορά τεράστιου όγκου δεδομένων στο υπολογιστικό νέφος (Cloud) προκαλεί συχνά κρίσιμες καθυστερήσεις και υπερβολική κατανάλωση εύρους ζώνης. Για την αντιμετώπιση αυτών των προκλήσεων, οι Tariq κ.ά. (2024) προτείνουν μια αρχιτεκτονική βασισμένη στις τεχνολογίες Fog και Edge computing, η οποία διευκολύνει την τοπική ανάλυση των δεδομένων των υποδομών έξυπνης μέτρησης (AMI). Αυτή η αλλαγή παραδείγματος εξασφαλίζει ταχύτατη απόκριση σε ανώμαλες δραστηριότητες και μειώνει δραστικά τον χρόνο που απαιτείται για την ανίχνευση εισβολών, ενισχύοντας τη συνολική ευελιξία του δικτύου.

Μια βασική εξέλιξη σε αυτό το αποκεντρωμένο πλαίσιο είναι η ενσωμάτωση Συστημάτων Ανίχνευσης Εισβολών (IDS) απευθείας στις συσκευές Edge και Fog. Αντί να βασίζεται σε κεντρικούς διακομιστές για βαριές υπολογιστικές εργασίες, η σύγχρονη έρευνα υποστηρίζει τη χρήση αλγορίθμων Support Vector Machine (SVM) σε συνδυασμό με την Ομοσπονδιακή Μάθηση (Federated Learning) (Tariq et al., 2024). Αυτή η μεθοδολογία δίνει τη δυνατότητα στις τοπικές οντότητες να εκπαιδεύουν τα μοντέλα ασφαλείας τους ανεξάρτητα, μοιραζόμενες μόνο τις παραμέτρους που έχουν «μάθει» με ένα παγκόσμιο μοντέλο. Κατά συνέπεια, το δίκτυο θωρακίζεται απέναντι σε εξελιγμένες επιθέσεις χωρίς να εκτίθενται ποτέ πρωτογενή, ευαίσθητα δεδομένα των καταναλωτών στον κεντρικό πυρήνα.

Η υιοθέτηση της Ομοσπονδιακής Μάθησης επιλύει επιπλέον το μακροχρόνιο παράδοξο μεταξύ της ανάγκης για μαζικά δεδομένα εκπαίδευσης και των αυστηρών απαιτήσεων για την προστασία της ιδιωτικότητας. Μέσα σε αυτή τη δομή, οι έξυπνοι μετρητές λειτουργούν ως τοπικοί κόμβοι εκπαίδευσης, διασφαλίζοντας ότι οι ευαίσθητες πληροφορίες παραμένουν εντός των ασφαλών ορίων του σπιτιού ή της επιχείρησης (Jithish et al., 2025). Η προσέγγιση αυτή όχι μόνο διασφαλίζει τη συμμόρφωση με τους διεθνείς κανονισμούς προστασίας δεδομένων, αλλά δημιουργεί και ένα «συλλογικό ανοσοποιητικό σύστημα» για το Smart Grid. Όπως παρατηρούν οι Tariq κ.ά. (2024), η γνώση για μια νέα απειλή που ανιχνεύεται σε ένα μόνο σημείο μπορεί να διαδοθεί γρήγορα σε ολόκληρο το σύστημα μέσω ενημερώσεων των μοντέλων, παρέχοντας καθολική προστασία.

Τέλος, αυτή η αποκεντρωμένη αρχιτεκτονική βελτιστοποιεί σημαντικά την υπολογιστική και ενεργειακή απόδοση του ίδιου του δικτύου επικοινωνιών.

Μεταφέροντας εργασίες από το Cloud στα επίπεδα Fog και Edge, η συμφόρηση στο κύριο δίκτυο (core network) μετριάζεται, επιτρέποντας στους πόρους του Smart Grid να χρησιμοποιούνται πιο ορθολογικά και βιώσιμα (Jithish et al., 2025; Tariq et al., 2024). Αυτή η ιεραρχική προσέγγιση Cloud-Fog-Edge διασφαλίζει ότι το δίκτυο παραμένει λειτουργικό και ανθεκτικό, διατηρώντας το επίπεδο ασφαλείας του ακόμη και σε περίπτωση τοπικών αστοχιών υλικού ή συντονισμένων κυβερνοεπιθέσεων μεγάλης κλίμακας.

5.2.2. Predictive security, real-time monitoring, anomaly detection.

Η εξέλιξη των δικτύων 5G και η επικείμενη μετάβαση προς το 6G επιβάλλουν τη χρήση συστημάτων ασφαλείας που δεν είναι πλέον απλώς στατικά, αλλά θεμελιωδώς προσαρμοστικά. Σε αυτά τα δίκτυα επόμενης γενιάς, η παρακολούθηση σε πραγματικό χρόνο υποστηρίζεται από προηγμένους αλγορίθμους Μηχανικής Μάθησης (ML), οι οποίοι επιτρέπουν την ανάλυση της κίνησης του δικτύου στο άκρο (Edge). Αυτή η αποκεντρωμένη αναλυτική προσέγγιση επιτρέπει την άμεση αναγνώριση κακόβουλων δραστηριοτήτων, γεγονός που είναι κρίσιμο για την προστασία των υποδομών IoT (Kalodanis et al., 2025). Με την επεξεργασία των δεδομένων πιο κοντά στην πηγή, τα συστήματα αυτά μειώνουν σημαντικά τους χρόνους απόκρισης και αποτρέπουν αποτελεσματικά την κλιμάκωση των κυβερνοεπιθέσεων σε ολόκληρο το δίκτυο.

Κεντρικό στοιχείο αυτής της αρχιτεκτονικής αποτελεί η ανάπτυξη Συστημάτων Ανίχνευσης και Πρόληψης Εισβολών (IDPS) βασισμένων σε AI, τα οποία διευκολύνουν την ανίχνευση ανωμαλιών με εξαιρετική ακρίβεια. Σύμφωνα με τους Kalodanis κ.ά. (2025), εξελιγμένοι αλγόριθμοι, όπως τα Random Forests και τα Νευρωνικά Δίκτυα, μπορούν να διακρίνουν τη διαφορά μεταξύ μιας νόμιμης αύξησης της κίνησης και μιας συντονισμένης επίθεσης DDoS, ακόμη και μέσα στο εξαιρετικά δυναμικό περιβάλλον των δικτύων 6G. Αυτή η ικανότητα προσαρμογής σε νέες, άγνωστες απειλές (zero-day attacks) μέσω συνεχούς μάθησης είναι ο κύριος παράγοντας που διαφοροποιεί την ασφάλεια που καθοδηγείται από την AI από τις παραδοσιακές μεθόδους που βασίζονται σε στατικές υπογραφές (Haider et al., 2025).

Πέρα από την άμεση ανίχνευση, οι στρατηγικές προγνωστικής ασφάλειας ενισχύονται περαιτέρω μέσω της προληπτικής ανάλυσης κινδύνου. Αντί το σύστημα

να παραμένει σε μια αντιδραστική κατάσταση, χρησιμοποιεί προγνωστικά μοντέλα για να εντοπίσει συγκεκριμένα μοτίβα συμπεριφοράς που συνήθως προηγούνται μιας εισβολής. Αυτή η προνοητικότητα επιτρέπει την αυτόματη εφαρμογή μέτρων μετριασμού, όπως ο περιορισμός του ρυθμού δεδομένων ή η απομόνωση μολυσμένων κόμβων, πριν εκδηλωθεί πλήρως η παραβίαση (Kalodanis et al., 2025). Μια τέτοια προληπτική στάση είναι ζωτικής σημασίας για τη σταθερότητα των Έξυπνων Δικτύων (Smart Grids), όπου ακόμη και μια μικρή καθυστέρηση στην απόκριση μπορεί να οδηγήσει σε καταστροφικές αποτυχίες του συστήματος ισχύος.

Τέλος, καθώς αυτά τα συστήματα γίνονται πιο αυτόνομα, οι διαστάσεις της ηθικής χρήσης της Τεχνητής Νοημοσύνης και της κανονιστικής συμμόρφωσης καθίστανται υψίστης σημασίας. Υπάρχει μια αυξανόμενη ανάγκη για «Επεξηγήσιμη Τεχνητή Νοημοσύνη» (Explainable AI - XAI), ώστε να διασφαλίζεται ότι οι αποφάσεις που λαμβάνονται στο άκρο του δικτύου είναι διαφανείς, τεκμηριωμένες και συμβατές με κανονισμούς όπως η Πράξη της ΕΕ για την Τεχνητή Νοημοσύνη (AI Act) (Kalodanis et al., 2025). Για την εξισορρόπηση της ισχυρής ασφάλειας με την ιδιωτικότητα των χρηστών, η Ομοσπονδιακή Μάθηση (Federated Learning) έχει αναδειχθεί ως κεντρική τεχνολογία, επιτρέποντας την εκπαίδευση μοντέλων χωρίς την ανάγκη κοινής χρήσης ακατέργαστων, ευαίσθητων δεδομένων (Haider et al., 2025). Αυτή η συνέργεια προηγμένων αναλύσεων και ηθικών πλαισίων διασφαλίζει ότι ο ψηφιακός μετασχηματισμός της ενέργειας παραμένει ασφαλής και αξιόπιστος.

5.3. Blockchain για ακεραιότητα και trust management

5.3.1. Ασφαλείς συναλλαγές ενέργειας

Η διασφάλιση των συναλλαγών στα έξυπνα δίκτυα (Smart Grids) αποτελεί τον κεντρικό πυλώνα για τη μετάβαση σε αποκεντρωμένα συστήματα peer-to-peer (P2P). Η τεχνολογία blockchain παρέχει το απαραίτητο πλαίσιο για την επίτευξη ακεραιότητας και τη διαχείριση της εμπιστοσύνης (trust management) μέσω ενός συνδυασμού κρυπτογραφικών μεθόδων και έξυπνων συμβολαίων, τα οποία καθιστούν κάθε ενεργειακή ανταλλαγή διαφανή, αμετάβλητη και απαλλαγμένη από την ανάγκη εξάρτησης από έμπιστα τρίτα μέρη (TTP) (Jyoti, 2022; Su et al., 2024; Dorri et al., 2019).

Η ακεραιότητα των δεδομένων εγγυάται από τη χρήση ψηφιακών υπογραφών και κρυπτογραφίας ελλειπτικής καμπύλης (ECC), μειώνοντας την υπολογιστική επιβάρυνση (Jyoti, 2022). Παράλληλα, η εισαγωγή «ατομικών μετα-συναλλαγών» (atomic meta-transactions) διασφαλίζει ότι μια αγοραπωλησία ενέργειας ολοκληρώνεται μόνο αν και τα δύο μέρη εκπληρώσουν τις υποχρεώσεις τους εντός προκαθορισμένου χρόνου, ενώ η χρήση αλγορίθμων αντιστοίχισης παραγγελιών (order-matching) διατηρεί τις τιμές σε λογικά επίπεδα, ενισχύοντας την εμπιστοσύνη των χρηστών (Dorri et al., 2019; Su et al., 2024).

Καθοριστικό ρόλο στη διαχείριση της εμπιστοσύνης παίζουν τα έξυπνα συμβόλαια (Smart Contracts), τα οποία αυτοματοποιούν την επιβολή των κανόνων της αγοράς. Η χρήση τους μειώνει τις διαφορές στις χρεώσεις (billing disputes) κατά 35%, ενώ η υιοθέτηση υβριδικών μηχανισμών συναίνεσης βασισμένων στην πίστωση (credit-based consensus) εξασφαλίζει ότι μόνο αξιόπιστοι κόμβοι συμμετέχουν στην επικύρωση, βελτιώνοντας την ασφάλεια και την απόδοση του συστήματος (Jyoti, 2022; Su et al., 2024).

Για την υποστήριξη συναλλαγών σε πραγματικό χρόνο, η επιλογή αποδοτικών πρωτοκόλλων είναι κρίσιμη, με το PBFT να προσφέρει ταχύτητες έως 1.500 TPS (Jyoti, 2022). Σύγχρονες αρχιτεκτονικές όπως το Secure Private Blockchain (SPB) μειώνουν την επιβάρυνση του δικτύου μέσω δρομολόγησης βασισμένης σε δημόσια κλειδιά (PK-based routing), επιτυγχάνοντας υψηλή διακίνηση (throughput) με εξαιρετικά χαμηλή κατανάλωση πόρων (Su et al., 2024; Dorri et al., 2019).

Τέλος, η προστασία της ιδιωτικότητας των χρηστών επιτυγχάνεται μέσω ανώνυμης αυθεντικοποίησης των έξυπνων μετρητών, διασφαλίζοντας ότι τα ευαίσθητα δεδομένα κατανάλωσης παραμένουν εμπιστευτικά (Dorri et al., 2019). Αυτή η προσέγγιση, σε συνδυασμό με την IoT ενσωμάτωση και τη βελτιστοποίηση της χρήσης ισχύος (έως 0.84), δημιουργεί ένα ολοκληρωμένο και ασφαλές οικοσύστημα που προστατεύει την ακεραιότητα ολόκληρου του ενεργειακού δικτύου (Su et al., 2024; Jyoti, 2022).

5.3.2. Consensus mechanisms, distributed ledger, smart contracts.

Η επιτυχής υλοποίηση του ψηφιακού μετασχηματισμού στα σύγχρονα ενεργειακά συστήματα βασίζεται σε μεγάλο βαθμό στην υιοθέτηση της τεχνολογίας του Κατανεμημένου Καθολικού (Distributed Ledger Technology - DLT). Το κατανεμημένο καθολικό αποτελεί τη θεμελιώδη υποδομή για την ακεραιότητα των συναλλαγών, επιτρέποντας την καταγραφή ενεργειακών ανταλλαγών σε μια αποκεντρωμένη βάση δεδομένων. Η δομή αυτή εξασφαλίζει τη διαφάνεια και το αμετάβλητο των δεδομένων, ενώ μέσω εξειδικευμένων πλαισίων, όπως το Electron Volt Exchange (EVE), διασφαλίζεται ότι οι συναλλαγές δεν αποτελούν απλές διμερείς ανταλλαγές, αλλά εγγυώνται την αξιόπιστη λειτουργία της αγοράς χωρίς την ανάγκη κεντρικών διαμεσολαβητών (Yao et al., 2024; Saha et al., 2020; Shamaseen et al., 2025).

Στο πλαίσιο αυτής της αποκεντρωμένης αρχιτεκτονικής, τα Έξυπνα Συμβόλαια (Smart Contracts) διαδραματίζουν καθοριστικό ρόλο ως εργαλεία αυτοματοποιημένης εμπιστοσύνης. Λειτουργώντας ως αυτοεκτελούμενοι κώδικες, τα συμβόλαια αυτά αυτοματοποιούν τη διαχείριση της εμπιστοσύνης και την επιβολή των συμφωνιών μεταξύ των χρηστών. Χρησιμοποιούνται για την τήρηση των φυσικών περιορισμών του δικτύου και την άμεση εκτέλεση πληρωμών, μειώνοντας δραστικά το λειτουργικό κόστος και διασφαλίζοντας ότι όλοι οι συμμετέχοντες συμμορφώνονται με τους προκαθορισμένους κανόνες, αποκλείοντας τη δυνατότητα μονομερών αλλαγών (Yao et al., 2024; Saha et al., 2020; Shamaseen et al., 2025).

Προκειμένου να διατηρηθεί η συνοχή του καθολικού σε ένα περιβάλλον με πολλούς συμμετέχοντες, οι Μηχανισμοί Συναίνεσης (Consensus Mechanisms) καθίστανται απαραίτητοι. Αλγόριθμοι όπως ο Practical Byzantine Fault Tolerance (PBFT) είναι κρίσιμοι για την προστασία του συστήματος από κακόβουλους κόμβους. Η ενσωμάτωση προηγμένων μηχανισμών Βυζαντινής Ανοχής Σφαλμάτων (BFT) διασφαλίζει την ακεραιότητα των εγγραφών, εμποδίζοντας την εισαγωγή ψευδών δεδομένων παραγωγής ή κατανάλωσης και θωρακίζοντας το δίκτυο από επιθέσεις χειραγώγησης των ενεργειακών αποθεμάτων (Yao et al., 2024; Saha et al., 2020).

Ωστόσο, η αύξηση του αριθμού των χρηστών στα μικροδίκτυα δημιουργεί προκλήσεις κλιμακωσιμότητας που απαιτούν προηγμένες λύσεις βελτιστοποίησης.

Μια αποτελεσματική προσέγγιση είναι η χρήση του αλγορίθμου Spectral Clustering, ο οποίος επιτρέπει τον διαχωρισμό του δικτύου σε μικρότερες ομάδες συναίνεσης. Η μέθοδος αυτή βελτιώνει σημαντικά την ταχύτητα επικύρωσης των συναλλαγών και μειώνει την υπολογιστική πολυπλοκότητα, επιτρέποντας στο σύστημα να ανταποκρίνεται σε απαιτήσεις μεγάλης κλίμακας χωρίς να θυσιάζεται η παρεχόμενη ασφάλεια (Yao et al., 2024).

Η διαχείριση της εμπιστοσύνης εντός αυτών των ομάδων ενισχύεται περαιτέρω από δυναμικές στρατηγικές εκλογής ηγέτη (leader election). Οι στρατηγικές αυτές βασίζονται στην αξιολόγηση της προηγούμενης απόδοσης και της συμπεριφοράς των κόμβων στο δίκτυο. Με αυτόν τον τρόπο, διασφαλίζεται ότι ο συντονισμός της συναίνεσης παραμένει στα χέρια των πιο αξιόπιστων μελών, ενώ παράλληλα απομονώνονται εγκαίρως κόμβοι που επιδεικνύουν ύποπτη ή χαμηλής ποιότητας δραστηριότητα (Yao et al., 2024; Shamaseen et al., 2025).

Παράλληλα με τη λειτουργική αξιοπιστία, η σύγχρονη έρευνα δίνει ιδιαίτερη έμφαση στην προστασία της ιδιωτικότητας και την πρόληψη της παραποίησης (counterfeiting). Μέσω κρυπτογραφικών μεθόδων, όπως οι αποδείξεις μηδενικής γνώσης (zero-knowledge proofs), καθίσταται δυνατή η επαλήθευση των συναλλαγών και της αυθεντικότητας των συσκευών χωρίς την αποκάλυψη ευαίσθητων προσωπικών δεδομένων. Οι τεχνικές αυτές είναι ζωτικής σημασίας για την ενίσχυση της εμπιστοσύνης των καταναλωτών στο ψηφιακό οικοσύστημα, καθώς προστατεύουν την ανωνυμία τους (Shamaseen et al., 2025; Yao et al., 2024).

Η ακεραιότητα του συστήματος ολοκληρώνεται με την υιοθέτηση μηχανισμών επαλήθευσης συμμόρφωσης και πρόληψης κλοπής ενέργειας. Ειδικοί αλγόριθμοι διασταυρώνουν τη συμμόρφωση των "prosumers" (παραγωγών-καταναλωτών) με τις προγραμματισμένες συναλλαγές τους, χρησιμοποιώντας δεδομένα από αισθητήρες του δικτύου (grid sensors). Αυτοί οι μηχανισμοί ανιχνεύουν άμεσα απόπειρες κλοπής ή επιθέσεις έγχυσης ψευδών δεδομένων (false data injection), διασφαλίζοντας ότι η φυσική ροή ενέργειας αντιστοιχεί πάντα στις ψηφιακές καταγραφές του blockchain (Saha et al., 2020; Shamaseen et al., 2025).

Συνοψίζοντας, ο συνδυασμός του κατανεμημένου καθολικού, των έξυπνων συμβολαίων και των προηγμένων μηχανισμών συναίνεσης δημιουργεί ένα

θωρακισμένο περιβάλλον για το Smart Grid. Η ιεραρχική οργάνωση των επιπέδων αυτών, από την απλή καταγραφή έως την προηγμένη κρυπτογραφική προστασία και τον φυσικό έλεγχο, αποτελεί την εγγύηση για έναν επιτυχημένο και ασφαλή ψηφιακό μετασχηματισμό της ενέργειας. Η διαλειτουργικότητα αυτών των τεχνολογιών εξασφαλίζει ένα δίκτυο που δεν είναι μόνο αποδοτικό, αλλά και ανθεκτικό στις προκλήσεις του μέλλοντος (Yao et al., 2024; Shamaseen et al., 2025).

5.4. Zero trust και quantum-safe frameworks

5.4.1. Αρχιτεκτονικές zero trust για Smart Grids

Στο πλαίσιο του ψηφιακού μετασχηματισμού των ενεργειακών συστημάτων, η φιλοσοφία του **Zero Trust (ZT)** αναδύεται ως η πλέον ενδεδειγμένη προσέγγιση για την ασφάλεια των σύγχρονων δικτύων. Η αρχιτεκτονική αυτή εδράζεται στην θεμελιώδη αρχή «ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις», καταργώντας ουσιαστικά την παραδοσιακή έννοια της εμπιστοσύνης που βασιζόταν στα στατικά και περιορισμένα όρια του δικτύου. Ειδικά στα Smart Grids, όπου ο αριθμός των συνδεδεμένων συσκευών Internet of Things (IoT) αυξάνεται εκθετικά, η προσέγγιση αυτή κρίνεται απαραίτητη. Καθώς τα συμβατικά συστήματα ασφαλείας αδυνατούν να καλύψουν τις ανάγκες των εξαιρετικά ανοιχτών και ετερογενών δικτύων 6G, το μοντέλο Zero Trust διασφαλίζει ότι κάθε αίτημα πρόσβασης, ανεξαρτήτως προέλευσης, ελέγχεται αυστηρά και αδιάλειπτα (Nie et al., 2025; Chen et al., 2024; Alnaim & Alwakeel, 2025).

Προκειμένου να υλοποιηθεί αυτή η δυναμική στρατηγική ασφάλειας, χρησιμοποιείται ο **Μηχανισμός Ελέγχου Πρόσβασης βάσει Ιδιοτήτων (Attribute-Based Access Control - ABAC)**. Το μοντέλο αυτό επιτρέπει τον καθορισμό ευέλικτων πολιτικών που δεν περιορίζονται μόνο στην ταυτότητα του χρήστη, αλλά λαμβάνουν υπόψη ένα σύνολο μεταβλητών χαρακτηριστικών που πρέπει να ικανοποιούνται ταυτόχρονα. Μέσω του ABAC, επιτυγχάνεται μια προσαρμοστική συνεργασία μεταξύ των τομέων ελέγχου, η οποία είναι ζωτικής σημασίας για την έγκαιρη αντιμετώπιση κακόβουλων συμπεριφορών, όπως οι επιθέσεις DDoS και η εξάπλωση κακόβουλου λογισμικού (Nie et al., 2025; Chen et al., 2024).

Η αποτελεσματικότητα αυτής της αρχιτεκτονικής ενισχύεται σημαντικά από την **ενσωμάτωση της τεχνολογίας Blockchain**, η οποία λειτουργεί ως ένα αμετάβλητο και αποκεντρωμένο σύστημα καταγραφής των πολιτικών πρόσβασης. Η χρήση του blockchain εξαλείφει το κρίσιμο πρόβλημα του «μοναδικού σημείου αποτυχίας» (single point of failure) που χαρακτηρίζει τα κεντρικά συστήματα, διασφαλίζοντας ταυτόχρονα ότι όλες οι αποφάσεις ελέγχου πρόσβασης είναι διαφανείς και ανιχνεύσιμες. Με αυτόν τον τρόπο, ενισχύεται η ακεραιότητα των Κυβερνο-Φυσικών Συστημάτων (CPS) του Smart Grid, καθιστώντας τα ανθεκτικά σε κάθε προσπάθεια αλλοίωσης (Nie et al., 2025; Chen et al., 2024; Alnaim & Alwakeel, 2025).

Παράλληλα με την αποκέντρωση, η προστασία της ιδιωτικότητας αποτελεί προτεραιότητα, η οποία επιτυγχάνεται μέσω προηγμένων τεχνικών, όπως η **Κρυπτογράφηση Εσωτερικού Γινομένου (Inner-Product Encryption - IPE)**. Η μέθοδος αυτή επιτρέπει την εκτέλεση ελέγχων ταύτισης πάνω σε κρυπτογραφημένα δεδομένα, επιτρέποντας στο σύστημα να επαληθεύει τα διαπιστευτήρια των συσκευών χωρίς να αποκαλύπτονται ευαίσθητες πληροφορίες. Έτσι, διατηρείται η εμπιστευτικότητα των δεδομένων των χρηστών και των έξυπνων μετρητών, χωρίς να θυσιάζεται η ανάγκη για αυστηρή επαλήθευση (Nie et al., 2025).

Σε ένα περιβάλλον Zero Trust, η αυθεντικοποίηση παύει να είναι μια εφάπαξ διαδικασία και μετατρέπεται σε μια λειτουργία **συνεχούς επαλήθευσης**. Η αρχιτεκτονική αυτή επιτρέπει τη διαρκή αξιολόγηση της κατάστασης ασφαλείας και τη δυναμική ανάλυση της συμπεριφοράς των συσκευών IoT. Σε περίπτωση που ανιχνευθεί οποιαδήποτε ανωμαλία, το σύστημα προβαίνει σε άμεση ανάκληση των δικαιωμάτων πρόσβασης, προσφέροντας ισχυρή άμυνα ακόμη και έναντι άγνωστων απειλών ή επιθέσεων zero-day (Nie et al., 2025; Chen et al., 2024; Alnaim & Alwakeel, 2025).

Η αυτοματοποίηση αυτών των διαδικασιών επιτυγχάνεται μέσω της χρήσης **Έξυπνων Συμβολαίων (Smart Contracts)** σε συνδυασμό με τη λογική των Δικτύων Καθοριζόμενων από Λογισμικό (Software-Defined Networking). Με την αποθήκευση των κανόνων ασφαλείας στο blockchain, η επιβολή των πολιτικών γίνεται με τρόπο αδιάβλητο και ελαστικό. Αυτή η Software-Defined προσέγγιση διασφαλίζει ότι η πρόσβαση στις κρίσιμες υποδομές του Smart Grid παραχωρείται μόνο μετά από

επιτυχή και συνεχή επαλήθευση, μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση και τα σχετικά λάθη (Nie et al., 2025; Chen et al., 2024).

Ωστόσο, η εφαρμογή τέτοιων σύνθετων συστημάτων σε περιβάλλοντα **6G** συνοδεύεται από σημαντικές προκλήσεις, κυρίως όσον αφορά την κλιμακωσιμότητα και την ανάγκη για εξαιρετικά χαμηλή καθυστέρηση (latency). Η αρχιτεκτονική πρέπει να είναι σχεδιασμένη έτσι ώστε να ελαχιστοποιεί την υπολογιστική επιβάρυνση των συσκευών, διατηρώντας ταυτόχρονα ένα αδιάρρηκτο καθεστώς ασφαλείας. Οι τρέχουσες ερευνητικές προσπάθειες αποδεικνύουν ότι είναι δυνατή η προστασία των Κυβερνο-Φυσικών Συστημάτων χωρίς να υπονομεύεται η απόδοση του δικτύου (Chen et al., 2024; Nie et al., 2025; Alnaim & Alwakeel, 2025).

Συμπερασματικά, η υιοθέτηση της στρατηγικής Zero Trust αποτελεί το κλειδί για την προστασία των μελλοντικών έξυπνων ενεργειακών συστημάτων. Μέσω του συνδυασμού του ABAC, του blockchain και των προηγμένων κρυπτογραφικών μεθόδων, διαμορφώνεται ένα πλαίσιο που είναι ταυτόχρονα ανθεκτικό, διαφανές και ικανό να ανταποκριθεί στις υψηλές απαιτήσεις της 6G εποχής. Η ενσωμάτωση αυτής της αρχιτεκτονικής δεν διασφαλίζει μόνο την ενεργειακή υποδομή, αλλά θέτει και τις βάσεις για έναν ασφαλή και βιώσιμο ψηφιακό μετασχηματισμό (Nie et al., 2025; Chen et al., 2024).

5.4.2. Προστασία απέναντι σε κβαντικές επιθέσεις

Η ραγδαία εξέλιξη των κβαντικών υπολογιστών δημιουργεί μια νέα, υπαρξιακή απειλή για τις κλασικές ψηφιακές υποδομές των Smart Grids. Οι παραδοσιακοί κρυπτογραφικοί μηχανισμοί δημόσιου κλειδιού, όπως ο RSA και ο ECC, οι οποίοι αποτελούν τον θεμέλιο λίθο της ασφάλειας των επικοινωνιών σήμερα, κινδυνεύουν με άμεση κατάρρευση. Η ικανότητα των κβαντικών συστημάτων να επιλύουν σύνθετα μαθηματικά προβλήματα μέσω εξειδικευμένων αλγορίθμων, όπως ο αλγόριθμος του Shor, καθιστά αναγκαία την έγκαιρη μετάβαση σε κβαντικά ανθεκτικά συστήματα για τη διασφάλιση της μακροπρόθεσμης ακεραιότητας των ενεργειακών υποδομών (Sanz et al., 2025; Mu'min et al., 2025).

Δεδομένης της πολυπλοκότητας και της γεωγραφικής διασποράς των σύγχρονων δικτύων, η άμεση αντικατάσταση των υφιστάμενων συστημάτων θεωρείται πρακτικά

αδύνατη. Στο πλαίσιο αυτό, προκρίνεται η υιοθέτηση υβριδικών πλαισίων ασφαλείας (Hybrid Frameworks), τα οποία γεφυρώνουν το χάσμα μεταξύ κλασικής και κβαντικής εποχής. Αυτά τα πλαίσια συνδυάζουν την Κβαντική Διανομή Κλειδιών (QKD) με τη Μετα-Κβαντική Κρυπτογραφία (PQC), προσφέροντας μια πολυεπίπεδη άμυνα που εξασφαλίζει ότι το δίκτυο παραμένει ασφαλές ακόμη και αν ένα από τα επιμέρους κρυπτογραφικά σχήματα παρουσιάσει αδυναμίες (Sanz et al., 2025).

Η τεχνολογία QKD αποτελεί μια επαναστατική προσέγγιση σε αυτό το υβριδικό μοντέλο, καθώς παρέχει ένα επίπεδο ασφάλειας που βασίζεται αποκλειστικά στις αρχές της κβαντομηχανικής. Επιτρέπει την ανίχνευση οποιασδήποτε προσπάθειας υποκλοπής κατά τη διάρκεια της ανταλλαγής κλειδιών, καθιστώντας τις επικοινωνίες φυσικά απαραβίαστες. Παρόλα αυτά, η ευρεία εφαρμογή της στα Smart Grids παρουσιάζει περιορισμούς, καθώς απαιτεί εξειδικευμένο εξοπλισμό οπτικών ινών, γεγονός που περιορίζει τη χρήση της κυρίως σε κρίσιμες διασυνδέσεις μεταξύ υποσταθμών και κέντρων ελέγχου (Sanz et al., 2025; Mu'min et al., 2025).

Συμπληρωματικά προς τη φυσική ασφάλεια του QKD, η Μετα-Κβαντική Κρυπτογραφία (Post-Quantum Cryptography - PQC) εστιάζει στην ανάπτυξη μαθηματικών αλγορίθμων ανθεκτικών σε κβαντικές επιθέσεις, οι οποίοι όμως μπορούν να εκτελεστούν σε συμβατικούς υπολογιστές. Κατηγορίες όπως η κρυπτογραφία βάσει πλεγμάτων (lattice-based), κωδίκων (code-based) και πολυωνύμων (multivariate) προσφέρουν την απαραίτητη ευελιξία για την προστασία των έξυπνων μετρητών και των συσκευών IoT. Η PQC αποτελεί την πλέον ρεαλιστική λύση για τα τερματικά σημεία του δικτύου που διαθέτουν περιορισμένους υπολογιστικούς πόρους (Mu'min et al., 2025; Sanz et al., 2025).

Η παγκόσμια προσπάθεια για την τυποποίηση αυτών των νέων αλγορίθμων καθοδηγείται από το NIST (National Institute of Standards and Technology), το οποίο διαδραματίζει κεντρικό ρόλο στην επιλογή των πλέον αξιόπιστων λύσεων. Η υιοθέτηση διεθνών προτύπων, όπως ο αλγόριθμος Kyber για την ανταλλαγή κλειδιών και ο Dilithium για τις ψηφιακές υπογραφές, προσδίδει την απαραίτητη εμπιστοσύνη στις εφαρμογές των Smart Grids. Η συμμόρφωση με αυτά τα πρότυπα διασφαλίζει ότι οι ενεργειακές υποδομές ακολουθούν διεθνώς δοκιμασμένες και αναγνωρισμένες πρακτικές ασφαλείας (Mu'min et al., 2025).

Ωστόσο, η εφαρμογή τέτοιων αλγορίθμων απαιτεί έναν προσεκτικό σχεδιασμό, καθώς ένα σύγχρονο κβαντικά ασφαλές πλαίσιο οφείλει να είναι προσαρμοστικό (adaptive). Η ικανότητα επιλογής του κατάλληλου επιπέδου κρυπτογράφησης με βάση τη σημασία των δεδομένων και τους διαθέσιμους πόρους επιτρέπει στο Smart Grid να διατηρεί την υψηλή του απόδοση. Αυτή η ευελιξία διασφαλίζει ότι η ισχυρότερη κβαντική προστασία εφαρμόζεται μόνο εκεί όπου είναι πραγματικά απαραίτητο, μειώνοντας έτσι την υπολογιστική επιβάρυνση του συστήματος (Sanz et al., 2025).

Για την πρακτική υλοποίηση αυτής της στρατηγικής, είναι απαραίτητη η χρήση εξειδικευμένων Συστημάτων Διαχείρισης Κλειδιών (Key Management Systems - KMS) που υποστηρίζουν διεπαφές REST-based. Τα συστήματα αυτά αναλαμβάνουν τη διανομή και την ανανέωση των κλειδιών, ενώ παράλληλα απαιτείται η αναβάθμιση υφιστάμενων πρωτοκόλλων, όπως το IPsec και το TLS. Η χρήση βιβλιοθηκών λογισμικού που υποστηρίζουν PQC επιτρέπει την άμεση προστασία των ψηφιακών συναλλαγών ενέργειας χωρίς την ανάγκη ριζικής αλλαγής της δικτυακής υποδομής (Sanz et al., 2025).

Τέλος, η άμεση υιοθέτηση αυτών των τεχνολογιών είναι κρίσιμη για την αντιμετώπιση της απειλής "Harvest Now, Decrypt Later", όπου δεδομένα αποθηκεύονται σήμερα για να αποκρυπτογραφηθούν στο μέλλον. Παρά τις προκλήσεις, όπως το μεγαλύτερο μέγεθος κλειδιών και η αυξημένη κατανάλωση ενέργειας των PQC αλγορίθμων, η συνεχιζόμενη έρευνα επικεντρώνεται στη βελτιστοποίηση τους για συσκευές IoT. Με αυτόν τον τρόπο, η κβαντική προστασία καθίσταται αναπόσπαστο κομμάτι του οικοσυστήματος των έξυπνων πόλεων, εξασφαλίζοντας ένα ασφαλές ενεργειακό μέλλον (Mu'min et al., 2025; Sanz et al., 2025).

Κεφάλαιο 6: Συμπεράσματα και Μελλοντικές Κατευθύνσεις

6.1. Σύνοψη ευρημάτων

6.1.1 Κύρια συμπεράσματα βιβλιογραφίας

Η βιβλιογραφική ανασκόπηση καταδεικνύει ότι τα Έξυπνα Δίκτυα (Smart Grids) αποτελούν μια κρίσιμη εξέλιξη των παραδοσιακών δικτύων, η οποία όμως συνοδεύεται από σύνθετες προκλήσεις ασφάλειας. Το κύριο συμπέρασμα των μελετών είναι ότι η μετάβαση σε αποκεντρωμένες ενεργειακές κοινότητες, όπου συμμετέχουν ενεργά κτίρια και ηλεκτρικά οχήματα, απαιτεί μια νέα προσέγγιση στη διαχείριση της πληροφορίας στο άκρο του δικτύου (edge grid). Η έρευνα των Wu et al. (2022) τονίζει ότι η αποκέντρωση είναι απαραίτητη για την ευστάθεια του συστήματος, αλλά εισάγει νέες μεταβλητές που πρέπει να ελέγχονται αυστηρά για την αποφυγή λειτουργικών αστοχιών.

Ένα κεντρικό συμπέρασμα που προκύπτει από την ανάλυση των απειλών είναι η ακραία ευπάθεια των συσκευών IoT που χρησιμοποιούνται στις υποδομές AMI και SCADA. Η βιβλιογραφία υπογραμμίζει ότι η έλλειψη ενσωματωμένων μηχανισμών ασφάλειας σε πολλούς αισθητήρες επιτρέπει τη δημιουργία τεράστιων δικτύων botnet, όπως το Mirai, τα οποία μπορούν να εξαπολύσουν επιθέσεις DDoS ικανές να παραλύσουν ολόκληρες γεωγραφικές περιοχές. Σύμφωνα με τους Zhang κ.ά. (2020), η ψηφιακή εγκληματολογία σε τέτοια περιβάλλοντα αναδεικνύει την ανάγκη για προληπτική θωράκιση κάθε μεμονωμένου κόμβου του δικτύου.

Στον τομέα της προστασίας δεδομένων, η βιβλιογραφία συμφωνεί ότι οι παραδοσιακές μέθοδοι ανωνυμοποίησης είναι πλέον ανεπαρκείς για τη διασφάλιση της ιδιωτικότητας των καταναλωτών. Τα ενεργειακά αποτυπώματα είναι τόσο μοναδικά που μπορούν να προδώσουν προσωπικές συνήθειες των χρηστών με μεγάλη ακρίβεια. Οι Xiao κ.ά. (2025) καταλήγουν στο συμπέρασμα ότι μόνο μέσω προηγμένων κρυπτογραφικών μεθόδων, όπως η ομομορφική κρυπτογράφηση (PHE και TFHE), είναι εφικτή η ανάλυση δεδομένων για την ανίχνευση ανωμαλιών χωρίς την έκθεση ευαίσθητων πληροφοριών.

Η τεχνολογία Blockchain αναδεικνύεται ως ο πλέον υποσχόμενος πυλώνας για τη διασφάλιση της ακεραιότητας των συναλλαγών ενέργειας. Τα συμπεράσματα των

ερευνητών συγκλίνουν στο ότι οι αλγόριθμοι συναίνεσης, όπως ο PBFT, προσφέρουν την απαραίτητη ταχύτητα και ασφάλεια για το εμπόριο ενέργειας σε τοπικά δίκτυα (microgrids). Όπως επισημαίνουν οι Yao κ.ά. (2024), η χρήση του Blockchain εξαλείφει την ανάγκη για κεντρικούς μεσάζοντες, μειώνοντας δραστικά την πιθανότητα μοναδικού σημείου αποτυχίας (single point of failure) στο σύστημα.

Η μελλοντική ενσωμάτωση των δικτύων 6G θεωρείται καταλύτης για την επίλυση των προβλημάτων καθυστέρησης στην επικοινωνία και την ασφάλεια. Η βιβλιογραφία αναφέρει ότι η ικανότητα των 6G δικτύων να υποστηρίζουν Τεχνητή Νοημοσύνη στο άκρο του δικτύου (Edge AI) επιτρέπει την αυτόνομη λήψη αποφάσεων για την αναχαίτιση επιθέσεων σε πραγματικό χρόνο. Οι Zhang κ.ά. (2020) υπογραμμίζουν ότι αυτή η «έξυπνη» απόκριση είναι η μόνη βιώσιμη λύση απέναντι σε επιθέσεις που εξελίσσονται με ταχύτητες μεγαλύτερες από αυτές που μπορεί να διαχειριστεί ο ανθρώπινος παράγοντας.

Σχετικά με τη διαχείριση της πληροφορίας, τα ευρήματα δείχνουν ότι η ασφαλής συγκέντρωση δεδομένων (data aggregation) αποτελεί τη βάση για τη λειτουργία του έξυπνου μετρητή. Η έρευνα των Wu, Zhang και Zhao (2022) καταδεικνύει ότι τα σχήματα που διασφαλίζουν την ανωνυμία του χρήστη ενώ ταυτόχρονα επιτρέπουν τη μετάδοση σε συγκεκριμένους παραλήπτες, είναι κρίσιμα για τη συμμόρφωση με το κανονιστικό πλαίσιο GDPR. Συμπεραίνεται ότι η τεχνική υλοποίηση της ιδιωτικότητας είναι εξίσου σημαντική με τη νομική της κατοχύρωση.

Επιπλέον, η βιβλιογραφία αναδεικνύει τη σημασία της κυβερνοανθεκτικότητας έναντι της απλής κυβερνοασφάλειας. Ενώ η ασφάλεια εστιάζει στην αποτροπή της εισβολής, η ανθεκτικότητα αφορά την ικανότητα του δικτύου να συνεχίζει τη λειτουργία του ακόμα και υπό καθεστώς επίθεσης. Οι σύγχρονες μελέτες, όπως αυτή των Xiao κ.ά. (2025), προκρίνουν τη χρήση υβριδικών μοντέλων προστασίας που συνδυάζουν την κρυπτογραφία με την ανίχνευση ανωμαλιών βάσει τεχνητής νοημοσύνης για τη συνεχή επιτήρηση του δικτύου.

Τέλος, το γενικό συμπέρασμα της βιβλιογραφικής ανασκόπησης είναι ότι η κυβερνοασφάλεια στα Smart Grids πρέπει να αντιμετωπίζεται ως μια δυναμική και πολυεπίπεδη διαδικασία. Η σύγκλιση τεχνολογιών όπως το 6G, το Blockchain και η προηγμένη κρυπτογραφία δημιουργεί ένα νέο πλαίσιο «ασφάλειας από τον

σχεδιασμό» (Security by Design). Σύμφωνα με τους Wu κ.ά. (2022) και Yao κ.ά. (2024), η επιτυχία των έξυπνων δικτύων εξαρτάται από την ικανότητά τους να εμπνέουν εμπιστοσύνη στους χρήστες μέσω της αποδεδειγμένης προστασίας των δεδομένων και των υποδομών τους.

6.1.2 Συνολική εκτίμηση απειλών και μέτρων προστασίας

Η συνολική εκτίμηση του τοπίου των απειλών στα Έξυπνα Δίκτυα αποκαλύπτει ότι η πολυπλοκότητα των σύγχρονων επιθέσεων απαιτεί μια δυναμική και πολυεπίπεδη στρατηγική άμυνας. Οι κυβερνοαπειλές δεν στοχεύουν πλέον μόνο στη διακοπή της υπηρεσίας, αλλά και στην αλλοίωση των δεδομένων μέτρησης, γεγονός που μπορεί να οδηγήσει σε οικονομική αποσταθεροποίηση και φυσικές καταστροφές στις υποδομές. Σύμφωνα με τους Wu et al. (2022), η ενσωμάτωση αποκεντρωμένων ενεργειακών κοινοτήτων στο άκρο του δικτύου (edge grid) καθιστά επιτακτική την ανάγκη για προηγμένα μέτρα προστασίας που θα διασφαλίζουν τη λειτουργική συνέχεια και την ακεραιότητα των συναλλαγών.

Οι επιθέσεις έγχυσης ψευδών δεδομένων (FDIA) και οι απειλές από δίκτυα botnet, όπως το Mirai, αποτελούν τις πιο κρίσιμες προκλήσεις για τη διαθεσιμότητα του δικτύου. Η ανάλυση των Zhang et al. (2020) καταδεικνύει ότι οι συσκευές IoT με ελλιπή μέτρα ασφάλειας λειτουργούν ως πύλες εισόδου για μαζικές επιθέσεις DDoS, οι οποίες μπορούν να παραλύσουν τα συστήματα ελέγχου SCADA. Ως μέτρο προστασίας, προτείνεται η ενίσχυση της ψηφιακής εγκληματολογίας και η υιοθέτηση αυστηρών πρωτοκόλλων πιστοποίησης σε κάθε κόμβο του δικτύου, ώστε να περιορίζεται η επιφάνεια επίθεσης.

Στο επίπεδο της προστασίας δεδομένων, η εκτίμηση δείχνει ότι η ιδιωτικότητα των χρηστών απειλείται άμεσα από την εκτεταμένη συλλογή πληροφοριών κατανάλωσης. Η βιβλιογραφία υποστηρίζει ότι η χρήση της ομομορφικής κρυπτογράφησης (PHE και TFHE) αποτελεί ένα από τα πιο ισχυρά μέτρα προστασίας, καθώς επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα για την ανίχνευση ανωμαλιών, χωρίς να εκτίθενται οι προσωπικές συνήθειες των καταναλωτών (Xiao et al., 2025). Το εύρημα αυτό τονίζει ότι η τεχνολογική θωράκιση πρέπει να συμβαδίζει με την ανάγκη για διαφάνεια και εμπιστοσύνη στο σύστημα.

Η διασφάλιση της ακεραιότητας των συναλλαγών ενέργειας σε περιβάλλοντα microgrids απαιτεί τη χρήση τεχνολογιών που εξαλείφουν το μοναδικό σημείο αποτυχίας. Η τεχνολογία Blockchain, μέσω αποδοτικών αλγορίθμων συναίνεσης όπως ο PBFT, προσφέρει ένα ασφαλές πλαίσιο για την προστασία από εσωτερικές απειλές και απάτες (Yao et al., 2024). Η συνολική εκτίμηση δείχνει ότι η αποκεντρωμένη διαχείριση της εμπιστοσύνης μειώνει σημαντικά το ρίσκο παραβίασης των αρχείων συναλλαγών, ενισχύοντας ταυτόχρονα την ανθεκτικότητα του δικτύου έναντι εξωτερικών παρεμβάσεων.

Οι προοπτικές των δικτύων 6G και της Τεχνητής Νοημοσύνης (Edge AI) αναβαθμίζουν σημαντικά τα μέτρα προστασίας, προσφέροντας δυνατότητες πρόληψης σε πραγματικό χρόνο. Η ικανότητα των συστημάτων να αναγνωρίζουν πρότυπα επιθέσεων μέσω ανάλυσης ακολουθιών και μετα-χαρακτηριστικών επιτρέπει την αυτόματη λήψη μέτρων πριν η απειλή κλιμακωθεί (Zhang et al., 2020). Αυτή η προληπτική προσέγγιση είναι απαραίτητη για τη θωράκιση των κρίσιμων υποδομών, καθώς οι επιθέσεις γίνονται όλο και πιο γρήγορες και εξελιγμένες.

Συμπερασματικά, η εκτίμηση των απειλών καταδεικνύει ότι η μόνη βιώσιμη λύση είναι η υιοθέτηση ενός υβριδικού μοντέλου ασφάλειας που συνδυάζει την κρυπτογραφία, το blockchain και την εγγενή νοημοσύνη των δικτύων 6G. Η στρατηγική «Security by Design» πρέπει να περιλαμβάνει ασφαλή σχήματα συγκέντρωσης δεδομένων που διασφαλίζουν την ανωνυμία των χρηστών, ενώ παράλληλα επιτρέπουν την απρόσκοπτη λειτουργία του δικτύου (Wu, Zhang & Zhao, 2022). Η συνοχή μεταξύ αυτών των μέτρων είναι αυτή που θα καθορίσει την τελική κυβερνοανθεκτικότητα των Έξυπνων Δικτύων στο μέλλον.

6.2. Προτάσεις για ασφαλή Smart Grids

6.1.3 Συνδυασμός AI, blockchain και edge computing

Η θωράκιση των σύγχρονων Έξυπνων Δικτύων απαιτεί τη συνέργεια τριών βασικών τεχνολογιών: της Τεχνητής Νοημοσύνης (AI), του Blockchain και του Edge Computing. Η στρατηγική αυτή πρόταση βασίζεται στην ανάγκη για μετατόπιση της υπολογιστικής ισχύος από το κέντρο στο άκρο του δικτύου (edge), ώστε να επιτυγχάνεται ταχύτερη απόκριση στις απειλές. Όπως επισημαίνουν οι Wu et al.

(2022), η χρήση αποκεντρωμένων κοινοτήτων στο edge grid επιτρέπει την αποτελεσματικότερη διαχείριση των ενεργειακών πόρων, ενώ η ενσωμάτωση AI επιταχύνει τη λήψη αποφάσεων σε πραγματικό χρόνο για την αποφυγή υπερφορτώσεων.

Η πρώτη γραμμή άμυνας ενισχύεται από τη χρήση της Τεχνητής Νοημοσύνης για την ανίχνευση ανωμαλιών στη ροή των δεδομένων. Μέσω προηγμένων αλγορίθμων, το σύστημα μπορεί να αναγνωρίζει μοτίβα επιθέσεων, όπως οι επιθέσεις έγχυσης ψευδών δεδομένων (FDIA), πριν αυτές επηρεάσουν τη λειτουργία του δικτύου. Σύμφωνα με τους Zhang et al. (2020), η ανάλυση ακολουθιών και μετα-χαρακτηριστικών μέσω AI είναι κρίσιμη για την αναχαίτιση εξελιγμένων απειλών από δίκτυα botnet, διασφαλίζοντας την ακεραιότητα των συστημάτων ελέγχου.

Σε αυτό το πλαίσιο, η υιοθέτηση της Ομόσπονδης Μάθησης (Federated Learning) στο άκρο του δικτύου επιτρέπει την εκπαίδευση μοντέλων AI χωρίς τη μεταφορά ευαίσθητων δεδομένων σε κεντρικούς διακομιστές (Ferrag et al., 2021). Αυτή η προσέγγιση ενισχύει την ιδιωτικότητα των καταναλωτών, καθώς τα δεδομένα παραμένουν τοπικά, ενώ το δίκτυο "μαθαίνει" συλλογικά να αναγνωρίζει νέες μορφές κυβερνοεπιθέσεων. Η συνδυαστική χρήση αυτής της τεχνολογίας με το Edge Computing μειώνει δραστικά την καθυστέρηση (latency) και την κατανάλωση εύρους ζώνης.

Το Blockchain έρχεται να συμπληρώσει αυτό το σχήμα, παρέχοντας ένα αδιάβλητο επίπεδο καταγραφής και επαλήθευσης των συναλλαγών και των εντολών ελέγχου. Η χρήση αλγορίθμων συναίνεσης, όπως ο PBFT (Practical Byzantine Fault Tolerance), διασφαλίζει ότι όλες οι ενέργειες στο microgrid είναι διαφανείς και προστατευμένες από κακόβουλες αλλοιώσεις (Yao et al., 2024). Το Blockchain λειτουργεί ως η "πηγή αλήθειας" για το σύστημα, εμποδίζοντας την παραποίηση ιστορικών δεδομένων κατανάλωσης ή παραγωγής από εσωτερικούς ή εξωτερικούς εισβολείς.

Η ενοποίηση του Blockchain με το Edge Computing δημιουργεί ένα αποκεντρωμένο πλαίσιο εμπιστοσύνης, όπου οι "έξυπνες συμβάσεις" (Smart Contracts) αυτοματοποιούν την ενεργειακή ανταλλαγή με βάση την ανάλυση που παρέχει η AI (Mollah et al., 2021). Με αυτόν τον τρόπο, το δίκτυο μπορεί να αυτοθεραπεύεται και να ανακατανέμει το φορτίο αυτόματα σε περίπτωση επίθεσης σε έναν κόμβο. Η

συγκεκριμένη αρχιτεκτονική εξαλείφει τα μοναδικά σημεία αποτυχίας (Single Points of Failure), καθιστώντας την υποδομή ανθεκτική ακόμα και σε μαζικές επιθέσεις DDoS.

Η προστασία της ιδιωτικότητας σε αυτόν τον τριπλό συνδυασμό επιτυγχάνεται μέσω προηγμένης κρυπτογραφίας που εφαρμόζεται απευθείας στις συσκευές edge. Η εφαρμογή ομομορφικής κρυπτογράφησης επιτρέπει στην AI να αναλύει τα δεδομένα και στο Blockchain να τα επικυρώνει, χωρίς ποτέ να "βλέπουν" το περιεχόμενο της πληροφορίας σε απλή μορφή (Xiao et al., 2025). Το συμπέρασμα είναι ότι ο συνδυασμός αυτός προσφέρει ένα ολιστικό πλαίσιο προστασίας που καλύπτει τόσο την κυβερνοασφάλεια όσο και την ιδιωτικότητα των δεδομένων.

Τέλος, η πρόταση για τον συνδυασμό AI, Blockchain και Edge Computing αποτελεί τη βάση για την ανάπτυξη των "εγγενώς ασφαλών" Smart Grids στην εποχή του 6G. Η δυνατότητα των δικτύων 6G να υποστηρίζουν μαζική συνδεσιμότητα με σχεδόν μηδενική καθυστέρηση είναι ο καταλύτης που επιτρέπει σε αυτές τις τεχνολογίες να λειτουργήσουν συνεργατικά (Zhang et al., 2020). Η υιοθέτηση αυτής της πολυεπίπεδης αρχιτεκτονικής δεν είναι πλέον μια θεωρητική επιλογή, αλλά μια αναγκαιότητα για τη θωράκιση των κρίσιμων ενεργειακών υποδομών του μέλλοντος.

6.1.4 Στρατηγικές πρόληψης και διαχείρισης περιστατικών

Η αποτελεσματική θωράκιση των Έξυπνων Δικτύων απαιτεί την υιοθέτηση μιας στρατηγικής «βαθιάς άμυνας», η οποία ξεκινά από το επίπεδο των συσκευών IoT και των έξυπνων μετρητών. Τα ευρήματα δείχνουν ότι η πρόληψη πρέπει να εστιάζει στην εξάλειψη των κενών ασφαλείας που επιτρέπουν τη δημιουργία δικτύων botnet, τα οποία αποτελούν τη βάση για μαζικές επιθέσεις DDoS. Σύμφωνα με τους Zhang et al. (2020), η προληπτική θωράκιση μέσω ψηφιακής εγκληματολογίας και συνεχούς ελέγχου των συσκευών AMI και SCADA είναι απαραίτητη για τη διασφάλιση της επιχειρησιακής συνέχειας του δικτύου (Zhang et al., 2020).

Μια κεντρική πρόταση για την πρόληψη αφορά την προστασία της ιδιωτικότητας των δεδομένων κατανάλωσης, ώστε να αποτρέπεται η χρήση τους για κακόβουλους σκοπούς. Η εφαρμογή προηγμένων κρυπτογραφικών μεθόδων επιτρέπει τη διαχείριση των δεδομένων χωρίς να αποκαλύπτεται η ταυτότητα ή οι συνήθειες του

χρήστη. Οι Xiao et al. (2025) υπογραμμίζουν ότι ο συνδυασμός PHE και TFHE ομομορφικής κρυπτογράφησης προσφέρει ένα ισχυρό πλαίσιο πρόληψης, επιτρέποντας την ανίχνευση ανωμαλιών σε πραγματικό χρόνο χωρίς να παραβιάζεται το ιδιωτικό απόρρητο (Xiao et al., 2025).

Για τη διαχείριση περιστατικών που αφορούν την αλλοίωση δεδομένων, η χρήση της τεχνολογίας Blockchain αναδεικνύεται ως μια από τις πιο αξιόπιστες στρατηγικές. Μέσω αλγορίθμων συναίνεσης, το δίκτυο μπορεί να εντοπίζει και να απομονώνει αυτόματα κακόβουλους κόμβους που προσπαθούν να εισάγουν ψευδείς πληροφορίες. Οι Yao et al. (2024) επισημαίνουν ότι ο αλγόριθμος PBFT διασφαλίζει την ακεραιότητα των ιστορικών δεδομένων και την εγκυρότητα των ενεργειακών συναλλαγών, καθιστώντας το σύστημα ανθεκτικό σε εσωτερικές και εξωτερικές απειλές (Yao et al., 2024).

Η αποκεντρωμένη διαχείριση των ενεργειακών πόρων αποτελεί επίσης μια κρίσιμη στρατηγική για τον περιορισμό της έκτασης ενός κυβερνοπεριστατικού. Με τη χρήση δομών edge grid, η διαχείριση της ενέργειας γίνεται τοπικά, γεγονός που εμποδίζει μια επίθεση να εξαπλωθεί σε ολόκληρο το εθνικό δίκτυο. Η έρευνα των Wu et al. (2022) καταδεικνύει ότι οι αποκεντρωμένες ενεργειακές κοινότητες ενισχύουν την ανθεκτικότητα του συστήματος, καθώς επιτρέπουν την αυτόνομη λειτουργία τμημάτων του δικτύου σε περίπτωση κρίσης (Wu et al., 2022).

Σημαντική στρατηγική πρόληψης αποτελεί και η χρήση εξειδικευμένων σχημάτων συγκέντρωσης δεδομένων που διασφαλίζουν την ανωνυμία του χρήστη κατά τη μετάδοση πληροφοριών. Τα σχήματα αυτά προστατεύουν το δίκτυο από διαρροές που θα μπορούσαν να οδηγήσουν σε στοχευμένες επιθέσεις κατά συγκεκριμένων χρηστών ή υποδομών. Οι Wu, Zhang και Zhao (2022) προτείνουν μοντέλα που επιτρέπουν τη μετάδοση δεδομένων μόνο σε εξουσιοδοτημένους παραλήπτες, ενισχύοντας έτσι τον έλεγχο πρόσβασης και την ασφάλεια του καναλιού επικοινωνίας (Wu, Zhang & Zhao, 2022).

Η αξιοποίηση των δυνατοτήτων των δικτύων 6G και της Τεχνητής Νοημοσύνης προσφέρει νέες προοπτικές στην αυτόματη διαχείριση περιστατικών. Η ικανότητα του συστήματος να αναγνωρίζει πρότυπα επιθέσεων μέσω ανάλυσης ακολουθιών επιτρέπει την άμεση αναχαίτιση κακόβουλων ενεργειών προτού προκληθεί φυσική

βλάβη στις υποδομές. Σύμφωνα με τους Zhang et al. (2020), η ενσωμάτωση «νοήμονων» μηχανισμών απόκρισης στο άκρο του δικτύου είναι ο μόνος τρόπος για την αντιμετώπιση επιθέσεων που εξελίσσονται με εξαιρετικά μεγάλες ταχύτητες (Zhang et al., 2020).

Συνοψίζοντας, οι στρατηγικές πρόληψης και διαχείρισης πρέπει να είναι ολιστικές, συνδυάζοντας την κρυπτογραφία, το Blockchain και την ανάλυση μεγάλων δεδομένων. Η ανθεκτικότητα του δικτύου εξαρτάται από την ικανότητά του να παρακολουθεί συνεχώς τις ροές δεδομένων και να προσαρμόζεται δυναμικά σε νέες απειλές. Οι Zhang, Huang και Bompard (2018) τονίζουν ότι η ανάλυση Big Analytics στα Smart Grids αποτελεί το θεμέλιο για την πρόβλεψη και την έγκαιρη αντιμετώπιση κινδύνων, διασφαλίζοντας τη μακροπρόθεσμη σταθερότητα του ενεργειακού συστήματος (Zhang, Huang & Bompard, 2018).

6.2. Μελλοντική έρευνα

6.2.1. AI-based resilience, quantum-safe solutions

Η μελλοντική έρευνα για τα Έξυπνα Δίκτυα πρέπει να επικεντρωθεί στη δημιουργία συστημάτων ανθεκτικότητας (resilience) που βασίζονται στην Τεχνητή Νοημοσύνη, τα οποία θα επιτρέπουν στο δίκτυο να αυτοθεραπεύεται. Η χρήση αλγορίθμων βαθιάς μάθησης επιτρέπει την αναγνώριση νέων, άγνωστων μορφών επιθέσεων μέσω της ανάλυσης ακολουθιών και μετα-χαρακτηριστικών (Zhang et al., 2020). Η ανάπτυξη τέτοιων μοντέλων θα επιτρέψει στα Smart Grids να διατηρούν τη λειτουργικότητά τους ακόμη και όταν συγκεκριμένοι κόμβοι έχουν παραβιαστεί από επιθέσεις τύπου Mirai (Zhang et al., 2020).

Παράλληλα, η έλευση των κβαντικών υπολογιστών δημιουργεί την ανάγκη για κβαντικά ασφαλείς λύσεις (quantum-safe solutions), καθώς οι τρέχουσες μέθοδοι κρυπτογράφησης θα καταστούν σύντομα ευάλωτες. Η έρευνα στη Μετα-κβαντική Κρυπτογράφηση (Post-Quantum Cryptography) είναι κρίσιμη, καθώς στοχεύει στην ανάπτυξη αλγορίθμων που είναι ανθεκτικοί σε επιθέσεις από κβαντικούς υπολογιστές, διασφαλίζοντας τη μακροπρόθεσμη προστασία των υποδομών (Bernstein & Lange, 2017). Η ενσωμάτωση αυτών των λύσεων σε συσκευές χαμηλής

ισχύος, όπως οι έξυπνοι μετρητές, αποτελεί μια από τις μεγαλύτερες προκλήσεις για τα επόμενα έτη (Xiao et al., 2025).

Μια άλλη πολλά υποσχόμενη κατεύθυνση είναι η συνδυαστική χρήση της AI με την ομομορφική κρυπτογράφηση για τη δημιουργία μοντέλων ανίχνευσης ανωμαλιών που δεν απαιτούν την αποκάλυψη των δεδομένων. Οι Xiao et al. (2025) καταδεικνύουν ότι ο συνδυασμός PHE και TFHE μπορεί να προσφέρει υψηλά επίπεδα ιδιωτικότητας, ωστόσο η μελλοντική έρευνα πρέπει να βελτιώσει την υπολογιστική τους απόδοση για χρήση σε πραγματικό χρόνο (Xiao et al., 2025). Η βελτιστοποίηση αυτή είναι απαραίτητη για να γίνει η κρυπτογραφία αυτή το πρότυπο στα μελλοντικά δίκτυα.

Η "Ομόσπονδη Μάθηση" (Federated Learning) αναδεικνύεται ως βασικό εργαλείο για την ενίσχυση της ανθεκτικότητας χωρίς την κεντρική συλλογή ευαίσθητων δεδομένων (Ferrag et al., 2021). Με αυτή τη μέθοδο, οι έξυπνοι μετρητές εκπαιδεύουν τοπικά μοντέλα AI και μοιράζονται μόνο τις ενημερώσεις των παραμέτρων, προστατεύοντας έτσι την ιδιωτικότητα των καταναλωτών (Ferrag et al., 2021). Η περαιτέρω διερεύνηση της ανθεκτικότητας αυτών των αποκεντρωμένων μοντέλων απέναντι σε εσωτερικές απειλές αποτελεί προτεραιότητα για την επιστημονική κοινότητα.

Επιπλέον, η μελλοντική έρευνα οφείλει να εξετάσει την ενσωμάτωση κβαντικά ανθεκτικών αλγορίθμων στην τεχνολογία Blockchain για την ενίσχυση της ακεραιότητας των συναλλαγών. Ο αλγόριθμος PBFT, αν και αποδοτικός σήμερα, θα πρέπει να αναβαθμιστεί με ψηφιακές υπογραφές που δεν μπορούν να παραβιαστούν από κβαντικά συστήματα (Yao et al., 2024). Η σύγκλιση κβαντικής ασφάλειας και αποκεντρωμένης εμπιστοσύνης θα αποτελέσει το απόλυτο οχυρό προστασίας για τις ενεργειακές κοινότητες (Yao et al., 2024).

Τέλος, η ανάπτυξη δυναμικών μοντέλων πρόβλεψης που βασίζονται σε AI θα επιτρέψει τη διαχείριση της ανθεκτικότητας σε περιβάλλοντα με υψηλή διείσδυση ΑΠΕ. Οι Zhang, Huang και Bompard (2018) τονίζουν ότι η ανάλυση Big Data στα Smart Grids αποτελεί το θεμέλιο για την πρόβλεψη κινδύνων (Zhang, Huang & Bompard, 2018). Η μελλοντική έρευνα θα πρέπει να ενοποιήσει αυτά τα αναλυτικά

εργαλεία με μηχανισμούς AI για την αυτόματη λήψη αποφάσεων σε καταστάσεις έκτακτης ανάγκης.

6.2.2. Edge intelligence και next-generation predictive security

Η μετάβαση προς το "Edge Intelligence" (Ευφυΐα στο Άκρο) μεταφέρει την επεξεργασία της πληροφορίας από τα κεντρικά νέφη απευθείας στους τοπικούς κόμβους του δικτύου. Αυτό επιτρέπει την άμεση αναγνώριση κακόβουλων ενεργειών, μειώνοντας δραστικά τον χρόνο απόκρισης σε επιθέσεις κατά συστημάτων AMI (Zhang et al., 2020). Η μελλοντική έρευνα θα πρέπει να εστιάσει στη δημιουργία ελαφριών αλγορίθμων AI που θα μπορούν να τρέχουν στους περιορισμένους πόρους υλικού των αισθητήρων IoT (Zhang et al., 2020).

Η προληπτική ασφάλεια επόμενης γενιάς θα βασίζεται στην ικανότητα του δικτύου να προβλέπει μια επίθεση πριν αυτή εκδηλωθεί, αναλύοντας μικροσκοπικές αποκλίσεις στις ενεργειακές ροές. Η ανάλυση Big Data στα Smart Grids επιτρέπει την ανακάλυψη νέων προτύπων συμπεριφοράς που υποδηλώνουν προσπάθεια διείσδυσης (Zhang, Huang & Bompard, 2018). Η πρόκληση για την έρευνα έγκειται στην ακρίβεια της πρόβλεψης, ώστε να αποφεύγονται οι ψευδείς συναγερμοί (Zhang, Huang & Bompard, 2018).

Στο πλαίσιο των δικτύων 6G, η ευφυΐα στο άκρο θα ενισχυθεί από την ικανότητα "δικτυακής κοπής" (network slicing), η οποία επιτρέπει τη δημιουργία απομονωμένων εικονικών δικτύων για κρίσιμες λειτουργίες (Zhang et al., 2018). Η έρευνα πρέπει να εξετάσει πώς η δυναμική διαχείριση αυτών των τμημάτων μπορεί να απομονώσει αυτόματα μια μολυσμένη περιοχή του edge grid (Wu et al., 2022). Η συνέργεια μεταξύ 6G και Edge AI θα προσφέρει μια δυναμική άμυνα (Wu et al., 2022).

Παράλληλα, η χρήση "ψηφιακών διδύμων" (digital twins) στο άκρο του δικτύου θα επιτρέψει τη συνεχή προσομοίωση σεναρίων επίθεσης και την εκπαίδευση των συστημάτων ασφαλείας σε εικονικό περιβάλλον. Αυτή η προσέγγιση επιτρέπει τη δοκιμή μέτρων προστασίας χωρίς να επηρεάζεται η λειτουργία των κτιρίων ή των ηλεκτρικών οχημάτων (Wu et al., 2022). Η μελλοντική έρευνα θα αναδείξει πώς τα

ψηφιακά αντίγραφα μπορούν να προβλέψουν την επίδραση μιας επίθεσης στη σταθερότητα (Wu et al., 2022).

Η επόμενη γενιά προληπτικής ασφάλειας θα περιλαμβάνει επίσης την "Κινούμενη Στόχευση" (Moving Target Defense), όπου οι παράμετροι επικοινωνίας αλλάζουν συνεχώς για να μπερδέψουν τον επιτιθέμενο (Zheng et al., 2022). Η έρευνα για τον βέλτιστο χρονισμό αυτών των αλλαγών είναι απαραίτητη για να μην επηρεάζεται η αξιοπιστία της μετάδοσης (Yao et al., 2024). Ο συνδυασμός ευφυΐας και δυναμικής αλλαγής της επιφάνειας επίθεσης θα καταστήσει τα Smart Grids εξαιρετικά δύσκολους στόχους (Yao et al., 2024).

Τέλος, η έρευνα πρέπει να εστιάσει στην "Predictive Privacy", όπου το σύστημα προβλέπει πιθανούς κινδύνους διαρροής ιδιωτικότητας πριν αυτοί συμβούν. Η χρήση βαθιάς μάθησης για τον εντοπισμό χαρακτηριστικών των καταναλωτών μπορεί να χρησιμοποιηθεί προληπτικά για την εφαρμογή κατάλληλων μέτρων ανωνυμοποίησης (Zhang et al., 2022). Η εξισορρόπηση μεταξύ πρόβλεψης ασφάλειας και προστασίας ιδιωτικότητας θα είναι το κλειδί για την αποδοχή των τεχνολογιών αυτών (Zhang et al., 2022).

6.2.3 Προοπτικές για επόμενα πρότυπα και πολιτικές κυβερνοασφάλειας

Η ανάπτυξη νέων διεθνών προτύπων είναι επιβεβλημένη για να διασφαλιστεί η διαλειτουργικότητα και η ασφάλεια των ετερογενών συστημάτων που συνθέτουν τα Smart Grids. Τα τρέχοντα πρωτόκολλα πρέπει να επικαιροποιηθούν για να συμπεριλάβουν προδιαγραφές για την ασφαλή συγκέντρωση δεδομένων και την ανωνυμία των χρηστών (Wu et al.,2022). Η μελλοντική πολιτική θα πρέπει να επιβάλλει το πρότυπο "Security by Design", διασφαλίζοντας ότι κάθε νέα συσκευή πληροί αυστηρά κριτήρια προστασίας (Wu et al.,2022).

Οι κανονιστικές πολιτικές, όπως ο GDPR, θα πρέπει να εξελιχθούν για να καλύψουν τις ιδιαιτερότητες της ενεργειακής πληροφορίας, η οποία μπορεί να αποκαλύψει ευαίσθητα προσωπικά δεδομένα. Η υιοθέτηση προτύπων που επιβάλλουν τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας (PETs) θα είναι καθοριστική για την αποδοχή των δικτύων από το κοινό (Xiao et al., 2025). Η έρευνα πρέπει να

υποστηρίξει τη δημιουργία ενός νομικού πλαισίου που θα εξισορροπεί την ανάγκη για δεδομένα με το δικαίωμα στην ιδιωτικότητα (Xiao et al., 2025).

Η θεσμοθέτηση προτύπων για τη χρήση του Blockchain στις ενεργειακές συναλλαγές είναι επίσης απαραίτητη για την εμπορική επέκταση των microgrids. Τα επόμενα πρότυπα θα πρέπει να ορίζουν τις τεχνικές προδιαγραφές για τους αλγορίθμους συναίνεσης, διασφαλίζοντας ότι είναι ενεργειακά αποδοτικοί (Yao et al., 2024). Μια τέτοια πολιτική θα διευκολύνει την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας και θα προστατεύσει τους παραγωγούς (Yao et al., 2024).

Επιπλέον, οι πολιτικές κυβερνοασφάλειας πρέπει να ενσωματώνουν την αρχιτεκτονική "Μηδενικής Εμπιστοσύνης" (Zero Trust Architecture), όπου καμία συσκευή δεν θεωρείται αξιόπιστη εξ ορισμού.Η δημιουργία κοινών προτύπων για την αναφορά περιστατικών θα επιτρέψει τη συλλογική άμυνα απέναντι σε οργανωμένες επιθέσεις (Zhang et al., 2020). Η μελλοντική έρευνα θα πρέπει να αξιολογήσει την αποτελεσματικότητα αυτών των συνεργατικών μοντέλων (Sun et al., 2021).

Η διεθνής συνεργασία για τη δημιουργία προτύπων κβαντικής ασφάλειας πρέπει να επιταχυνθεί, καθώς οι απειλές δεν αναγνωρίζουν σύνορα (Bernstein & Lange, 2017). Οι πολιτικές θα πρέπει να προβλέπουν τη σταδιακή αντικατάσταση των παλαιών κρυπτογραφικών συστημάτων με νέα, μετα-κβαντικά πρότυπα (Bernstein & Lange, 2017). Αυτό απαιτεί έναν μακροχρόνιο στρατηγικό σχεδιασμό από τους διαχειριστές των δικτύων.

Τέλος, τα επόμενα πρότυπα θα πρέπει να ενσωματώνουν απαιτήσεις για "κυβερνοανθεκτικότητα", ορίζοντας πώς ένα δίκτυο πρέπει να ανακάμπτει μετά από μια παραβίαση. Αυτό περιλαμβάνει την υποχρεωτική χρήση αποκεντρωμένων αρχιτεκτονικών που αποτρέπουν την ολική κατάρρευση του συστήματος (Wu et al., 2022). Η δημιουργία ενός ολοκληρωμένου πλαισίου πολιτικής θα αποτελέσει τον οδικό χάρτη για την ασφαλή μετάβαση στην εποχή των 6G δικτύων (Wu et al., 2022).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity*, *7*(1), 10.

Adewole, K. S., & Torra, V. (2022). DFTMicroagg: a dual-level anonymization algorithm for smart grid data. *International Journal of Information Security*, *21*(6), 1299-1321.

AEMO (2025). *Australian Energy Sector Cyber Security Framework (AESCSF): 2025 Overview and Maturity Assessment*. Australian Energy Market Operator.

Ahadipour, A., Mohammadi, M., & Keshavarz-Haddad, A. (2019). Statistical-based privacy-preserving scheme with malicious consumers identification for smart grid. *arXiv preprint arXiv:1904.06576*.

Ahmed, I., El-Rifaie, A. M., Akhtar, F., Ahmad, H., Alaas, Z., & Ahmed, M. M. R. (2025). Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. *Energy Strategy Reviews*, *58*, 101654.

Albarakati, A. J., Boujoudar, Y., Azeroual, M., Eliysaouy, L., Kotb, H., Aljarbouh, A., ... & Pupkov, A. (2022). Microgrid energy management and monitoring systems: A comprehensive review. *Frontiers in Energy Research*, *10*, 1097858.

Almousa, O., & Hamdallh, B. (2025). Enhancing IoT Security: A comparative analysis of machine learning and deep learning techniques for botnet detection. *Engineering, Technology & Applied Science Research*, *15*(4), 24498-24505.

Alnaim, A. K., & Alwakeel, A. M. (2025). Zero trust strategies for cyber-physical systems in 6G networks. *Mathematics*, *13*(1108).

Alomari, M. A., Al-Andoli, M. N., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J. A. J., & Gaid, A. S. (2025). Security of smart grid: cybersecurity issues, potential cyberattacks, major incidents, and future directions. *Energies*, *18*(1), 141.

Alshamasi, R. Z., & Ibrahim, D. M. (2025). Federated intelligence for smart grids: a comprehensive review of security and privacy strategies. *Journal of Electrical Systems and Information Technology*, *12*(1), 43.

Angara, S., Niure Kandel, L., & Dhakal, R. (2025). Cybersecurity in Smart Grids: A Domain-Centric Review. *Systems*, *13*(12), 1119.

Armoogum, S., & Bassoo, V. (2019). Privacy of energy consumption data of a household in a smart grid. In *Smart power distribution systems* (pp. 163-177). Academic Press.

Balaji, C. G., Menaka, S., Rajeswari, G., & Ponnusamy, S. (2025). A unified AI-driven framework for quantum-secured 6G THz networks with intelligent reflecting surfaces and federated edge learning: CG Balaji et al. *Scientific Reports*, *15*(1), 42510.

Batista, N. C., Melício, R., & Mendes, V. M. F. (2014). Layered Smart Grid architecture approach and field tests by ZigBee technology. *Energy Conversion and Management*, 88, 49–59.

Ben Dhaou, I. S., et al. (2020). *Internet of Things Technologies for Smart Grid*. In: Tools and Technologies for the Development of Cyber-Physical Systems, pp. 256-284. doi:10.4018/978-1-7998-1974-5.ch010.

Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.

Bharathi, Y. H. (2024). Edge AI for Real-Time Motor Condition Monitoring in Smart Grids. *International Journal of Intelligent Systems and Applications in Engineering*, 12(12s), 1011–1020.

Bibi, H., Abolhasan, M., Lipman, J., Abdollahi, M., & Ni, W. (2025). A comprehensive survey on privacy-preserving technologies for Smart Grids. *Computers and Electrical Engineering*, *124*, 110371.

Bimpas, A., Violos, J., Leivadeas, A., & Varlamis, I. (2024). Leveraging pervasive computing for ambient intelligence: A survey on recent advancements, applications and open challenges. *Computer Networks*, *239*, 110156.

Böck, L., Sundermann, V., Fusari, I., Karuppayah, S., Mühlhäuser, M., & Levin, D. (2023). The End of the Canonical IoT Botnet: A Measurement Study of Mirai's Descendants. *arXiv preprint arXiv:2309.01130*.

Bouslimani, M., Benbouzid-Si Tayeb, F., Amirat, Y., & Benbouzid, M. (2025). Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures. *Applied Sciences*, *15*(23), 12367.

Chee, K. O., Ge, M., Bai, G., & Kim, D. D. (2025). Unveiling the evolution of IoT threats: Trends, tactics, and simulation analysis. *Computers & Security*, 104537.

Chen, X., Feng, W., Ge, N., & Zhang, Y. (2024). Zero trust architecture for 6G security. *arXiv preprint arXiv:2401.03153*.

de Caldas Filho, F. L., Soares, S. C. M., Oroski, E., de Oliveira Albuquerque, R., Da Mata, R. Z. A., De Mendonça, F. L. L., & de Sousa Júnior, R. T. (2023). Botnet detection and mitigation model for IoT networks using federated learning. *Sensors*, *23*(14), 6305.

Diamantoulakis, P. D., Kapinas, V. M., & Karagiannidis, G. K. (2015). Big Data Analytics for Dynamic Energy Management in Smart Grids. *Big Data Research*, 2(3), 94-101.

Dokku, N. S., David Amar Raj, R., Bodapati, S. K., Pallakonda, A., Reddy, Y. R. M., & Krishna Prakasha, K. (2025). Resilient cybersecurity in smart grid ICS communication using BLAKE3-driven dynamic key rotation and intrusion detection. *Scientific Reports*, *15*(1), 32754.

Dorri, A., Luo, F., Kanhere, S. S., Jurdak, R., & Dong, Z. Y. (2019). SPB: A secure private blockchain-based solution for energy trading. *IEEE Communications Magazine, 57*(12), 120-126. (Βασισμένο στο arXiv:1807.10897v1).

Eltamaly, A. M., & Elghaffar, A. N. A. (2021). Basic definitions of smart grid technologies and applications. In *2nd International Baku Conference on Scientific Research*.

ENISA (2024b). *Network and Information Systems Directive 2 (NIS2)*. European Union Agency for Cybersecurity. Ανακτήθηκε από https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

ENISA. (2025). *Technical implementation guidance on cybersecurity risk-management measures, version 1.0*. European Union Agency for Cybersecurity. Ανακτήθηκε από το παρεχόμενο έγγραφο οδηγιών για τον εφαρμοστικό κανονισμό (EU) 2024/2690 της οδηγίας NIS2.

Esmail, E. M., Elsadd, M. A., Elkalashy, N. I., & Kawady, T. (2020). A review: Smart distribution grid management using agents. *WSEAS Trans. Syst*, *19*, 257-270.

EU Cyber Laws (2024). *GDPR Compliance Guide*. Ανακτήθηκε από https://eu-cyber-laws.com/gdpr/compliance/

European Commission (2024). *Commission Delegated Regulation (EU) 2024/1366 on cybersecurity aspects of cross-border electricity flows*. Official Journal of the European Union.

Fang, X. (2023). Energy management system technology in smart grid. *technology*, *76*.

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEe Access*, *9*, 138509-138542.

Fragkos, G., Johnson, J., & Tsiropoulou, E. E. (2022). Centralized and Decentralized Distributed Energy Resource Access Control Implementation Considerations. *Energies*, 15(17), 6375.

Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques. *Sensors*, *24*(11), 3571.

Goodridge, M. P., Zocca, A., & Lakshminarayana, S. (2023, October). Analysis of cascading failures due to dynamic load-altering attacks. In *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (pp. 1-6). IEEE.

Haider, Z. A., Zeb, A., Rahman, T., Singh, S. K., Akram, R., Arishi, A., & Ullah, I. (2025). A Survey on anomaly detection in IoT: Techniques, challenges, and opportunities with the integration of 6G. *Computer Networks*, 270, 111484.

Hasan, M. K., Habib, A. A., Islam, S., Safie, N., Abdullah, S. N. H. S., & Pandey, B. (2023). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports*, *9*, 1318-1326.

Huang, C., Tong, J., Liao, S., Wang, J., Zhou, F., Kong, W., ... & Li, J. (2025, November). Quantum-Enhanced Security Framework for Next-Generation Space–Terrestrial Networks. In *Photonics* (Vol. 12, No. 12, p. 1182). MDPI.

Huang, G., Li, D., Wang, Y., Wang, L., Zhang, M., & Yue, H. (2026). Factors Affecting Citizens' Security Perception of Smart City Construction: From the Perspective of Participatory Governance. *Systems*, *14*(1), 57.

Ibrahim, M., & Kashef, R**.** (2025). Digital Twin and LLM-based anomaly detection in smart grids: A real-time security perspective. *Journal of Systems Architecture*, 158, 103310.

Ibrahim, N., & Kashef, R. (2025). Exploring the emerging role of large language models in smart grid cybersecurity: a survey of attacks, detection mechanisms, and mitigation strategies. *Frontiers in Energy Research*, *13*, 1531655.

Islam, M. Z., Lin, Y., Vokkarane, V. M., & Venkataramanan, V. (2023). Cyber-physical cascading failure and resilience of power grid: A comprehensive review. *Frontiers in Energy Research*, *11*, 1095303.

ISO (2024). *ISO/IEC 27701:2024 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. Online Browsing Platform (OBP). Ανακτήθηκε από https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27701:ed-2:v1:en

Jin, H., Jeon, G., Choi, H. W. A., Jeon, S., & Seo, J. T. (2024). A threat modeling framework for IoT-Based botnet attacks. *Heliyon*, *10*(20).

Jithish, J., Mahalingam, N., Wang, B., & Yeo, K. S. (2025). Ruj, S., & Pal, A. (2024). Cascading Failures in Smart Grids under Random, Targeted, and Adaptive Attacks. In *A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations* (pp. 173-211).*Cybersecurity*, *8*(1), 61.

Jithish, J., Mahalingam, N., Wang, B., & Yeo, K. S. (2025). Towards enhancing security for upcoming 6G-ready smart grids through federated learning and cloud solutions. *Cybersecurity*, *8*(1), 61.

Jyoti, G. (2022). Blockchain-enabled decentralized energy trading in smart grid systems. *REDVET - Revista Electrónica de Veterinaria*, *23*(1), 554-563.

Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. *Future Internet*, 17(312).

Khan, M. F. (2025). 6G-Enabled Smart Energy IoT Infrastructure for Next-Generation Power Systems. *Dialogue Social Science Review (DSSR)*, 4(1), 1-7.

Kharbouch, A., Aghdam, F. H., Gholipoor, N., & Rasti, M. (2025). Digital-Twin-6G Empowered Future Smart Grid Applications. *IEEE Wireless Communications*, *32*(3), 90-97.

Khare, V. (2024**).** *Internet of Things in Smart Grid: A Comprehensive Review of Opportunities, Trends, and Challenges.*

Khavari, F., Badri, A., Zangeneh, A., & Shafiekhani, M. (2017). A Comparison of Centralized and Decentralized Energy-Management Models of Multi-microgrid Systems. In *2017 Smart Grids Conference (SGC)*. Tehran, Iran.

Kirmani, S., Mazid, A., Khan, I. A., & Abid, M. (2022). A survey on IoT-enabled smart grids: technologies, architectures, applications, and challenges. *Sustainability*, *15*(1), 717.

Kordi, M., Ali, S. M. F., Lollini, P., & Bondavalli, A. (2025). Analyzing the 2015 Ukraine power grid cyber-attack: a quantitative assessment of adversary behavior and impact. In *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.

Kordi, S., et al. (2025). Self-healing mechanisms in SCADA systems: Lessons from a decade of cyber-physical attacks. *International Journal of Critical Infrastructure Protection*, 48, 100612.

Kurt, M. N., Yılmaz, Y., & Wang, X. (2018). Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, *14*(2), 498-513.

Lernefalk, M. (2021). Evaluating the Effects of Denial-of-Service Attacks from IoT Devices.

Lin, I. C., Lin, K. Y., Wu, N. I., & Hwang, M. S. (2025). A quantum key distribution for securing smart grids. *Cryptography*, *9*(2), 28.

Liu, X., & Nielsen, P. S. (2016). *Regression-based Online Anomaly Detection for Smart Grid Data*. arXiv preprint arXiv:1606.05781.

Ma, Z., Xie, J., Li, H., Sun, Q., Si, Z., Zhang, J., & Guo, J. (2017). The Role of Data Analysis in the Development of Intelligent Energy Networks. *IEEE*, 1-6. (Αναφορά στο PDF: 1705.11132v1).

Mahmood, M., Chowdhury, P., Yeassin, R., Hasan, M., Ahmad, T., & Chowdhury, N.-U.-R. (2024). Impacts of digitalization on smart grids, renewable energy, and demand response: An updated review of current applications. *Energy Conversion and Management: X*, 24, 100790.

Mathas, C. M., et al. (2020). *Threat Landscape for Smart Grid Systems*. In 15th International Conference on Availability, Reliability and Security (ARES 2020). arXiv preprint arXiv:2105.04264.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12-22.

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., ... & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things journal*, *8*(1), 18-43.

Mu'min, M. A., Safitri, Y., Saputra, S., Sulistianingsih, N., Ragimova, N., & Abdullayev, V. (2025). Post-quantum cryptography review in future cybersecurity strengthening efforts. *Scientific Journal of Engineering Research*, *1*(3), 135-141.

Nafi, N. S., Ahmed, K., Gregory, M. A., & Datta, M. (2016). A survey of smart grid architectures, applications, benefits and standardization. *Journal of Network and Computer Applications*, 76, 23–36.

Naja, R., Soni, A., & Carletti, C. (2023). Electric Vehicles Energy Management for Vehicle-to-Grid 6G-Based Smart Grid Networks. *Journal of Sensor and Actuator Networks*, 12(79), 1-18.

Nambundo, J. M., Gomes, O. S., de Souza, A. D., & Machado, R. C. S. (2025). Cybersecurity and Major Cyberthreats of Smart Meters: A Systematic Mapping Study.

Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, *25*(2), 550.

NISA (2024a). *NIS2 Technical Implementation Guidance*. European Union Agency for Cybersecurity. Ανακτήθηκε από https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

NIST (2024). *NIST IR 8498: Cybersecurity for Smart Inverters in Residential and Commercial Solar Systems*. National Institute of Standards and Technology.

Norouzi, F., Hoppe, T., Kamp, L. M., Manktelow, C., & Bauer, P. (2023). Diagnosis of the implementation of smart grid innovation in The Netherlands and corrective actions. *Renewable and Sustainable Energy Reviews*, *175*, 113185.

Ohanu, C. P., Rufai, S. A., & Oluchi, U. C. (2024). A comprehensive review of recent developments in smart grid through renewable energy resources integration. *Heliyon*, *10*(3).

Omheni, N., Koubaa, H., & Zarai, F. (2025). Artificial intelligence for 5G and 6G networks: A taxonomy-based survey of applications, trends, and challenges. *Technologies*, *13*(12), 559.

Pacific Northwest National Laboratory. (n.d.). *Smart grid*. PNNL Explainer Articles. Ανακτήθηκε στις 14 Ιανουαρίου 2026, από https://www.pnnl.gov/explainer-articles/smart-grid

Panda, D. K., & Das, S. (2021). Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. *Journal of Cleaner Production*, 301, 126877.

Qays, M. O., Ahmad, I., Abu-Siada, A., Hossain, M. L., & Yasmin, F. (2023). Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. *Energy Reports*, *9*, 2440-2452.

Radovanovic, D., Unterweger, A., Eibl, G., Engel, D., & Reichl, J. (2022). How unique is weekly smart meter data?. *Energy Informatics*, *5*(Suppl 1), 13.

Saha, S., Ravi, N., Hreinsson, K., Baek, J., Scaglione, A., & Johnson, N. G. (2020). A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain. *arXiv preprint arXiv:2011.06983*.

Sahu, B. K., & Mahapatra, T. K. ROLE OF IOT IN SMART GRIDS: A REVIEW.

Sanz, A., Franco, D., Salegi, E., Astorga, J., Atutxa, A., & Jacob, E. (2025). Extending quantum-safe communications to real-world networks: An adaptive security framework. *arXiv preprint arXiv:2511.22416*.

Shamaseen, A., Qatawneh, M., & Elshqeirat, B. (2025). Smart grid system based on blockchain technology for enhancing trust and preventing counterfeiting issues. *Energies, 18*(13), 3523.

Shome, S., Das, S., Das, S., & Pal, D. (2025). An Extensive Review of THz Communication in 6G: Facilitating Technologies with Edge Computing and Native AI. *Franklin Open*, 100434.

Singh, A. R., et al. (2025). A scalable cloud-integrated AI platform for real-time optimization of EV charging and resilient microgrid energy management. *Scientific Reports*, 15, 37692.

SlideGeeks. (n.d.). *Difference between traditional and smart grid smart grid working*. https://www.slidegeeks.com/difference-between-traditional-and-smart-grid-smart-grid-working

Stojnic, T., Kayes, A. S. M., Rahayu, W., & Chowdhury, M. J. M. (2025). A comprehensive literature review of cyber threats and vulnerabilities in IoT-driven satellite networks: Research challenges and future directions. *Computer Networks*, 111678.

Su, K., Yu, Y., & Zhang, J. (2024). Blockchain-based smart grid power trading technology. *Journal of Engineering and Applied Science, 71*(1), 220.

Szczepaniuk, E. K., & Szczepaniuk, H. (2025). Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. *Energies*, *18*(1), 141.

Tan, R., Krishna, V. B., Yau, D. K. Y., & Kalbarczyk, Z. (2016**).** *Impact of Integrity Attacks on Real-Time Pricing in Smart Grids*. arXiv preprint arXiv:1602.02860v1.

Tariq, N., Alsirhani, A., Humayun, M., Alserhani, F., & Shaheen, M. (2024). A fog-edge-enabled intrusion detection system for smart grids. *Journal of Cloud Computing*, *13*(1), 43.

Teixeira, A., Dán, G., Sandberg, H., & Johansson, K. H. (2010). *A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator*. arXiv preprint arXiv:1011.1828.

Tightiz, L., & Yang, H. (2020). *A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication*. Energies, 13(11), 2762. doi:10.3390/en13112762.

Ullah, A., Fawad, Nadeem, A., Arif, M., Bashir, M. M., & Choi, W. (2025). 6G Internet-of-Things assisted smart homes and buildings: Enabling technologies, opportunities and challenges. *Internet of Things*, 32, 101658.

Unsal, D. B., Ustun, T. S., Hussain, S. S., & Onen, A. (2021). Enhancing cybersecurity in smart grids: False data injection and its mitigation. *Energies*, *14*(9), 2657.

Unterweger, A., Knirsch, F., Eibl, G., & Engel, D. (2016). Privacy-preserving load profile matching for tariff decisions in smart grids. *EURASIP Journal on Information Security*, *2016*(1), 21.

Voyez, A., Allard, T., Avoine, G., Cauchois, P., Fromont, E., & Simonin, M. (2025). The privacy cost of fine-grained electrical consumption data. *Scientific Reports*, *15*(1), 17391.

Wissner, M. (2011). The Smart Grid–A saucerful of secrets?. *Applied Energy*, *88*(7), 2509-2518.

Wu, C. J., Huang, S. Y., Yoshioka, K., & Matsumoto, T. (2020). IoT malware analysis and new pattern discovery through sequence analysis using meta-feature information. *IEICE Transactions on Communications*, *103*(1), 32-42.

Wu, L., Zhang, W., & Zhao, W. (2022). Privacy preserving data aggregation for smart grid with user anonymity and designated recipients. *Symmetry*, *14*(5), 847.X

Wu, Y., Wu, Y., Guerrero, J. M., & Vasquez, J. C. (2022). Decentralized transactive energy community in edge grid with positive buildings and interactive electric vehicles. *International Journal of Electrical Power & Energy Systems*, 135, 107510.

Xiao, Y., Xu, J., Lin, Z., Xie, Y., Liu, R., Yan, L., & Feng, P. (2025). Privacy Protection Anomaly Detection in Smart Grids Based on Combined PHE and TFHE Homomorphic Encryption. *Electronics*, *14*(12), 2386.

Yao, Z., Fang, Y., Pan, H., Wang, X., & Si, X. (2024). A secure and highly efficient blockchain PBFT consensus algorithm for microgrid power trading. *Scientific Reports*, *14*(1), 8300.

Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). Iot botnet forensics: A comprehensive digital forensic case study on mirai botnet servers. *Forensic Science International: Digital Investigation*, *32*, 300926.

Zhang, Y., Huang, T., & Bompard, E. F. (2018). Big data analytics in smart grids: a review. *Energy Informatics*, 1, 8.

Zhang, Z., Lu, Q., Xu, H., Xu, G., Kong, F., & Yu, Y. (2022). Privacy-preserving deep learning for electricity consumer characteristics identification. *Frontiers in Energy Research*, *10*, 992117.