
**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

**ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ**

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**

# Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη στα Ευφυή Συστήματα Ηλεκτρικής Ενέργειας

Μεταπτυχιακή Διπλωματική Εργασία

Βασιλάκος Νικόλαος

Επιβλέπων: Δρ. Δασκαλοπούλου Ασπασία

Νοέμβριος 2022


**UNIVERSITY OF THESSALY**

**SCHOOL OF ENGINEERING**

**DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING**

# Cybersecurity and Artificial Intelligence in SmartGrids

MSc Thesis

VASILAKOS NIKOLAOS

Supervisor: Daskalopulu Aspasia

November 2022

Εγκρίνεται από την Επιτροπή Εξέτασης:

| | |
|---|---|
| Επιβλέπουσα | **Δασκαλοπούλου Ασπασία**<br>Αναπληρώτρια Καθηγήτρια, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας |
| Μέλος | **Χροναίος Αλέξανδρος**<br>Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας |
| Μέλος | **Τσουκαλάς Ελευθέριος**<br>Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας |

**ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ**

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα μεταπτυχιακή διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής..

Ο Δηλών

Βασιλάκος Νικόλαος

**DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS**

Being fully aware of the implications of copyright laws, I expressly state that this MSc thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work/ contributions of third parties for which the permission of the authors/beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and/or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually, and personally undertake all legal and administrative consequences that may arise if it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Vasilakos Nikolaos

# Ευχαριστίες

Με την παρούσα μεταπτυχιακή διπλωματική εργασία ολοκληρώνεται ο κύκλος σπουδών μου στο μεταπτυχιακό πρόγραμμα σπουδών «Ευφυή Δίκτυα Ηλεκτρικής Ενέργειας» του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Θεσσαλίας.

Θα ήθελα αρχικά να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου, Κα. Δασκαλοπούλου Ασπασία, για την υπομονή της καθ' όλη την διάρκεια της εκπόνησης της εργασίας μου. Επίσης, ευχαριστώ θερμά και τα υπόλοιπα μέλη της τριμελούς επιτροπής για τη συμμετοχή τους.

Θα ήταν παράλειψη να μην ευχαριστήσω όλους τους καθηγητές του Μεταπτυχιακού Προγράμματος διότι πέραν από την μετάδοση των επιστημονικών τους γνώσεων, υπήρξαν κοντά στους φοιτητές και πρόσδωσαν αξία στην εμπειρία του εν λόγω Μεταπτυχιακού.

Τέλος, δε μπορώ να μην εκφράσω την ευγνωμοσύνη μου στην σύζυγό μου για τη συμπαράσταση της καθώς και για την ηθική της στήριξη στις επιλογές μου όλα αυτά τα χρόνια.

Cybersecurity and Artificial Intelligence in SmartGrids

Μεταπτυχιακή Διπλωματική Εργασία

# Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη στα Ευφυή Συστήματα Ηλεκτρικής Ενέργειας

Βασιλάκος Νικόλαος

## Περίληψη

Καθώς η Ελλάδα αποτελεί κράτος-μέλος μιας Ενιαίας Ευρωπαϊκής Κοινότητας στη σύγχρονη αυτή εποχή, για τον λόγο αυτό, επιτακτική κρίνεται η ανάγκη για άμεση αναβάθμιση των υπαρχόντων δικτύων ηλεκτρικής ενέργειας και ενσωμάτωσης της τεχνολογίας που έχει αναπτυχθεί για τον εκσυγχρονισμό αυτών με βάση την ασφάλεια των προσωπικών δεδομένων και τη χρήση της Τεχνικής Νοημοσύνης για λόγους βελτιστοποίησης της αποδοτικότητας του ηλεκτρικού συστήματος.

Στα πλαίσια αυτά, τις τελευταίες δεκαετίες, κάνει την εμφάνισή της μία νέα τεχνολογία που η χρησιμότητά της θα δημιουργήσει νέους ορίζοντες για ανάπτυξη και αποτελεσματική απόδοση και μετατροπή των υπαρχόντων ηλεκτρικών συστημάτων σε έξυπνα.

Ο λόγος για την Τεχνητή Νοημοσύνη, η οποία αντιπροσωπεύει ένα εργαλείο επανάστασης στο χώρο της τεχνολογίας, σύμφωνα με την οποία, ο ρόλος της και η αποτελεσματικότητά της κρίνεται με βάση της ικανοποίηση των αναγκών των πολιτών καθώς επίσης και στη βάση της ποιότητας των αποτελεσμάτων που αποδίδονται με την χρήση της. Η τεχνολογία αυτή θα προσφέρει φερεγγυότητα και βέλτιστο αποτέλεσμα με την σωστή χρήση της.

Η παρούσα διπλωματική εργασία πραγματεύεται την χρήση της Τεχνητής Νοημοσύνης, καθώς και τον τρόπο που μπορεί να διευκολύνει τη διοχέτευση της ηλεκτρικής ενέργειας κάνοντας το ηλεκτρικό δίκτυο “Έξυπνο” και να αποτρέψει τυχόν, κυβερνοεπιθέσεις και διαρροή ευαίσθητων δεδομένων από το Smart Grid.

Αναλυτικότερα λοιπόν, μετά από συστηματική δευτερογενή έρευνα αναλύονται οι ενέργειες που έχουν πραγματοποιηθεί τα τελευταία χρόνια όσον αφορά τον εκσυγχρονισμό του ηλεκτρικού δικτύου οι οποίες προσανατολίζονται κυρίως προς τον πολίτη. Διερευνάται επίσης, η επιρροή που έχει η νέα τεχνολογία, στις υφιστάμενες συνθήκες και εντοπίζονται τα χαρακτηριστικά στοιχεία που πρέπει να υιοθετηθούν από την πολιτική ηγεσία του τόπου ώστε να υλοποιηθούν στο άμεσο μέλλον. Επίσης, η εργασία, επεξηγεί τις σχετικές σύγχρονες μεταρρυθμίσεις σε συνδυασμό με τα πρότυπα και τα μέτρα απόδοσης.

Συγκεκριμένα, παρουσιάζονται και αναλύονται οι δείκτες μέτρησης και αποτίμησης της απόδοσης, της αποτελεσματικότητας και της αποδοτικότητας της Τεχνητής Νοημοσύνης, υπό το πρίσμα του Smart Grid, σε θέματα ασφάλειας και διαχείρισης.

Σκοπός της παρούσας διπλωματικής εργασίας αποτελεί η μελέτη και η κατανόηση του τρόπου με τον οποίο η Τεχνητή Νοημοσύνη θα βοηθήσει στην ασφάλεια των δεδομένων του πολίτη από την νέα αυτή υιοθέτηση της τεχνολογίας παρουσιάζοντας μια σαφή εικόνα της δυναμικής του εν λόγου μεταρρυθμιστικού μοντέλου. Επιχειρείται λοιπόν, μια προσέγγιση στις βασικές έννοιες που συνθέτουν το λόγο της χρήσης, της Τεχνητής Νοημοσύνης ως ασπίδα σε κυβερνοεπιθέσεις. Με τον τρόπο αυτό, πρώτον, καθίσταται δυνατή η διασφάλιση των δεδομένων και δεύτερον επισημαίνονται οι ουσιαστικές διαφορές σε σχέση με το παλιό μοντέλο του ηλεκτρικού δικτύου που ευδοκιμούσε τόσα χρόνια.

Αρχικά, στην εν λόγω εργασία θα γίνει αναφορά στις βασικές αρχές που διέπουν τη Τεχνητή Νοημοσύνη καθώς και στους λόγους που οδήγησαν την τεχνολογία να εισχωρήσει στην καθημερινότητά μας. Εν συνεχεία, θα ερευνηθεί η εφαρμογή του "Έξυπνου" ηλεκτρικού συστήματος στους κόλπους της παλιάς δομής αναφορικά με τον δείκτη αποδοτικότητας και της ασφάλειας. Κατόπιν, θα αναλυθεί η περίπτωση του ελληνικού παραδείγματος και πώς μπορεί να λειτουργήσει σε αυτό. Εν κατακλείδι, θα καταλήξουμε στα απαραίτητα συμπεράσματα έτσι ώστε, να γίνει αντιληπτή στον αναγνώστη η σημασία της ενσωμάτωσης, της Τεχνητής Νοημοσύνης, καθώς και η σπουδαιότητα της εφαρμογής της.

Όντας μέλος της κοινωνίας και με βάσει την επαγγελματική μου ιδιότητα μέσα στο χώρο της Τεχνολογίας των πληροφοριών και των δεδομένων με απασχόλησε εντόνως ο τρόπος χρήσης, της Τεχνητής Νοημοσύνης. Έτσι λοιπόν, το επιστημονικό μου ενδιαφέρον για το συγκεκριμένο θέμα προέκυψε από το κίνητρο για βελτίωση της υφιστάμενης δομής και της εκπορευόμενης συνολικής κοινωνικοοικονομικής αναδιοργάνωσης. Η ακολουθούμενη μεθοδολογική προσέγγιση είναι η ανάδειξη της Τεχνητής Νοημοσύνης ως βασικό εργαλείο προσαρμογής του ηλεκτρικού δικτύου στη σύγχρονη συγκυρία με σκοπό τη μέγιστη απόδοση και την αποτελεσματικότερη χρήσης της ηλεκτρικής ενέργειας στην κοινωνία μας.

**Λέξεις-κλειδιά:**

Ευφυή Δίκτυα, Τεχνητή Νοημοσύνη, Ηλεκτρικό Σύστημα, κρυπτογραφικές τεχνικές, Ασφάλεια του Κυβερνοχώρου, Είδη Επιθέσεων, Κυβερνοασφάλεια, Κυβερνοαπειλές

MSc Thesis

# Cybersecurity and Artificial Intelligence in SmartGrids

Vasilakos Nikolaos

## Abstract

As Greece is a member state of a Single European Community in this modern era, for this reason, the need for an immediate upgrade of the existing electricity networks and the integration of the technology that has been developed to modernize them based on the safety of personal data and usage of Artificial Intelligence for purposes of optimizing the efficiency of the electrical system.

In this context in the last decades an innovative technology has appeared whose utility will create new horizons for development and efficient performance and transformation of existing electrical systems into smart ones.

The reason for Artificial Intelligence, which represents a tool of revolution in the field of technology, according to which, its role and its effectiveness are judged based on satisfying the needs of citizens as well as based on the quality of the results that are attributed with its use. This technology will offer solvency and optimal results with its correct use.

This thesis deals with the use of Artificial Intelligence as well as how it can facilitate the channeling of electricity by making the electrical grid "Smart" and prevent any cyber-attacks and leakage of sensitive data from the Smart electrical grid.

In more detail, after systematic secondary research, the actions that have been conducted in recent years regarding the modernization of the electricity network, which are oriented towards the citizen, are analyzed. The influence that the innovative technology has on the existing conditions is also investigated and the characteristic elements that must be adopted by the political leadership of the place to be implemented in the immediate future are identified.

Also, the paper explains relevant contemporary reforms along with standards and performance measures. Specifically, the measurement and valuation indicators of the performance, effectiveness and efficiency of Artificial Intelligence are presented and analyzed, in the light of the Smart electrical grid, in terms of security and management.

The purpose of this thesis is to study and understand how Artificial Intelligence will help in the security of citizen data from this new adoption of technology, presenting a clear picture of the dynamics of the said reform model. It therefore attempts an approach to the basic concepts that make up the reason for the use of Artificial Intelligence as a shield in cyberattacks. In this way, firstly, it becomes possible to secure the data and, secondly, it highlights the essential differences compared to the old model of the electrical grid that thrived for so many years.

Initially, in this paper reference will be made to the basic principles that govern Artificial Intelligence as well as the reasons that led the technology to enter our daily lives. Subsequently, the application of the "Smart" electrical system within the old structure will be investigated in terms of the efficiency and safety index. Then, the case of the Greek example will be analyzed and how it can work in it. In conclusion, we will reach the necessary conclusions so that the reader can understand the importance of the integration of Artificial Intelligence, as well as the importance of its application.

Being a member of society and based on my professional status in the field of information and data technology. I was intensely concerned with the way of using Artificial Intelligence. Thus, my scientific interest in this subject arose from the motivation to improve the existing structure and the emanating overall socio-economic reorganization. The methodological approach followed is the promotion of Artificial Intelligence as a key tool for adapting the electricity network to the modern times with the aim of maximum performance and the most efficient use of electricity in our society.

**Keywords:**

Intelligent Networks, Artificial Intelligence, Electrical, System Cryptographic Techniques, Cyber Security, Types of Attacks, Cyber-Security, Cyber Threats

# Πίνακας περιεχομένων

# Κατάλογος πινάκων

# Συντομογραφίες

| | |
|---|---|
| ΑΠΕ | Ανανεώσιμες Πηγές Ενέργειας |
| ΕΕ | Ευρωπαική Ένωση |
| κ.α. | και άλλα |
| κ.λπ. | και λοιπά |
| π.χ. | παραδείγματος χάρη |
| ΤΠΕ | Τεχνολογίες Πληροφοριών και Επικοινωνίας |
| Φ/Β | Φωτοβολταικό |
| AGI | Artificial General Intelligence |
| AI | Artificial Intelligence |
| AMI | Advanced Metering Infrastructure |
| ASI | Artificial Super Intelligence |
| BAN | Business Area Networks |
| DoS | Denial-of-Service |
| DL | Deep Learning |
| ESI | Energy Services Interface |
| EV | Electric Vehicles |
| HAN | Home Area Network |
| IAN | Industrial Area Networks |
| ICT | Information and Communication Technology |
| IDS | Intrusion Detection System |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPS | Internet Provider Service |
| LAN | Local Area Network |
| MitM | Man-in-the-Middle |

| | |
|---|---|
| ML | Machine Learning |
| NAN | Neighbourhood Area Networks |
| NIST | National Institute of Standards and Technology |
| reCAPTCHA | Completely Automated Public Turing test to tell Computers and Humans Apart |
| SCADA | Supervisory Control And Data Acquisition |
| SOCs | Security Operation Centers |
| UART | Universal Asynchronous Receiver-Transmitter |
| VI-DAS | Vision Inspired Driver Assistance Systems |
| Wi-Fi | Wireless Fidelity |

# Κεφάλαιο 1 Εισαγωγή

Η AI είναι ο ορίζοντας της τεχνολογίας στην εποχή μας που επινοήθηκε το 1979 από έναν επιστήμονα των υπολογιστών τον John McCarthy, είναι η επιστήμη των υπολογιστών που αναφέρεται στην ικανότητα μιας μηχανής να αναπαράγει τις ανθρώπινες γνωστικές λειτουργίες, όπως η μάθηση, ο σχεδιασμός και η δημιουργικότητα, για να ολοκληρώσει εργασίες αντικαθιστώντας κατά μεγάλο βαθμό την ανθρώπινη νοημοσύνη, ποιο συγκεκριμένα η ML θα παίξει πολύ σημαντικό ρόλο στην υλοποίηση και βελτιστοποίηση εφαρμογών σε συστήματα ασύρματης επικοινωνίας 6G, καθώς και ορισμένες πιθανές μελλοντικές τάσεις για την παροχή κινήτρων για περαιτέρω έρευνα σε αυτόν τον τομέα.

Η AI επιτρέπει στις μηχανές να «καταλαβαίνουν» το περιβάλλον τους, να λύνουν προβλήματα και να ενεργούν προς έναν συγκεκριμένο στόχο. Ο υπολογιστής επεξεργάζεται δεδομένα και αποκρίνεται με τρόπο που βασίζεται σε αυτά τα δεδομένα, έτσι όπως και το ηλεκτρικό δίκτυο εξελίσσεται σε προγραμματιζόμενο και ευέλικτο περιβάλλον θα βασίζεται πλέον και αυτό σε αυτοματοποιημένα AI/ML δίκτυα.

Τα συστήματα AI μπορούν να προσαρμόσουν τη συμπεριφορά τους με τρόπο που να λαμβάνουν υπόψη τους τα αποτελέσματα προηγούμενων ενεργειών και να μπορούν να επιλύουν τα προβλήματα μόνα τους.

Ωστόσο, η εξέλιξη των υπολογιστών, η αφθονία των δεδομένων και οι νέοι αλγόριθμοι επέτρεψαν την ταχεία ανάπτυξη της AI. Οι αλγόριθμοι AI μπορούν να βοηθήσουν στη βελτίωση της μάθησης, της επίλυσης προβλημάτων, της κατανόησης της γλώσσας και του λογικού συλλογισμού αν και υπάρχει έλλειψη εμπιστοσύνης των ανθρώπων ως προς την πρόβλεψη ενός AI. Η AI πλέον χρησιμοποιείται με πολλούς και διάφορους τρόπους στην καθημερινότητά μας, από προσωπικούς βοηθούς μέχρι και αυτοοδηγούμενα αυτοκίνητα. Η επιστήμη της AI αναπτύσσεται ραγδαία και έχει τη δυνατότητα να μας βοηθήσει να λύσουμε πολλές σημαντικές προκλήσεις της ζωής μας.

**Τα κυριότερα χαρακτηριστικά γνωρίσματα της AI είναι τα παρακάτω:**

- Να μπορεί να προβλέπει και να προσαρμόζεται, καθώς και να εντοπίζει μοτίβα από μεγάλες ποσότητες πληροφοριών και δεδομένων με την χρήση αλγορίθμων.
- Να λαμβάνει αποφάσεις αυτοβούλως και να έχει την ικανότητα να αυξήσει την ανθρώπινη νοημοσύνη, να διοχετεύει πληροφορίες, δεδομένα και να βελτιώνει την παραγωγικότητα.

- Να έχει τη δυνατότητα να "μαθαίνει" συνεχώς, και να χρησιμοποιεί αλγόριθμους για τη δημιουργία αναλυτικών μοντέλων και να ανακαλύπτει πώς να εκτελεί εργασίες μέσω απεριόριστων δοκιμών και σφαλμάτων.
- Να είναι ένα εργαλείο που επιτρέπει στους ανθρώπους να επανεξετάσουν τον τρόπο με τον οποίο αναλύουν δεδομένα, να ενσωματώνουν πληροφορίες και να χρησιμοποιούν αυτές τις πληροφορίες για τη λήψη καλύτερων αποφάσεων.
- Να έχει την ικανότητα αντίδρασης, δηλαδή να αντιδράσει σύμφωνα με προγράμματα και στοιχεία δράσης ενσωματωμένα στο λογισμικό και να επιτρέπει να ανταποκριθεί σε μια πράξη σύμφωνα με την προηγούμενη καθιερωμένη του κατάσταση.
- Να έχει τη δυνατότητα να μάθει από ορισμένες καταστάσεις, δημιουργώντας σε αυτήν μια μικρή συγκρατητική μνήμη. όπου λαμβάνονται οι πληροφορίες και όταν παρατηρείται μια παρόμοια ενέργεια, αντιδρά σαν να σκέφτεται μόνη της.
- Να επιλύει προβλήματα και να εξελίσσεται σταδιακά.
- Να είναι ικανή να αντιλαμβάνεται και να ψηλαφίζει ακουστικές, οπτικές και απτικές αλλοιώσεις, δημιουργώντας μια άμεση δράση σύμφωνα με την προκαθορισμένη κατάσταση.
- Να αναπτύσσει δομές όπου μπορεί να μάθει να διαχειρίζεται πτυχές που σχετίζονται με καταστάσεις, και να επιτρέπει τη δημιουργία μιας συμπεριφοράς.

Η AI χωρίζεται σε τέσσερις τύπους:

- Αντιδραστικές μηχανές
- Μηχανές με περιορισμένη μνήμη
- Μηχανές με θεωρία του Νου
- Μηχανές με αυτογνωσία

Ποιο αναλυτικά και αναφορικά με τον πρώτο τύπο, τις αντιδραστικές μηχανές, είναι αυτές που έχουν νοημοσύνη όπως το IBM Deep Blue, το IBM Watson και το Google AlphaGo, όπου οι προγραμματιστές δημιουργούν αυτές τις μηχανές γύρω από περίπλοκα σύνολα κανόνων. Εκτός από αυτούς τους κανόνες, μπορεί να περιλαμβάνουν νευρωνικά δίκτυα που τους επιτρέπουν να μάθουν και να προσαρμοστούν στη στιγμή. Αν και αυτός ο τύπος AI δεν μπορεί να σχηματίσει αναμνήσεις ή να δράσει βάσει προηγούμενων εμπειριών, καθώς δεν μπορούν να δημιουργήσουν αναμνήσεις, δεν μπορούν να πάρουν παρελθόντα γεγονότα, ακόμη και αυτά που τους συνέβησαν και να τα χρησιμοποιήσουν για να λάβουν νέες αποφάσεις. Έτσι, περιορίζονται στα σενάρια και τις πληροφορίες που καλύπτονται στα

σύνολα κανόνων τους. Μπορούν βέβαια να χρησιμοποιήσουν τους κανόνες τους αλλά μόνο εντός των ορίων που καθορίζονται από τα σύνολα κανόνων τους. Άρα δεν μπορούν να αλλάξουν τις μελλοντικές τους ενέργειες βάσει προηγούμενων περιστατικών και έτσι έχουμε ως αποτέλεσμα ότι οι αντιδραστικές μηχανές δεν μπορούν να μάθουν.

Στο δεύτερο τύπο, στις Μηχανές με περιορισμένη μνήμη, ανήκουν τα αυτοκίνητα, που παρακολουθούν συνεχώς τις συνθήκες γύρω τους και αποθηκεύουν αυτές τις πληροφορίες σε προσωρινή κατάσταση για να επηρεάσουν τις ενέργειές τους. (Intelligent Speed Assistance, Adaptive Cruise Control, Lane Keeping Aid, Drive Me)

Στον τρίτο τύπο, και τις μηχανές με θεωρία του Νου, που μπορούμε να θεωρήσουμε ότι ανήκουν κάποια είδη ρομπότ που μπορούν να καταλάβουν ότι πρέπει να μάθουν και να προσαρμόσουν τις αποφάσεις τους με βάση αυτά τα συναισθήματα και το "μυαλό" τους. Έτσι καταλαβαίνουν και δημιουργούν σκέψεις και συναισθήματα (ακόμη και αν δεν καταλαβαίνουν πραγματικά) και ότι οι σκέψεις και τα συναισθήματα που αναπτύσσουν επηρεάζουν τη συμπεριφορά τους. Το AI πρέπει να χρησιμοποιεί αυτούς τους παράγοντες στο πλαίσιο λήψης αποφάσεων.

Τέλος, και στο τέταρτο τύπο, στις Μηχανές με αυτογνωσία, είναι το τελευταίο και πιο περίπλοκο και ώριμο επίπεδο AI. Είναι μια οντότητα με αληθινή συνείδηση που γνωρίζει την ύπαρξή του και τις εσωτερικές του καταστάσεις (και πιθανώς συναισθήματα), μπορεί να σχηματίσει αναμνήσεις του παρελθόντος και να κάνει προβλέψεις. Επίσης, έχει επίγνωση άλλων συνειδητοποιήσεων και μπορεί να τις λάβει υπόψη κατά τη λήψη αποφάσεων. Βασικά, μπορεί να μάθει και να γίνει πιο έξυπνο με βάση τις εμπειρίες του. Αυτός ο τύπος δεν υπάρχει προς το παρόν και πιθανότατα απέχει πολλά χρόνια από την επίτευξή του.

Η AI σήμερα είναι γνωστή ως στενή AI (ή αδύναμη AI), είναι δηλαδή μία μη συναισθηματική ευφυΐα μηχανής, που είναι τυπικά σχεδιασμένη ώστε να εκτελεί μία και μόνο εργασία. Ωστόσο, ο μακροπρόθεσμος στόχος της επιστήμης και των ερευνητών είναι να δημιουργηθεί μια τεχνητή γενική νοημοσύνη AGI (ή αλλιώς ισχυρή AI) που είναι μια μηχανή με την ικανότητα να εφαρμόζει τη νοημοσύνη σε οποιοδήποτε πρόβλημα, και όχι μόνο σε ένα και μόνο πρόβλημα.

Η AGI θα μπορούσε θεωρητικά να ξεπεράσει τους ανθρώπους σε σχεδόν οποιοδήποτε πεδίο γνωστικής δραστηριότητας, συμπεριλαμβανομένων εργασιών όπως το σκάκι ή η επίλυση εξισώσεων. Ο απώτερος σκοπός και βέβαια υποθετικός στόχος είναι να επιτευχθεί

η ASI, μία νοημοσύνη που ξεπερνά κατά πολύ αυτή του πιο έξυπνου και ταλαντούχου ανθρώπου.

Η AI χρησιμοποιείτε πλέον στην καθημερινότητά μας και τείνει να γίνει αναπόσπαστο μέρος της ζωής μας. Παρακάτω αναφέρονται μερικά παραδείγματα εφαρμογών της AI.

**Διαδικτυακές αγορές και διαφήμιση**

Η AI χρησιμοποιείται συχνά για την παροχή εξατομικευμένων αναλύσεων και απόδοσης στενευμένων διαφημίσεων, όπως αυτές που βασίζονται σε προηγούμενες αναζητήσεις και αγορές. Η AI είναι ένα σημαντικό εργαλείο του εμπορικού τομέα, συμβάλλοντας στη βελτίωση των προϊόντων, του σχεδιασμού αποθεμάτων και της εφοδιαστικής αλυσίδας.

**Διαδικτυακή αναζήτηση**

Οι μηχανές αναζήτησης χρησιμοποιούν τα δεδομένα που εισάγουν οι χρήστες για να παρέχουν στοχευμένα αποτελέσματα.

**Προσωπικοί ψηφιακοί βοηθοί**

Τα smartphone χρησιμοποιούν την AI για να παρέχουν στους χρήστες προσαρμοσμένες ρυθμίσεις για τις ατομικές τους ανάγκες. Ο εικονικός βοηθός λειτουργεί ως προσωπικός γραμματέας του χρήστη, καθώς απαντά σε ερωτήσεις, προτείνει και υπενθυμίζει για συναντήσεις. Είναι επίσης ένα chatbot που προσαρμόζεται στα ατομικά χαρακτηριστικά ενός συγκεκριμένου ατόμου, λαμβάνοντας υπόψη του το περιβάλλον, τα ενδιαφέροντα και τις συνήθειες του χρήστη.

**Αυτόματες μεταφράσεις**

Το λογισμικό αυτό που χρησιμοποιείται για την αυτόματη μετάφραση και τον υποτιτλισμό που βασίζεται κυρίως σε γραπτή ή προφορική γλώσσα χρησιμοποιεί AI για να αποδώσει την βέλτιστη μετάφραση.

**Έξυπνα σπίτια και πόλεις**

Οι έξυπνοι θερμοστάτες χρησιμοποιούν δεδομένα συμπεριφοράς για εξοικονόμηση ενέργειας, ενώ τα έξυπνα συστήματα ελέγχου κυκλοφορίας πόλεων βασίζονται σε έξυπνα συστήματα διαχείρισης της κυκλοφορίας και τη μείωση της κυκλοφοριακής συμφόρησης.

**Αυτοκίνητα**

Αν και τα αυτόνομα οχήματα δεν αποτελούν επί του παρόντος μέρος της καθημερινότητάς μας, τα αυτοκίνητα γενικότερα αποτελούνται ήδη από έξυπνα συστήματα ασφαλείας που χρησιμοποιούν AI. Η ΕΕ έχει συμμετάσχει στη χρηματοδότηση αυτόματων αισθητήρων VI-DAS που εντοπίζουν πιθανούς κινδύνους και ατυχήματα. Τα συστήματα πλοήγησης βασίζονται στην AI για τη λειτουργία τους.

**Κυβερνοασφάλεια**

Η AI μπορεί να βοηθήσει στον εντοπισμό και την αντιμετώπιση επιθέσεων και απειλών στον κυβερνοχώρο εισάγοντας συνεχώς δεδομένα.

**Τεχνητή νοημοσύνη κατά του COVID-19**

Στην περίπτωση του COVID-19, η AI χρησιμοποιείται σε συσκευές θερμικής απεικόνισης για να βοηθήσει στον εντοπισμό πιθανών απειλών. Στην ιατρική, η AI μπορεί να χρησιμοποιηθεί για να βοηθήσει στην ακριβή διάγνωση του κορονοϊού χρησιμοποιώντας αλγόριθμους που εξετάζουν αξονικές τομογραφίες του θώρακα. Η συλλογή δεδομένων σχετικά με τον ιό είναι χρήσιμη για την παρακολούθηση της εξάπλωσής του.

**Καταπολέμηση της παραπληροφόρησης**

Ορισμένες εφαρμογές AI μπορούν να βοηθήσουν στον εντοπισμό ψεύτικων ειδήσεων και παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης, εντοπίζοντας συγκεκριμένες λέξεις και εκφράσεις, καθώς και αξιόπιστες πηγές πληροφοριών.

**Υγεία**

Οι ερευνητές μελετούν πώς η AI μπορεί να χρησιμοποιηθεί για την ανάλυση δεδομένων υγείας και τον εντοπισμό προτύπων που θα μπορούσαν να οδηγήσουν σε νέες επιστημονικές ανακαλύψεις και βελτιωμένη προσωπική διάγνωση. Για παράδειγμα, οι ερευνητές έχουν αναπτύξει ένα έξυπνο πρόγραμμα που μπορεί να ανιχνεύσει περιπτώσεις καρδιακής προσβολής σε κλήσεις έκτακτης ανάγκης, καλύτερα ακόμη και από τους ειδικούς των τηλεφωνικών κέντρων έκτακτης ανάγκης.

**Μεταφορές**

Η AI μπορεί να βελτιώσει την ασφάλεια, την ταχύτητα και την αποτελεσματικότητα της σιδηροδρομικής κυκλοφορίας ελαχιστοποιώντας τις τριβές των σιδηροδρομικών μεταφορών και επιτρέποντας την αυτόνομη οδήγηση.

**Μεταποιητικός κλάδος**

Η AI θα μπορούσε να οδηγήσει στην ταχεία ανάπτυξη της κατασκευής και του «έξυπνου» σχεδιασμού εργοστασίων στην Ευρώπη, μεταξύ άλλων, της χρήσης ρομπότ, της έγκαιρης πρόβλεψης σφαλμάτων και της συντήρησης μηχανικών δομών, καθώς και συστημάτων επαυξημένης πραγματικότητας για την αύξηση της ικανοποίησης των εργαζομένων με τα έξυπνα εργαστήρια.

**Τρόφιμα και γεωργία**

Η AI μπορεί να χρησιμοποιηθεί για τη δημιουργία πιο βιώσιμων συστημάτων τροφίμων: πιο συγκεκριμένα, μπορεί να εξασφαλίσει την παραγωγή πιο υγιεινών τροφίμων ελαχιστοποιώντας τη χρήση λιπασμάτων, ζιζανιοκτόνων και άρδευσης, αυξάνοντας την παραγωγικότητα και μειώνοντας τις περιβαλλοντικές επιπτώσεις. Η χρήση ρομπότ θα μπορούσε επίσης να βοηθήσει στην απομάκρυνση των ζιζανίων και στη μείωση της χρήσης φυτοφαρμάκων, καθώς πολλές φάρμες χρησιμοποιούν ήδη συστήματα AI για την παρακολούθηση της κίνησης και της θερμοκρασίας των ζώων, καθώς και την κατανάλωση ζωοτροφών.

**Δημόσια διοίκηση και υπηρεσίες**

Χάρη στο ευρύ φάσμα των διαθέσιμων δεδομένων και την ικανότητα αναγνώρισης προτύπων, η AI είναι σε θέση να παρέχει έγκαιρη προειδοποίηση για φυσικές καταστροφές, συμβάλλοντας στη διασφάλιση της κατάλληλης ετοιμότητας και του μετριασμού.

**Συμπερασματικά**, η AI είναι ένα σημαντικό εργαλείο που μπορεί να αλλάξει τη ζωή μας με τρόπους που ακόμα δεν μπορούμε να φανταστούμε. Η AI έχει τεράστιες δυνατότητες και όπου χρησιμοποιείται βελτιώνει σημαντικά την ταχύτητα εύρεσης λύσης και την ακρίβεια των αποτελεσμάτων. Εάν συνδυαστεί με τις σωστές ενέργειες και δεξιότητες, καθώς και με το σωστό τρόπο για ενσωμάτωση στον τρόπο λειτουργίας του σώματος, είναι δυνατό να μεγιστοποιηθούν τα οφέλη της AI και να τεθούν τα θεμέλια για τη μηχανική νοημοσύνη στο μέλλον. [16]

## 1.1 Αντικείμενο της διπλωματικής

Είναι γεγονός πως διανύουμε έναν αιώνα έντονης τεχνολογικής έκρηξης, οι πόλεις και ο κόσμος γενικότερα αναπτύσσεται με ραγδαίους ρυθμούς. Στα πλαίσια αυτής της τεράστιας τεχνολογικής ανάπτυξης, τα συστήματα ηλεκτρισμού της τελευταίας χρονικής περιόδου έχουν αρχίσει να ενσωματώνουν ψηφιακές τεχνολογίες και καινούργια ήλεκτρο-μηχανολογικά συστήματα σε δραστηριότητες που εφάπτονται με την παραγωγή, μεταφορά, διανομή, προμήθεια της Ηλεκτρικής Ενέργειας. Τα νέα ηλεκτρικά δίκτυα έχουν ως στόχο να επιτυγχάνουν αξιόπιστες και αποδοτικότερες λειτουργίες με σαφώς μειωμένες περιβαλλοντικές επιπτώσεις. Τα ευφυή αυτά ηλεκτρικά συστήματα όπως πλέον χαρακτηρίζονται από τους ειδικούς συνδυάζουν αποτελεσματικά τις παραπάνω τεχνολογίες με τη χρήση των ΑΠΕ (Αιολική, Ηλιακή, κ.λπ). Σκοπός της συγκεκριμένης διπλωματικής εργασίας, η οποία βασίστηκε εξ ολοκλήρου σε δευτερογενή έρευνα (αυτό σημαίνει ότι τα

στοιχεία που θα παρουσιαστούν έχουν συλλεχθεί από προηγούμενες έρευνες, από διαθέσιμα στοιχεία σε αρχεία οργανισμών και από υπάρχουσα βιβλιογραφία καθώς και από ερευνητικά και επιστημονικά άρθρα του διαδικτύου), είναι να παρουσιάσει τα χαρακτηριστικά γνωρίσματα της AI, τους τύπους χρήσης όπως και μια σειρά αλγορίθμων που μπορούν να χρησιμοποιηθούν ως μηχανισμοί για την κυβερνοασφάλεια.

Στην παρούσα εργασία λοιπόν αναλύονται τα πλεονεκτήματα που θα επωμιστούμε από τη χρήση της ως "εργαλείο" μεταμόρφωσης του "παλιού" Ηλεκτρικού Δικτύου σε "Έξυπνο" Ηλεκτρικό Δίκτυο, όμως και τα Θέματα Ασφαλείας που θα προκύψουν θα πρέπει να απαλειφθούν, καθώς υπάρχουν είδη επιθέσεων και κίνδυνοι μέσω Διαδικτύου που θα μπορέσουν να υποκλέψουν δεδομένα καταναλωτών προς όφελος εταιρειών.

Αρχικά, εφόσον αξιολογήσουμε την εφαρμογή του "Έξυπνου" Ηλεκτρικού Δικτύου θα αναλύσουμε τις ιδιότητες ασφαλείας και θα αναφέρουμε τους τρόπους αντιμετώπισης με στρατηγικές σχεδιασμού ασφάλειας και τρόπους ασφάλισης του "Έξυπνου" Ηλεκτρικού Δικτύου με τη χρήση κρυπτογραφικών τεχνικών. Εν συνεχεία, εκτός των πλεονεκτημάτων, δεν μπορούμε να μην παραθέσουμε και τις αρνητικές συνέπειες της χρήσης της AI.

Εν κατακλείδι λοιπόν μπορεί μέχρι πρότινος όλα αυτά για κάποιους να φάνταζαν μακρινά και ουτοπικά πλέον όμως είναι η νέα πραγματικότητα. Οι πολίτες θα έχουν ενεργό ρόλο στην παραγωγή, αποθήκευση, πώληση και διαχείριση της ενέργειας, θα απολαμβάνουν τα σημαντικά οφέλη της χρήσης των έξυπνων δικτύων (Smart Grids) έχοντας την δυνατότητα της ενεργειακής ανεξαρτησίας σε περιπτώσεις που το κεντρικό δίκτυο έχει βλάβη.

Επιπρόσθετα τα σπίτια που θα έχουν ευφυής μετρητές ηλεκτρικού ρεύματος και ελεγκτές φορτίων χωρίς να χρειάζεται κεντρικός έλεγχος, θα αντιλαμβάνονται από μόνα τους την κατάσταση του Δικτύου από τους γειτονικούς μετρητές και θα αποφασίζουν μέσω προγράμματος και αυτόνομα ποιες καταναλώσεις θα απομονώσουν, χρησιμοποιώντας τη χρονική μετάθεση του φορτίου. Με τον τρόπο αυτό δεν θα υπάρχουν επιπτώσεις αφενός στην ποιότητα και αφετέρου όλο αυτό θα γίνεται με την μικρότερη επιβάρυνση του ηλεκτρικού δικτύου.

### 1.1.1 Συνεισφορά

Στόχοι αυτής της Διπλωματικής Εργασίας και η αναμενομένη συνεισφορά της είναι η ανάλυση των θεμάτων Ασφαλείας, η κατηγοριοποίηση των επιθέσεων και των κινδύνων που ανακύπτουν από την χρήση της AI και τέλος η συμπερασματική ανακεφαλαίωση των τρόπων ασφάλισης του "Έξυπνου" Ηλεκτρικού Δικτύου με την χρήση κρυπτογραφικών,

τεχνικών για την βέλτιστη χρήση της ηλεκτρικής ενέργειας για να μπορέσουμε να αντιμετωπίσουμε το πρόβλημα της κλιματικής αλλαγής.

1. Αναφέρθηκαν τα Θέματα και τα σημεία ασφαλείας.
2. Κατηγοριοποιήθηκαν οι επιθέσεις/απειλές.
3. Επισημάνθηκαν τα κενά ασφαλείας.
4. Σημειωθήκαν οι τρόποι αντιμετώπισης ασφάλειας.
5. Προτάθηκαν λύσεις ασφαλείας του "Έξυπνου" Ηλεκτρικού Δικτύου.
6. Συνοψίσαμε τους λόγους για τους οποίους η AI πρέπει να χρησιμοποιηθεί για την Ασφάλεια του "Έξυπνου" Ηλεκτρικού Δικτύου.

## 1.2 Οργάνωση του τόμου

Στο κεφάλαιο 1, γίνεται μια εισαγωγή στην AI, τα σχετικά γνωρίσματά της καθώς και οι εφαρμογές της στην καθημερινότητά μας.

Στο κεφάλαιο 2, γίνεται μια εκτεταμένη αναφορά στον τρόπο χρήσης και ανάπτυξης της AI, παρουσιάζεται το Νέο Μοντέλο "Έξυπνο" Ηλεκτρικό Δίκτυο, τα πλεονεκτήματά του, ποια προβλήματα επιλύει σε σχέση με το "Παλιό" Ηλεκτρικό Δίκτυο καθώς και οι διαφορές τους.

Στο Κεφάλαιο 3, παρουσιάζεται το Νέο Μοντέλο "Έξυπνο" Ηλεκτρικό Δίκτυο ως μία καινοτόμα λύση και σημειώνονται τα θέματα Ασφαλείας, τα είδη των επιθέσεων, οι κίνδυνοι του Διαδικτύου και αξιολογείται η εφαρμογή του "Έξυπνου" Ηλεκτρικού Δικτύου.

Στο Κεφάλαιο 4, αναφέρεται η χρηστικότητα της AI ως μέτρο ασφάλειας στο "Έξυπνο" Ηλεκτρικό Δίκτυο, οι τρόποι αντιμετώπισης των απειλών με τη χρήση της κρυπτογράφησης, οι τρόποι ασφάλισης και η εφαρμογή της AI.

Και τέλος στο Κεφάλαιο 5, παρουσιάζονται τα συμπεράσματα και οι Μελλοντικές επεκτάσεις της AI ως επίπεδο ασφάλειας σε ένα Έξυπνο Ηλεκτρικό Δίκτυο.

# Κεφάλαιο 2 Τεχνητή Νοημοσύνη

## 2.1.Εισαγωγή στην Τεχνητή Νοημοσύνη

Η AI επικεντρώνεται στην ανάπτυξη τεχνικών ML προκειμένου να επεξεργάζεται πολύ μεγάλες ποσότητες πληροφοριών, δεδομένων και απειλών. Η ικανότητα της AI να μπορεί να πραγματοποιεί αυτού του είδους τις ενέργειες χωρίς περιορισμούς και σε πραγματικό χρόνο την καθιστά πολύτιμο σύμμαχο για την εφαρμογή μιας σύγχρονης, αποτελεσματικής νοημοσύνης στον κυβερνοχώρο για την παροχή βοήθειας και ασφάλειας πριν, κατά τη διάρκεια και μετά από μια κυβερνοεπίθεση. Ωστόσο, η AI δεν θα αντιγράψει την ανθρώπινη διορατικότητα. Δεν χρειάζεται να εξαλειφθεί η ανάγκη για ανθρώπινους ειδικούς στον κυβερνοχώρο προκειμένου να επιτευχθεί αποτελεσματική ασφάλεια στον κυβερνοχώρο.

Φυσικά, η AI δεν επιλύει όλες τις προκλήσεις ασφαλείας. Η AI μπορεί να είναι αποτελεσματική μόνο εάν χρησιμοποιηθεί για να βοηθήσει στην επίτευξη των στόχων του οργανισμού, εάν παρέχει πραγματικό όφελος. Η AI μπορεί να είναι ένα πολύτιμο εργαλείο στα κέντρα επιχειρήσεων ασφαλείας, αλλά έχει περιορισμούς. Οι ομάδες πρέπει να γνωρίζουν αυτές τις δυνατότητες και τους περιορισμούς προκειμένου να χρησιμοποιούν την AI με τον καλύτερο δυνατό τρόπο. Πρέπει επίσης να διασφαλιστεί ότι μπορεί να επωφεληθούμε από την AI αυτοματοποιώντας τυπικές διαδικασίες ανάλυσης απειλών, έτσι ώστε οι άνθρωποι να μπορούν να επικεντρωθούν σε ένα μικρό υποσύνολο κακόβουλων και περίπλοκων δραστηριοτήτων.

Αξιοποιώντας στο βέλτιστο τις δυνατότητες και τη λειτουργικότητα της AI, τα κέντρα επιχειρήσεων μπορούν να αυξήσουν ακόμα και να διπλασιάσουν τον αριθμό των υποθέσεων που μπορούν να χειριστούν χωρίς όμως να χρειαστεί να διπλασιάσουν τον αριθμό των αναλυτών. Η AI βοηθά τα συστήματα να γίνουν πιο ευφυή καθώς βασίζονται σε περισσότερα δεδομένα για να μάθουν και να γίνουν πιο αυτόνομα καθώς χρησιμοποιούν εξειδικευμένα στατιστικά εργαλεία για την ανάλυση μεγάλου όγκου δεδομένων.

Παρακάτω αναφέρονται συνοπτικά η χρηστικότητα των αλγορίθμων AI, για να μπορέσουμε να κατανοήσουμε πως μπορούν να χρησιμοποιηθούν στην κυβερνοασφάλεια.
**Regression**: Εύρεση συσχετίσεων μεταξύ διαφορετικών δεδομένων. Μπορούμε να χρησιμοποιήσουμε αυτούς τους αλγόριθμους για να ανιχνεύσουμε ανωμαλίες στα δεδομένα συγκρίνοντας τα προβλεπόμενα αποτελέσματα με αυτά που έχουμε στην πραγματικότητα.

**Clustering**: Είναι μια διαδικασία ομαδοποίησης δεδομένων σε ομάδες με βάση κοινές ομοιότητες. Ο αλγόριθμος είναι σε θέση να επεξεργάζεται δεδομένα που δεν έχει δει πριν.
**Classification**: Εκχωρεί ένα όνομα στις ομάδες δεδομένων. Αφού μελετά τι έχει, αποφασίζει να δώσει "ονόματα" νέων συνόλων δεδομένων με βάση αυτά που έχει μάθει.

Πιθανές εφαρμογές των παραπάνω είναι, η αυτόματη αναγνώριση κακόβουλων email, επικίνδυνων ιστοσελίδων, ύποπτης διαδικτυακής δραστηριότητας κλπ. Πολλές εταιρείες ήδη εφαρμόζουν την AI για να προστατεύσουν τις υποδομές τους και τους πελάτες τους (Google, IBM, Microsoft κ.α.). Αυτό όμως που παρουσιάζει εξαιρετικό ενδιαφέρον είναι η χρήση της AI στα SOCs.

Το μέλλον της κυβερνοασφάλειας είναι άρρηκτα συνδεδεμένο με τη χρήση βαθιάς εκμάθησης (Deep learning) για την αναγνώριση και τη διερεύνηση κυβερνοαπειλών. Η πλειονότητα των σημερινών SOCs βρίσκεται μπροστά σε ένα βουνό καινούργιων απειλών, οι οποίες θα αυξηθούν τα επόμενα χρόνια.

Η εισαγωγή των δικτύων 5G είναι ένας νέος τομέας πιθανών απειλών για την ασφάλεια. Οι μεγάλες προσδοκίες του 5G μπορεί να γίνουν οι μεγαλύτερες αποτυχίες αν δεν προετοιμαστεί η υποδομή αρχικά. Το Deap learning, δίνει την δυνατότητα αυτόματης απόκρισης σε κυβερνο-απειλές σε πολύ μικρούς χρόνους με πολύ καλύτερη απόδοση.

Τα SOCs του μέλλοντος (όχι πολύ μακρινού), είτε θα είναι εξοπλισμένα με συστήματα αυτόματης προστασίας (AI, DL, ML) είτε απλά θα αποτύχουν στην δουλειά τους. Η εισαγωγή της AI στην κυβερνο-άμυνα/ασφάλεια είναι υποχρέωση των κυβερνήσεων. Έχουν την υποχρέωση της πιστοποίησης διαδικασιών και εργαλείων AI για διαδικτυακές εφαρμογές, ορίζοντας πολιτικές, κανονισμούς και όχι μόνο. Οι κυβερνήσεις θα λειτουργούν σε ένα δυναμικό άκρα απαιτητικό περιβάλλον (5G, IoT κλπ) και θα πρέπει να προσαρμοστούν αναλόγως.

Η εισαγωγή αυτής της νέας τεχνολογίας σε κυβερνητικό επίπεδο πρέπει να προστατευθεί επενδύοντας ταυτόχρονα σε εκπαίδευση των ανθρώπων αλλά και στην χρήση εξελιγμένων λύσεων κυβερνο-ασφάλειας.

Οι αλγόριθμοι AI δεν είναι τίποτα άλλο από απλούς παραδοσιακούς αλγόριθμους ML που έχουν προσαρμοστεί για να λειτουργούν με δεδομένα AI. Η ML είναι μια διαδικασία με την οποία οι υπολογιστές μπορούν να «μάθουν» μόνοι τους. Αυτό γίνεται μέσω ενός συνδυασμού στατιστικών τεχνικών και προγραμματισμού. Τα συστήματα ML είναι αλγόριθμοι που μπορούν να μάθουν από δεδομένα, πληροφορίες για να βελτιώσουν την απόδοση των ηλεκτρονικών υπολογιστών σε συγκεκριμένες εργασίες, χωρίς να χρειάζεται να προγραμματιστούν.

Αυτή η τεχνολογία χρησιμοποιείται ήδη καθώς κάθε «συναλλαγή» μας με την Google, το Amazon, το Meta και το Spotify διευκολύνεται από συστήματα ML. Οι τεχνολογίες ML και AI έχουν σημειώσει μεγάλη πρόοδο τα τελευταία χρόνια. Έχουν ενεργοποιήσει εργαλεία όπως αυτόνομα οχήματα, εικονικούς βοηθούς, chatbots και αναγνώριση προσώπου/αντικειμένων.

Ταυτόχρονα, παρά την αυξανόμενη χρήση ισχυρών λύσεων ασφαλείας, οι απειλές στον κυβερνοχώρο εξελίσσονται συνεχώς, καθώς οι μέθοδοι που χρησιμοποιούνται για τον εντοπισμό κακόβουλου λογισμικού ενημερώνονται συνεχώς. Ένα σύστημα κινδυνεύει εάν δεν προστατεύεται.

Αυτό συμβαίνει καθώς οι απλοί μέθοδοι που χρησιμοποιούνται για τον εντοπισμό κακόβουλων λογισμικών θεωρούνται πλέον αναποτελεσματικές. Οι κυβερνοεγκληματίες βρίσκουν συνεχώς νέους μεθόδους για να μπορέσουν να παρακάμψουν τα προγράμματα ασφαλείας που χρησιμοποιούνται και έτσι καταφέρνουν να μολύνουν δίκτυα και συστήματα με διαφορετικούς τύπους κακόβουλων λογισμικών. Η AI χρησιμοποιείται για την αξιολόγηση πιθανών απειλών και την προστασία του συστήματος αποθαρρύνοντας τη δυνητικά επιβλαβή συμπεριφορά. Υπό αυτή την έννοια, η ML είναι ο τρόπος εκμάθησης προτύπων που αποσκοπούν σε κακόβουλη συμπεριφορά. Ερευνητές και προγραμματιστές λογισμικού ασφαλείας προσπαθούν να εκμεταλλευτούν τη δύναμη της AI για να αναπτύξουν λύσεις που μπορούν να ανιχνεύσουν και να διορθώσουν εξελιγμένες απειλές στον κυβερνοχώρο και να ελέγξουν τις παραβιάσεις δεδομένων. Η ενσωμάτωση τεχνολογιών AI στα υπάρχοντα συστήματα κυβερνοασφάλειας, για να είναι ποιο αποτελεσματική, θα χρειαστεί χρόνο καθώς δεν είναι κάτι που θα μπορέσει να υλοποιηθεί εν μία νυκτί.[29]

## 2.2 Το Νέο Μοντέλο “Εξυπνο” Ηλεκτρικό Σύστημα

Η ηλεκτρική ενέργεια έχει γίνει πλέον ένα πολύ σημαντικό και ζωτικό κομμάτι της καθημερινής μας ζωής, καθώς ήταν το κυριότερο αντικείμενο επιστημονικού ενδιαφέροντος στα τέλη του 17ου αιώνα. Το σημερινό σύστημα παραγωγής ενέργειας προέρχεται πηγές ενέργειας υψηλής πυκνότητας άνθρακα, φυσικού αερίου και πετρελαίου, καθώς και διάχυτες ΑΠΕ όπως η υδροηλεκτρική ενέργεια, η βιομάζα, η ηλιακή ενέργεια και ο αέρας. Ως γνωστόν, πλέον πολλές βασικές μας ανάγκες βασίζονται στον ηλεκτρισμό και έτσι μπορούμε να καταλάβουμε τη σημαντικότητα του δικτύου όταν υπάρχει διακοπή ρεύματος καθώς πολλές δραστηριότητές μας παραλύουν. Σύμφωνα με δεδομένα ένα μεγάλο ποσοστό της

ηλεκτρικής ενέργειας προέρχεται από την καύση ορυκτών. Το σύστημα μεταφοράς αποτελείται συνήθως από γραμμές υψηλής τάσης που μεταφέρουν την ηλεκτρική ενέργεια σε μεγάλες αποστάσεις στους υποσταθμούς όπου η τάση μειώνεται ώστε να γίνει η διανομή στους καταναλωτές μέσω δικτύων διανομής μέσης/χαμηλής τάσης.

Το "έξυπνο" δίκτυο αποτελεί θέμα προς συζήτηση από οργανισμούς, ερευνητικά κέντρα και κυβερνητικά τμήματα ανά τον κόσμο. Πλέον με τον όρο "έξυπνο δίκτυο" αναφερόμαστε σε μια ομάδα τεχνολογιών που χρησιμοποιείται για να μετατρέψουμε τα συστήματα παροχής ηλεκτρικής ενέργειας στον 21ο αιώνα, χρησιμοποιώντας απομακρυσμένο έλεγχο και αυτοματισμούς βασισμένους σε ηλεκτρονικούς υπολογιστές. Αυτά τα συστήματα θα είναι δυνατό να λειτουργήσουν χρησιμοποιώντας τεχνολογίες αμφίδρομης επικοινωνίας και υπολογιστικής επεξεργασίας. Συμπεραίνουμε λοιπόν, ότι το βασικό συστατικό είναι η ενσωμάτωση τεχνολογιών πληροφορικής και επικοινωνιών στο δίκτυο ώστε να συλλέγουμε πληροφορίες για την καλυτέρευση της διαχείρισης. Η ανάπτυξη των έξυπνων δικτύων καλύπτει ένα ευρύ φάσμα δυνατοτήτων και υπηρεσιών συστημάτων ηλεκτρικής ενέργειας. Το Εθνικό Εργαστήριο Ενεργειακής Τεχνολογίας, χρησιμοποιεί ψηφιακές τεχνολογίες για να βελτιώσει την αξιοπιστία, την ασφάλεια και την αποδοτικότητα (οικονομικά και ενεργοβόρα) συστημάτων παραγωγής ηλεκτρικής ενέργειας μεγάλης κλίμακας, την ανθεκτικότητα στις απειλές και τον περιβαλλοντικό μας αντίκτυπο μέσω των συστημάτων διανομής ηλεκτρικής ενέργειας στους καταναλωτές.

Τέλος, αν και δεν υπάρχει ακριβής ορισμός, μπορούμε τουλάχιστον να αναφέρουμε ότι συνδυάζει ψηφιακές τεχνολογίες, από την παραγωγή έως τους τελικούς καταναλωτές και βέβαια ότι θα βελτιώσει την αξιοπιστία, την ασφάλεια και την αποδοτικότητα των συστημάτων παροχής ενέργειας.

Βέβαια δεν μπορούμε να μην αναφέρουμε τα κυριότερα πλεονεκτήματα του Smart Grid που είναι τα εξής:

- Θα γίνεται ποιο άμεσα η ανίχνευση και η διόρθωση των προβλημάτων που θα προκύπτουν, σε αρχικό στάδιο (αυτό-θεραπεία).
- Θα δοθεί στους καταναλωτές η δυνατότητα να διαχειριστούν ενεργά την παραγωγή, τη διανομή και τη χρήση της ηλεκτρικής ενέργειας.
- Θα αξιοποιηθεί με τον καλύτερο δυνατό τρόπο οι υπάρχουσες εγκαταστάσεις του Ηλεκτρικού Δικτύου.
- Θα αυξηθεί η χωρητικότητα και θα βελτιωθεί η αποτελεσματικότητα των οι υπαρχόντων εγκαταστάσεις του Ηλεκτρικού Δικτύου.

- Θα αντιμετωπιστούν ποιο γρήγορα και εύκολα οι διακοπές παροχής ισχύος (blackout-s).
- Θα σχεδιαστεί κατάλληλα ώστε να εξασφαλιστεί η αξιοπιστία και η ασφάλεια.
- Θα διανέμεται υψηλότερης ποιότητας ηλεκτρικής ισχύος.
- Θα υπάρξει η δυνατότητα ευελιξίας και προσαρμογής, ανάλογα με τις αλλαγές που ανακύπτουν.
- Θα υπάρχει η δυνατότητα παραγωγής και αποθήκευσης.
- Θα δημιουργηθεί/αναπτυχτεί η αγοραστική ικανότητα της ηλεκτρικής ενέργειας.
- Θα γίνει ποιο αποτελεσματική η χρήση της ηλεκτρικής ενέργειας.
- Θα χρησιμοποιούνται ως επί το πλείστων οι ΑΠΕ

Ας σημειώσουμε παρακάτω τα γενικά χαρακτηριστικά του Smart Grid που θα βοηθήσουν στην ανάπτυξη και στην καλύτερη διαχείρισή του.

- Θα καταστεί δυνατή η μαζική ανάπτυξη και αποτελεσματική χρήση κατανεμημένων πηγών ενέργειας, συμπεριλαμβανομένων των ΑΠΕ και των συστημάτων αποθήκευσης ενέργειας.
- Θα βελτιώσει την αποτελεσματικότητα, την ανθεκτικότητα και τη βιωσιμότητα του ηλεκτρικού δικτύου με την ενσωμάτωση κατανεμημένης ευφυΐας σε πραγματικό χρόνο που επιτρέπει αυτόματες λειτουργίες προστασίας, βελτιστοποίησης και ελέγχου.
- Θα επιτρέψει την αλληλεπίδραση των καταναλωτών με συστήματα διαχείρισης ενέργειας για να επιτρέψει την απόκριση της ζήτησης και τις λειτουργίες διαμόρφωσης φορτίου.
- Θα καταστεί δυνατή η πραγματική επίγνωση σε πραγματικό χρόνο της κατάστασης του δικτύου και των λειτουργιών μέσω της ανάπτυξης προηγμένων συστημάτων μέτρησης και παρακολούθησης.
- Θα υποστηρίξει την ηλεκτροδότηση των συστημάτων μεταφοράς, διευκολύνοντας την εγκατάσταση ηλεκτρικών οχημάτων και τη χρήση τους ως κινητών ενεργειακών πόρων.[25]

## 2.3 Αντιμετώπιση των Προβλημάτων του “Παλιού” Ηλεκτρικού Συστήματος

Ασχέτως από την γήρανση του εξοπλισμού και καθώς η ανάγκη για ενέργεια αυξάνεται και οι γραμμές μεταφοράς και διανομής πλησιάζουν στο όριο, θα έχουμε ως αποτέλεσμα ότι θα πρέπει να δημιουργηθούν καινούργιες συνδέσεις όμως οι ΑΠΕ δεν θα μπορέσουν να χρησιμοποιηθούν. Έτσι για να διατηρηθεί η αξιοπιστία και η ποιότητα της ενέργειας,

απαιτείται η συνεχής επένδυση κεφαλαίου για συντήρηση/αναβάθμιση και επέκταση των υποδομών. Δυστυχώς όμως η δυσκολία στην εγκατάσταση νέων υποδομών, θα έχει ως αποτέλεσμα τη χρήση και την αξιοποίηση των ήδη υπαρχόντων. Με την εξέλιξη της τεχνολογίας κατέστη δυνατή η μετάβαση από το "παλιό" ηλεκτρικό δίκτυο σε ψηφιακά συστήματα, όπως για παράδειγμα τα θυρίστορ, και η ενσωμάτωση ψηφιακών αισθητήρων σε όλο το μήκος δικτύου, που κάνουν δυνατή έτσι την παρακολούθηση διάφορων μεταβλητών σε πραγματικό χρόνο. Τέλος, με την αρχική σχεδίαση των συστημάτων ηλεκτρικής ενέργειας, κάποιες έννοιες είτε είχαν πολύ μικρή προτεραιότητα είτε δεν υπήρχαν ως μεταβλητές στο σχεδιασμό. Κάποιες από αυτές ήταν και η απόδοση του δικτύου, αφού η ενέργεια στα πρώτα έτη λειτουργίας ήταν πολύ φθηνή και κάλυπτε μικρές ανάγκες (πχ. φωτισμός), η ελεύθερη αγορά όσον αφορά την επιλογή παρόχου και τις περιβαλλοντολογικές επιπτώσεις. Γενικότερα η έννοια του συμβατικού δικτύου απέχει κατά πολύ από εκείνη του νέου "έξυπνου" δικτύου.

Από τη σύγκριση των δύο αυτών δικτυών προκύπτουν σημαντικές διαφορές, εκ των οποίων μερικές αναφέρονται παρακάτω.

- ✓ Ως προς τον ορισμό, ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας, είναι ένα διασυνδεδεμένο δίκτυο με μετατροπείς, μετασχηματιστές και γραμμές μεταφοράς που αναπτύχθηκε για τη μεταφορά της ηλεκτρικής ενέργειας από τους παραγωγούς στους καταναλωτές, με μονόδρομη επικοινωνία, ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας έχει οριστεί ως να οριστεί ως η διαφανής, απρόσκοπτη και στιγμιαία αμφίδρομη παράδοση ενέργειας και πληροφοριών που επιτρέπει στη βιομηχανία ηλεκτρικής ενέργειας να διαχειρίζεται καλύτερα την παράδοση και τη μεταφορά ενέργειας και να δίνει τη δυνατότητα στους καταναλωτές να έχουν περισσότερο έλεγχο στις ενεργειακές αποφάσεις.
- ✓ Ως προς τον τύπο εγκατάστασης και συναρμολόγησης, ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας έχει διάταξη με ρελέ, διακόπτες, μετρητές κ.λπ. που χρησιμοποιούνται στο συμβατικό πλέγμα είναι ηλεκτρομηχανικού και στερεάς κατάστασης ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας βασίζεται στα ψηφιακά ηλεκτρονικά και στους μικροεπεξεργαστές.
- ✓ Ως προς τον τύπο παραγωγής ενέργειας, ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας περιλαμβάνει μία κεντρική παραγωγή ηλεκτρικής ενέργειας, όπου η ισχύς παράγεται από μια κεντρική τοποθεσία που εξαλείφει τις δυνατότητες ενσωμάτωσης ΑΠΕ στο ηλεκτρικό δίκτυο ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας υπάρχει η κατανεμημένη

παραγωγή ηλεκτρικής ενέργειας όπου η ηλεκτρική ενέργεια μπορεί να παραχθεί και να διανεμηθεί από πολλαπλές μονάδες παραγωγής.

- ✓ Ως προς την επικοινωνία μεταξύ συσκευών, ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας χρησιμοποιεί τεχνολογία που θεωρείται συνήθως ανόητη επειδή δεν διαθέτει μέσα επικοινωνίας δεδομένων μεταξύ των διαφόρων συσκευών του συστήματος, ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας περιλαμβάνει ψηφιακή τεχνολογία βασισμένη σε μικροεπεξεργαστή που επιτρέπει την επικοινωνία δεδομένων μεταξύ των συσκευών του συστήματος και καθιστά δυνατό τον τηλεχειρισμό.
- ✓ Ως προς την κατεύθυνση ροής ηλεκτρικής ενέργειας και των πληροφοριών, σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας παρέχετε μόνο μονόδρομη ροή ηλεκτρικής ενέργειας και μόνο τοπική αμφίδρομη επικοινωνία είναι δυνατή, ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας παρέχεται αμφίδρομη ροή ηλεκτρικής ενέργειας και πληροφοριών.
- ✓ Ως προς το σύστημα προστασίας, σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας είναι χειροκίνητο ή ημιαυτόματο ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας υπάρχει πλήρως αυτοματοποιημένη προστασία.
- ✓ Ως προς το σύστημα ελέγχου στο συμβατικό δίκτυο ηλεκτρικής ενέργειας παρέχεται περιορισμένο και αργό ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας προβλέπονται μέτρα ελέγχου ευρείας περιοχής και γρήγορου ελέγχου.
- ✓ Ως προς τον αριθμό αισθητήρων που χρησιμοποιούνται, ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας είναι εξοπλισμένο με λίγους αισθητήρες και σε συγκεκριμένο εξοπλισμό, γεγονός που καθιστά δύσκολο τον προσδιορισμό της θέσης της βλάβης στο δίκτυο και έτσι υπάρχει μεγαλύτερη καθυστέρηση στην αποκατάσταση της βλάβης, ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας βασίζονται πλήρως σε αισθητήρες καθ' όλη την έκταση της εγκατάστασης και με αυτόν τον τρόπο είναι ευκολότερος ο προσδιορισμός της θέσης της βλάβης.
- ✓ Ως προς την παρακολούθηση, σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας λόγω της χρήσης περιορισμένου αριθμού αισθητήρων, η παρακολούθηση της διανομής ενέργειας είναι χειροκίνητη, ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας περιλαμβάνει ψηφιακές τεχνολογίες βασισμένες σε αισθητήρες, οι οποίες παρέχουν αυτό-παρακολούθηση της διανομής ενέργειας.
- ✓ Ως προς την αποκατάσταση της παροχής (blackout-s), σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας γίνεται χειροκίνητα, δηλαδή οι τεχνικοί πρέπει να επισκεφθούν το σημείο της αστοχίας για να κάνουν επισκευές, ενώ το "έξυπνο" δίκτυο ηλεκτρικής ενέργειας έχει αυτο-θεραπευόμενη ιδιότητα, δηλαδή αποτελείται από αισθητήρες που

μπορούν να ανιχνεύσουν τα προβλήματα στο δίκτυο και να προχωρήσουν σε ενέργειες με την χρήση διαγραμμάτων ροής, (αντιμετώπισης προβλημάτων) και να γίνει αποκατάσταση της βλάβη χωρίς παρέμβαση τεχνικών στο χώρο. Ενώ σε περίπτωση ζημιών που σχετίζονται με την υποδομή, τα "έξυπνα" δίκτυα επικαλούνται αμέσως τους τεχνικούς μέσω του κέντρου παρακολούθησης για να ξεκινήσουν τις απαιτούμενες επισκευές.

- ✓ Ως προς την ξαφνική βλάβη του εξοπλισμού, σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας μπορεί να οδηγήσει σε πλήρη διακοπή ρεύματος ενώ σε ένα "έξυπνο" δίκτυο ηλεκτρικής ενέργειας εάν υπάρχει οποιαδήποτε αστοχία στην υποδομή, τότε η τροφοδοσία μπορεί να επανα-δρομολογηθεί για να περάσει γύρω από την περιοχή του προβλήματος και ως εκ τούτου να περιορίσει την περιοχή που επηρεάζεται από τη διακοπή ρεύματος.
- ✓ Ως προς την συμμετοχή των πελατών, σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας δεν υπάρχει συμμετοχή των καταναλωτών στη διανομή ενέργειας, ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας υπάρχει ενεργή εμπλοκή και συμμετοχή των καταναλωτών.
- ✓ Τέλος, ως προς την περιβαλλοντικές επιπτώσεις σε ένα συμβατικό δίκτυο ηλεκτρικής ενέργειας, υπάρχουν συμβατικοί σταθμοί ηλεκτροπαραγωγής όπως θερμικοί, φυσικό αέριο, ντίζελ κ.λπ. που παράγουν ενέργεια που δημιουργούν σοβαρές και κρίσιμες αρνητικές επιπτώσεις στο περιβάλλον, ενώ στο "έξυπνο" δίκτυο ηλεκτρικής ενέργειας περιλαμβάνει την ενσωμάτωση των ΑΠΕ που μειώνει τις επιπτώσεις στο περιβάλλον, όπως οι εκπομπές CO2 και η υπερθέρμανση του πλανήτη.[18]

Παρακάτω αναφέρονται επιγραμματικά μερικές διαφορές του υπάρχοντος δικτύου σε σχέση με το Smart Grid [5]

Πίνακας 2.23-1 Διαφορές Υπάρχοντος & Νέου Δικτύου

| **Υπάρχον δίκτυο** | **Έξυπνο δίκτυο** |
|---|---|
| Είναι ηλεκτρομηχανολογικό | Είναι ψηφιακό |
| Έχει μονόδρομη επικοινωνία | Έχει αμφίδρομη επικοινωνία |
| Έχει κεντρική παραγωγή | Έχει κατανεμημένη παραγωγή |
| Έχει λίγους αισθητήρες | Έχει αισθητήρες παντού |
| Παρακολουθείται χειροκίνητα | Αυτό-παρακολουθείται |
| Η αποκατάστασή του γίνεται χειροκίνητα | Αυτοΐαση (self-healing) |
| Διακοπές ρεύματος που προκαλούνται από βλάβες | Προσαρμοστικότητα |
| Περιορισμένος έλεγχος | Εξονυχιστικός έλεγχος |
| Ελάχιστες επιλογές των πελατών | Πλήθος επιλογών των πελατών |

# Κεφάλαιο 3 Το "Έξυπνο" Ηλεκτρικό Σύστημα και τα Θέματα Ασφάλειας

## 3.1 Η Έννοια του "Έξυπνου" Ηλεκτρικού Συστήματος

Το «έξυπνο δίκτυο» είναι ένα δίκτυο της επόμενης γενιάς που θα έχει τη δυνατότητα να επικοινωνεί πληροφορίες και να διοχετεύει ενέργεια με άμεσο και αμφίδρομο τρόπο. Μπορούν να ενσωματώνουν αποτελεσματικά τη συμπεριφορά και τις ενέργειες του όλοι οι χρήστες που συνδέονται με αυτό, όπως γεννήτριες, καταναλωτές προκειμένου να διασφαλιστεί ένα οικονομικά αποδοτικό, βιώσιμο σύστημα ηλεκτρικής ενέργειας με χαμηλές απώλειες, υψηλή ποιότητα και ασφάλεια. Δημιουργώντας ένα «έξυπνο δίκτυο» δεν είναι επομένως μόνο ένα θέμα εκσυγχρονισμού του δικτύου ηλεκτρικής ενέργειας αλλά και η ανάπτυξη των φυσικών περιουσιακών στοιχείων (ΑΠΕ) και τεχνολογιών (ΤΠΕ). Βασικό ρόλο παίζουν τα νέα επιχειρηματικά μοντέλα και πρακτικές, νέοι κανονισμοί, καθώς και άλλα άυλα στοιχεία όπως η συμπεριφορά των καταναλωτών, αλλαγές και η κοινωνική αποδοχή. Η καθοδήγηση αυτής της μετάβασης είναι μια πρόκληση, μακροπρόθεσμη που απαιτεί τη σύζευξη ενός οράματος που καθοδηγείται από την πολιτική με γνώμονα την αγορά, την εξισορρόπηση της ενεργειακής πολιτικής και στόχους για την κερδοφορία της αγοράς. Τα τελευταία χρόνια η τεχνολογίες και οι καινοτομίες που χρησιμοποιούνται στα Smart Grid έχουν αυξηθεί σε αριθμό και εύρος. Άλλα χαρακτηριστικά που κάνουν αυτό το Smart Grid ξεχωριστό είναι η δυνατότητα παρακολούθησης και ελέγχου των δικτύων μέσης και χαμηλής τάσης, καθώς θεωρείτε και η πιο πράσινη πλευρά των υπαρχόντων δικτύων.

Το Smart Grid εκ των πραγμάτων θεωρείτε και είναι πιο ασφαλές και αποτελεσματικό από τα συμβατικά παραδοσιακά δίκτυα. Ένα Smart Grid ή αλλιώς ένα σύγχρονο ηλεκτρικό δίκτυο ενσωματώνει ΤΠΕ και πληροφορίες, για να μπορέσουμε να διαχειριστούμε καλύτερα τον τρόπο παραγωγής, διανομής, κατανάλωσης, και αποθήκευσης της ηλεκτρικής ενέργειας. Με τη συλλογή πληροφοριών και δεδομένων σε πραγματικό χρόνο από ένα ηλεκτρικό δίκτυο και έχοντας τη δυνατότητα προσαρμογής των δυνατοτήτων του απομακρυσμένα, μπορούμε να βοηθήσουμε τον πάροχο ενέργειας ώστε να διαχειρίζεται ποιο εύκολα και αποτελεσματικότερα τις διακυμάνσεις της προσφοράς και της ζήτησης της ηλεκτρονικής ενέργειας και έτσι να μπορεί να παράγει την απαιτούμενη ποσότητα ηλεκτρικής ενέργειας και βέβαια όταν αυτή χρειάζεται. Αυτό αποδίδει στο ηλεκτρικό δίκτυο την ευελιξία που

χρειάζεται και τη δυνατότητα να ενσωματώσει τις ΑΠΕ και να προσφέρει περισσότερα εργαλεία διαχείρισης της ενέργειας και ευνοϊκότερες επιλογές τιμολόγησης.

Το Smart Grid δεν έχει κάποιον συγκεκριμένο ορισμό, καθώς διαφορετικές χώρες του αποδίδουν διαφορετικά αναλόγως τη χρήση και την αξιοποίησή του. Στην πιο ευρεία διαδεδομένη του μορφή, το Smart Grid μπορεί να θεωρηθεί ως η επέκταση του κλασικού συμβατικού δικτύου με την χρήση τεχνολογιών ΤΠΕ. Αυτές οι τεχνολογίες μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός κατανεμημένου συστήματος που μπορεί να παράγει και να αποθηκεύει ανανεώσιμη ενέργεια.

Ποιο συγκεκριμένα το Smart Grid έχει ως στόχο να προσφέρει την πιο οικονομική και αξιόπιστη διαχείριση της ζήτησης της ηλεκτρικής ενέργειας ως προς τη διανομή και τη μετάδοση της από τους προμηθευτές στους τελικούς χρήστες και αντιστρόφως. Το Smart Grid θεωρείτε ένα εξελιγμένο δίκτυο, και έχει μοναδικά πλεονεκτήματα, σε σχέση με τα παλαιότερα συμβατικά δίκτυα[2].

Από την πλευρά της κατανάλωσης, οι καταναλωτές θα μπορούν να μειώσουν τη χρήση της ενέργειας ως απόκριση στις τιμές του ηλεκτρικού ρεύματος. Θα μπορούν να επιλέξουν από ένα ευρύτερο φάσμα παρόχων (πωλητές ενέργειας, συσσωρευτές κ.λπ.) και επιλογές ισχύος (π.χ. πράσινο ασφάλιστρα ποιότητας ηλεκτρικής ενέργειας και ισχύος). από την πλευρά της παραγωγής, το Smart Grid μπορεί να δημιουργήσει ευκαιρίες στους καταναλωτές όσον αφορά την αγορά ηλεκτρικής ενέργειας υποστηρίζοντας τη σύνδεση και τη χρήση του με κατανεμημένη παραγωγή (π.χ. Φ/Β) και αποθήκευση ενέργειας (π.χ. EV). Βέβαια τα περισσότερα από αυτά τα οφέλη για τους καταναλωτές είναι συστημικού χαρακτήρα. Επίσης, αξίζει να σημειωθεί ότι δεν θα μπορέσουν να επωφεληθούν όλοι οι καταναλωτές στον ίδιο βαθμό από το Smart Grid. Ως αποτέλεσμα θα είναι απαραίτητο, για να προσφέρουμε σαφή απτά οφέλη σε ολόκληρο το σύστημα, η πλήρης συμμετοχή όλων των καταναλωτών.[22]

## 3.2 Η Χρηστικότητα του "Έξυπνου" Ηλεκτρικού Συστήματος

Το σύστημα ηλεκτρικής ενέργειας βασίζεται σε ένα διασυνδεδεμένο δίκτυο για να παρέχει ασφαλή, σταθερή, οικονομική και βιώσιμη παροχή επαρκών ποσοτήτων ηλεκτρικής ενέργειας υψηλής ποιότητας σε προμηθευτές. Τα Smart Grid διευκολύνουν την ενσωμάτωση κατανεμημένων, καθαρών ενεργειακών πόρων στο σύστημα και συμβάλλουν στην ενδυνάμωση των καταναλωτών ενέργειας. Με την ανάπτυξη της έξυπνης ενέργειας, θα πρέπει να ακολουθήσουν οι υποδομές, με τον ίδιο ρυθμό, προκειμένου να υποστηριχθεί αυτός ο μετασχηματισμός.

Τα δίκτυα επικοινωνίας θα έχουν κυρίαρχο ρόλο στην υποδομή του Smart Grid, καθώς θα περιέχουν δεδομένα και πολυτροφίες σε πραγματικό χρόνο, και θα διαχωριστούνε ως ακολούθως:

- **Consumer Premises Networks (CPNs):** Αυτά τα δίκτυα παρέχουν επικοινωνία μεταξύ των συσκευών και του εξοπλισμό με τις εγκαταστάσεις των καταναλωτών. Αυτά τα δίκτυα διαχωρίζονται σε σχέση με την περιοχή. (πχ. HAN, BAN, IAN κ.α.)
- **Neighborhood Area Network (NAN):** Αυτό το δίκτυο συλλέγει τις πληροφορίες από τις συσκευές των καταναλωτών μέσω του έξυπνου μετρητή και τις αποστέλλει με βοηθητικό πρόγραμμα στο κέντρο διαχείρισης δεδομένων για περαιτέρω επεξεργασία.
- **Access Area Network:** Αυτό το δίκτυο είναι υπεύθυνο για το δίκτυο περιοχής που είναι συνδεδεμένο στο επίπεδο διανομής, και μπορεί να εξυπηρετήσει ρυθμιστές τάσης, διακόπτες που λειτουργούν από απόσταση, συστοιχίες πυκνωτών ρελέ σφάλματος και ελεγκτές σφάλματος γραμμής, ΑΠΕ
- **Backhaul Network:** Αυτό το δίκτυο είναι υπεύθυνο για το δίκτυο περιοχής που είναι συνδεδεμένο στο επίπεδο διανομής, και μπορεί να εξυπηρετήσει υποσταθμούς SCADA–RTUs, έξυπνες ηλεκτρονικές συσκευές, ρελέ προστασίας, στάθμη λαδιού, πίεσης, Αισθητήρες θερμοκρασίας και κάμερες παρακολούθησης.
- **Core and Office Network:** Αυτό το δίκτυο είναι υπεύθυνο για τη συνεργασία επικοινωνιών και υπηρεσιών όπως Voice and Data, Planning and QoS.
- **External Access Networks:** Αυτό το δίκτυο θεωρείτε ως δημόσιο δίκτυο που δίνει πρόσβαση στα οικοσυστήματα των παρόχων και σε ορισμένα από τα παραπάνω δίκτυα. Τα εξωτερικά δίκτυα χρησιμοποιούν κυρίως δημόσια δίκτυα πρόσβασης.

Το Smart Grid μπορούμε να το χωρίσουμε σε επτά τομείς, οι οποίοι βέβαια εμπεριέχουν επιπλέον τομείς, εφαρμογές αλλά και οντότητες, οι οποίες έχουν ρόλους που τους κάνουν να συνδέονται μεταξύ τους με διάφορες συσχετίσεις, μέσω διεπαφών.

Οι **οντότητες** αποτελούνται από συσκευές, όπως έξυπνους μετρητές, συστήματα, προγράμματα, οργανισμούς ή ακόμα και άτομα, εντός ενός **τομέα** που πρέπει να διεκπεραιώσουν μία τουλάχιστον εντολή/ενέργεια και έχουν το δικό τους **ρόλο** στο δίκτυο. Οι οντότητες έχουν τη δυνατότητα να διεκπεραιώνουν εντολές και να ανταλλάζουν δεδομένα και πληροφορίες που είναι απαραίτητες ώστε να ολοκληρώσουν κάποιες **εφαρμογές**.

**Το NIST** έχει ταξινομήσει τα έξυπνα δίκτυα σε επτά τομείς που περιλαμβάνουν φορείς και εφαρμογές, οι οποίες είναι ο τομέας των Πελατών, των Αγορών, της Παροχής Υπηρεσιών, του Κέντρου Ενεργειών/Λειτουργειών, της Παραγωγής, του Δικτύου

Μεταφοράς, της Διανομής. Το μοντέλο αυτό παρουσιάζει όλες τις επικοινωνίες και την ροή ηλεκτρικής ενέργειας μεταξύ των τομέων καθώς και τον τρόπο με το οποίο συσχετίζονται. Οι απαιτήσεις για την εφαρμογή κυμαίνονται από την αποδοχή των καταναλωτών έως τις εμπορικές επενδύσεις έως τον διαχωρισμό των ρόλων της πολιτείας και της ομοσπονδιακής κυβέρνησης στη χάραξη μακροπρόθεσμων σχεδίων και στη δημιουργία του σωστού ρυθμιστικού περιβάλλοντος. Κάθε επιμέρους τομέας αποτελείται από σημαντικά στοιχεία των έξυπνων δικτύων τα οποία συνδέονται μεταξύ τους με τρόπο που εξασφαλίζεται η αμφίδρομη επικοινωνία και η ροή ενέργειας.

**Τομέας Πελατών**

Ο τομέας των πελατών περιλαμβάνει οικιακούς και μεγάλους καταναλωτές, όπως εμπορικούς και βιομηχανικά φορτία. Οι πελάτες μπορούν να δημιουργήσουν, να διαχειριστούν και να αποθηκεύσουν την ηλεκτρική ενέργεια, είναι ένας από τους βασικούς τομείς, καθώς ο καταναλωτής τελικά είναι το κύριο ενδιαφερόμενο μέρος για τον οποίο δημιουργείται όλο το δίκτυο. Σε αυτό τον τομέα καταναλώνεται η ηλεκτρική ενέργεια και οι οντότητες βοηθούν τους καταναλωτές να διαχειρίζονται την χρήση αλλά και την παραγωγή της. Για κάθε πελάτη μπορούν να υπάρχουν πολλαπλές διαδρομές επικοινωνίας. Τα σημεία εισόδου του τομέα επιτρέπουν εφαρμογές όπως ο απομακρυσμένος έλεγχος φορτίου, η κατανεμημένη παρακολούθηση και ο έλεγχος παραγωγής, οθόνες προβολής χρήσης ενέργειας, ανάγνωση δεδομένων από μετρητές. Επίσης μπορούν να διευκολύνουν καταγραφές και ελέγχους για σκοπούς κυβερνο-ασφάλειας.

**Τομέας Αγορών**

Στον τομέα της αγοράς δίνεται η δυνατότητα της αγοραπωλησίας των πόρων του δικτύου. Ο τομέας αυτός χειρίζεται παράγοντες όπως η διαχείριση της αγοράς, η χονδρική πώληση, το εμπόριο, και η λιανική πώληση. Ο τομέας των αγορών επικοινωνεί με όλους τους άλλους τομείς στο Smart Grid. Η επικοινωνία μεταξύ του τομέα της αγοράς και των τομέων παροχής ενέργειας είναι κρίσιμη, λόγω της ανάγκης για αποτελεσματική αντιστοίχιση παραγωγής και κατανάλωσης. Μέσω του τομέα αυτού επίσης γίνεται και ο συντονισμός της κατανάλωσης με την παραγωγή καθώς μόνο οι μεγάλοι παραγωγοί ενέργειας μπορούν να συμμετάσχουν στις αγορές. Ένα χαρακτηριστικό του τομέα των αγορών είναι οι φορείς συγκέντρωσης ενέργειας, οι οποίοι συγκεντρώνουν την ισχύ από πολλές μικρές κατανεμημένες μονάδες παραγωγής, όπως για παράδειγμα οικιακές ΑΠΕ, οι οποίες υπό κανονικές συνθήκες δεν θα είχαν τη δυνατότητα να δραστηριοποιηθούν στις αγορές, και την παρουσιάζουν ως έναν

μεγάλο, σημαντικό παραγωγό ο οποίος μπορεί να ανταγωνιστεί και να διαπραγματευτεί με καλύτερους όρους.

**Τομέας Παροχής Υπηρεσιών**

Στον τομέα αυτό δημιουργούνται και παρέχονται νέες και καινοτόμες υπηρεσίες αξιοποιώντας τις ευκαιρίες που προσφέρουν οι νέες μορφές δικτύων. Οι φορείς στον τομέα υποστηρίζουν επιχειρηματικές διαδικασίες ισχύος παραγωγούς, διανομείς και πελάτες, που κυμαίνονται από υπηρεσίες κοινής ωφέλειας όπως η τιμολόγηση στη διαχείριση της χρήσης και της παραγωγής ενέργειας. Η διεπαφή επικοινωνίας είναι κοινόχρηστη με τη Δημιουργία, τη Διανομή, τις Αγορές, τις Λειτουργίες και τον Πελάτη. Η σύνδεση με τον τομέα λειτουργιών είναι κρίσιμη για τη διασφάλιση του ελέγχου του συστήματος και της κατάστασης επίγνωσης. Οι εταιρείες που τις παρέχουν είναι εταιρείες ενέργειας ή νέες εταιρείες που χρησιμοποιούν νέες μορφές δικτύων χωρίς απαραίτητα να παράγουν ούτε να σχετίζονται με την ηλεκτρική ενέργεια. Ο τομέας αυτός είναι ο κυριότερος καθώς παρέχει διεπαφές, αναφορικά με την προστασία των δικαιωμάτων του καταναλωτή που του δίνουν τη δυνατότητα να αλληλοεπιδρά με το Smart Grid με μεγαλύτερη αποτελεσματικότητα και ταχύτητα.

**Τομέας Κέντρου Ενεργειών/Λειτουργειών**

Οι φορείς στον τομέα του Ενεργειακού Κέντρου είναι υπεύθυνοι για τη διασφάλιση της ομαλής λειτουργίας του συστήματος ηλεκτρικής ενέργειας. Ο τομέας είναι υπεύθυνος για τις λειτουργίες του συστήματος. Συμπεριλαμβανομένου της παρακολούθησης, του ελέγχου, της ανίχνευσης και της διαχείριση σφαλμάτων, τη συντήρηση δικτύου και την υποστήριξη των πελατών. Με την δημιουργία των Smart Grids περισσότερες από αυτές τις αρμοδιότητες θα μεταφερθούν στους παρόχους υπηρεσιών Για να επιτευχθεί αυτό, απαιτούνται διαδικασίες παρακολούθησης για μεταβλητές δικτύου, όπως συνθήκες φορτίου και κατάσταση εξοπλισμού, έλεγχος δικτύου, διαχείριση σφαλμάτων και κατασκευή και συντήρηση του δικτύου. Ενώ σήμερα αυτές οι διαδικασίες γίνονται συνήθως από εταιρείες, ένα Smart Grid θα τους επιτρέψει να διαχωρίζονται και να εκτελούνται από διαφορετικούς παρόχους υπηρεσιών. Σε αυτόν τον τομέα περιλαμβάνονται επίσης εφαρμογές συλλογής δεδομένων για τη δημιουργία αναφορών και τη συλλογή στατιστικών στοιχείων, καθώς και την ανάλυσή τους για μελλοντικές αποφάσεις που μπορεί να σχετίζονται με την επέκταση του ηλεκτρικού δικτύου, ακόμα και την αλλαγή του ως προς τον τρόπο λειτουργίας του. Δεδομένου ότι αυτός ο τομέας ελέγχει τη ροή της ενέργειας σε διάφορους τομείς, έχει αμφίδρομη επικοινωνία με όλους για να εξασφαλίσει το έργο της.

**Τομέας Παραγωγής**

Ο τομέας της Παραγωγής είναι υπεύθυνος για την παραγωγή ενέργειας σε μικρές ή μεγάλες ποσότητες. Αυτό μπορεί να προέρχεται, για παράδειγμα, από ορυκτά καύσιμα, νερό, άνεμος ή ηλιακή ενέργεια. Η παραγωγή ενέργειας περιλαμβάνει την κατανεμημένη ενέργεια από πόρους ΑΠΕ. Τα Smart Grids επιτρέπουν στους τελικούς χρήστες να λειτουργούν και ως παραγωγοί ηλεκτρικής ενέργειας, για χρήση, αποθήκευση ή ακόμα και για μεταπώληση. Με τα Smart Grids, η παραγωγή ηλεκτρικής ενέργειας δεν περιορίζεται σε μεγάλες εγκαταστάσεις ορυκτών ή υδροηλεκτρικής ενέργειας που τροφοδοτούν το δίκτυο μεταφοράς. Τα Smart Grids επιτρέπουν και μικρότερης κλίμακας παραγωγή ηλεκτρικής ενέργειας που συνδέεται με το δίκτυο διανομής. Αυτό μπορεί να είναι πάρκα αιολικής ενέργειας, ηλιακά πάρκα, Φ/Β πάνελ τοποθετημένα σε στέγες τελικών χρηστών, ή ηλεκτρικά οχήματα που τροφοδοτούν το δίκτυ. Η επικοινωνία με τον τομέα της Μεταφοράς και τον τομέα της Διανομής είναι σημαντική για τη διατήρηση της παροχής ενέργειας στους πελάτες. Για παράδειγμα, λαμβάνοντας την πληροφορία για αυξημένη ζήτηση ενέργειας, ο τομέας θα μπορούσε να ανταποκριθεί είτε αυξάνοντας την παραγωγή (μέσω του τομέα Ενεργειών/Λειτουργειών), είτε να εισάγει ενέργεια από άλλα δίκτυα (μέσω του τομέα Αγορών). Ο τομέας της Παραγωγής θα υποστεί τις μεγαλύτερες αλλαγές προκειμένου να επιτευχθούν στόχοι όπως η μείωση εκπομπών διοξειδίου του άνθρακα και η ενσωμάτωση ανανεώσιμων πηγών ενέργειας.

**Τομέας Δικτύου Μεταφοράς**

Το δίκτυο μεταφοράς αποτελεί σημαντικό μέρος των συστημάτων ηλεκτρικής ενέργειας, συνδέοντας γεννήτριες με σταθμούς διανομής και εξυπηρετώντας μεγάλους καταναλωτές. Παρακολουθείται και ελέγχεται στενά μέσω Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA) που επικοινωνεί με συσκευές πεδίου και ελέγχου σε όλο το δίκτυο μετάδοσης. Μπορεί επίσης να ανταλλάσσει ενέργεια με άλλα συστήματα για να καλύψει τις ανάγκες.

**Τομέας Δικτύου Διανομής**

Το δίκτυο διανομής είναι αυτό που συνδέει το δίκτυο μεταφοράς με τους καταναλωτές. Παραδοσιακά είχε ακτινική μορφή, καθώς μεταφέρει ενέργεια προς μια κατεύθυνση, από τους σταθμούς παραγωγής προς τους τελικούς πελάτες, και δεν βασιζόταν ιδιαίτερα σε συστήματα τηλεμετρίας. Ο τομέας της διανομής συνδυάζει και επικοινωνεί με τον τομέα της αγοράς λόγω της δυνατότητας των τομέων της αγοράς να επηρεάζουν τοπικά την κατανάλωση και την παραγωγή ενέργειας. Με την έλευση του Smart Grid, η μορφή του

συστήματος διανομής θα αλλάξει, ώστε να υποστηρίζει αμφίδρομες συνδέσεις, τόσο για επικοινωνίες, όσο και ηλεκτρικές, αφού πλέον οι καταναλωτές θα μπορούν να είναι και παραγωγοί ενέργειας. [17]

## 3.3 Τα Θέματα Ασφάλειας & Διαχείρισης Δεδομένων στα Ευφυή Δίκτυα

Η ασφάλεια των συστημάτων αποτελεί σημαντική πρόκληση για την ανάπτυξη των Ευφυών δικτύων. Είναι σημαντικό να ληφθούν μέτρα για την προστασία των συστημάτων από μη εξουσιοδοτημένη πρόσβαση ή χρήση και να διατηρηθούν αξιόπιστα τα συστήματα στα οποία μπορούμε να βασιστούμε σε περίπτωση έκτακτης ανάγκης. Πολλές από αυτές είναι κρίσιμες όπως, η χρήση εσφαλμένων ή κακόβουλων δεδομένων μπορεί να έχει σοβαρές συνέπειες, οι συμβατικές λύσεις ασφαλείας όπως ο έλεγχος ταυτότητας, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, είναι κρίσιμες επειδή λανθασμένα ή κακόβουλα δεδομένα μπορεί να έχουν σοβαρές συνέπειες. Τα ζητήματα ασφάλειας παραμένουν μεγάλα εμπόδια στην υιοθέτηση και ανάπτυξη του Smart Grid παγκοσμίως. Με άλλα λόγια, οι χρήστες δεν θα υιοθετήσουν πλήρως την χρήση τους εάν δεν υπάρχει εγγύηση ότι θα προστατεύσει το απόρρητό τους.

Το Smart Grid είναι πολύ ευάλωτο σε επιθέσεις για πολλούς λόγους: οι περισσότερες επικοινωνίες είναι ασύρματες, κατά συνέπεια, τα μηνύματα που ανταλλάσσονται ενδέχεται να υπόκεινται σε υποκλοπή, κακόβουλη δρομολόγηση, παραβίαση μηνυμάτων κ.α. ζητήματα ασφαλείας που μπορούν να επηρεάσουν την ασφάλεια ολόκληρου του Δικτύου.

Τα συνδεδεμένα αντικείμενα έχουν τις δικές τους ευπάθειες που σχετίζονται με τις συγκεκριμένες δυνατότητές τους. Αυτές οι νέες ευπάθειες προκαλούνται λόγω των παρακάτω λόγων:

- Δεν υπάρχουν γνωστά πρότυπα ασφαλείας.
- Υπάρχουν πολλά ιδιόκτητα πρωτόκολλα.
- Οι αρχιτεκτονικές είναι πολύ ετερογενείς και η φυσική ασφάλεια συχνά διακυβεύεται.
- Η ενημέρωση ακεραιότητας λογισμικού συνδεδεμένων αντικειμένων δεν είναι εγγυημένη.
- Η ασφάλεια των αποθηκευμένων δεδομένων δεν είναι εγγυημένη.
- Οι περιορισμένοι πόροι εμποδίζουν τη χρήση κλασικών κρυπτογραφικών συναρτήσεων και πρωτοκόλλων ασφαλείας.

Μπορούμε να ταξινομήσουμε πιθανές επιθέσεις στο Smart Grid σε τρεις κύριες κατηγορίες με βάση τον στόχο της επίθεσης: επιθέσεις εναντίον μιας συσκευής (όπως ένας

έξυπνος μετρητής), επιθέσεις κατά των χρηστών και των διαχειριστών (κατασκευαστές συσκευών για παράδειγμα) και επιθέσεις κατά της επικοινωνίας μεταξύ συσκευών και χρηστών/διαχειριστών.

- ✓ Attack the device
- ✓ Attack the communications
- ✓ Attack the ecosystem

Η ασφάλεια του Smart Grid απειλείται καθώς η ενσωμάτωση νέων τεχνολογιών και με κυριότερες αυτές που σχετίζονται με το Διαδίκτυο που μετατρέπει το απομονωμένο και κλειστό δίκτυο σε κοινό/δημόσιο δίκτυο δημιουργήσει νέες απειλές. Οι προχωρημένες αυτές τεχνικές προσφέρουν σημαντικά πλεονεκτήματα και δυνατότητες, όμως ως αρνητικό αποτέλεσμα θα έχουμε την αύξηση των προβλήματα σε σχέση με την προστασία και τη διαθεσιμότητα των δεδομένων / πληροφοριών. Δεν είναι μόνο οι απειλές του κυβερνοχώρου, (malware, spyware, computer viruses), που αυτή τη στιγμή απειλούν τα δίκτυα των υπολογιστών και γενικότερα των επικοινωνιών, καθώς η εισαγωγή των νέων και κατανεμημένων τεχνολογιών, όπως αυτή των έξυπνων μετρητών, οι αισθητήρες, μπορούν να δημιουργήσουν ευάλωτα σημεία ή ευπάθειες (vulnerabilities) στο Smart Grid. Βέβαια όμως οι προαναφερθείσες επιθέσεις του κυβερνοχώρου μπορεί να επωφεληθούν από την προσβασιμότητα μέσω των δικτύων HAN και NAN, έχοντας ως κύριο στόχο την απομακρυσμένη πρόσβαση ώστε να θέσουν σε κίνδυνο ή να ελέγξουν ηλεκτρονικές συσκευές[6].

Μερικά από τα κύρια θέματα που προκύπτουν όσον αφορά την Ασφάλεια των Πληροφοριών και την Προστασία Προσωπικών Δεδομένων αναφέρονται παρακάτω:

I. Τα δεδομένα και οι πληροφορίες που μεταφέρονται μέσω των Smart Grid, αναφορικά με την κατανάλωση της ηλεκτρικής ενέργειας των χρηστών/καταναλωτών δίνεται η δυνατότητα να υποκλαπούν. Ο κύριος σκοπός θα είναι να αναλυθεί από τους εισβολείς η κατανάλωση της ηλεκτρικής ενέργειας και γενικότερα τα προφίλ κατανάλωσης με απώτερο σκοπό να αποκτήσουν πληροφορίες σχετικά με τον τρόπο ζωής και τις συνήθειες των καταναλωτών.
II. Οι εισβολείς θα έχουν τη δυνατότητα να θέσουν σε κίνδυνο τους έξυπνους μετρητές των χρηστών, παρεμβαίνοντας στα συστήματά τους, και με αυτόν τον τρόπο να έχουν τη δυνατότητα να μπορούν παραποιήσουν τα δεδομένα ή δώσουν εντολές ελέγχου στο δίκτυο.

III. Η χρησιμότητα θεωρείτε μία αρχή που διαχειρίζεται τα φορτία των χρηστών και τα προσωπικά δεδομένα. Η χρήση λιγότερων προσωπικών πληροφοριών θα μπορούσε να είναι κρίσιμη κατά την εκτέλεση λειτουργιών ρουτίνας, όπως οι πληρωμές και ο έλεγχος.

Το ποιο σημαντικό είναι βέβαια η προστασία του απορρήτου ώστε να υπάρξει απηχήσει για τη χρήση του. Έχουν γίνει πολλές εύρυνες για να βρεθούν τρόποι και πρωτοκόλλα που θα μπορέσουν να προστατεύσουν το απόρρητο και τα δεδομένα που συλλέγονται από τους έξυπνους μετρητές[8].

### 3.3.1. Σημεία ασφάλειας & Ιδιωτικότητας προς Επίθεση

Υπάρχουν δύο κύριοι τύποι επιθέσεων ασφαλείας που μπορούν να θέσουν σε κίνδυνο την ασφάλεια του Smart Grid οι οποίες είναι οι Παθητικές επιθέσεις και Ενεργές Επιθέσεις. Οι Παθητικές Επιθέσεις στοχεύουν στην εκμάθηση, στη διαχείριση και την χρήση των δεδομένων και των πληροφοριών του συστήματος χωρίς να επηρεάζουν τους πόρους του συστήματος. Ο στόχος αυτής της επίθεσης είναι μόνο οι μεταδιδόμενες πληροφορίες ώστε να μπορέσει ο εισβολέας να καταλάβει την διαμόρφωση του συστήματος, την αρχιτεκτονική και την συμπεριφορά λειτουργίας. Αυτοί οι τύποι επιθέσεων είναι δύσκολο να εντοπιστούν, καθώς τα δεδομένα δεν τροποποιούνται και ως εκ τούτου, η κύρια εστίαση είναι στην πρόληψη και όχι στην ανίχνευση. Οι Ενεργές Επιθέσεις σχεδιάζονται ώστε να επηρεάσουν τη λειτουργία του συστήματος μέσω τροποποίησης δεδομένων ή εισαγωγής ψευδών πληροφοριών στο σύστημα.

Οι κύριοι λόγοι που γίνονται οι επιθέσεις στο Smart Grid είναι η δολιοφθορά και η κατασκοπεία. Διάφοροι τύποι εισβολέων μπορούν να κάνουν επιθέσεις εναντίον του Smart Grid, όπως οι κρατικοί χάκερ, οι τρομοκράτες, οι δυσαρεστημένοι υπάλληλοι / εισβολείς από μέσα, ακτιβιστές χάκερ και νόμιμες δοκιμές διείσδυσης. Παρακάτω αναφέρονται συνοπτικά οι επιθέσεις ασφάλειας στον κυβερνοχώρο που μπορούν να συμβούν σε ένα Smart Grid.

Η διαχείριση πολλών πληροφοριών είναι ένα ευάλωτο σημείο προς επίθεση όπως:

- Skimming (Υποκλοπή),
- Eaves dropping (Υποκλοπή Δεδομένων),
- Traffic Analysis,
- Impersonation/Identity Spoofing (Πλαστοπροσωπία),
- Data Tampering (Αλλοίωση δεδομένων),

- Authorization and Control Access issues (Εξουσιοδότηση και έλεγχος πρόσβασης),
- Compromising and Malicious code (Έκθεση σε κακόβουλο κώδικα) [7]

### 3.3.2. Είδη Επιθέσεων

Τα Smart Grid, όπως αναφέραμε έχουν πολλά πλεονεκτήματα σε σχέση με το υπάρχον δίκτυο αλλά, η ανάπτυξή του όμως θα επιφέρει και κάποια προβλήματα αναφορικά με την ακεραιότητα των πληροφοριών που θα μεταφέρονται και έτσι θα είναι ευάλωτες από επιθέσεις όπως φυσικές απειλές (physical), ηλεκτρονικές απειλές (cyber) και τέλος συνδυασμένες απειλές (cyber-physical), από τις οποίες οι ηλεκτρονικές επιθέσεις είναι αυτές που θα χρειαστούν την προσοχή μας και με τις τεχνικές που θα αναφέρουμε παρακάτω θα προσπαθήσουμε να αποτρέψουμε τη διαρροή δεδομένων, την αλλαγή δεδομένων και την παραπλάνηση του διαχειριστή του συστήματος ελέγχου, τη ζημιά στον εξοπλισμό μετά από εφαρμογή ανακριβών δεδομένων και απώλεια υπηρεσίας εάν ο εισβολέας απενεργοποιήσει τη συσκευή.

Συνήθως χρησιμοποιούνται τρεις τύποι επιθέσεων οι οποίες αναφέρονται περιληπτικά παρακάτω:

I. **Εξωτερική επίθεση (external attack):** Ο εξωτερικός εισβολέας παρακολουθεί τις μεταδιδόμενες πληροφορίες από των χρήστη προς το δίκτυο και με αυτόν τον τρόπο προσπαθεί να θέσει σε κίνδυνο τα δεδομένων του.
II. **Εσωτερική Επίθεση (Inside Attack):** Ο εισβολέας που συνήθως είναι ένας απογοητευμένος χρήστης/υπάλληλος προσπαθεί με μη εξουσιοδοτημένη πρόσβαση να θέσει σε κίνδυνο το δεδομένα του έξυπνου μετρητή.
III. **Κακόβουλη επίθεση εξόρυξης δεδομένων**: Ο εισβολέας προσπαθεί να παραποιήσει τα αποτελέσματα του έξυπνου μετρητή χρησιμοποιώντας έναν τροποποιημένο έξυπνο μετρητή για προσομοίωση και να ανακαλύψει τις μετρήσεις των έξυπνων μετρητών των χρηστών.

Παρακάτω θα αναφέρουμε ποιο αναλυτικά τα είδη των απειλών:

**I. Φυσικές απειλές (physical Vulnerabilities):** Για να υπάρξει τέτοιου είδους ευπάθεια, θα χρειαστούν ειδικά εργαλεία και φυσική παρουσία. Η γραμμή μεταφοράς του ηλεκτρικού ρεύματος μπορεί να υπονομευθεί οπουδήποτε κατά όλο το μήκος της. Η γραμμή διανομής τοποθετείται σε χαμηλό ύψος, καθιστώντας την ευάλωτη σε

κακόβουλες επιθέσεις. Οι έξυπνοι μετρητές είναι επίσης εύκολο να κλαπούν, καθώς εγκαθίστανται στις εγκαταστάσεις του χρήστη/καταναλωτή.

II. **Ηλεκτρονικές απειλές (Cyber Vulnerabilities):** Μια ευπάθεια στον κυβερνοχώρο προσδιορίζεται ως η αδυναμία που μπορεί να χρησιμοποιηθεί από έναν εισβολέα για την εκτέλεση επιβλαβών δραστηριοτήτων στα μέρη του Smart Grid που χρησιμοποιούν ένα δικτυωμένο σύστημα. Οι ευπάθειες στον κυβερνοχώρο του Smart Grid μπορούν συνήθως να στοχεύουν μέσω της επικοινωνίας, του λογισμικού ή του απορρήτου.

**-Ευπάθεια Επικοινωνίας (Communication Vulnerabilities):** Τα τοπικά δίκτυα είναι τα δίκτυα που βασίζονται σε Ethernet συνδεσμολογία και είναι ευάλωτα σε υποκλοπές και Man-in-the-Middle (MitM) επιθέσεις. Τέτοιου είδους επιθέσεις δίνουν τη δυνατότητα στους εισβολείς να πλαστογραφούν στοιχεία και να εισάγουν ψευδή δεδομένα καθώς και να μπορούν να αποκαλύπτουν εμπιστευτικές πληροφορίες. Η υποδομή πληροφοριών του δικτύου ηλεκτρικής ενέργειας εξαρτάται από το περιορισμένο πρωτόκολλο Διαδικτύου και τα πρότυπα που αφορούν γνωστά τρωτά σημεία που θα μπορούσαν να χρησιμοποιηθούν για την έναρξη επιθέσεων στο δίκτυο. Η συνδεσιμότητα ορισμένων πρωτοκόλλων επικοινωνίας όπως το TCP/IP που είναι συνδεδεμένο με το Διαδίκτυο υποτίθεται ότι συνδέεται με το κέντρο ελέγχου. Το κυριότερο μειονέκτημα είναι ότι τα δίκτυα που βασίζονται στο Διαδίκτυο συνδέονται άμεσα ή έμμεσα με κέντρα ελέγχου και έτσι που προκαλούν τρωτά σημεία στο δίκτυο.

**-Ευπάθεια Λογισμικού (Software vulnerabilities):** Οι διακομιστές στα κέντρα ελέγχου που είναι συνδεδεμένοι στο Διαδίκτυο σε ένα το τοπικό δίκτυο μπορεί να είναι ευάλωτοι σε κακόβουλες επιθέσεις που επηρεάζουν την επιθυμητή διαχείριση. Ορισμένες συσκευές όπως οι έξυπνοι μετρητές, οι οποίοι μπορούν να αναβαθμιστούν εξ αποστάσεως, είναι περισσότερο ευάλωτοι. Τέτοιες συσκευές ανοίγουν τις πόρτες στους εισβολείς και έτσι για να ελέγξουν τους διακόπτες που προκαλούν μπλακ άουτ. Επιπλέον, τα σφάλματα λογισμικού μπορούν να εκμεταλλευτούν τέτοια ευπάθεια από κακόβουλο εισβολείς καθώς τα στοιχεία του δικτύου είναι διαθέσιμα σε κάθε νοικοκυριό.

**-Ευπάθεια Ασφάλειας (Privacy vulnerabilities):** Οι αμφίδρομες επικοινωνίες που συνδέουν τον έξυπνο μετρητή του χρήστη/καταναλωτή στο σύστημα του δικτύου και έτσι δημιουργούνται τρωτά σημεία / κενά ασφαλείας σχετικά με το απόρρητο του πελάτη. Κατά αυτόν τον τρόπο οι ιδιωτικές πληροφορίες του χρήστη/καταναλωτή

όπως οι καθημερινές συνήθειες του καθώς και η παρουσία ή η απουσία του από το σπίτι μπορούν να βοηθήσουν τους εισβολείς που ελέγχουν του έξυπνου μετρητή.

III. **Συνδυασμένες απειλές (cyber-physical Vulnerabilities):** Οι ευπάθειες αυτές προσδιορίζονται ως η αδυναμία που προκύπτει από την ενσωμάτωση του τμήματος της τεχνολογίας με το φυσικό μέρος του. Τα τρωτά σημεία του Smart Grid έχουν αυξηθεί τα τελευταία χρόνια και συνήθως εμφανίζονται μέσω του δικτύου επικοινωνίας ή των κενών ασφαλείας των έξυπνων μετρητών. Καθώς οι επιθέσεις στον κυβερνοχώρο μπορούν να έχουν και φυσικές συνέπειες μπορούν να επηρεάσουν και την ηλεκτρονική υποδομή.

**- Ευπάθεια Δικτυακής Επικοινωνίας (Network Communication vulnerabilities):** Η υποδομή του Smart Grid εξαρτάται από πρωτόκολλα που χρησιμοποιούνται σε τυπικές επικοινωνίες και βασίζονται σε βασικά μέτρα ασφαλείας που την καθιστούν ευάλωτη στις επιθέσεις υποκλοπής καθώς υπάρχει έλλειψη κρυπτογράφησης και ελέγχου ταυτότητας και για αυτό το λόγο αμφισβητείται η ακεραιότητα των δεδομένων του χρήστη/καταναλωτή.

**-Ευπάθεια του Έξυπνου μετρητή (Smart meter vulnerabilities):** Οι αλληλεπιδράσεις μεταξύ της επικοινωνίας των έξυπνων μετρητών δημιουργούν σοβαρές ανησυχίες για την ασφάλεια των δεδομένων του χρήστη/καταναλωτή. Οι έξυπνοι μετρητές έχουν "πίσω πόρτα" που θα μπορούσε να αξιοποιηθεί από τον πάροχο ή από τον χρήστη και έτσι να έχει πρόσβαση σε όλο το Smart Grid. Μια επιπλέον αδυναμία είναι ότι η επικοινωνία μεταξύ των έξυπνων μετρητών γίνεται μέσω Telnet το οποίο μεταδίδει μη κρυπτογραφημένα δεδομένα και έτσι οι εισβολείς μπορούν να έχουν πρόσβαση στα ευπαθή δεδομένα του χρήστη/καταναλωτή. Επιπλέον οι εισβολείς θα μπορούσαν να χρησιμοποιήσουν τους έξυπνους μετρητές ως "Bot" για να για να εξαπολύσουν επιθέσεις εναντίον άλλων συστημάτων εντός του δικτύου. Τέλος, ο λογαριασμός ρεύματος θα μπορούσε να αλλάξει έχοντας ψευδή δεδομένα προκειμένου να μειωθεί το κόστος του ρεύματος. [24]

### 3.3.3. Κίνδυνοι μέσω Διαδικτύου

Ο αριθμός των κυβερνοεπιθέσεων και των εισβολών έχει αυξηθεί ραγδαία τα τελευταία χρόνια, καθώς οι εισβολείς μπορούν να έχουν πρόσβαση σε προσωπικές πληροφορίες σχετικά με πελάτες και παρόχους υπηρεσιών και να προκαλέσουν μπλακ άουτ. Η πιο κοινή μορφή διαδικτυακής επίθεσης είναι η άρνηση υπηρεσίας (επίθεση DoS). Αυτά τα νέα τρωτά σημεία δεν έχουν γνωστά πρότυπα ασφαλείας, έχουν πολλά ιδιόκτητα πρωτόκολλα, δεν είναι

εγγυημένα ότι θα ενημερώσουν την ακεραιότητα του σχετικού λογισμικού και έχουν περιορισμένους πόρους για τυπικά πρωτόκολλα κρυπτογράφησης και ασφάλειας.

### 3.3.4. Βασικοί τύποι επιθέσεων

Ο ποιο εύκολος τρόπος επίθεσης σε ένα Smart Grid είναι με ηλεκτρονικές επιθέσεις σε ένα HAN όπου διάφορες ετερογενείς συσκευές συνδέονται μεταξύ τους και οι συσκευές διαχειρίζονται εξ αποστάσεως. Έτσι ένας αντίπαλος που πάντα ψάχνει να βρει ένα σημείο εισόδου για να εισέλθει στο δίκτυο χρησιμοποιεί διαφορετικούς τύπους επιθέσεων όπως:

- **Network-Based insecurities:** Αυτές οι ευπάθειες ενεργοποιούνται από άλλες συσκευές από αυτές που δέχονται την επίθεση.
- **Communication Systems insecurities:** Η ευπάθεια των συστημάτων επικοινωνίας είναι αυτή στην οποία οποιοσδήποτε από τους κόμβους δεν είναι αξιόπιστη πλατφόρμα και οι επικοινωνίες σε κάθε σύνδεσμο δεν προστατεύονται. Η επικοινωνία είναι κρίσιμη για τον ενεργειακό τομέα.
- **Embedded Processors Insecurities:** Τα ενσωματωμένα συστήματα περιλαμβάνουν υλικό και λογισμικό. Μπορούν να είναι προγραμματιζόμενα και να έχουν σχεδιαστεί για συγκεκριμένες λειτουργίες. Οι μικροεπεξεργαστές που χρησιμοποιούνται σε αυτά τα συστήματα ονομάζονται ενσωματωμένοι επεξεργαστές. Οποιαδήποτε ευπάθεια που τα διακυβεύει ονομάζονται ευπάθειες ενσωματωμένου επεξεργαστή.
- **Control Systems Insecurities:** Ένα σύστημα ελέγχου που αποτελείται από ένα σύνολο συσκευών που συνήθως προορίζονται να διοικούν, να κατευθύνουν και να ρυθμίζουν τη λειτουργία άλλων συστημάτων. Η δολιοφθορά τέτοιων συστημάτων οδηγεί σε ευπάθειες του συστήματος ελέγχου.
- **Telecommunication Network Insecurities:** Αυτές είναι οι ευπάθειες στοχεύουν στη διακοπή, άρνηση ή υποκλοπή επικοινωνιών. [19]

**Παρακάτω θα αναφέρουμε κάποιες από τις ευπάθειες που επηρεάζουν την ακεραιότητα του συστήματος και που ανήκουν στις παραπάνω κατηγορίες.**

- **Spoofing**: Το “spoofing” είναι μία επίθεση πού όταν κάποιος "αντίπαλος" προσποιείται ότι είναι ο καταναλωτής με σκοπό να αποκτήσει πρόσβαση στο σύστημα και έτσι να περιορίσει τους πόρους ή να υποκλέψει χρήσιμα δεδομένα και πληροφορίες. Για παράδειγμα, ένας "αντίπαλος" μπορεί να χρησιμοποιήσει εικονικά τη διεύθυνση IP ενός νόμιμου χρήστη για να αποκτήσει πρόσβαση στον λογαριασμό.

- **Denial-of-Service(DoS):** Οι επιθέσεις DoS αποτελούν σημαντικό πρόβλημα στο Smart Grid και αποτελούν μία από τις σημαντικότερες απειλές για την ασφάλεια. Οι επιθέσεις DoS δεν επιχειρούν απλώς να καταστρέψουν ή να κατακερματίσουν δεδομένα, αλλά ο κύριος στόχος τους είναι να διαταράξουν τις υπηρεσίες προσπαθώντας να περιορίσουν την πρόσβαση σε ένα μηχάνημα ή μια υπηρεσία αντί να υπονομεύσουν την ίδια την υπηρεσία. Αυτές οι επιθέσεις μπορεί να βλάψουν δεδομένα, αλλά μπορούν επίσης να βλάψουν πόρους, γεγονός που μπορεί να δυσκολέψει την εργασία ή τη χρήση των δεδομένων.
- **Impersonation Attack:** Γενικότερα, η κατάσταση κάθε ηλεκτρικής συσκευής είναι (ON/OFF) και αποθηκεύεται στη μνήμη του έξυπνου μετρητή. Έτσι κάθε 15 λεπτά η συσκευή στέλνει την κατανάλωσή της στον έξυπνο μετρητή. Εάν μια συσκευή έχει παραβιαστεί και μιμείται κάποια άλλη συσκευή, αυτό μπορεί να οδηγήσει σε λανθασμένη ανάγνωση για ένα χρονικό διάστημα, εκτός εάν εντοπιστεί και ανακτηθεί, καθώς για παράδειγμα, εάν το κλιματιστικό είναι ενεργοποιημένο και μιμείται έναν ανεμιστήρα ή και αντίστροφα, τότε έχει τεράστιο αντίκτυπο στη χρέωση του ρεύματος ή ακόμα και σε κλοπή ηλεκτρικής ενέργειας.
- **Eavesdropping:** Το Smart Grid δεν προορίζονται μόνο για την παροχή ηλεκτρικής ενέργειας από το δίκτυο στο σπίτι αλλά και ως κανάλι επικοινωνίας μεταξύ ενός έξυπνου σπιτιού στο Smart Grid και επίσης θα στέλνει διάφορα μηνύματα ελέγχου και θα προβλέπει εκ των προτέρων τη ζήτηση ισχύος. Αυτές οι πληροφορίες καθώς και το απόρρητο του πελάτη μπορεί να χρησιμοποιηθεί για τον κλοπές αλλά και άλλες δραστηριότητες. Η επίθεση στοχεύει το επίπεδο του δικτύου. Η δικτυακή σάρωση είναι η διαδικασία λήψης πακέτων από το δίκτυο και στη συνέχεια ανάγνωσης του περιεχομένου για αναζήτηση ευαίσθητων πληροφοριών. Η επίθεση μπορεί να πραγματοποιηθεί χρησιμοποιώντας εργαλεία που συλλέγουν πακέτα και αναλύουν τα δεδομένα που έχουν συλλεχθεί.
- **Man-in-the-middle:** Είναι ένας τύπος κυβερνο-επίθεσης κατά την οποία παρεμποδίζονται οι επικοινωνίες μεταξύ δύο μερών, συχνά για την κλοπή διαπιστευτηρίων σύνδεσης ή προσωπικές πληροφορίες, την κατασκοπεία θυμάτων, την δολιοφθορά των επικοινωνιών ή ακόμα και την καταστροφή δεδομένων. Αυτή η επίθεση χρησιμοποιείται συχνά για να αποκτήσει ο εισβολέας μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Ο εισβολέας εμποδίζει τη νόμιμη επικοινωνία μεταξύ των δύο μερών. Ο εισβολέας μπορεί έτσι να ελέγξει τη ροή της επικοινωνίας, εξάγοντας ή παραμορφώνοντας

τις πληροφορίες που αποστέλλονται από έναν από τους αρχικούς συμμετέχοντες. Στη συνέχεια, μπορεί να επεξεργαστεί το περιεχόμενό τους και να στείλει ψεύτικα μηνύματα στους παραλήπτες.

- **Replay Attack:** Τα έξυπνα σπίτια και τα Smart Grid επικοινωνούν και μοιράζονται συνεχώς πληροφορίες σχετικά με χρήση ηλεκτρικής ενέργειας και σχετικά με την πρόβλεψη των μελλοντικών απαιτήσεων ενέργειας. Εάν υπάρχει διαρροή δεδομένων από μία ηλεκτρική συσκευή ή του έξυπνου μετρητή, ένας "αντίπαλος" μπορεί να δει την αναφορά κατανάλωσης και να δημιουργήσει μια παλιά αναφορά στη θέση της τρέχουσας και έτσι θα μπορέσει να αλλάξει την αναφορά ζήτησης ηλεκτρικής ενέργειας προς προσφορά.
- **Alteration Attack:** Μια επίθεση αλλοίωσης συμβαίνει όταν το HAN, μια συσκευή ή ο έξυπνος μετρητής παραβιάζεται και έτσι ένας "αντίπαλος" αλλοιώνει την αναφορά κατανάλωσης. Η πλαστή αναφορά κατανάλωσης μπορεί να οδηγήσει σε ψευδή εκτέλεση, για παράδειγμα, αντί να ρυθμίσει το φούρνο στους 120 °C να ρυθμίσει το σύστημα θέρμανσης νερού στους 120 °C με αποτέλεσμα τον τραυματισμό ενός ατόμου στο σπίτι ή μπορεί επίσης να οδηγήσει σε βλάβη του συστήματος ή βραχυκύκλωμα. Ακόμα κι αν μια αναφορά κατανάλωσης είναι πλαστή, μπορεί να αναγκάσει τον πελάτη να πληρώσει για την ηλεκτρική ενέργεια που δεν έχει καταναλώσει.
- **Message Modification Attack:** Η επικοινωνία είναι ένας βασικός τρόπος με τον οποίο το Smart Grid διαφέρει από ένα παραδοσιακό Δίκτυο. Αν υπάρχει ένας "αντίπαλος" μεταξύ Smart Grid και του HAN, μπορεί να τροποποιήσει τα μηνύματα που αποστέλλονται ή λαμβάνονται αντιστοίχως, το οποίο μπορεί να οδηγήσει σε έλλειψη εμπιστοσύνης μεταξύ των οντοτήτων και συνεπώς οδηγώντας σε σοβαρές ζημιές και στις δύο πλευρές.
- **Energy Import/Export Attack:** Το Smart Grid θα επιτρέπει την κατανεμημένη παραγωγή ενέργειας, όπου ο καταναλωτής μπορεί να εγκαταστήσει ΑΠΕ και να τροφοδοτεί με την υπολειπόμενη ενέργειας στο δίκτυο και έτσι να μπορεί να απαιτήσει επιπλέον ενεργειακούς πόρους από το δίκτυο όταν χρειάζεται. Για παράδειγμα, ένας "αντίπαλος" απαιτεί την παροχή της ηλεκτρικής ενέργειας στο δίκτυο που δεν χρειάζεται ακόμα και όταν χρειάζεται.
- **ΙΟΣ (virus):** Ένας ιός θεωρείτε κομμάτι ενός κώδικα που μπορεί να αντιγραφεί και με τη βοήθεια του χρήστη για να ενεργοποιηθεί και να εξαπλωθεί. Ένας ιός μπορεί να μεταδοθεί από ένα μέσο αποθήκευσης, όπως μια μονάδα flash (flash USB). Ως αποτέλεσμα της υψηλής ταχύτητας και της υψηλής διασύνδεσης των κόμβων του Διαδικτύου, είναι

δύσκολο να εντοπιστεί και να αποκλειστεί η κακόβουλη κίνηση. Επομένως, λόγω της υψηλής ταχύτητας και της δια-λειτουργικότητας των κόμβων του Διαδικτύου, οι ιοί μεταδίδονται πολύ ποιο γρήγορα.

- **Σκουλήκι (worm):** Ένα "σκουλήκι" είναι ένα πρόγραμμα που μπορεί να εξαπλωθεί σε ένα δίκτυο, προκαλώντας προβλήματα ασφάλειας σε υπηρεσίες μεγάλης κλίμακας. Υπάρχει διαφορά μεταξύ των ιών τύπου "σκουλήκι" και των ιών, καθώς οι ιοί μολύνουν αρχεία που δεν χρησιμοποιεί ο χρήστης, ενώ τα "σκουλήκια" αναζητούν και καταστρέφουν ενεργά αρχεία. Αυτός είναι ο λόγος που οι ιοί εξαπλώνονται πιο αργά από τα σκουλήκια. Οι ιοί δεν χρειάζονται άλλο λογισμικό για να διαδοθούν από τον έναν υπολογιστή στον άλλο, αλλά τα σκουλήκια μπορούν να εξαπλωθούν αυτόματα μέσω του δικτύου χωρίς την ανάγκη άλλου λογισμικού.
- **Δούρειος Ίππος (Trojan Horse):** Ο Δούρειος Ίππος είναι ένα πρόγραμμα που αν και φαίνεται χρήσιμο, στην πραγματικότητα μπορεί να περιέχει επιβλαβείς προθέσεις. Ο Δούρειος ίππος μοιάζει με ένα κανονικό πρόγραμμα, αλλά όταν εκτελείτε, ο κακόβουλος κώδικας που περιέχει ενεργοποιείται και ο υπολογιστής μολύνεται.

### 3.3.5. Κατηγοριοποίηση Επιθέσεων

Οι ευπάθειες σε ένα Smart Grid μπορούν να αξιοποιηθούν από εισβολείς ή χρήστες συνειδητά ή ασυνείδητα για να αποκτήσουν πρόσβαση σε διαφορετικά επίπεδα στο σύστημα για διαφορετικούς σκοπούς. Ορισμένοι καταναλωτές μπορούν να επιτεθούν σε ορισμένα στοιχεία του συστήματος για να μειώσουν τους λογαριασμούς ηλεκτρικής ενέργειας και αρκεί να συνδεθούν στο πλησιέστερο AMI. Ορισμένοι τελικοί χρήστες μπορούν επίσης να στοχεύουν στην παροχή οικονομικών οφελών αλλάζοντας τις πληροφορίες παραγωγής και κατανάλωσης με πρόσβαση στο σύστημα τιμολόγησης. Οι μέθοδοι που χρησιμοποιούνται για τις επιθέσεις αυτές μέσω του Διαδικτύου διαφέρουν ανάλογα με τον εισβολέα και το κίνητρό του. Κάποιοι από τους εισβολείς μπορούν να αποκτήσουν πρόσβαση σε μία ιστοσελίδα μέσω τοπικής παρακολούθησης (surveillance) και κάποιοι άλλοι να κάνουν την επίθεση από κάποιον απομακρυσμένο υπολογιστή. Είναι πολύ δύσκολο ένας εισβολέας να αποκτήσει πρόσβαση σε υπολογιστή ή σύστημα SCADA χωρίς εξουσιοδότηση και θα χρειαζόταν πολλές ώρες έρευνας για να το κάνει. Οι επιθέσεις σε ένα Smart Grid, μπορούν να πραγματοποιηθούν για διάφορους λόγους. Οι επιτιθέμενοι ταξινομούνται ανάλογα με τους στόχους και τα κίνητρά τους. Τα κίνητρα των επιθέσεων σε ένα Smart Grid μπορεί να κυμαίνονται από κυβερνο-πόλεμο, τρομοκρατία, βιομηχανική κατασκοπεία, ακτιβισμό, οικονομικούς λόγους, δυσαρεστημένους εργαζόμενους. Οι εισβολείς μπορεί να είναι

ερασιτέχνες, επαγγελματίες, τρομοκράτες, εργαζόμενοι, ανταγωνιστές, ακόμη και οι ίδιοι οι πελάτες. Οι μη κακόβουλοι εισβολείς θεωρούνται οι επιτιθέμενοι από περιέργεια των οποίων ο κύριος σκοπός δεν είναι να βλάψουν το σύστημα. Μερικοί από τους εισβολείς που στοχεύουν στην παροχή προσωπικού οφέλους μπορεί να είναι και πελάτες του δικτύου. Αυτοί οι τελικοί χρήστες μπορούν να επιτεθούν στους έξυπνους μετρητές ή στις γραμμές μετάδοσης δεδομένων με τρόπο ώστε να τους ωφελεί, συνήθως, οικονομικά. Με την σειρά τους οι εισβολείς (τρομοκρατικές) με την επίθεση στα συστήματα ηλεκτρικού δικτύου στοχεύουν να θέσουν εκτός λειτουργίας κρίσιμα σημεία των υποδομών. Οι εισβολείς (δυσαρεστημένοι εργαζόμενοι) μπορούν να επιτεθούν σκόπιμα στο σύστημα με στόχο να αλλάξουν τις ρυθμίσεις των αλγόριθμων του λογισμικού ή να διαμορφώσουν τα δεδομένα στις συσκευές του συστήματος για να αποκομίσουν αυτό-ικανοποίηση ή για ιδία οφέλη. Οι εισβολείς (ανταγωνιστές) μπορούν να επιτεθούν για οικονομικά οφέλη, και να υποκλέψουν εταιρικά δεδομένα ή προσωπικά δεδομένα πελατών από τη βάση δεδομένων λόγω του ανταγωνισμού μεταξύ των παρόχων υπηρεσιών. Αυτού του είδους οι εισβολείς ονομάζονται ανταγωνιστές επιτιθέμενοι. Οι εισβολείς (Κρατικοί χάκερ), ή αλλιώς εισβολείς του οργανωμένου εγκλήματος, έχουν διαφορετικά κίνητρα. Τα Smart Grid είναι η διασταύρωση της νοημοσύνης, της ενέργειας, της πολιτικής και των κοινωνικών ανησυχιών και έτσι εξηγείτε η ποικιλία των εισβολέων και των προθέσεών τους.

**Ποιο αναλυτικά, θα αναφερθούμε παρακάτω:**

### 3.3.6. Κατηγοριοποίηση επιθέσεων σύμφωνα με το κίνητρο

Τα κίνητρα των εισβολέων μπορούν να κατηγοριοποιηθούν σε πέντε τομείς, και ποιο συγκεκριμένα : στην περιέργεια που έχει ένας εισβολέας, με κίνητρο την ανάκτηση/μεταβολή/διαχείριση των πληροφοριών/ δεδομένων που διαμοιράζονται μέσα στο Smart Grid, ανήθικη κλοπή ενέργειας, κλοπή εξουσίας δεδομένων αναφορικά με την κατανάλωση της ενέργειας, και για οικονομικά οφέλη.

### 3.3.7. Κατηγοριοποίηση επιθέσεων σύμφωνα με τον αριθμό των επιτιθέμενων

Μπορούν να χαρακτηριστούν ως **μεμονωμένες (ατομικές)** με στόχο τη συλλογή όλων των απαραίτητων πληροφοριών ώστε να προκαλέσουν μια μικρής κλίμακας black-out. Επίσης μπορούν να είναι **Οργανωμένες επιθέσεις** που οργανώνονται από ομάδες εισβολέων που συνεργάζονται για να προκαλέσουν φθορές σε κρίσιμες υποδομές, και κυρίως στοχεύουν σε ένα σύνθετο αποτέλεσμα με μεγαλύτερο αντίκτυπο από αυτό των μεμονωμένων επιθέσεων. Για να επιτύχουν τον στόχο τους χρησιμοποιούν σύγχρονες τηλεπικοινωνίες ώστε

να πραγματοποιήσουν συντονισμένες επιθέσεις από ευρέως διασκορπισμένες τοποθεσίες. Για παράδειγμα, ένας εισβολέας θα μπορούσε να απενεργοποιήσει το διακόπτη τροφοδοσίας σε ένα κτίριο, επιτρέποντας σε άλλον εισβολέα να εισβάλει στο κτίριο χωρίς να ενεργοποιήσει τον συναγερμό. Συχνά προσπαθούν να επιτύχουν ένα πιο περίπλοκο αποτέλεσμα με μεγαλύτερο αντίκτυπο από τις μεμονωμένες επιθέσεις.

### 3.3.8. Κατηγοριοποίηση ηλεκτρονικών επιθέσεων σύμφωνα με το στόχο

Μια απόπειρα ηλεκτρονικής επίθεσης μπορεί να στοχεύει σε οποιαδήποτε υποδομή του δικτύου ηλεκτρικής ενέργειας, όπως της παραγωγή όπου οι επιθέσεις εναντίον σταθμών ηλεκτροπαραγωγής έχουν σχεδιαστεί για να απενεργοποιούν ή να διακόπτουν τις γεννήτριες, της διανομής και του ελέγχου καθώς αυτό το εργαλείο περιλαμβάνει πληροφορίες σχετικά με εισβολές, αλλαγές φάσης και άλλες πληροφορίες κατάστασης δικτύου, όμως ο τελικός στόχος είναι η αλλαγή της κατάστασης δικτύου πληροφοριών, με αποτέλεσμα απότομη αλλαγή στο φορτίο που προκαλείται από το Διαδίκτυο επηρεάζει κρίσιμες περιοχές του δικτύου ηλεκτρικής ενέργειας, προκαλώντας υπερφόρτωση των γραμμών μεταφοράς ηλεκτρικής ενέργειας

### 3.3.9. Κυβερνοασφάλεια – Κυβερνοαπειλές

Με τη βελτίωση της προστασίας των υποδομών και των συστημάτων πληροφοριών, η κυβερνοασφάλεια είναι αναμφίβολα ένας από τους τομείς στους οποίους η AI έχει ωφεληθεί πολύ. Με τη βοήθεια σύγχρονων μοντέλων ML, η αποτελεσματική εφαρμογή αυτής της τεχνολογίας βοηθά στη δημιουργία δικτύων που αυτοπροστατεύονται και αυτοθεραπεύονται, ενώ βελτιώνει την ικανότητα ανίχνευσης και μετριασμού απειλών άγνωστων ή μη.

**Ο ρόλος του ανθρώπου στην εποχή του Cybersecurity**

Τα συστήματα πληροφοριών προσαρμόζουν πάντα την ασφάλειά τους για να ανταποκρίνονται στις ανάγκες του μέλλοντος, μετριάζοντας τις απειλές και μετριάζοντας τις επιπτώσεις τους. Ωστόσο, ενώ η AI αναδύεται ως ένα εξαιρετικά χρήσιμο εργαλείο για την πληροφορική, η πραγματική της αξία μπορεί να εξαχθεί μόνο σε συνδυασμό με την ανθρώπινη εμπειρία. Οι βέλτιστες πρακτικές για την ασφάλεια των επιχειρήσεων θα πρέπει να επεκταθούν σε περιβάλλοντα οικιακού γραφείου. Η συνεχής εκπαίδευση των χρηστών για την ασφαλή χρήση προσωπικών συσκευών, αυστηροί έλεγχοι πρόσβασης τόσο σε εταιρικά όσο και οικιακά δίκτυα, αλλά και μηδενική εμπιστοσύνη (zero trust), είναι μερικές μόνο από τις προϋποθέσεις για την επιτυχή αντιμετώπιση των αναδυόμενων απειλών.

**Συμπερασματικά**, η AI έχει μεγάλες δυνατότητες να επιταχύνει και να βελτιώσει την ακρίβεια της ανίχνευσης απειλών. Συνδυάζοντας βελτιωμένες διαδικασίες με τις σωστές δεξιότητες και ενσωματώνοντάς τις στις διαδικασίες του οργανισμού, μεγιστοποιείτε τα προσφερόμενα οφέλη και βάζει τα θεμέλια για τη λεγόμενη «μηχανική νοημοσύνη».

## 3.4. Η Αξιολόγηση της Εφαρμογής του "Έξυπνου" Ηλεκτρικού Συστήματος

Με την εφαρμογή των "Έξυπνων" Ηλεκτρικών συστημάτων, θα τοποθετηθούν και τα έξυπνα συστήματα μέτρησης που αναμένεται να αποφέρουν μεγάλο οικονομικό όφελος ανά καταναλωτή και, παράλληλα, εξοικονόμηση ενέργειας. Ο στόχος του Smart Grid είναι η μεγιστοποίηση της αξιοπιστίας, της ανθεκτικότητας και της σταθερότητας του συστήματος και έτσι θα υπάρξει ελαχιστοποίηση του κόστους χρήσης, παραγωγής και κατανάλωσης καθώς και μείωση των περιβαλλοντικών επιπτώσεων με το συντονισμό των αναγκών και των πόρων των τελικών χρηστών και της παραγωγής, των φορέων του δικτύου και της αγοράς. Δεδομένου ότι τα έξυπνα δίκτυα βασίζονται κυρίως στην ανταλλαγή πληροφοριών, οι νέες τεχνολογίες πληροφοριών και επικοινωνιών θα είναι ο ζωτικός τους κινητήριος μοχλός. Το πρώτο επίπεδο είναι η "εξυπνάδα" που διασφαλίζεται από τους έξυπνους μετρητές και τα τυποποιημένα πρωτόκολλα επικοινωνίας. Οι έξυπνοι μετρητές που αναμένονται να εγκατασταθούν σε όλους τους καταναλωτές σε όλο το μήκος του ηλεκτρικού δικτύου, θα πρέπει να είναι προσεκτικά σχεδιασμένοι και να διαθέτουν τις κατάλληλες λειτουργικές δυνατότητες με σκοπό την εξασφάλιση της τεχνικής και εμπορικής διαλειτουργικότητας ή ακόμα και να υπάρχει η δυνατότητα προσθήκης λειτουργικών δυνατοτήτων σε μεταγενέστερο στάδιο. Επίσης, θα πρέπει να υπάρχει η δυνατότητα παροχής ασφάλειας του απορρήτου των δεδομένων του χρήστη/καταναλωτή. Επιπλέον, θα πρέπει να βοηθούν στην εξέλιξη της ανταπόκρισης στη ζήτηση και άλλων ενεργειακών υπηρεσιών και να παρέχουν πρόσβαση και σε άλλες ενεργειακές υπηρεσίες και τέλος να βοηθούν τις λιανικές αγορές που παρέχουν τα οφέλη που χρειάζονται οι καταναλωτές και το ενεργειακό σύστημα.

Η κύρια λειτουργία που θα πρέπει να προστεθεί αν και μπορεί να παρουσιάζει τις περισσότερες δυσκολίες υλοποίησης έχει να κάνει με τη συχνότητα με την οποία τα δεδομένα κατανάλωσης θα πρέπει να ενημερώνονται και να είναι διαθέσιμα στους χρήστες το δικτύου. Με αυτή τη λειτουργία θα μπορούν να παρέχονται άμεσες πληροφορίες κόστους

για τους καταναλωτές, και να τους επιτρέπει να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τις καταναλωτικές τους συνήθειες.

Δυστυχώς, η μη επιλογή όλων των ελάχιστων κοινών λειτουργιών από μια ομάδα συστημάτων δεν σημαίνει πάντα ότι τα συστήματα θα είναι λιγότερο ακριβά. Η μεταβλητότητα των δεδομένων «κόστος ανά σημείο μέτρησης» υποδηλώνει ότι η συνολική επένδυση επηρεάζεται πολύ περισσότερο από άλλους παράγοντες, μεταξύ άλλων από:

- ✓ Δοκιμή εξοπλισμού / συστημάτων στις εγκαταστάσεις της κοινής ωφέλειας
- ✓ Επιτόπιες έρευνες
- ✓ Προετοιμασία δικτύου, συμπεριλαμβανομένου του δικαιώματος διέλευσης και απόκτησης διυπηρεσιακών υπηρεσιών
- ✓ Δημιουργία εγκαταστάσεων ως υλικοτεχνικούς κόμβους για ανάπτυξη πεδίου
- ✓ Απομάκρυνση υφιστάμενου εξοπλισμού / συστήματος
- ✓ Εγκατάσταση νέου εξοπλισμού / συστήματος
- ✓ Έλεγχος απόδοσης και ακρίβειας ως μέρος της θέσης σε λειτουργία

Κατά τις σχετικές έρευνες υπάρχουν ανησυχίες όσον αφορά το ιδιωτικό απόρρητο:

- ➢ Δημιουργία προφίλ χρήστη
- ➢ Κλοπή δεδομένων/πληροφοριών της ταυτότητας του χρήστη
- ➢ Προσδιορισμός ειδικών συσκευών που χρησιμοποιούνται
- ➢ Στοχευμένες εισβολές στο σπίτι
- ➢ Λογοκρισία δραστηριότητας
- ➢ Παρακολούθηση Συμπεριφοράς Ενοικιαστών/Μισθωτών
- ➢ Δημόσιες συγκεντρωτικές αναζητήσεις που αποκαλύπτουν ατομική συμπεριφορά

Με βάση τα παραπάνω, θα πρέπει να λαμβάνονται υπόψη και τα σύστημα ελέγχου ταυτότητας ώστε να διατηρήσουμε την ιδιωτικότητα μας με τη χρήση των έξυπνων μετρητών να είναι συνδεδεμένες με συσκευή ανθεκτική στην παραβίαση και τη δημιουργία ψευδό-ταυτοτήτων και υπογραφών. Αυτή η συσκευή θα δίνεται στον χρήστη όταν θα ανοίγει έναν λογαριασμό ή όταν εγγράφετε ως ένας νέος αγοραστής έξυπνου μετρητή. Τα χαρακτηριστικά γνωρίσματα της αρχιτεκτονικής θα είναι τα εξής:

- ✓ **Έλεγχος ταυτότητας μηνυμάτων (Message authentication):** Προτού ένας έξυπνος μετρητής διαβιβάσει ένα μήνυμα αίτησης στο κέντρο ελέγχου δικτύου, θα πρέπει να συμπεριλαμβάνει μια "υπογραφή" κωδικού ελέγχου ταυτότητας μηνυμάτων.
- ✓ **Απόρρητο ταυτότητας (Identity privacy):** Σε όλα τα μηνύματα αιτήματος που αποστέλλονται από έναν έξυπνο μετρητή, να χρησιμοποιούνται ψευδό-ταυτότητες αντί για τις πραγματικές ταυτότητες.
- ✓ **Αίτημα εμπιστευτικότητας μηνύματος (Request Message confidentiality):** Η ποσότητα ηλεκτρικής ενέργειας που απαιτείται από έναν έξυπνο μετρητή να κρυπτογραφείται χρησιμοποιώντας ένα δημόσιο κλειδί του κέντρου ελέγχου. Έτσι, εκτός από το κέντρο ελέγχου, κανείς δεν θα μπορεί να αποκρυπτογραφήσει τις πληροφορίες που αντιπροσωπεύει το μήνυμα. [23]

# Κεφάλαιο 4 Χρήση της Τεχνητής νοημοσύνης ως Πανάκια στο Έξυπνο Ηλεκτρικό Συστήματα

## 4.1 Το "Εξυπνο" Ηλεκτρικό Σύστημα ως Σύγχρονη Πρόταση

Το ηλεκτρικό δίκτυο γνώρισε τεχνολογική και θεσμική εξέλιξη καθ' όλη τη διάρκεια της ζωής του. Τη δεδομένη στιγμή, αντιμετωπίζουμε μια δραματική δομική μεταμόρφωση και οι διασυνδεδεμένες "δυνάμεις" οδηγούν στον μετασχηματισμό του δικτύου, επιβάλλοντας απαιτήσεις για προηγμένες λειτουργικές δυνατότητες και διαμορφώνονται με βάσει τα θέλω των επιχειρήσεων κοινής ωφέλειας και τις ρυθμιστικές αρχές ώστε να εφαρμόσουν την τεχνολογία στο Smart Grid.

Η πρόοδος της τεχνολογίας εφαρμόζεται σε τρεις σημαντικούς τομείς: α) στις εφαρμογές του Smart Grid, β) στην πρόοδο που σημειώθηκε στις ΑΠΕ και τη χρήση τους από επιχειρήσεις κοινής ωφέλειας, πελάτες και τρίτους έμπορους· και τέλος γ) στην ηλεκτροδότηση των καταναλωτικών προϊόντων, όπως ηλεκτρικά οχήματα και αντλίες θερμότητας και την σύνδεση αυτών στο δίκτυο.

Οι ομοσπονδιακές, πολιτειακές και τοπικές πολιτικές, συμπεριλαμβανομένου των αγορών, που ενθαρρύνουν την χρήση ΑΠΕ και προωθούν της ενεργειακή διαχείριση από τους πελάτες. Η εμφάνιση νέων συμμετεχόντων, όπως πελάτες κοινής ωφελείας, ενεργειακές υπηρεσίες, εταιρείες, και έμποροι τεχνολογίας, στη διαχείριση και παραγωγή της ηλεκτρικής ενέργειας και με ρόλο παρόχων υπηρεσιών δικτύου. Η σύγκλιση του ηλεκτρικού δικτύου με άλλα συστήματα, όπως με το φυσικό αέριο, μεταφορές και κτιριακές υποδομές και τα τέλος οι αυξανόμενες ανησυχίες σχετικά με την ασφάλεια και την ανθεκτικότητα του ηλεκτρικού δικτύου που απαιτούν την εφαρμογή προληπτικών και μετριαστικών στρατηγικών, συμπεριλαμβανομένων των εκτιμήσεων για εναλλακτικές διαμορφώσεις δικτύου (π.χ. μικρό-δίκτυα), για την αντιμετώπιση κυβερνο και φυσικών απειλών αποτελούν κάποιους από τους παράγοντες που ου διαμορφώνουν την ανάπτυξη του Smart Grid. Δεν μπορούμε βέβαια να μην αναφέρουμε και τους παράγοντες που οδηγούν σε μονόδρομο στη δημιουργία του (Smart Grid) και είναι οι ακόλουθη:

I. Η αύξηση της ζήτησης της ηλεκτρικής ενέργειας καθώς δημιουργήθηκαν και θα δημιουργηθούν και άλλες νέες ανάγκες στους καταναλωτές.
II. Το Παγκόσμιο πρόβλημα κλιματικής αλλαγής.

III. Η έλλειψη της δυνατότητας αποθήκευσης της παραγόμενης ενέργειας και η κατά βούληση χρήση της.
IV. Η περιορισμένη παραγωγή ηλεκτρικής ενέργειας, (χωρίς της χρήση/διαχείριση της ηλεκτρικής ενέργειας των ΑΠΕ)
V. Ο μονόδρομος επικοινωνίας των υποσυστημάτων και των κέντρων διαχείρισης,
VI. Η μείωση των αποθεμάτων των ορυκτών καυσίμων,
VII. Η εμφάνιση βλαβών καθώς το υπάρχον δίκτυο είναι παλαιωμένο.

Λόγω όλων των παραπάνω παραγόντων, αλλά και εξαιτίας των απαιτήσεων που αυξάνονται, θα πρέπει να γίνει αντικατάσταση των παλαιών υλικών, να συνδεθεί με τις ΤΠΕ και να επεκταθεί το ήδη υπάρχον δίκτυο. Έτσι με τη δημιουργία του Smart Grid της επόμενης γενιάς με τη βοήθεια των ΤΠΕ με την εφαρμοσμένη μηχανική του συστήματος ηλεκτρικής ενέργειας θα υπάρξει ορθότερη παρακολούθηση του δικτύου και ποιο ουσιαστικός έλεγχός του.[28]

## 4.2 Διορθωτικές Παρεμβάσεις στο "Παλιό" Ηλεκτρικό Δίκτυο

Σχετικά με την μετάβαση από το "Παλιό" στο "Νέο", θα υπάρχουν μέτρα που θα πρέπει να παρθούν και προφανώς να γίνουν σημαντικές διορθωτικές παρεμβάσεις. Η αντλησιοταμίευση είναι η πιο διαδεδομένη μορφή αποθήκευσης ηλεκτρικής ενέργειας μεγάλης κλίμακας διεθνώς. Για αρκετές δεκαετίες, ήταν μια δημοφιλής επιλογή για τις επιχειρήσεις κοινής ωφέλειας που χρησιμοποιούν ακόμα και σήμερα για την εξομάλυνση των διακυμάνσεων στο ηλεκτρικό δίκτυο. Πλέον όμως, οι διεθνείς εξελίξεις αναπτύσσονται ραγδαία για άλλες μορφές αποθήκευσης, είτε για μεγάλες είτε για μικρές εγκαταστάσεις, και ειδικά για μπαταρίες διαφόρων τύπων. Ενδιαφέρον υπάρχει επίσης για εφαρμογές αποθήκευσης με τη μετατροπή ηλεκτρικής ενέργειας σε αέριο (π.χ. υδρογόνο), στο πλαίσιο των οποίων διερευνάται και η διασύνδεση δικτύων ηλεκτρικής ενέργειας και φυσικού αερίου. Αξίζει να σημειωθεί ότι, εκτός από την ανάγκη για αποθήκευση, θα πρέπει να υλοποιηθεί και ο μετασχηματισμός του συστήματος ηλεκτρικής ενέργειας ώστε να επιτευχθούν επίπεδα διείσδυσης ΑΠΕ της τάξης του 50%. Το γεγονός αυτό θα επιφέρει σημαντικές αλλαγές, που θα έχουν μεγάλο αντίκτυπο διεθνώς στη βιομηχανία της ηλεκτρικής ενέργειας, συμπεριλαμβανομένων των διαχειριστών των ηλεκτρικών δικτύων.

Τα σημαντικότερα μέτρα για τη βελτίωση της ενεργειακής απόδοσης και την εγκατάσταση μονάδων Συμπαραγωγής Ηλεκτρισμού και Θερμότητας έχουν ήδη υλοποιηθεί αρχικά στον βιομηχανικό τομέα. Πιο συγκεκριμένα χρηματοδοτήθηκαν στοχευμένες

παρεμβάσεις εξοικονόμησης ενέργειας και ΑΠΕ. Οι παρεμβάσεις αυτές αφορούσαν την ανάπτυξη και την εφαρμογή των συστημάτων ανάκτησης/υποκατάστασης της ενέργειας στην παραγωγική διαδικασία. Η υποκατάσταση αφορούσε τα υγρά κυρίως καύσιμα με υγραέριο ή φυσικό αέριο. Όσο αφορά τις ΑΠΕ χρηματοδοτήθηκαν κυρίως έργα προμήθειας εξοπλισμού για αυτοπαραγωγή. Τα μέτρα αυτά αφορούν ως επί των πλείστων δράσεις για τη βελτίωση της ενεργειακής απόδοσης των κτιρίων και την προώθηση συσκευών υψηλής ενεργειακής απόδοσης και αποδοτικού εξοπλισμού θέρμανσης.

Επιπλέον, για να προχωρήσουμε στην βελτιστοποίηση του δικτύου θα πρέπει οι τεχνολογικές προκλήσεις στη διάσταση της έρευνας, της καινοτομίας και της ανταγωνιστικότητας και με μια σειρά μέτρων με στόχο τον ενεργειακό σχεδιασμό να χρησιμοποιήσουν τις νέες τεχνολογίες των ΑΠΕ ώστε να ικανοποιηθούν οι ανάγκες της παραγωγής, της μεταφοράς, της διανομής και της αποθήκευσης ηλεκτρικής ενέργειας με τους παρακάτω τρόπους:

- ✓ Τη συνεχή αύξηση της ανταγωνιστικότητας, από πλευράς κόστους παραγωγής, των τεχνολογιών παραγωγής ενέργειας από ΑΠΕ.
- ✓ Την αύξηση της απόδοσης και της ευελιξίας των σταθμών που χρησιμοποιούν συμβατικά καύσιμα σαν συνέπεια του νέου ρόλου που θα παίζουν στην αγορά της ηλεκτρικής ενέργειας.
- ✓ Τη συνολική αύξηση των αναγκών ευελιξίας του συστήματος ηλεκτρικής ενέργειας και η αποθήκευσή της.
- ✓ Την ενσωμάτωση των τεχνολογιών ΑΠΕ στα δίκτυα διανομής στον έλεγχο της κατανάλωσης καθώς και η ενσωμάτωση των τεχνολογιών Πληροφορικής και Επικοινωνιών.
- ✓ Τη περαιτέρω διείσδυση των τεχνολογιών της ηλιακής ενέργειας σε όλες τις χρήσεις.
- ✓ Την υιοθέτηση νέων τεχνολογιών και μεθόδων αύξησης της ενεργειακής απόδοσης στον τριτογενή τομέα.
- ✓ Τη μείωση των απωλειών των δικτύων και η βελτιστοποίηση της λειτουργίας τους.
- ✓ Τη μείωση του κόστους τεχνολογιών της μικρής αποθήκευσης ηλεκτρικής ενέργειας και της ηλεκτροκίνησης.
- ✓ Την ανάπτυξη των έξυπνων υποδομών για την ηλεκτροκίνηση[9].

## 4.3 Βελτιστοποίηση του "Εξυπνου" Ηλεκτρικού Συστήματος

Η AI έχει πολλές δυνατότητες που μπορούν να χρησιμοποιηθούν στον τομέα της τεχνολογίας πληροφοριών και της ασφάλειας στον κυβερνοχώρο. Τα τυπικά συστήματα κυβερνοασφάλειας δεν μπορούν να εντοπίσουν μεγάλο αριθμό των απειλών και η AI αναμένεται να είναι ένας πολύτιμος σύμμαχος σε αυτή τη μάχη. Η AI μπορεί να χρησιμοποιηθεί στην ασφάλεια στον κυβερνοχώρο για να βοηθήσει στην αποφυγή πιθανών απωλειών και να αυξήσει το επίπεδο ασφάλειας ενός οργανισμού. Η ML μπορεί να βοηθήσει στον εντοπισμό μοτίβων στα δεδομένα που οδηγούν σε πιο ακριβείς και αυτοματοποιημένες διαδικασίες για την προστασία δεδομένων. Η ασφάλεια της AI έχει πολλά οφέλη και δεν πρέπει να αγνοηθούν.

- ✓ **Ασφάλεια παραγωγής δεδομένων (Data generation security):** Αρχικά συνοψίζουμε διάφορα δεδομένα πηγές στο σύστημα Smart Grid και τις κατηγοριοποιούμε στα: παραγωγή, μεταφορά και διανομή ηλεκτρικής ενέργειας, και διαχείριση φορτίου.
- ✓ **Ασφάλεια απόκτησης δεδομένων (Data acquisition security):** Η διαδικασία απόκτησης δεδομένων βασίζεται στα υποκείμενα πρωτόκολλα επικοινωνίας για τη συγκέντρωση των δεδομένων έως και την αποθήκευση των δεδομένων. Επομένως, τα γενικά πρωτόκολλα επικοινωνίας απευθύνονται στα ζητήματα ασφάλειας συλλογής δεδομένων και διατήρησης της ιδιωτικής ζωής κοινή τη χρήση δεδομένων.
- ✓ **Ασφάλεια αποθήκευσης δεδομένων (Data storage security):** Μεγάλος όγκος και αξιόπιστα δεδομένα Οι αποθηκευτικοί χώροι είναι απαραίτητοι για τις ροές δεδομένων σε ένα Smart Grid. Σε αυτό το μέρος, υπάρχουν διαφορετικοί μηχανισμοί αποθήκευσης δεδομένων και ελέγχουμε τις σχετικές εργασίες ασφάλειας αποθήκευσης δεδομένων.
- ✓ **Ασφάλεια επεξεργασίας δεδομένων (Data processing security):** Τα δεδομένα του Smart Grid υποβάλλονται σε επεξεργασία σε ορισμένες εφαρμογές. Είναι απαραίτητο να τονιστεί η ασφάλεια και οι μηχανισμοί εφαρμογών στο Smart Grid.
- ✓ **Αναλύσεις ασφαλείας (Security analytics):** Από την άποψη της ασφάλειας, τα δεδομένα μπορούν να είναι και το πρόβλημα αλλά και η λύση. Με άλλα λόγια, η ανάλυση των δεδομένων θα μπορούσε επίσης να παρέχει πολλές υποσχόμενες λύσεις για τη διασφάλιση της ασφάλειας.
- ✓ **Επεξεργασία μεγάλου όγκων δεδομένων (Processing large volumes of Data):** Το μεγαλύτερο πλεονέκτημα της χρήσης της AI αναφορικά με τη διατήρηση της ασφάλειας των δεδομένων και των πληροφοριών είναι ότι μπορεί να επεξεργαστεί γρήγορα πολλά δεδομένα. Αυτό βέβαια μπορεί να επιτευχθεί με την χρήση αλγορίθμων για τον

εντοπισμό απειλών ασφαλείας. Βέβαια τα επεξεργασμένα δεδομένα καλύπτουν ένα ευρύ φάσμα στοιχείων, συμπεριλαμβανομένων των κοινόχρηστων αρχείων, των email, καθώς και διάφορα μοτίβα κυβερνοεγκληματικής δραστηριότητας. Η ικανότητα αυτή της επεξεργασίας τεράστιων ποσοτήτων δεδομένων δεν συγκρίνεται με τις ανθρώπινες δυνατότητες επεξεργασίας. Η ταχύτητα της ανθρώπινης προσπάθειας είναι πολύ πίσω από την ταχύτητα της AI, η οποία είναι πιο εμπεριστατωμένη και επεξεργάζεται τα δεδομένα πιο γρήγορα, εντοπίζοντας ανωμαλίες και κινδύνους.

- ✓ **Ασφάλεια πληροφοριών (Data Security):** Η AI μπορεί να βοηθήσει στον εντοπισμό σφαλμάτων ασφαλείας στους πόρους πληροφοριών ενός οργανισμού. Η AI δεν καταπονείται αλλά δεν αποσπάται και η προσοχή της κάνοντας τα ίδια πράγματα ξανά και ξανά. Αυτό σημαίνει ότι τα ποσοστά σφάλματος είναι σημαντικά χαμηλότερα από αυτά του ανθρώπου. Ως επί το πλείστων οι ομάδες αυτές που διαχειρίζονται την ασφάλεια των πληροφοριών δυσκολεύονται να αξιολογήσουν τον κίνδυνο όλων των δεδομένων. Η επεξεργασία δεδομένων με τη χρήση μηχανισμών AI βοηθά στον ποιο γρήγορο εντοπισμό απειλών. Αυτό επιτρέπει στις ομάδες αυτές να εστιάζουν σε άλλες πιο σημαντικές εργασίες, περιορίζοντας ταυτόχρονα τον αριθμό των σφαλμάτων.
- ✓ **Διακρίνοντας τις κυβερνοαπειλές (Distinguishing cyber threats):** Οι "εγκληματίες" του κυβερνοχώρου αναζητούν πάντα νέους τρόπους για να εισέλθουν και να εκμεταλλευτούν συστήματα και συνεχώς εξελίσσουν τις τεχνικές τους. Έχουν κάνει σημαντικά άλματα στις τεχνολογίες που χρησιμοποιούν για να καλύψουν τα ίχνη τους, αλλά οι επιθέσεις τους μπορούν ακόμα να ανιχνευθούν χρησιμοποιώντας την AI. Η AI μπορεί να εντοπίσει ακόμη και την παραμικρή "επικίνδυνη" κίνηση ή ενέργειες που θα μπορούσαν να είναι σημάδια κακόβουλης δραστηριότητας. Ως εκ τούτου, η AI αποφέρει πολλά οφέλη αναφορικά με την ασφάλεια στον κυβερνοχώρο. Όταν η ανίχνευση απειλών είναι αυτοματοποιημένη, είναι εφικτός ο γρήγορος εντοπισμός πιθανών απειλών και λήψη των κατάλληλων μέτρων. Τέλος, η AI μπορεί να προσαρμόζεται ανάλογα και να μαθαίνει από άλλες πηγές, όπως η εμπειρία κ.α. πρότυπα, ώστε να χρησιμοποιηθεί ως υποβοήθησα δύναμη στην ασφάλεια στον κυβερνοχώρο. Η AI χρησιμοποιεί συλλογισμούς για να εντοπίσει ύποπτους συνδέσμους, αρχεία ή και απειλές δεδομένων ώστε να λάβει τα κατάλληλα μέτρα για την εξάλειψή των.
- ✓ **Πιο γρήγορος εντοπισμός & μικρότερος χρόνος απόκρισης (Faster detection & shorter response time):** Η AI είναι ένα χρήσιμο εργαλείο ώστε να γίνει ποιο γρήγορος ο εντοπισμός πιθανών προβλημάτων. Η AI βοηθά στην επεξεργασία του αυξημένου

φόρτου εργασίας της απόκρισης σε πολλαπλές ειδοποιήσεις ασφαλείας. Ενώ οι επαγγελματίες ασφάλειας πληροφοριών εξακολουθούν να υπαγορεύουν τη σειρά των υποθέσεων, ενώ το μεγαλύτερο μέρος της ανάλυσης γίνεται από την AI. Ο ανθρώπινος παράγοντας στον αντίποδα χρειάζεται περισσότερο χρόνο. Αυτές οι στρατηγικές μπορούν να δημιουργήσουν καλύτερη ασφάλεια στον κυβερνοχώρο. Τα μέτρα ασφαλείας του οργανισμού θα μπορούσαν να βελτιωθούν με την εφαρμογή αυτού.

- ✓ **Εξάλειψη προηγμένων τεχνικών εισβολής (Elimination of Advanced Hacking Techniques):** Οι "εγκληματίες" του κυβερνοχώρου χρησιμοποιούν προηγμένες τεχνικές για να διεισδύσουν σε δεδομένα και δίκτυα. Αυτού του είδους οι προηγμένες τεχνικές εισβολής είναι αρκετά δύσκολο να εντοπιστούν και να αποφευχθούν. Συνδυάζοντας την έλλειψη ειδικών σε θέματα ασφάλειας πληροφοριών παγκοσμίως και την ικανότητα των εγκληματιών του κυβερνοχώρου να εκμεταλλεύονται την ανθρώπινη ψυχολογία, αυτές οι απειλές μπορεί να έχουν σοβαρές συνέπειες. Οι εγκληματίες του κυβερνοχώρου μπορούν να έχουν γρήγορη πρόσβαση σε ευαίσθητες πληροφορίες μέσω της έξυπνης εκμετάλλευσης των συναισθημάτων του ανθρώπου. Ένας άλλος τρόπος προστασίας από επιθέσεις στον κυβερνοχώρο είναι η χρήση social honeypot. Αυτές οι μέθοδοι (όπως δολώματα) χρησιμοποιούνται ώστε να προσπαθήσουν να εντοπίσουν τους "εγκληματίες", να καταλάβουν τις μεθόδους και τις προηγμένες τεχνικές.
- ✓ **Ασφαλής έλεγχος ταυτότητας (Secure Authentication):** Αρκετές ιστοσελίδες προτρέπουν τους επισκέπτες να εγγραφούν συμπληρώνοντας φόρμες ή ακόμα και να πραγματοποιήσουν ηλεκτρονικές πληρωμές πριν αποκτήσουν πλήρη πρόσβαση στον ιστότοπο. Αυτοί οι οργανισμοί χρειάζονται περισσότερη ασφάλεια. Η AI μπορεί να βοηθήσει να γίνει πιο ασφαλής η διαδικασία ελέγχου ταυτότητας χρησιμοποιώντας τη φυσική αναγνώριση.

Η AI βασίζεται σε τρόπους ταυτοποίησης όπως reCAPTCHA, σαρωτές δακτυλικών αποτυπωμάτων ή ακόμα και αναγνώριση προσώπου. Η ιστοσελίδα με τη βοήθεια αυτού του προγράμματος ελέγχει τα δεδομένα και στη συνέχεια προχωρά στη σύνδεση. Αυτός ο έλεγχος ταυτότητας είναι εξαιρετικά σημαντικός για ιστοσελίδες που επεξεργάζονται ευαίσθητα δεδομένα. Η AI είναι ένα βήμα ποιο κοντά ώστε να διασφαλίσει να δεδομένα και οι πληροφορίες του οργανισμού δεν θα παραβιαστούν κυβερνοεγκληματίες. [26]

## 4.4 Θέματα ασφάλειας των ασύρματων δικτύων και των έξυπνων μετρητών

Υπάρχουν πολλές τεχνολογίες και εφαρμογές που έχουν ενσωματωθεί για να λειτουργούν ως μία σε ένα σύστημα AMI, όπως οι έξυπνοι μετρητές, οι υποδομές επικοινωνίας ευρείας περιοχής και τα τοπικά δίκτυα (HAN). Τα ασύρματα δίκτυα βέβαια είναι αυτά που χρησιμοποιούνται ευρέως σε ένα Smart Grid καθώς είναι ποιο πρακτικά και έχουν χαμηλότερο κόστος. Μεταξύ των εργασιών που μπορεί να κάνει ένας έξυπνος μετρητής είναι η τιμολόγηση, η συλλογή δεδομένων κατανάλωσης, Net-metering, έλεγχος απώλεια ισχύος και ειδοποίηση του κέντρου ελέγχου, απομακρυσμένη ενεργοποίηση/απενεργοποίηση λειτουργιών, παρακολούθηση, παραβίαση μετρητών και ανίχνευση κλοπής ενέργειας, μείωση κόστους σε λανθασμένες εκτιμήσεις λογαριασμών. Τα πολλαπλά μονοπάτια επικοινωνίας που διαθέτουν μπορούν να δημιουργηθούν ευπάθειες και κατάρρευση ορισμένων κόμβων επικοινωνίας. Αν και όλες αυτές οι εργασίες μπορεί να μην υποστηρίζονται από αυτόν τον συγκεκριμένο μετρητή, η γενική ιδέα είναι ότι οι έξυπνοι μετρητές καθιστούν δυνατή την προσθήκη κάποιου είδους «νοημοσύνης» στο δίκτυο και στα επιμέρους χαρακτηριστικά κάθε οικιακού καταναλωτή. Οι κύριες παράμετροι για τη διαχείριση της πλευράς της ζήτησης δεν είναι η ωριαία κατανάλωση ενέργειας, αλλά η μέγιστη ζήτηση. Κάθε περιοχή εφαρμογής θα έχει διαφορετικές ανάγκες, επειδή οι πελάτες τους θα έχουν επίσης διαφορετικές απαιτήσεις. Το ζήτημα που σχετίζεται με το απόρρητο είναι αυτό που χρίζει ιδιαίτερη προσοχή. Ως εκ τούτου, ενώ αυτό το έξυπνο σύστημα θα μπορούσε να προσφέρει πολλά μεγάλα οφέλη, υστερεί σημαντικά στο επίπεδο του απορρήτου. Ο έξυπνος μετρητής είναι το βασικό στοιχείο στην πλευρά του πελάτη σε ένα σύστημα AMI. Ένας έξυπνος μετρητής είναι συνήθως ηλεκτρικός μετρητής που καταγράφει την κατανάλωση ηλεκτρικής ενέργειας σε διαστήματα μιας ώρας ή λιγότερο και μεταδίδει αυτές τις πληροφορίες καθημερινά στο βοηθητικό πρόγραμμα ελέγχου Συγκεκριμένα, οι έξυπνοι μετρητές βασίζονται συνήθως σε μικρό-ελεγκτές και υποστηρίζουν λειτουργίες ψηφιακής επεξεργασίας σήματος για χαρακτηριστικά μέτρησης ποιότητας ισχύος, με κοινόχρηστη μνήμη (RAM, ROM και flash), θύρες επικοινωνίας (π.χ. USB, Ethernet, οπτικό Ethernet, σειριακή υποδοχή) και δυνατότητες επικοινωνίας όπως π.χ. Καθολικός ασύγχρονος δέκτης/πομπός (UART), RS-485, Wi-Fi και ZigBee.

Το απόρρητο των χρηστών του έξυπνου δικτύου είναι ένα πολύ σημαντικό ζήτημα. Η χρήση των τεχνολογιών (ΤΠΕ) στη λειτουργία του έξυπνου δικτύου εισάγουν

διαφορετικούς τύπους ανησυχιών για το απόρρητο. Εξαρτάται από μέθοδος με τον οποίο ο καταναλωτής χρησιμοποιεί την ηλεκτρική ενέργεια.

- Τα δεδομένα του χρήστη ή το προφίλ του καταναλωτή ενδέχεται να συλλέγονται κακόβουλα μέσω της χρήσης ηλεκτρικής ενέργειας.
- Το σύστημα επικοινωνιών μπορεί να είναι ευάλωτο σε επιθέσεις (DoS), που θα μπλόκαραν τη μεταφορά των μετρήσεων.
- Υπάρχουν κενά ασφαλείας που θα μπορούσαν να επιτρέψουν στους hacker να έχουν πρόσβαση στους έξυπνους μετρητές και να τροποποιούν τα δεδομένα του χρήστη ή να στέλνουν εντολές που θα προκαλούσαν την αποσύνδεση των μετρητών.[31]

#### 4.4.1. Ιδιότητες ασφάλειας

Ένα Smart Grid, πρέπει να υποστηρίζει όλες ή μερικές από τις ακόλουθες τέσσερις λειτουργίες: παραγωγή, διανομή, μεταφορά, και έλεγχο της ηλεκτρικής ενέργειας. Για την σωστή λειτουργία του απαιτείτε ένα επίπεδο ICT για την ενεργοποίηση ενός αμφίδρομου ασφαλούς καναλιού επικοινωνίας, όπου οι κύριοι στόχοι ασφαλείας είναι η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα και η διαθεσιμότητα, και αναλυτικότερα αναφέρονται παρακάτω:

- **Εμπιστευτικότητα (Confidentiality):** Οι οικιακές ηλεκτρικής συσκευές καθώς θα στέλνουν τις μετρήσεις στον έξυπνο μετρητή θα πρέπει να υπάρχει πρόληψη της μη εξουσιοδοτημένης αποκάλυψης πληροφοριών προκειμένου να διασφαλιστεί η ασφάλεια των εργαζομένων και του κοινού. Εάν το απόρρητο των οικιακών χρηστών διακυβεύεται, τότε η εμπιστευτικότητα παραβιάζεται αυτόματα. Για τη διασφάλιση της εμπιστευτικότητας, χρησιμοποιούνται διάφορα συστήματα για το HAN, π.χ. ομομορφική κρυπτογράφηση, τυφλή υπογραφή, συνάθροιση εντός δικτύου κ.λπ. Επομένως, ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλυφθούν σε μη εξουσιοδοτημένα άτομα, οντότητες ή προγράμματα. Τέλος, δεν πρόκειται μόνο για την αποτροπή της μη εξουσιοδοτημένης διαρροής των δεδομένων από τον τελικό χρήστη προς τον πάροχο μέσω του έξυπνου μετρητή, αλλά και για το γεγονός ότι τα ίδια τα δεδομένα θα υπάρχουν καταχωρημένα και στο σύστημα.
- **Ακεραιότητα (Integrity):** Οι έξυπνες συσκευές καθώς θα στέλνουν πανομοιότυπες καταναλώσεις θα είναι φυσικά ασφαλής αλλά θα είναι ευάλωτες σε επιθέσεις man-in-middle και έτσι θα τεθούν σε κίνδυνο πολύτιμες πληροφορίες και θα διακυβευτεί η ακεραιότητα των δεδομένων και ενδέχεται να ληφθούν λανθασμένες αποφάσεις για τη διαχείριση και τον έλεγχο του δικτύου. Τα δεδομένα που μεταδίδονται μέσω του δικτύου

επικοινωνιών δεν πρέπει να παραβιάζονται με κακόβουλο τρόπο. Επίσης, τα ευαίσθητα δεδομένα δεν θα πρέπει να διαγράφονται ή να δημιουργούνται νέα δεδομένα με μη εξουσιοδοτημένο και μη ανιχνεύσιμο τρόπο.

- **Ανωνυμία (Anonymity):** Η ανωνυμία αναφέρεται στην κατάσταση όπου η πραγματική ταυτότητα ενός ατόμου παραμένει μυστική. Κατά την κοινή χρήση μυστικών σημάτων ελέγχου ή την ανάγνωση, μια συσκευή μπορεί να προστατεύσει την πραγματική τους ταυτότητα από άλλες συσκευές. Ακόμη και μια συσκευή ή κάποιος έξυπνος μετρητής δεν μπορεί να αναγνωρίσει άλλες συσκευές που επικοινωνούν μαζί του σε ένα HAN. Ο σκοπός της ανωνυμίας είναι να κρύψει κανείς τη δική του ταυτότητα από συσκευή σε συσκευή, από συσκευή σε έξυπνο μετρητή, κ.α..
- **Διαθεσιμότητα (Availability):** Η διαθεσιμότητα υποδηλώνει την ικανότητά του να έχει διαθέσιμα τα δεδομένα, τις εφαρμογές και τα συστήματα και να παρέχει πρόσβαση στα πληροφοριακά συστήματα γρήγορα και χωρίς καθυστέρηση όταν χρειάζεται από εξουσιοδοτημένους φορείς. Η διαθεσιμότητα διακυβεύεται εάν κάποιος προσποιείται ότι είναι εξουσιοδοτημένος χρήστης για να έχει πρόσβαση στο σύστημα και να κάνει το δίκτυο απασχολημένο. Η επίθεση (DDoS) είναι η πιο βασική επίθεση διαθεσιμότητας. Μια επίθεση DDoS σε συσκευές IoT συμβαίνει λόγω έλλειψης των μέτρων ασφαλείας. Οι εξουσιοδοτημένοι χρήστες του δικτύου πρέπει να έχουν πρόσβαση στις υπηρεσίες του όταν τις χρειάζονται.

Ποιο συγκεκριμένα οι στόχοι για τη διασφάλιση του απορρήτου είναι ότι για παράδειγμα όταν τα δεδομένα που θα συλλέγονται από τον έξυπνο μετρητή, όπως η κατανάλωση της ηλεκτρικής ενεργείας από κάθε οικιακή συσκευή (ανά 15 λεπτά), και θα δημιουργείτε μία αναφορά κατανάλωσης που θα αποστέλλετε στην εταιρεία παροχής να μην υπάρχει ακόμα και η ελάχιστη πιθανότητα διαρροής αυτών των δεδομένων.

Έτσι, καθώς αυτό αποτελεί απειλή για την ασφάλεια καθώς και την ιδιωτικότητα του έξυπνου σπιτιού και για να μπορέσουμε να διατηρήσουμε την ιδιωτική μας ζωή και την ασφάλειας, η αναφορά κατανάλωσης της ηλεκτρικής ενέργειας θα πρέπει να κρυπτογραφείται είτε σε επίπεδο συσκευής είτε πριν φύγει από το HAN.

Για το δίκτυο ηλεκτρικής ενέργειας, η διαθεσιμότητα είναι το πιο σημαντικό ζήτημα ασφάλειας. Αυτά τα συστήματα παρακολουθούν συνεχώς την κατάσταση του ηλεκτρικού δικτύου και η απώλεια των επικοινωνιών τους μπορεί να προκαλέσει η απώλεια ισχύος. Το δεύτερο πιο σημαντικό ζήτημα ασφάλειας στο Smart Grid είναι η διασφάλιση της ακεραιότητας των δεδομένων. Η ποιότητα της ηλεκτρικής ενέργειας εξαρτάται από την

ακρίβεια των τρεχουσών πληροφοριών, και αυτό εξαρτάται από την ποιότητα των δεδομένων που συλλέγονται από διάφορους αισθητήρες. Έτσι, η μη εξουσιοδοτημένη τροποποίηση των δεδομένων μπορεί να οδηγήσει σε βλάβη στο ηλεκτρικό δίκτυο. Το τελευταίο πράγμα που θέλουμε είναι να παραβιαστούν τα δεδομένα των καταναλωτών. Εάν παραβιαστούν, σημαίνει ότι και τα άλλα μέρη του συστήματος κινδυνεύουν. Ωστόσο, η εμπιστευτικότητα των πληροφοριών των πελατών και των ηλεκτρονικού εμπορίου είναι το πιο σημαντικό από τα παραπάνω.

**Μερικές ακόμα πλευρές ασφάλειας που είναι απαραίτητες να αναφερθούν είναι οι εξής:**

**Ιδιωτικότητα (Privacy):** Το απόρρητο προβλέπει να μην μπορούν να χρησιμοποιηθούν τα δεδομένα χρήστη για διαφορετικούς σκοπούς χωρίς την έγκριση του χρήστη, να μην μπορεί να διαχειρίζεται από διαφορετικά άτομα και να χρησιμοποιείται μόνο για συγκεκριμένους σκοπούς. Για παράδειγμα, τα δεδομένα κατανάλωσης ενέργειας και οι χρεώσεις να μην μπορούν να χρησιμοποιηθούν για άλλους σκοπούς

**Εξουσιοδότηση (Authorization):** Να μπορεί να διασφαλίζει ότι ένα αντικείμενο με έλεγχο ταυτότητας ή άτομο έχει προκαθορισμένα δικαιώματα για την εκτέλεση ορισμένων λειτουργιών σε ορισμένους πόρους. Για παράδειγμα, ένας εξουσιοδοτημένος διαχειριστής που πρέπει να ρυθμίσει τις παραμέτρους σε έναν έξυπνο μετρητή πρέπει να έχει προκαθορίσει δικαιώματα χρήσης και ελέγχου πρόσβασης.

**Μη αποποίησης ευθύνης (Non repudiation):** Να γίνεται η επαλήθευση ότι μια συγκεκριμένη ενέργεια εκτελείται από ένα σύστημα ή χρήστη και ότι δεν μπορεί να απορριφθεί αργότερα. Ο στόχος της μη αποποίησης είναι να μπορεί να αποδείξει ότι ένα συγκεκριμένο μήνυμα σχετίζεται με ένα συγκεκριμένο άτομο.

**Ταυτοποίηση (Identification):** Είναι η ικανότητα να αναγνωρίζουμε με μοναδικό τρόπο έναν χρήστη ενός συστήματος ή μια εφαρμογή που εκτελείται στο σύστημα.

**Αυθεντικοποίηση (Authentication):** Είναι η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη. Ο έλεγχος ταυτότητας είναι η ικανότητα να αποδεικνύεται ότι ένας χρήστης ή μία εφαρμογή είναι εκείνο το πρόσωπο ή αυτή η εφαρμογή που ισχυρίζεται ότι είναι και εφόσον αποδεικνύει την ταυτότητα του χρήστη ή υπολογιστή-πελάτη να συνδεθεί.

**Έλεγχος πρόσβασης (Access Control):** Αναφέρεται στη διαχείριση της πρόσβασης σε πόρους του συστήματος και του δικτύου. Με αυτόν τον τρόπο, μόνο οι πιστοποιημένοι χρήστες μπορούν να έχουν πρόσβαση σε συγκεκριμένους πόρους με βάση τις πολιτικές της εταιρείας που συχνά περιλαμβάνει και έλεγχο ταυτότητας.

**Έλεγχος (Auditing):** Είναι μια συστηματική αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος με τη μέτρηση του πόσο καλά ταιριάζει σε ένα σύνολο καθορισμένων κριτηρίων. Ένας ολοκληρωμένος έλεγχος που αξιολογεί την ασφάλεια του συστήματος, τις διαδικασίες, τη διαχείριση των πληροφοριών και το λογισμικό. Ο έλεγχος που διασφαλίζει ότι τόσο οι χρήστες όσο και οι διαχειριστές θα πρέπει να συμμορφώνονται και να συμμετέχουν στις πολιτικές ασφαλείας.

**Αξιοπιστία/Συνέπεια (Reliability/Consistency):** Αναφέρεται στην αξιοπιστία του συστήματος που το κάνει αυτό που αναμένεται ή που έχει σχεδιαστεί να κάνει το σύστημα.

**Ευθύνη (Accountability):** Σημαίνει ότι πρέπει να παρέχονται η ιχνηλασιμότητα κάθε ενέργεια του κάθε χρήστη που εκτελούνται σε ένα σύστημα. Η χρήση, η αναγνώριση και ο έλεγχος ταυτότητας του κάθε χρήστη χρίζει λογοδοσίας.[21,30]

### 4.4.2. Αντιμετώπιση ασφάλειας (security)

Τα περιστατικά κυβερνοασφάλειας δείχνουν ότι υπάρχει μεγάλος αριθμός πιθανών επιθέσεων στον κυβερνοχώρο και είναι όλο και πιο πιθανές σε συστήματα τόσο περίπλοκα όσο το έξυπνο δίκτυο. Οι μηχανικοί ενέργειας χρησιμοποιούν τον όρο ασφάλεια για να περιγράψουν το μεγαλύτερο μέρος της ικανότητας του δικτύου να αντέχει σε απρόσμενες βλάβες, όπως φυσικά αίτια, blackout(s) και απώλειες εξαρτημάτων συστήματος λόγω ανθρώπινων φυσικών ή ηλεκτρονικών επιθέσεων.

Βέβαια, ο όρος ασφάλεια περιλαμβάνει την αξιοπιστία των συστημάτων, αλλά και την αξιοπιστία των συστημάτων επικοινωνίας που είναι ενσωματωμένα στα συστήματα ισχύος εξυπηρέτησης. Αυτό έχει ως αποτέλεσμα, το ποιο ουσιώδες να είναι οι επικοινωνίες που θα πρέπει να προστατεύονται από οποιεσδήποτε κακόβουλες εισβολές και να πρέπει να αναπτυχθεί ένα σύστημα παρακολούθησης και ελέγχου υψηλότερου επιπέδου προς όφελος των χρηστών και των διαχειριστών του δικτύου.

### 4.4.3. Τρόπος αντιμετώπισης ασφάλειας

Για να καταφέρουμε να έχουμε την μέγιστη δυνατή ασφάλεια σε ένα Smart Grid υπάρχουν οι παρακάτω απαραίτητες προϋποθέσεις:

- **Τα συστήματα ασφαλείας** όπου γίνεται η διαχείριση κλειδιών, ο έλεγχος ταυτότητας, η εξουσιοδότηση και η περιμετρική προστασία που συμβάλλουν στην προστασία των ιδιοτήτων από διάφορες επιθέσεις.
- **Τα συστήματα εντοπισμού** όπου υπάρχει ο μηχανισμός αναγνώρισης κακόβουλων δραστηριοτήτων και επιθέσεων.

- **Τα συστήματα απόκρισης** όπου υπάρχουν τοίχοι προστασίας ώστε να περιοριστεί η ροή δεδομένων και πληροφοριών του συστήματος προς και από τους αντιπάλους και έτσι να αντιμετωπιστεί μία εισβολή.

#### 4.4.4. Περαιτέρω λύσεις για την ασφάλεια του Έξυπνου Δικτύου

Προκειμένου να διατηρηθεί η ασφάλεια στο Smart Grid, πρέπει να ενσωματώνονται ισχυροί μηχανισμοί ελέγχου ταυτότητας σε ετήσια βάση και πρέπει να εκτελείται κατά καιρούς αξιολόγηση ευπάθειας, σε ορισμένες περιπτώσεις οι ενέργειες των χρηστών μπορούν να ανοίξουν ευπάθειες. Οι τεχνολογίες πληροφοριών που σχετίζονται με το Smart Grid θα πρέπει να μπορούν να αναβαθμιστούν και, τέλος, να δημιουργηθούν εταιρείες που θα παρακολουθούν μόνο ζητήματα ασφάλειας στη μετάδοση δεδομένων.

#### 4.4.5. Στρατηγικές σχεδιασμού ασφάλειας

Οι τυπικές υπηρεσίες ασφαλείας πρέπει να μπορεί να ενσωματώνει τη διαχείριση της ασφάλειας, λειτουργίες ασφαλείας και άλλες τεχνολογίες ασφαλείας. Οι στρατηγικές αυτές αποτελούνται από στρατηγικές σχεδιασμού μιας αποτελεσματικής λύσης ασφάλειας για το Smart Grid και είναι οι εξής:

- **Επεκτασιμότητα (Scalability):** Είναι η ικανότητα του συστήματος να αυξομειώνει την ικανότητα προστασίας των συστημάτων αυτοματισμού δικτύου ηλεκτρικής ενέργειας. Αναφέρεται επίσης στην ικανότητα να αυξομειώσει το μέγεθος ή και την ικανότητα του κόστους με ελάχιστη επίπτωση στα οικονομικά της επιχείρησης. Κατά τη διάρκεια του σχεδιασμού, η επεκτασιμότητα πρέπει να ληφθεί υπόψη ώστε να διατηρηθεί το ίδιο επίπεδο ανάπτυξης. Η απόδοση ασφαλείας πρέπει να παραμένει αμείωτη καθώς η υποδομή αυξάνεται σε φορτίο και όγκο στο σύστημα.
- **Επεκτατικότητα (Extensibility):** Είναι η δυνατότητα του συστήματος που περιλαμβάνει μηχανισμούς ώστε να μπορέσει να επεκταθεί χωρίς να χρειάζεται να γίνουν σημαντικές αλλαγές στην υποδομή του δικτύου. Εφόσον, βέβαια μπορούν πάντα να βρεθούν νέες μέθοδοι κυβερνοεπίθεσης, το πλαίσιο ασφαλείας πρέπει να διασφαλίζει την επεκτασιμότητα του. Πρέπει επίσης να θεωρηθεί ότι η προτεινόμενη λύση είναι σε θέση να χειριστεί οποιαδήποτε μελλοντική κατάσταση του δικτύου ηλεκτρικής ενέργειας, συμπεριλαμβανομένων των νέων τεχνολογιών και πρωτοκόλλων επικοινωνίας
- **Διαλειτουργικότητα (Interoperability):** Είναι η ιδιότητα που αναφέρεται στην ικανότητα διαφορετικών συστημάτων να συνεργάζονται. Δεδομένου ότι τα συστήματα

αυτοματισμού του δικτύου χρησιμοποιούν διάφορες τεχνολογίες σε σχέση με τον εξοπλισμό, τα λειτουργικά συστήματα και τα πρωτόκολλα επικοινωνιών, το πλαίσιο και τα εξαρτήματα ασφαλείας πρέπει να είναι σε θέση συνεργάζονται ανεξάρτητα από την τεχνολογία στην οποία βρίσκονται εκτελούνται ή αναπτύσσονται.

- **Μη παρεμβατικότητα (Nonintrusiveness):** Είναι η ικανότητα του συστήματος να υποκινείται σε δραστηριότητες ασφαλείας χωρίς να θέτει σε κίνδυνο τη λειτουργία ελέγχου και την απόδοση. Αυτή είναι απαίτηση προϋπόθεση ώστε να αντιμετωπίσει την πρόκληση που αντιμετωπίζουν τα υπάρχοντα, παλαιού τύπου, συστήματα και ενδέχεται να μην έχει την δεσμευμένη υπολογιστική ισχύ για την εκτέλεση λειτουργιών ασφαλείας. Για αυτό το λόγο, θα πρέπει να εξεταστεί η ενσωμάτωση της νέας λύσης ασφάλειας στην υπάρχουσα.
- **Ευελιξία (flexibility):** Είναι η ικανότητα γρήγορης και αποτελεσματικής προσαρμογής στις μεταβαλλόμενες ανάγκες κατά την αναβάθμιση ή τη λειτουργία σε πραγματικό χρόνο. Δεδομένου ότι, σε αντίθεση με το σχετικά στατικό αυτοματισμό του υπάρχοντος δικτύου, το μελλοντικό έξυπνο δίκτυο μπορεί να είναι πολύ δυναμικό λόγω της συμμετοχής περισσότερων συμμετεχόντων, της ευελιξίας, των επεκτάσεων στο σύστημα που μπορούν να γίνουν είτε με την προσθήκη ή την αφαίρεση νέας λειτουργικότητας ή μέσω της τροποποίησης της υπάρχουσας λειτουργικότητας και της προσθήκης ή της αφαίρεσης νέων οντοτήτων στον αυτοματισμό του δικτύου και έτσι να κατασκευαστεί ποιο εύκολα. [15]

## 4.5. Τρόπος Ασφάλισης του Έξυπνου Δικτύου

Η ασφάλεια είναι απαραίτητη κατά την κατασκευή ενός κατανεμημένου συστήματος, προκειμένου να δημιουργηθεί μια αξιόπιστη και ασφαλής πλατφόρμα. Ο σκοπός του σχεδιασμού ενός κατανεμημένου συστήματος είναι να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών που μεταδίδονται.

Υπάρχουν διάφοροι τρόποι με τους οποίους ένα σύστημα μπορεί να τεθεί σε κίνδυνο.

- Η υποκλοπή μπορεί να συμβεί όταν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση σε μια υπηρεσία ή μια πηγή δεδομένων, όπως η παράνομη αντιγραφή δεδομένων μετά την είσοδο σε ένα σύστημα αρχείων.
- Μπορεί να προκύψει διακοπή όταν τα αρχεία είναι κατεστραμμένα ή διαγράφονται ως αποτέλεσμα επίθεσης ή ιού.
- Η τροποποίηση μπορεί να συμβεί όταν κάποιος άλλος παραποιεί τα δεδομένα ή κάνει αλλαγές στο σύστημα.
- Μπορούν να δημιουργηθούν δεδομένα που συνήθως δεν υπάρχουν, κάτι που στη συνέχεια επιτρέπει την παραγωγή.

Ο αρχικός στόχος της ασφάλειας του Smart Grid είναι η διασφάλιση της εμπιστευτικότητας, δηλαδή η διασφάλιση ότι μόνο όσοι είναι εξουσιοδοτημένοι μπορούν να έχουν πρόσβαση σε δεδομένα και πληροφορίες. Για να μπορέσουμε να επιτύχουμε αυτόν τον στόχο είναι η χρήση της κρυπτογράφησης. Με την κρυπτογράφηση, είμαστε σε θέση να διασφαλίσουμε την εμπιστευτικότητα και τον έλεγχο της ταυτότητας των χρηστών. Σε αυτή τη λύση θα πρέπει να χρησιμοποιηθεί ένας αλγόριθμος για τη μετατροπή του αρχικού μηνύματος σε μια ακατανόητη μορφή, και με αυτόν τον τρόπο το μήνυμα να μπορεί να αποκωδικοποιηθεί μόνο από τον προοριζόμενο παραλήπτη και εφόσον είμαστε σίγουροι ότι έχει φτάσει σε αυτόν. Η κρυπτογραφία χωρίζεται σε δύο κατηγορίες: τη συμμετρική και την ασύμμετρη. Η συμμετρική χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος, ενώ η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση του μηνύματος. Οι κρυπτογραφικές τεχνικές, όπως η κρυπτογράφηση, ο έλεγχος ταυτότητας και οι ψηφιακές υπογραφές, είναι οι πιο αποτελεσματικοί τρόποι για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Για να επιτύχουμε την υψηλή ασφάλεια δεδομένων, θα πρέπει να προχωρήσουμε σε κρυπτογράφηση δεδομένων.

#### 4.5.1. Ασφάλεια του Κυβερνοχώρου & των δικτύων επικοινωνίας του Έξυπνου Δικτύου

Γενικά, η ύπαρξη ασφάλειας σε ενσύρματο ή ασύρματο δικτύου, είναι κρίσιμης σημασίας επειδή καθώς μεταφέρονται προσωπικά ή ακόμα και εμπιστευτικά δεδομένα που δεν πρέπει να κοινοποιηθούν ή να γίνουν γνωστά σε τρίτους. Αυτός είναι ο κύριος λόγος για τον οποίο χρησιμοποιούνται εργαλεία και ειδικές τεχνικές, καθώς θα πρέπει να διασφαλιστεί η ακεραιότητα των δεδομένων και να υπάρχει μια ασφαλή σύνδεση, το οποίο επιτυγχάνεται με τη θέσπιση εμπιστευτικότητας δεδομένων, ακεραιότητας δεδομένων και διαθεσιμότητας δεδομένων για τα μεταδιδόμενα δεδομένα.

#### 4.5.2. Οι κρυπτογραφικές τεχνικές

Τα θέματα ασφάλειας δεδομένων μπορούν να συνοψιστούν ως ανησυχίες σχετικά με την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων. Οι κρυπτογραφικές τεχνικές, η αναγνώριση και ο έλεγχος ταυτότητας, οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά διαδραματίζουν σημαντικό ρόλο στη διασφάλιση της ασφάλειας των δεδομένων. Για να επιτύχουμε το υψηλότερο επίπεδο ασφάλειας, πρέπει να κρυπτογραφήσουμε τα δεδομένα μας.

#### 4.5.3. Κρυπτογραφία συμμετρικού κλειδιού (symmetric key cryptography)

Στην συμμετρική κρυπτογραφία χρησιμοποιείτε το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Αυτό το κλειδί είναι γνωστό μόνο σε μέλη της αλυσίδας της επικοινωνίας ώστε να μπορεί να μεταδοθεί με ασφάλεια. Εάν αυτό δεν καταστεί δυνατό, τότε η συμμετρική κρυπτογραφία θα θεωρηθεί αναποτελεσματική, καθώς ένα μη εξουσιοδοτημένο άτομο θα μπορεί να κλέψει το κλειδί, να αποκωδικοποιήσει το μήνυμα και να κατασκοπεύσει τη συνομιλία.

#### 4.5.4. Κρυπτογραφία ασύμμετρου κλειδιού (Asymmetric-key cryptography)

Στην ασύμμετρη κρυπτογραφία, δύο διαφορετικά κλειδιά χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση: το δημόσιο κλειδί και το ιδιωτικό κλειδί.

#### 4.5.5. Hash Function

Οι συναρτήσεις κατακερματισμού είναι μια τρίτη μορφή κρυπτογράφησης. Αυτή η μέθοδος δεν χρησιμοποιεί κλειδί, όπως οι μέθοδοι δημόσιου κλειδιού και συμμετρικού κλειδιού.

#### 4.5.6. Εξαπάτηση (Deception)

Η εξαπάτηση χρησιμοποιείται συχνά για την προστασία των υπολογιστών από επιθέσεις στον κυβερνοχώρο. Για παράδειγμα, το honeypot είναι ένας υπολογιστής που έχει σχεδιαστεί για να προσελκύει επιτιθέμενους. Στην πραγματικότητα, ωστόσο, αυτός ο υπολογιστής είναι απλώς μια απομίμηση της πραγματικής μηχανής και δεν αξίζει πραγματικά να επιτεθεί. Ο μηχανισμός της εξαπάτησης είναι συνήθως σκόπιμος και στοχεύει στη διαστρέβλωση της πραγματικότητας του αντιπάλου και έτσι να φέρει τον αντίπαλο σε μειονεκτική θέση. [20]

**Η εξαπάτηση αποτελείται από τις:**

##### 4.5.6.1. Προσποίηση (Dissimulation)

Για να επιτευχθεί η Προσποίηση (Dissimulation) χρησιμοποιούνται οι παρακάτω τρεις τεχνικές:

- **Masking**: Είναι η τεχνική η οποία αντικαθιστά το πραγματικό με ένα σχετικό αντικείμενο μη ανιχνεύσιμο ώστε να μπορεί να αγνοηθεί.
- **Repackaging**: Είναι η τεχνική η οποία κρύβει το πραγματικό κάνοντας ένα σχετικό αντικείμενο να φαίνεται ότι είναι κάτι που δεν είναι
- **Dazzling:** Είναι η τεχνική που κρύβει το πραγματικό κάνοντας λιγότερο βέβαιο τον προσδιορισμό ενός σχετικού αντικειμένου μπερδεύοντας τον αντίπαλο για την πραγματική του φύση. Μπορεί να χρησιμοποιηθεί για την απόκρυψη πληροφοριών σχετικά με υπηρεσίες δικτύου από τρίτα μέρη. Αυτό γίνεται χρησιμοποιώντας μεθόδους κρυπτογράφησης ή εκχωρώντας τυχαίες διευθύνσεις IP.

##### 4.5.6.2. Προσομοίωση (Simulation)

Με τους παρακάτω τρόπους μπορούμε να βρούμε το "λάθος"

- **Εφεύρεση (Inventing):** Είναι η τεχνική που δημιουργεί το ψευδές και έτσι δημιουργεί μια αντίληψη ότι ένα σχετικό αντικείμενο υπάρχει όταν δεν υπάρχει.
- **Μίμηση (Mimicking):** Είναι η τεχνική που επινοεί το ψευδές παρουσιάζοντας χαρακτηριστικά ενός πραγματικού και σχετικού αντικειμένου.
- **Δελεασμός (Decoying):** Είναι η τεχνική που εμφανίζει το ψευδές έτσι ώστε να τραβήξει την προσοχή μακριά από ένα πιο σχετικό αντικείμενο.

### 4.5.7. Intrusion Detection System IDS-Σύστημα Ανίχνευσης Εισβολής (ΣΑΕ)

Το IDS είναι ένα σύστημα παρακολούθησης και ανάλυσης συμβάντων που μπορούν να ταξινομηθούν ως συστήματα βασισμένα σε υπογραφές, ανίχνευση εισβολής βάσει προδιαγραφών και βάσει ανωμαλιών. Τα συστήματα που βασίζονται σε ανωμαλίες λειτουργούν πολύ καλύτερα στην περίπτωση της πρώτης εμφάνισης μιας επίθεσης καθώς επισημαίνουν δραστηριότητες που θεωρούν ότι διαφέρουν σημαντικά από τις συνήθεις δραστηριότητες. Ο στόχος του IDS είναι να εντοπίσει στοιχεία πιθανών προσπαθειών εισβολής, τα οποία συχνά εντοπίζουν ίχνη παραβιάσεων της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πόρων πληροφοριών. [14]

#### 4.5.7.1. Οι βασικές λειτουργίες ενός IDS

- **Συσκευή συλλογής δεδομένων (αισθητήρας) (Data-gathering device (sensor)):** Συλλέγει δεδομένα από συστήματα που εξετάζονται/προστατεύονται. Η παρακολούθηση και η ανάλυση των δραστηριοτήτων χρήστη και συστήματος είναι ένα σημαντικό μέρος της ασφάλειας.
- **Ανιχνευτής (μηχανή ανίχνευσης εισβολής) (Detector (intrusion-detection engine)):** Η διαδικασία που αναλύει δεδομένα από αισθητήρες για πιθανές εισβολές.
- **Βάση γνώσεων (βάση δεδομένων) (Knowledge base (database)):** Ορισμοί δειγμάτων επιθέσεων για χρήση στον εντοπισμό πιθανών εισβολών.
- **Συσκευή διαμόρφωσης (Configuration** device): Μηχανισμοί για τον προσδιορισμό των τρεχουσών ρυθμίσεων και της κατάστασης IDS.
- **Στοιχείο απόκρισης (Response component) :** Ένας μηχανισμός για την ενεργοποίηση ενεργειών για την αντιμετώπιση πιθανών απειλών εντοπιστεί.

Ένα IDS/IPS που προορίζεται για εφαρμογές έξυπνου δικτύου και υποστηρίζεται με μηχανισμούς τεχνητής νοημοσύνης θα πρέπει να λάβει πλήρης εκτίμηση της εγγενούς επιχειρηματικής λογικής των πληροφοριακών συστημάτων που υποστηρίζονται από τα πρότυπα συμπεριφοράς τους σε λογικές διαδικασίες ώστε τέτοιου είδους συστήματα θα πρέπει να είναι σε θέση:

- Να συλλέγει πληροφορίες σχετικά με τη λειτουργία συσκευών που αποτελούν μέρος του συστήματος.
- Να συλλέγει και να επεξεργάζεται πληροφορίες σχετικά με τους χρήστες και τη δραστηριότητά τους στο σύστημα.

- Να μπορεί να καθορίζει και να παρακολουθεί τα επίπεδα εξουσιοδότησης των χρηστών του έξυπνου δικτύου.
- Να μπορεί να καθορίζει και να παρακολουθεί τους ρόλους των στοιχείων και των χρηστών του έξυπνου δικτύου.
- Να μπορεί να καθορίζει τα δικαιώματα πρόσβασης στις συσκευές, τις ρυθμίσεις τους και τα δεδομένα που δημιουργούν.
- Να παρακολουθεί τις ροών δεδομένων στο δίκτυο υπολογιστών.
- Να δημιουργεί και παρακολουθεί προφίλ που καθορίζουν τις τυπικές συμπεριφορές συσκευών και χρηστών.
- Να εφαρμόζει μηχανισμούς αξιολόγησης κινδύνου απόδοσης του συστήματος.
- Να λαμβάνει μέτρα για τη μείωση αυτού του κινδύνου.[27]

#### 4.5.8. Ανίχνευση Ανωμαλιών

Το IDS διαθέτει μια βάση δεδομένων με κοινά πρότυπα χρήσης. Οποιαδήποτε συμπεριφορά που είναι σημαντικά διαφορετική από αυτή που συνήθως φαίνεται θα πρέπει να θεωρείται εισβολή. Εάν ένας χρήστης συνδέεται και απενεργοποιείται συχνά ή χρησιμοποιεί διαφορετικές εντολές συχνά, αυτό μπορεί να θεωρηθεί μη φυσιολογική συμπεριφορά. Μπορεί επίσης να υποψιάζεται ότι χρησιμοποιεί τον υπολογιστή σας όταν κανείς δεν έχει πρόσβαση σε αυτόν. Το IDS παρακολουθεί τα προγράμματα που εκτελείτε σε τακτική βάση. Εάν αρχίσετε να χρησιμοποιείτε ένα λογιστικό πρόγραμμα, το σύστημα θα ενημερώσει τον διαχειριστή της επιχείρησής σας.

#### 4.5.9. Ανίχνευση υπογραφής (signature detection)

Αυτή η μέθοδος χρησιμοποιεί τα πρότυπα μη εξουσιοδοτημένης συμπεριφοράς για την πρόβλεψη και τον εντοπισμό μελλοντικών παράνομων δραστηριοτήτων. Οι υπογραφές είναι πρότυπα που βοηθούν στη δημιουργία ενός συνεπούς και αναγνωρίσιμου στυλ όταν γράφετε. Ένα παράδειγμα υπογραφής είναι οι "τρεις αποτυχημένες συνδέσεις." Μια εσφαλμένη υπογραφή δεν σημαίνει απαραίτητα ότι έχει συμβεί μια προσπάθεια μη εξουσιοδοτημένης πρόσβασης. Θα μπορούσε να είναι αποτέλεσμα σφάλματος χρήστη.

#### 4.5.10. Παρακολούθηση στόχου (target monitoring)

Αυτά τα συστήματα παρακολουθούν τις αλλαγές σε συγκεκριμένα αρχεία. Με αυτόν τον τρόπο, βρίσκουν μια μη εξουσιοδοτημένη τροποποίηση αφού έχει ήδη συμβεί για να την αναιρέσουν. Για την κρυπτογράφηση ενός φακέλου, δημιουργούν ένα κρυπτογραφικό

κατακερματισμό των περιεχομένων του φακέλου για μια χρονική περίοδο. Εάν εντοπιστούν αλλαγές, το αναφέρουν στον διαχειριστή.

4.5.11. Stealth probes

Αυτή η τεχνική αναζητά μη εξουσιοδοτημένη δραστηριότητα που διαρκεί για μεγάλο χρονικό διάστημα. Για παράδειγμα, ο εισβολέας θα σαρώσει το σύστημα για τρωτά σημεία, θα ανοίξει τις πόρτες για δύο μήνες και θα περιμένει άλλους δύο μήνες για να πραγματοποιήσει την επίθεση. Το Stealth Probes συλλέγει δεδομένα συστήματος που αντιπροσωπεύουν τη συμπεριφορά του συστήματος για μεγάλο χρονικό διάστημα και επαληθεύει τις επιθέσεις χρησιμοποιώντας μια μεθοδολογία. Το λογισμικό προσπαθεί να βρει τυχόν επιθέσεις με κοινούς συσχετισμούς.

## 4.6. Η Εφαρμογή της Τεχντητής Νοημοσύνης

**Μερικές από τις εφαρμογές της Τεχνητής Νοημοσύνης στους μηχανισμούς κυβερνοασφάλειας είναι οι παρακάτω:**

**Διαχείριση ευπαθειών –** Επί του παρόντος, ορισμένες λύσεις ασφάλειας πληροφοριών αναλαμβάνουν δράση αφού εντοπιστεί μια ευπάθεια στην υποδομή πληροφορικής ενός οργανισμού, ανάλογα με τη φύση της ευπάθειας. Τα εργαλεία ML και τεχνικής νοημοσύνης είναι ένας διαφορετικός τρόπος προσέγγισης της ασφάλειας. Τα συστήματα που χρησιμοποιούν αυτά τα εργαλεία εντοπίζουν προληπτικά τα τρωτά σημεία στο τεχνολογικό περιβάλλον του οργανισμού. Μπορούν να αναλύσουν μοτίβα και να βρουν τρωτά σημεία. Αναγνωρίζοντας το μοτίβο των εισβολέων, μπορούν να ανακαλυφθούν μέθοδοι διείσδυσης και γίνεται ευκολότερο να πούμε πότε και πώς μια ευπάθεια θα μπορούσε να είναι το αδύναμο σημείο στο δίκτυο ή το σύστημα που μπορούν να εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου.

**Βελτίωση του ελέγχου ταυτότητας**–Οι περισσότεροι οργανισμοί και άτομα εξακολουθούν να βασίζονται στην παραδοσιακή μέθοδο εισαγωγής του αναγνωριστικού σύνδεσης και του κωδικού πρόσβασης για σκοπούς ελέγχου ταυτότητας. Πολλοί άνθρωποι αντιμετωπίζουν δυσκολίες ή δεν δίνουν στους ισχυρούς κωδικούς πρόσβασης την προσοχή που χρειάζονται και είναι σύνηθες να χρησιμοποιούνται κοινόχρηστοι κωδικοί πρόσβασης για όλους ή τους περισσότερους λογαριασμούς υπηρεσιών που χρησιμοποιούμε. Οι βιομετρικές μέθοδοι ελέγχου ταυτότητας, όπως η αναγνώριση προσώπου και η αναγνώριση ίριδας, είναι πολύ ασφαλείς, επομένως η χρήση τους αντί των παραδοσιακών μεθόδων ελέγχου ταυτότητας

σύνδεσης μπορούν να οδηγήσουν σε λιγότερους κινδύνους ασφαλείας. Η χρήση της AI σε βιομετρικούς μηχανισμούς μπορεί να βοηθήσει και να διασφαλίσει ότι οι εγκληματίες του κυβερνοχώρου δεν μπορούν να «πλαστογραφήσουν» αυτούς τους μηχανισμούς.

**Ανάλυση Συμπεριφοράς** – Το μεγάλο πλεονέκτημα της χρήσης AI στην ασφάλεια στον κυβερνοχώρο είναι ότι μπορεί να κατανοήσει και να προβλέψει πώς θα συμπεριφερθούν οι άνθρωποι. Η τεχνική νοημοσύνη μπορεί να αναπτύξει πρότυπα μέσω της πρόσβασης των χρηστών στα συστήματα του οργανισμού ή μέσω των μεθόδων εργασίας τους. Σε περίπτωση επίθεσης στον κυβερνοχώρο, η λειτουργία αλλάζει και η AI είναι σε θέση να ανιχνεύσει γρήγορα την ανωμαλία, η οποία μπορεί να κυμαίνεται από ασυνήθιστη χρήση του διαδικτύου, αλλαγή στην ταχύτητα πληκτρολόγησης, αυξημένη δραστηριότητα στο παρασκήνιο, έως προειδοποιήσεις που σχετίζονται με άλλα τεχνικά μέτρα.

**Έλεγχος επιθέσεων ηλεκτρονικού ψαρέματος (phising) –** Το ηλεκτρονικό ψάρεμα είναι ένας από τους πιο συνηθισμένους τρόπους με τους οποίους οι hacker προσπαθούν να κλέψουν τα προσωπικά στοιχεία χρηστών. Η AI μπορεί να είναι πολύ χρήσιμη για τον εντοπισμό και την πρόληψη επιθέσεων ηλεκτρονικού ψαρέματος, καθώς μπορεί να εντοπίσει τις πιο κοινές πηγές ηλεκτρονικού ψαρέματος και να τις αναφέρει στο σύστημα για να δημιουργήσει ένα ‘‘τοίχος’’ προστασίας. Η AI μπορεί εύκολα να εντοπίσει τη διαφορά ανάμεσα σε έναν ψεύτικο και έναν νόμιμο ιστότοπο και να αναλύσει το μοτίβο των μηνυμάτων ηλεκτρονικού ταχυδρομείου σύμφωνα με μια σειρά παραμέτρων, πολύ γρήγορα.

**Ανίχνευση και άμυνα έναντι απειλών –** Οι παραδοσιακοί μηχανισμοί ασφαλείας χρησιμοποιούν τις υπογραφές για τον εντοπισμό απειλών. Αυτή η τεχνική είναι αποτελεσματική μόνο για επιθέσεις στο παρελθόν και καθίσταται αναποτελεσματική στην περίπτωση νέων απειλών που δεν εμφανίστηκαν πριν, ενώ με τη χρήση της AI, οι νέες απειλές μπορούν να εντοπιστούν ποιο γρήγορα, με παρενέργεια την αύξηση της συχνότητα ανίχνευσης ψευδώς θετικών επιθέσεων. Για να μειωθεί ο αριθμός των ψευδώς θετικών επιθέσεων, τόσο η παραδοσιακή μέθοδος ανίχνευσης όσο και η ανάλυση ανίχνευσης συμπεριφοράς πρέπει να χρησιμοποιούνται μαζί.

## 4.7.Αποδοτικότητα και Ασφάλεια

Ο όρος «ψηφιακός μετασχηματισμός» αναφέρεται συνήθως στη χρήση ψηφιακών τεχνολογιών για τη βελτίωση της αποδοτικότητας ή της αποτελεσματικότητας μιας

διαδικασίας. Πολλές τεχνολογίες μπορούν να εμπλακούν στον ψηφιακό μετασχηματισμό, αλλά οι τελευταίες τάσεις είναι το cloud computing, το (IoT), τα Big Data και η AI.

Στην ιδανική περίπτωση, οι σύγχρονοι οργανισμοί έχουν διαφορετικά επίπεδα προστασίας, συμπεριλαμβανομένων των περιμέτρων, των επιπέδων δικτύου και των τελικών σημείων: επίπεδο εφαρμογής και επίπεδο δεδομένων. Για παράδειγμα, μπορεί να υπάρχουν τείχη προστασίας υλικού ή λογισμικού ή λύσεις ασφάλειας δικτύου που παρακολουθούν και προσδιορίζουν τις επιτρεπόμενες συνδέσεις δικτύου και αποκλείουν άλλες συνδέσεις δικτύου. Εάν οι εγκληματίες του κυβερνοχώρου μπορέσουν να ξεπεράσουν αυτές τις άμυνες, θα δημιουργήσουν προβλήματα προστασίας με ιούς και κακόβουλο λογισμικό. Το "παιχνίδι" μπορεί να περιλαμβάνει λύσεις ανίχνευσης / πρόληψης εισβολής (IDS/IPS) και πολλά άλλα. Προς το παρόν, ωστόσο, οι περισσότερες από τις τεχνολογίες που αναφέρονται (antimalware ή antivirus, IDS/IPS κ.λπ.) δεν είναι τόσο αποτελεσματικές όσο θα μπορούσαν να είναι.

Η τεχνική ανίχνευσης βάσει υπογραφών είναι συχνά αναποτελεσματική στον εντοπισμό νέων απειλών. Επιπλέον, εάν τα μέτρα ασφάλειας πληροφοριών ενός οργανισμού εξαρτώνται μόνο από την ικανότητα παρακολούθησης του τεχνολογικού περιβάλλοντος με βάση τον ανθρώπινο παράγοντα, τότε η κατάσταση θα γινόταν προβληματική.

Οι επιθέσεις στον κυβερνοχώρο δεν ακολουθούν ένα συγκεκριμένο μοτίβο. Πρέπει να βρισκόμαστε σε θέση να αναγνωρίζουμε και να αντιμετωπίζουμε τις απειλές 24/7/365, ανεξάρτητα από αργίες, ώρες εργασίας ή όταν οι υπάλληλοι δεν είναι διαθέσιμοι.

Η AI μπορεί να βοηθήσει στην εύρεση των κατάλληλων λύσεων στις δυσκολίες που βιώνουμε και, μαζί με τη ML, μπορεί να ξεπεράσει τους περιορισμούς που συνεπάγονται από τους αμυντικούς μηχανισμούς. Η AI μπορεί να ανταποκριθεί ποιο γρήγορα σε κυβερνοεπιθέσεις εν αντιθέσει με τον χρόνο που χρειάζεται να αντιδράσει ένας άνθρωπος. Μερικά από αυτά τα χαρακτηριστικά της AI είναι τα εξής:

- ✓ Η δυνατότητα δημιουργίας πιο ακριβέστερων βιομετρικών τεχνικών σύνδεσης.
- ✓ Ο εντοπισμός απειλών και κακόβουλων δραστηριοτήτων χρησιμοποιώντας προγνωστικά αναλυτικά στοιχεία.
- ✓ Η βελτιστοποίηση της μάθησης και της ανάλυσης είναι ένας τρόπος βελτίωσης της αποδοτικότητας και της αποτελεσματικότητας.
- ✓ Η εξασφάλιση ελέγχου ταυτότητας και πρόσβασης υπό όρους.

**Αρνητικές συνέπειες της χρήσης Τεχνικής Νοημοσύνης**

Όμως η AI έχει δύο όψεις. Έχει βέβαια πολλά πλεονεκτήματα, όπως και η δυνατότητα να βοηθήσει στην επίλυση προβλημάτων και των κινδύνων που εγκυμονούν για την ασφάλεια των πληροφοριών, όμως πρέπει να σταθμίσουμε τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης του προτού βασιστούμε σε αυτό ως βασικό εργαλείο για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

- **Πόροι**: Παρά τα πολλά οφέλη από την ύπαρξη ενός συστήματος AI, μπορεί όμως να είναι και πολύ δαπανηρή η συντήρησή του. Η AI απαιτεί μεγάλη υπολογιστική ισχύ, μνήμη, δεδομένα και άλλους πόρους. Είναι δύσκολο για τις μικρές και μεσαίες επιχειρήσεις να ανταποκριθούν στις ανάγκες των συστημάτων AI όσον αφορά τους υπολογιστικούς πόρους.
- **Ανήθικη χρήση:** Η AI δεν είναι απλώς ένας τομέας για ερευνητές και παρόχους ασφάλειας. Ακόμη και εγκληματίες και άλλοι κακόβουλοι χρήστες μπορούν να τη χρησιμοποιήσουν για ακατάλληλους σκοπούς. Η AI μπορεί να βοηθήσει τους εγκληματίες του κυβερνοχώρου να δημιουργήσουν κακόβουλο λογισμικό που να είναι πιο ανθεκτικό στα μέτρα ασφαλείας. Αυτό σημαίνει ότι το κακόβουλο λογισμικό μπορεί να συνεχίσει να λειτουργεί ακόμα και αν εντοπιστεί και αποκλειστεί από λογισμικό ασφαλείας. Μπορεί εισχωρήσει στο σύστημα με τη βοήθεια της AI και να το καταστρέψει.
- **Σύνολα δεδομένων**: Για να εκπαιδευτεί αποτελεσματικά ένα σύστημα AI, οι οργανισμοί πρέπει να δημιουργήσουν μεγάλο αριθμό συνόλων δεδομένων. Μέσω αυτών, μπορούν να μάθουν περισσότερα για το σύστημα AI. Το σύστημα AI συνεχίζει να εξελίσσεται και να δημιουργεί μοτίβα για ανάλυση συμπεριφοράς. Όσο περισσότερα δεδομένα διαθέτει μια εταιρεία, τόσο πιο αποτελεσματικές μπορεί να είναι οι προσπάθειές της για «εκπαίδευση». Η συλλογή και η διαχείριση μεγάλου αριθμού συνόλων δεδομένων μπορεί να είναι μια χρονοβόρα εργασία και πολλοί οργανισμοί δεν έχουν τους πόρους για να το κάνουν.
- **Ψευδείς εντοπισμοί:** Οι εταιρείες ασφαλείας εξακολουθούν να εργάζονται για να βελτιώσουν τα προγράμματα ασφαλείας τους που βασίζονται στην AI. Η τεχνολογία της AI αργεί να αναπτυχθεί και να μάθει για τις απειλές και συχνά επικεντρώνεται στην ανάλυση ασφάλειας πληροφοριών χωρίς επίβλεψη. Η χρήση της μηχανικής εκμάθησης χωρίς επίβλεψη για τον εντοπισμό σπάνιων ή μη φυσιολογικών μοτίβων μπορεί να βοηθήσει στον εντοπισμό νέων επιθέσεων. Ωστόσο, μπορεί επίσης να προκαλέσει περισσότερους ψευδείς συναγερμούς, κάτι που απαιτεί σημαντική προσπάθεια ανάλυσης

για τη διερεύνηση της ακρίβειας αυτών των ψευδών συναγερμών. Οι ψευδείς συναγερμοί μπορούν να οδηγήσουν σε κόπωση του συναγερμού, που μπορεί τελικά να οδηγήσει σε επιστροφή σε λύσεις που εστιάζονται στην ανάλυση και στις αδυναμίες.

- **Περικοπή εργασιακών θέσεων**: Ένα πιθανό μειονέκτημα της AI είναι ότι θα μπορούσε να γίνει ευρύτερα αποδεκτή, πράγμα που θα μπορούσε να σημαίνει ότι υπάρχει λιγότερη ανάγκη για ανθρώπινη συμβολή και συμμετοχή. Η τεχνολογία AI μπορεί να μας βοηθήσει να αυτοματοποιήσουμε ορισμένες εργασίες, οι οποίες θα μπορούσαν να οδηγήσουν σε περικοπές θέσεων εργασίας για πολλούς εργαζόμενους στον τομέα της πληροφορικής. Αυτό με τη σειρά του θα μπορούσε να οδηγήσει σε αύξηση της ανεργίας.

## 4.8.Οι Σύγχρονες Προκλήσεις

Ο κύριος στόχος της ενεργειακής πολιτικής είναι η μείωση του ενεργειακού περιβαλλοντολογικού αποτυπώματος, καθώς το φαινόμενο της κλιματικής αλλαγής αποτελεί τροχοπέδη στην παγκόσμια ανάπτυξη της ποιότητας της ζωής. Έτσι, θα πρέπει να παρθούν σημαντικές αποφάσεις από διεθνείς οργανισμούς και κρατικών φορέων που σχετίζονται με την εκμετάλλευση, διαχείριση και κατανάλωση ενεργειακών πόρων, δεδομένου ότι ο ενεργειακός τομέας ευθύνεται για το 80% των εκπομπών αερίων που ευθύνονται για το φαινόμενο του θερμοκηπίου.

Οι ανάγκες και οι προκλήσεις που θα πρέπει να αντιμετωπίσει το Smart Grid μπορούν να κατηγοριοποιηθούν όπως παρακάτω:

**Προκλήσεις του περιβάλλοντος:** Η παραγωγή της ηλεκτρικής ενέργειας με την καύση ορυκτών παράγει ρύπους και θα πρέπει να μειωθεί, και να μεταβούμε στα έξυπνα δίκτυα που θα συμβάλουν στην ανάπτυξη συστημάτων διεσπαρμένης παραγωγής από ΑΠΕ.

**Ανάγκες των καταναλωτών:** Είναι αναγκαίο ο καταναλωτής να έχει τη δυνατότητα να αλληλοεπιδρά με το ηλεκτρικό δίκτυο, και να έχει πρόσβαση σε δεδομένα αναφορικά με την αυτοπαραγωγή, συμπαραγωγή, κατανάλωση και προμήθεια.

**Προκλήσεις υποδομής:** Άμεσος στόχος είναι η εγκατάσταση νέου τύπου εργαλείων για ανάλυση δεδομένων, μέτρηση καταναλώσεων, έλεγχο του δικτύου και ασφάλισής του για προστασία σφαλμάτων ή και υποκλοπή δεδομένων.

**Καινοτόμες τεχνολογίες:** Σημαντική εξέλιξη στο ήδη υπάρχον δίκτυο είναι η αναβάθμιση του ώστε να μπορέσει να συνεργαστεί με νέες καινοτόμες τεχνολογίες που θα μπορέσουν να βελτιώσουν την ποιότητα παροχής της ηλεκτρικής ενέργειας με χαμηλότερο κόστος παραγωγής, και, καθώς και αξιοποίησής του σε νέα τεχνολογικά επιτεύγματα.

Για να φτάσουμε στην επίτευξη των παραπάνω στόχων που αφορούν ποιο συγκεκριμένα στη διείσδυση των ΑΠΕ στην ηλεκτροπαραγωγή, απαιτείται η επέκταση και αναβάθμιση του ηλεκτρικού δικτύου, την ανάπτυξη της διεσπαρμένης παραγωγής και την ανάπτυξη μεγάλων έργων ΑΠΕ[11].

# Κεφάλαιο 5 Συμπεράσματα

Η ασφάλεια των έξυπνων δικτύων έχει να αντιμετωπίσει όχι μόνο τις σκόπιμες επιθέσεις αλλά και ακούσιους συμβιβασμούς της πληροφοριακής υποδομής που οφείλονται σε λάθη των χρηστών, αστοχίες του εξοπλισμού και σε φυσικές καταστροφές.

Η ομάδα για την ασφάλεια της δια-λειτουργικότητας των έξυπνων δικτύων (Smart Grid Interoperability Panel-SGIP-Cyber Security Working Group), στοχεύει να αντιμετωπίσει τις ανάγκες ασφάλειας ως προς:

- Την υποδομή προηγμένης μετρικής AMI,
- Την διαχείριση κλειδιού κρυπτογράφησης (encryption key management),
- Τις απαιτήσεις ασφάλειας AMI,
- Τα κριτήρια δοκιμών για απομακρυσμένες αναβαθμίσεις AMI,
- Τις προτάσεις προστασίας της ιδιωτικότητας για χρήση δεδομένων τρίτων μερών.

Καθώς η βιομηχανία ηλεκτρικής ενέργειας εξελίσσεται με την ανάπτυξη νέων τεχνολογιών έξυπνων δικτύων, αντιμετωπίζει νέες και μεταβαλλόμενες απειλές, τρωτά σημεία και απαιτήσεις στο δίκτυο. Έχουν ξεκινήσει οι προσπάθειες να λυθούν παρόμοια προβλήματα σε άλλους τομείς, όπως ο τραπεζικός τομέας, τα ομοσπονδιακά συστήματα, τα αμυντικά δίκτυα και τα συστήματα βιομηχανικού ελέγχου. Η νέα τεχνική ιδέα είναι να προσαρμόσει τις υπάρχουσες μεθοδολογίες και εργαλεία βέλτιστης πρακτικής στον κυβερνοχώρο και να κατανοήσει πώς να τα εφαρμόσει στον ηλεκτρικό τομέα, εντοπίζοντας παράλληλα κενά και μοναδικές απαιτήσεις δικτύου που απαιτούν νέες μεθοδολογίες και εργαλεία.

## 5.1 Σύνοψη και συμπεράσματα

Υπάρχουν πολλά οφέλη από τη χρήση της AI, σε διάφορα επίπεδα. Ένας τρόπος παρακολούθησης της ηλεκτρικής δραστηριότητας είναι να υπάρχει ένας άμεσος και εύκολος τρόπος πρόσβασης σε αυτές τις πληροφορίες. Τα οικονομικά οφέλη για τους πελάτες και τους προμηθευτές είναι πολύ σημαντικά. Τα οφέλη της αξιοπιστίας περιλαμβάνουν τόσο οικονομικά οφέλη όσο και εξοικονόμηση ενέργειας. Αυτά τα οφέλη γίνονται πιο εύκολα αντιληπτά από τους καταναλωτές και γίνονται ακόμη περισσότερα αν λάβουμε υπόψη σενάρια όπου εξοικονομείται ενέργεια σε περιόδους αιχμής, ακόμη και χωρίς μετατόπιση φορτίου.

## 5.2.Μελλοντικές επεκτάσεις

Αναμφισβήτητα, η AI αποτελεί και θα αποτελέσει αναπόσπαστο κομμάτι της καθημερινότητάς μας. Υπάρχει ο ενδεδειγμένος χώρος για περαιτέρω ανάπτυξη και ως στόχος μας θα είναι η καλυτέρευση της βιωσιμότητας και αναβάθμισης του δικτύου Ηλεκτρικής ενέργειας. Η Διπλωματική εργασία έχει ως βασικό κριτήριο τη συγγένεια του γνωστικού αντικειμένου με το πεδίο έρευνας όπως περιγράφεται από το θέμα της εργασίας και μπορεί να βοηθήσει ως ερέθισμα τον αναγνώστη για την ανάπτυξη αλγορίθμου, επιλέγοντας ως κατευθυντήριες γραμμές τις αναφορές που έχουν γίνει στα είδη των επιθέσεων και τους τρόπους αντιμετώπισής των. Ο ρόλος του ανθρώπου είναι αρκετά σημαντικός, καθώς μόνο με την βοήθειά του μπορεί η AI να χρησιμοποιηθεί κατάλληλα ως τεχνολογία για την αντιμετώπιση της κλιματικής αλλαγής που μαστίζει την ανθρωπότητα στην εποχή μας.

# Βιβλιογραφία


[1] Ανδρώνης Χρήστος (2021). Η συγγραφή Διπλωματικής Εργασίας: Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στα Ασύρματα Δίκτυα Επόμενης Γενιάς, Πανεπιστήμιο Πειραιά, Πειραιάς.

[2] Ζώτου Ευφροσύνη (2012). Η συγγραφή Διπλωματικής Εργασίας: Σύγχρονες Τεχνολογίες Πρόσβασης και Διαδικτύου σε Έξυπνα Δίκτυα (SmartGrids), Εθνικό Μετσόβειο Πολυτεχνείο, Αθήνα

[3] Καλδή Κυριακή (2020). Η συγγραφή Διπλωματικής Εργασίας: Πηγές Ηλεκτρικής Ενέργειας και Πρόβλεψη τιμών τους. Πανεπιστήμιο Μακεδονίας, Θεσσαλονική.

[4] Λεονάρδου Παντισκα (2016). Η συγγραφή Διπλωματικής Εργασίας: Έξυπνα Ενεργειακά Δίκτυα: Διαχείριση και Εφαρμογές, Πανεπιστήμιο Πατρών, Πάτρα.

[5] Παναγιώτης Καλαντζής, 11 Ιούν 2021, Τεχνητή Νοημοσύνη και Κυβερνοασφάλεια – Συνεργάτες ή Αντίπαλοι;, Smart Press A.E., IT issue 69, τεχνητή νοημοσύνη, Αθήνα

[6] Παπακωνσταντίνου Βασίλειος (2016). Η συγγραφή Διπλωματικής Εργασίας: Ευφυή Δίκτυα στο Ελληνικό ΣΗΕ. Πανεπιστήμειο Θεσσαλίας, Βόλος.

[7] Ραφιάς Ανάργυρος (2014). Η συγγραφή Διπλωματικής Εργασίας: Δίκτυα Μεταφοράς Συστημάτων Ευφυούς Μέτρησης. Εθνικό Μετσόβειο Πολυτεχνείο, Αθήνα.

[8] Σαμουρκασίδης Άγγελος, Κοντοβάς Αθανάσιος (2018). Η συγγραφή Διπλωματικής Εργασίας: Η Ζεύξη των Συστημάτων Ηλεκτρικής Ενέργειας και του Διαδικτύου. Πανεπιστήμειο Θεσσαλίας, Βόλος.

[9] Σουλτάνος Νικόλαος (2018). Η συγγραφή Διπλωματικής Εργασίας: Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας (Smart Grids) και Σύγχρονες Τεχνολογίες Επικοινωνίας. Πανεπιστήμιο Πειραιά, Πειραιάς.

[10] Σταύρου Σωτήρης (2015). Η συγγραφή Διπλωματικής Εργασίας: Μετάβαση στο ευφυές ηλεκτρικό δίκτυο και διαχείριση της ζήτησης ηλεκτρικής ενέργειας. Εθνικό Μετσόβειο Πολυτεχνείο, Αθήνα.

[11] Τσιράκης Χρήστος (2012). Η συγγραφή Διπλωματικής Εργασίας: Θέματα Ασφαλείας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid. Εθνικό Μετσόβειο Πολυτεχνείο, Αθήνα.

[12] Χατζηβασιλειάδης Γιάννης (2009). ΙΕΝΕ B2B 12.11.2009, Έξυπνα Ηλεκτρικά Δίκτυα για Μεγάλη Διείσδυση ΑΠΕ

[13] Ζαππής Σωκράτης (2015). Η συγγραφή Διπλωματικής Εργασίας: Έξυπνα Δίκτυα Ενέργειας. Πανεπιστήμιο Πατρών, Πάτρα.

[14] Dinesh Mohanty, Kamalakanta Sethi, Sai Prasath, Rashmi Ranjan Rout, and Padmalochan Bera, 2021, Intelligent Intrusion Detection System for Smart Grid Applications, International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA) |978-1-6654-2529-2/20/$31.00 ©2021 IEEE | DOI: 10.1109/CyberSA52016.2021.9478200

[15] Dong Wei, Yan Lu, Mohsen Jafari, Paul M. Skare, and Kenneth Rohde, 2011, Protecting Smart Grid Automation Systems Against Cyberattacks, IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4.

[16] H.M.K.K.M.B. Herath, Mamta Mittal, 30 April 2022, Adoption of artificial intelligence in smart cities: A comprehensive review, International Journal of Information Management Data Insights 2 (2022) 100076

[17] Ibrahim Alotaibi, Mohammed A. Abido, Muhammad Khalid and Andrey V. Savkin, November 2020, A Comprehensive Review of Recent Advances in Smart Grids: A Sustainable Future with Renewable Energy Resources, Energies 2020, 13, 6269; doi:10.3390/en13236269, www.mdpi.com/journal/energies

[18] Jinju Zhou, Lina He, Canbing Li, Yijia Caom Xubin Liu and Yinghui Geng, 2013, What is the Difference between Traditional Power Grid and Smart Grid? – from Dispatching Perspective, 978-1-4799-2522-3/13/$31.00 ©2013 IEEE

[19] Konstantinos Demertzis and Lazaros Iliadis, 2018, A Computational Intelligence System Identifying Cyber-Attacks on Smart Energy Grids, School of Engineering, Department of Civil Engineering, Faculty of Mathematics Programming and General Courses, Democritus University of Thrace, Xanthi, Greece

[20] Mladen Kezunovic, Vijay Vittal, Sakis Meliopoulos, Tim Mount, Peter W. Sauer, Vincent J. Forte, Jr., S. Massoud Amin, Anthony M. Giacomoni, H. Vincent Poor, February 2015, Smart Grid and Renewable Energy, Editorial inquiries: IEEE-Eta Kappa Nu, 445 Hoes Lane, Piscataway, NJ 08854, USA

[21] M. Zekeriya Gunduz, Resul Das, 2018, Analysis of cyber-attacks on smart grid applications, 978-1-5386-6878-8/18/$31.00 ©2018 IEEE

[22] Nenad Šijaković, Violeta Kogalniceanu, 13 May 2020, Smart Grid opportunities in the Energy Community Scoping Study, Energy Community.

[23] Noel Schulz, President, IEEE PES, March 15, 2013, Smart Grid: Challenges & Opportunities, IEEE Power & Energy Society 445 Hoes Lane Piscataway, NJ 08854 USA

[24] Smadi, A.A.; Ajao, B.T.; Johnson, B.K.; Lei, H.; Chakhchoukh, Y.; Abu Al-Haija, Q. A Comprehensive Survey on Cyber-Physical Smart Grid Testbed Architectures: Requirements and Challenges. Electronics 2021, 10, 1043. https://www.mdpi.com/2079-9292/10/9/1043

[25] S. Massoud Amin, 2011, Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control, European Journal of Control (2011)5-6:547–567, DOI:10.3166/EJC.17.547–567

[26] Song Tan, Debraj De, WenZhan Song, Junjie Yang, Sajal K. Das, 2016, Survey of Security Advances in Smart Grid: A Data Driven Approach.

[27] Tomasz Kisielewicz, Stanislaw Stanek and Mariusz Zytniewski, 28 June 2022, A Multi-Agent Adaptive Architecture for Smart-Grid-Intrusion Detection and Prevention, Energies 2022, 15, 4726. https://doi.org/10.3390/en15134726

[28] US Department of Energy, January 2022, United States Department of Energy Washington, DC 20585

[29] Vasileios P. Rekkas, Sotirios Sotiroudis, Panagiotis Sarigiannidis, Shaohua Wan, George K. Karagiannidis and Sotirios K. Goudos, 14 November 2021. Machine Learning in Beyond 5G/6G Networks—State-of-the-Art and Future Trends, Electronics 2021, 10,2786. https://doi.org/10.3390/electronics10222786

[30] Wajahat Ali, Ikram Ud Din, Ahmad Almogren and Byung-Seo Kim, 15 March 2022, A Novel Privacy Preserving Scheme for Smart Grid-Based Home Area Networks, https://doi.org/10.3390/s22062269

[31] Zeadally S., A. Pathan, C. Alcaraz, and M. Badra, 2012 “Towards Privacy Protection in Smart Grid”, Wireless Personal Communications, vol. 73, pp.23-50. http://doi.org/10.1007/s11277-012-0939-1 NICS Lab. Publications: https://www.nics.uma.es/publications