ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ &
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΠΡΟΛΗΨΗ ΕΙΣΒΟΛΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΜΕ ΤΕΧΝΙΚΕΣ ΒΑΘΙΑΣ ΜΑΘΗΣΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του/της

ΓΡΗΓΟΡΙΑΔΟΥ ΣΕΒΑΣΤΗ

Επιβλέποντες:

Αναπληρωτής Καθηγητής - ΣΑΡΗΓΙΑΝΝΙΔΗΣ ΠΑΝΑΓΙΩΤΗΣ

Επίκουρος Καθηγητής - ΜΠΟΥΛΟΓΕΩΡΓΟΣ ΑΛΕΞΑΝΔΡΟΣ-ΑΠΟΣΤΟΛΟΣ

ΚΟΖΑΝΗ/ΣΕΠΤΕΜΒΡΙΟΣ/2022

HELLENIC DEMOCRACY
UNIVERSITY OF WESTERN MACEDONIA

FUCULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL &
COMPUTER ENGINEERING

Deep Learning-based Intrusion and Prevention System for the Internet Of Things

DIPLOMA THESIS

GRIGORIADOU SEVASTH

SUPERVISORS:

Associate Professor - SARHGIANNIDIS PANAGIOTIS

Assistant Professor - MPOULOGEORGOS ALEXANDROS-APOSTOLOS

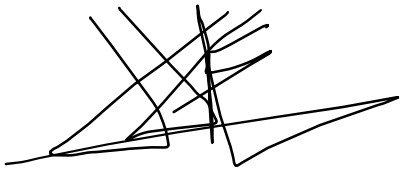
KOZANI/SEPTEMBER/2022

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο **"Ανίχνευση και Πρόληψη Εισβολών στο Διαδίκτυο των Πραγμάτων με Τεχνικές Βαθιάς Μάθησης"** καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος **κ. Σαρηγιαννίδη Παναγιώτη και Μπουλογεώργου Αλέξανδρου-Απόστολου** αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. 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. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:



Περίληψη

Τα τελευταία χρόνια, η εισαγωγή της τεχνολογίας σε κάθε πτυχή της ανθρώπινης ζωής είναι γεγονός. Με την πάροδο των χρόνων τα υπολογιστικά συστήματα αναπτύχθηκαν και αυτοματοποιήθηκαν με γρήγορους ρυθμούς. Ωστόσο, η διασύνδεση στο διαδίκτυο κάθε πιθανού στοιχείου του περιβάλλοντος, προκειμένου να υπάρχει δυνατότητα παρακολούθησης και διαχείρισης τους, επέφερε και την αύξηση της πολυπλοκότητας των συστημάτων αυτών. Αυτό έχει ως αποτέλεσμα τα υπολογιστικά συστήματα να είναι ευάλωτα σε εξωτερικές κυβερνοεπιθέσεις, αφού δεν διαθέτουν όλα τους απαραίτητους μηχανισμούς ασφαλείας. Συνεπώς, κρίνεται απαραίτητη η ανάπτυξη συστημάτων ανίχνευσης και πρόληψης εισβολών ικανών να ανιχνεύσουν επερχόμενες εισβολές που σε άλλη περίπτωση θα έθεταν σε κίνδυνο την ακεραιότητα και την αξιοπιστία των υπολογιστικών συστημάτων. Η παρούσα διπλωματική εργασία έχει ως σκοπό την ανάπτυξη ενός Συστήματος Ανίχνευσης και Πρόληψης Εισβολών (ΣΑΠΕ) στο Διαδίκτυο των Πραγμάτων με Τεχνικές Βαθιάς μάθησης.

Σε πρώτο επίπεδο γίνεται μελέτη και ανάλυση των Συστημάτων Ανίχνευσης Εισβολών (ΣΑΕ), της αρχιτεκτονικής τους αλλά και των τρόπων με τον οποίο αυτά αποκρίνονται σε εισβολές. Στη συνέχεια αναλύεται ο τομέας της Μηχανικής Μάθησης άλλα και των Τεχνικών Νευρωνικών Δικτύων (ΤΝΔ), που διαδραμάτισαν καθοριστικό ρόλο στην υλοποίηση του ΣΑΕ. Ακόμα παρουσιάζονται και οι υπόλοιποι αλγόριθμοι που χρησιμοποιήθηκαν για την διαδικασία της ανίχνευσης Εισβολών. Παράλληλα, καθώς οι κυβερνοεπιθέσεις είναι πρόβλημα δεκαετιών, γίνεται μια ανάλυση παρόμοιων συστημάτων που αναπτύχθηκαν προκειμένου να εκπληρώσουν το στόχο της ορθής ανίχνευσης. Έπειτα σε επόμενο στάδιο παρουσιάζεται η αρχιτεκτονική του προτεινόμενου συστήματος αλλά και τα βήματα που ακολουθήθηκαν για την σύνθεση και την προ-επεξεργασία του συνόλου δεδομένων, προκειμένου αυτό να δομηθεί σωστά και να εξάγει τα επιθυμητά αποτελέσματα. Τέλος, παρουσιάστηκαν σε πίνακες τα πειραματικά αποτελέσματα των μεθόδων που εφαρμόσθηκαν στην βάση δεδομένων CIC-IoT Dataset 2022 τόσο με το λογισμικό του CICFlowMeter όσο και με το NFStream. Καλύτερα αποτελέσματα παρουσίασαν οι αλγόριθμοι Βαθιά Νευρωνικά Δίκτυα (Deep Neural Network-DNN), κ πλησιέστερων γειτόνων (k-nearest neighbor-k-NN), Τυχαίο Δάσος (Random Forest) και Δένδρο Αποφάσεων (Decision Tree) με ποσοστά ακρίβειας και F1-Score να είναι από 97% και πάνω.

Λέξεις-Κλειδιά: Σύστημα Ανίχνευσης Εισβολών, Μηχανική Μάθηση, Βαθιά Μάθηση, CICFlowMeter ,NFStream, Τεχνητά Νευρωνικά Δίκτυα, CIC IoT Dataset 2022, ανίχνευση ανωμαλιών, μετρικές αξιολόγησης, confusion matrix

Abstract

In recent years, the introduction of technology into every aspect of human life is a fact. Over the years, computer systems developed and automated at a rapid pace. However, the internet connection of every possible element of the environment, to be able to monitor and manage them, led to an increase in the complexity of these systems. This results in computer systems being vulnerable to external cyber-attacks since they do not have all the necessary security mechanisms. Therefore, the development of intrusion detection and prevention systems, capable of detecting incoming intrusions that would otherwise endanger the integrity and reliability of computer systems, is deemed necessary. The purpose of this thesis is to develop a Deep Learning-based Intrusion and Prevention System for the Internet of Things.

At the first level, the Intrusion Detection Systems are studied and analyzed, their architecture and the ways in which they respond to intrusions. Then the field of Machine Learning and Neural Network Techniques are analyzed, which played a decisive role in the implementation of Intrusion Detection System. The rest of the algorithms used for the Intrusion detection process are also presented. At the same time, as cyber-attacks are a decades-old problem, an analysis is made of similar systems developed to fulfill the goal of proper detection. Then, in a subsequent stage, the architecture of the proposed system is presented, as well as the steps followed for the synthesis and pre-processing of the data set, for it to be properly structured and to produce the desired results. Finally, the experimental results of the methods applied to the CIC-IoT Dataset 2022 database with both CICFlowMeter and NFStream software were presented in tables. Better results were presented by DNN, k-NN, Random Forest and Decision Tree algorithms with accuracy rates and F1-Score of 97% and above.

Keywords: Intrusion Detection System, Machine Learning, Deep Learning, CICFlowMeter, NFStream, Artificial Neural Networks, CIC IoT Dataset 2022, anomaly detection, evaluation metrics, confusion matrix

Ευχαριστίες

Η παρούσα διπλωματική εργασία αποτελεί το τελευταίο κομμάτι της φοίτησης μου στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Δυτικής Μακεδονίας. Στην πορεία της φοιτητικής μου ζωής, απέκτησα όλα τα απαραίτητα εφόδια για την εξέλιξη της επαγγελματικής μου πορείας. Για αυτό πρωτίστως θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου που συνέβαλλαν στην απόκτηση των γνώσεων αλλά και στην αλλαγή του τρόπου σκέψης μου.

Στην συνέχεια, θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή Παναγιώτη Σαρηγιαννίδη και τον επίκουρο καθηγητή Μπουλογεώργο Αλέξανδρο–Απόστολο για την υποστήριξή τους στην περάτωση της παρούσας διπλωματικής. Ακόμα αισθάνομαι την ανάγκη να ευχαριστήσω θερμά τον υποψήφιο διδάκτορα Παναγιώτη Ράδογλου-Γραμματίκη για την υποστήριξη, την βοήθεια αλλά και την ιδιαίτερη καθοδήγησή του προκειμένου να ολοκληρώσω ορθά την διπλωματική μου εργασία.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου για την στήριξή τους, αλλά και για την εμπιστοσύνη που μου έδειξαν σε όλη την διάρκεια των σπουδών μου.

Αφιερώνεται στον πολυαγαπημένο μου πατέρα,
που έφυγε ξαφνικά από τη ζωή πριν ένα μήνα.

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος εικόνων

Κατάλογος πινάκων

Κεφάλαιο 1: Εισαγωγή

Στον σύγχρονο κόσμο, όπου η τεχνολογία έχει γνωρίσει και γνωρίζει ολοένα και μεγαλύτερη ανάπτυξη, η ποιότητα της ανθρώπινης ζωής έχει βελτιωθεί σε πολλαπλούς τομείς. Πλέον, η αξιοποίηση των κλάδων της πληροφορικής και των δικτύων αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας.

Τις τελευταίες δεκαετίες, η συνεχής χρήση του διαδικτύου από τα υπολογιστικά συστήματα, επέφερε και την δυνατότητα πρόσβασης και αξιοποίησης ευαίσθητων δεδομένων, όπως κωδικών πρόσβασης, επικοινωνιών με φυσικά και νομικά πρόσωπα κ.λπ. Με την μετάβαση της καταχώρησης των δεδομένων από αναλογικό σε ψηφιακό τρόπο, αναπτύχθηκαν τακτικές υποκλοπής και κακόβουλης χρήσης τους, οι οποίες παλαιότερα ήταν επιτυχείς με καταστροφικές συνέπειες στα υπολογιστικά συστήματα.

Η αυτοματοποίηση ολοένα και περισσότερων διαδικασιών απαιτεί μέγιστη προσοχή και αξιοπιστία. Ωστόσο, πολλά υπολογιστικά συστήματα δεν έχουν κατασκευαστεί με τέτοιο τρόπο ώστε να παρέχουν την απαραίτητη ασφάλεια . Έτσι, χρήζει επιτακτικής ανάγκης η ανάπτυξη νέων ανανεωμένων μεθόδων ανίχνευσης πιθανών εισβολών σε συστήματα.

Συνεπώς η δημιουργία Συστημάτων Ανίχνευσης και Πρόληψης Εισβολών (ΣΑΠΕ) είναι αναγκαία αφού επιφέρει σημαντικά πλεονεκτήματα στην διασφάλιση της ορθής ανταλλαγής υπηρεσιών και λειτουργίας των συστημάτων. Ακόμα, δύο στάδια που διαχωρίζουν τους τρόπους με τους οποίους αντιμετωπίζονται πιθανές εισβολές, είναι η ανίχνευση ανωμαλιών και η πρόληψη αυτών.

Σημαντικό ρόλο στην εξέλιξη των παραπάνω συστημάτων διαδραμάτισε και η ανάπτυξη του τομέα της Μηχανικής Μάθησης (Machine Learning), μέσω του οποίου παρέχονται εργαλεία και υπηρεσίες για την ανίχνευση των ανωμαλιών. Ο τομέας αυτός αξιοποιήθηκε πλήρως για την υλοποίηση της παρούσας διπλωματικής εργασίας.

1.1 Αντικείμενο και στόχοι της διπλωματικής

Η παρούσα πτυχιακή εργασία έχει ως στόχο την υλοποίηση ενός ΣΑΠΕ στο διαδίκτυο των πραγμάτων με τεχνικές βαθιάς μάθησης. Για την επίτευξη του στόχου αυτού, πραγματοποιείται αρχικά εκτενής διερεύνηση και μετέπειτα ανάλυση των βασικών εννοιών και προσεγγίσεων που αφορούν το πεδίο της μηχανικής μάθησης και της ανίχνευσης ανωμαλιών. Για την ανάπτυξη του ΣΑΠΕ, αξιοποιήθηκε η εφαρμογή διαφόρων αλγορίθμων μηχανικής μάθησης σε ένα σύνολο δεδομένων με δικτυακές ροές που κατηγοριοποιήθηκαν σε επιθέσεις και μη. Στη συνέχεια, παρουσιάζεται η αρχιτεκτονική του προτεινόμενου συστήματος και αξιολογούνται/συγκρίνονται μεταξύ τους οι αποδόσεις όλων των αλγορίθμων που χρησιμοποιήθηκαν. Κλείνοντας, γίνεται σύντομη αναφορά στα πεπραγμένα της πτυχιακής εργασίας αλλά και σε ζητήματα που χρήζουν περισσότερη ενασχόληση.

1.2 Οργάνωση του τόμου

Η παρούσα διπλωματική εργασία, αποτελείται από επτά κεφάλαια που καλύπτουν το σύνολο των γνώσεων που χρειάζονται για την υλοποίηση του ΣΑΠΕ.

Στο παρόν και πρώτο κεφάλαιο παρουσιάζεται το αντικείμενο και οι στόχοι της διπλωματικής εργασίας.

Στο δεύτερο κεφάλαιο πραγματοποιείται εισαγωγή και ανάλυση στα ΣΑΠΕ και πιο συγκεκριμένα στην αρχιτεκτονική τους, στα μοντέλα των εισβολών, στον τρόπο οργάνωσής τους αλλά και στην απόκρισή τους σε εισβολές.

Στο τρίτο κεφάλαιο γίνεται ανάλυση του τομέα της μηχανικής μάθησης αλλά και των Τεχνητών Νευρωνικών Δικτύων (ΤΝΔ) που διαδραμάτισαν καθοριστικό ρόλο στην υλοποίηση του ΣΑΠΕ. Ακόμα παρουσιάζονται και οι υπόλοιποι αλγόριθμοι πέρα από τα ΤΝΔ που χρησιμοποιήθηκαν για την ανάπτυξη του προτεινόμενου συστήματος.

Στο τέταρτο κεφάλαιο γίνεται μία εκτενής αναφορά σε παρόμοια συστήματα ανίχνευσης εισβολών (ΣΑΕ). Ειδικότερα δίδεται έμφαση στον τρόπο ανάπτυξής τους αλλά και στην αποδοτικότητα ορθής ανίχνευσης επιθέσεων.

Στο πέμπτο κεφάλαιο παρουσιάζεται η αρχιτεκτονική του προτεινόμενου συστήματος αλλά και των προγραμματιστικών εργαλείων που χρησιμοποιήθηκαν.

Στο έκτο κεφάλαιο, παρατίθενται οι μετρικές αξιολόγησης που χρησιμοποιήθηκαν για την εκτίμηση της αποτελεσματικότητας των αλγορίθμων, η περιγραφή του συνόλου δεδομένων και τελικά τα αποτελέσματα της απόδοσης εφαρμογής μεθόδων για την ανίχνευση εισβολών.

Στο τελευταίο και έβδομο κεφάλαιο γίνεται σύνοψη της διπλωματικής εργασίας, εξάγονται αντίστοιχα συμπεράσματα αλλά και μελλοντικές επεκτάσεις.

Κεφάλαιο 2: Συστήματα Ανίχνευσης Εισβολών

Συστήματα Ανίχνευσης Εισβολών

Στη σημερινή εποχή, το πρόβλημα της ασφάλειας τόσο στα δίκτυα όσο και στα υπολογιστικά συστήματα έχει απασχολήσει, απασχολεί και θα απασχολεί εκείνους που εμπλέκονται με τη χρήση των δικτύων υπολογιστών. Η διακίνηση δεδομένων εσωτερικά του δικτύου, επιφέρει προβλήματα, αφού τα παραπάνω καθίστανται ευπρόσβλητα σε κακόβουλες ενέργειες. Εξαιτίας αυτού, στο παρόν κεφάλαιο αναλύονται ζητήματα που αφορούν την προστασία των συστημάτων. Ειδικότερα, παρουσιάζονται οι στόχοι των ΣΑΕ και πραγματοποιείται ανάλυση της αρχιτεκτονική τους, των μοντέλων εισβολών, καθώς και η κατηγοριοποίηση των παραπάνω.

2.1 Στόχοι συστημάτων ανίχνευσης εισβολών

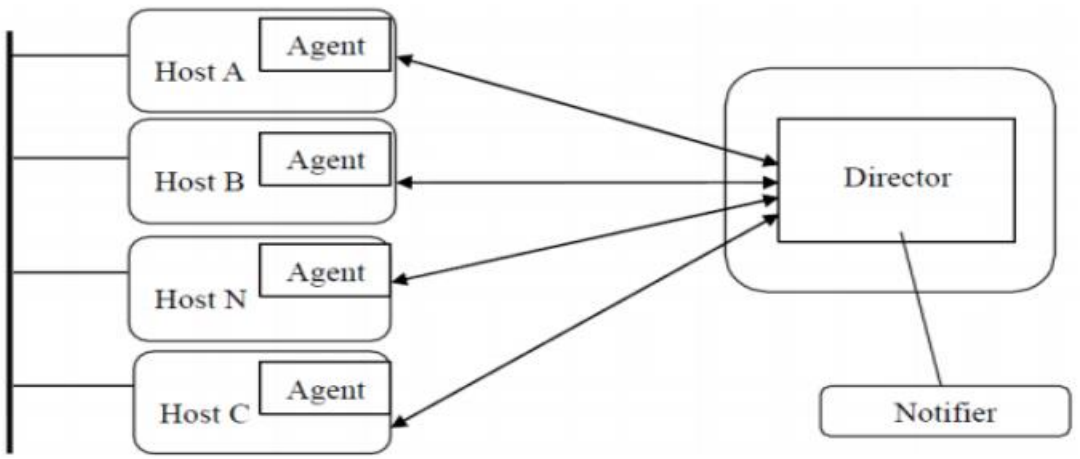
Όπως προαναφέρθηκε η συνεχής εξέλιξη των υπολογιστικών συστημάτων επέφερε την δημιουργία νέων, άγνωστων μορφών δικτυακών επιθέσεων. Σκοπός των συστημάτων ανίχνευσης εισβολών αποτελεί ο εντοπισμός πιθανών επερχόμενων εισβολών που κλονίζουν την ακεραιότητα και την αξιοπιστία τους. Υπάρχουν πολλοί λόγοι για τους οποίους μια επιχείρηση/οργανισμός θα ήθελε να εγκαταστήσει ένα τέτοιου είδους σύστημα και κάποιοι από αυτούς θα αναλυθούν παρακάτω [1].

- ***Ανίχνευση μεγάλου εύρους εισβολών***: Τα μοντέλα ανίχνευσης εισβολών εντοπίζουν απειλές που προέρχονται τόσο από το εξωτερικό περιβάλλον, όσο και από εσωτερικούς χρήστες του συστήματος. Ακόμα παρέχουν την δυνατότητα εντοπισμού άγνωστων μορφών επιθέσεων. Συμπερασματικά τα Συστήματα Ανίχνευσης Εισβολών (ΣΑΕ) ανιχνεύουν τόσο γνωστές όσο και άγνωστες εισβολές.
- ***Έγκαιρη ανίχνευση εισβολών:*** Τα ΣΑΕ πρέπει να αναγνωρίζουν επιθέσεις σε εύλογο χρονικό διάστημα και όχι απαραίτητα σε πραγματικό χρόνο.
- ***Να παρέχουν ακριβείς πληροφορίες:*** Υπάρχουν δύο ειδών ψευδή σήματα που προκύπτουν όταν ένα ΣΑΕ αναφέρει μία επίθεση. Το πρώτα είναι τα ψευδώς θετικά. Σε αυτήν την περίπτωση το σύστημα αναφέρει μια εισβολή που δεν υφίσταται. Τα σήματα αυτά, μειώνουν την αξιοπιστία του συστήματος και επιφέρουν μεγάλο φόρτο εργασίας στους υπευθύνους. Αντίθετα, υπάρχουν και τα ψευδώς αρνητικά σήματα, όπου το ΣΑΕ, αποτυγχάνει της αναφοράς πραγματικής επίθεσης, γεγονός που δεν πραγματώνει τον σκοπό τους. Συμπερασματικά, τα ΣΑΕ πρέπει να ελαχιστοποιούν τις ενδείξεις των παραπάνω δύο κατηγοριών σημάτων.

- ***Απλή και εύχρηστη διεπαφή χρήστη:*** Είναι γενικά επιθυμητό τα αποτελέσματα της προσπάθειας ανίχνευσης εισβολής να προκύπτουν σε αντιληπτή μορφή. Ωστόσο , οι διαδικτυακές επιθέσεις είναι πολύπλοκες και τα δεδομένα που εξάγονται από αυτές ακόμα πιο σύνθετα, γεγονός που καθιστά δύσκολη την επίτευξη του στόχου αυτού. Για τον συγκεκριμένο λόγο ο μηχανισμός ανίχνευσης παρουσιάζει περισσότερα δεδομένα στον διαχειριστή, ο οποίος αποφασίζει αν θα ληφθούν κάποια μέτρα.

2.2 Αρχιτεκτονική συστημάτων ανίχνευσης εισβολών

Κάθε σύστημα ανίχνευσης εισβολών αποτελεί έναν αυτοματοποιημένο μηχανισμό παρακολούθησης και ελέγχου. Ο μηχανισμός αυτός αποτελείται από τρία μέρη όπως απεικονίζεται στο παρακάτω Σχήμα 8.1 (Figure 1): έναν ή περισσότερους agent (αντιπροσώπους), έναν director (διευθυντή) και έναν notifier (αγγελιαφόρο).



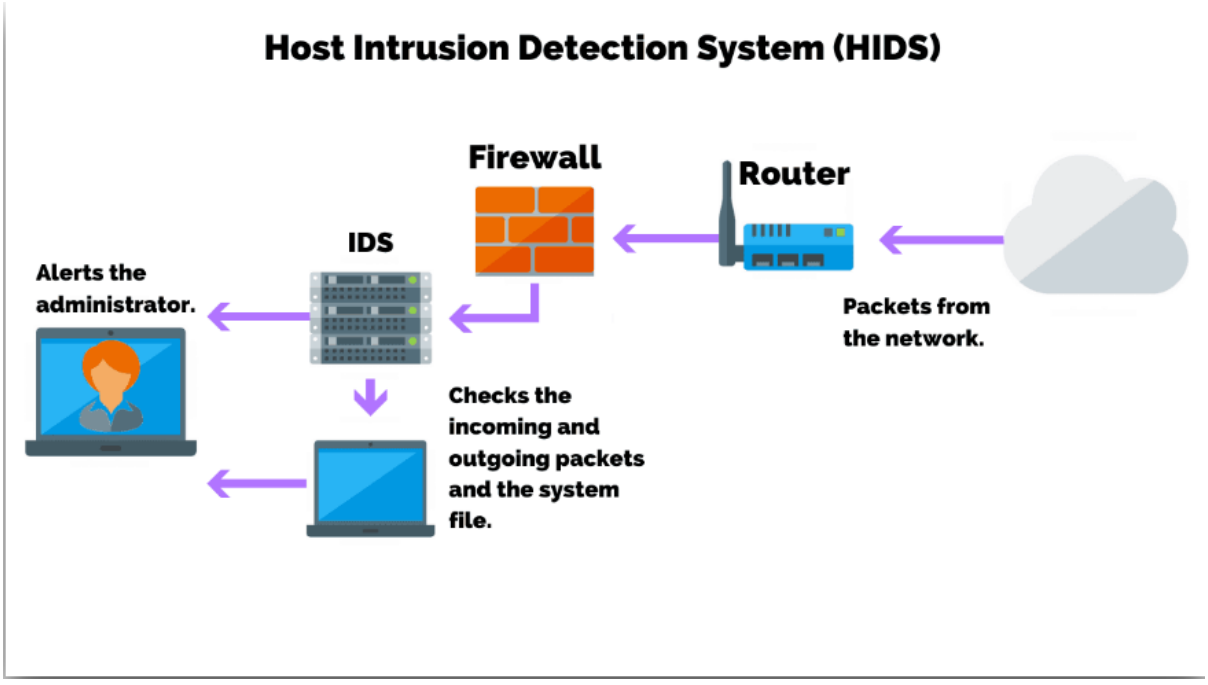
Εικόνα 1 :Αρχιτεκτονική συστήματος ανίχνευσης εισβολών [2]

2.2.1 Αντιπρόσωπος

Ο αντιπρόσωπος συλλέγει πληροφορίες από μία ή περισσότερες πηγές δεδομένων, όπως αρχεία καταγραφής συμβάντων ή από πληροφορίες που εξάγει το λειτουργικό σύστημα και οι εφαρμογές του ή από τα δικτυακά χαρακτηριστικά. Ο αντιπρόσωπος έχει την δυνατότητα αποστολής πληροφοριών στον διευθυντή, αλλαγής της μορφής της πληροφορίας προκειμένου να τον διευκολύνει αλλά και απόρριψη αυτής, αν την θεωρήσει άχρηστη. Ακόμα ένας αντιπρόσωπος μπορεί να συλλέξει πληροφορίες από έναν ή πολλούς υπολογιστές αλλά και από ολόκληρο το δίκτυο [1].

2.2.1.1 Σύστημα ανίχνευσης εισβολών μεμονωμένου συστήματος

Τα ΣΑΕ που βασίζονται σε κεντρικούς υπολογιστές, τα λεγόμενα ΣΑΕ βάσει του host (HIDS) [1] παρακολουθούν τη δραστηριότητα στο σύστημα με διάφορους τρόπους για τον εντοπισμό ύποπτης συμπεριφοράς. Σε ορισμένες περιπτώσεις ένα ΣΑΕ μπορεί να σταματήσει μια επίθεση πριν γίνει οποιαδήποτε ζημιά αλλά ο κύριος σκοπός του είναι να ανιχνεύει εισβολές, να καταγράφει ύποπτα συμβάντα και να αποστέλλει ειδοποιήσεις. Το κύριο πλεονέκτημα ενός HIDS είναι ότι μπορεί να ανιχνεύσει τόσο εξωτερικές όσο και εσωτερικές εισβολές κάτι που δεν είναι δυνατό ούτε με ΣΑΕ που βασίζονται σε δίκτυο ούτε με firewalls. Όπως αναφέρθηκε προηγουμένως, θεμελιώδες στοιχείο της ανίχνευσης των εισβολών είναι οι αντιπρόσωποι, που συλλέγουν δεδομένα. Οι κοινές πηγές δεδομένων είναι τα αρχεία καταγραφής του συστήματος, το λειτουργικό και οι εφαρμογές του αλλά και τα δικτυακά χαρακτηριστικά. Ουσιαστικά τα host-based συστήματα ερευνούν για ίχνη εισβολής στο τοπικό σύστημα του host. Πιο συγκεκριμένα, ψάχνουν για ασυνήθιστη δραστηριότητα που περιορίζεται στον τοπικό host, όπως logins, παράξενη πρόσβαση σε αρχεία, μετατροπές σε δικαιώματα συστήματος, καθώς και μη εγκεκριμένη αύξηση αυτών.



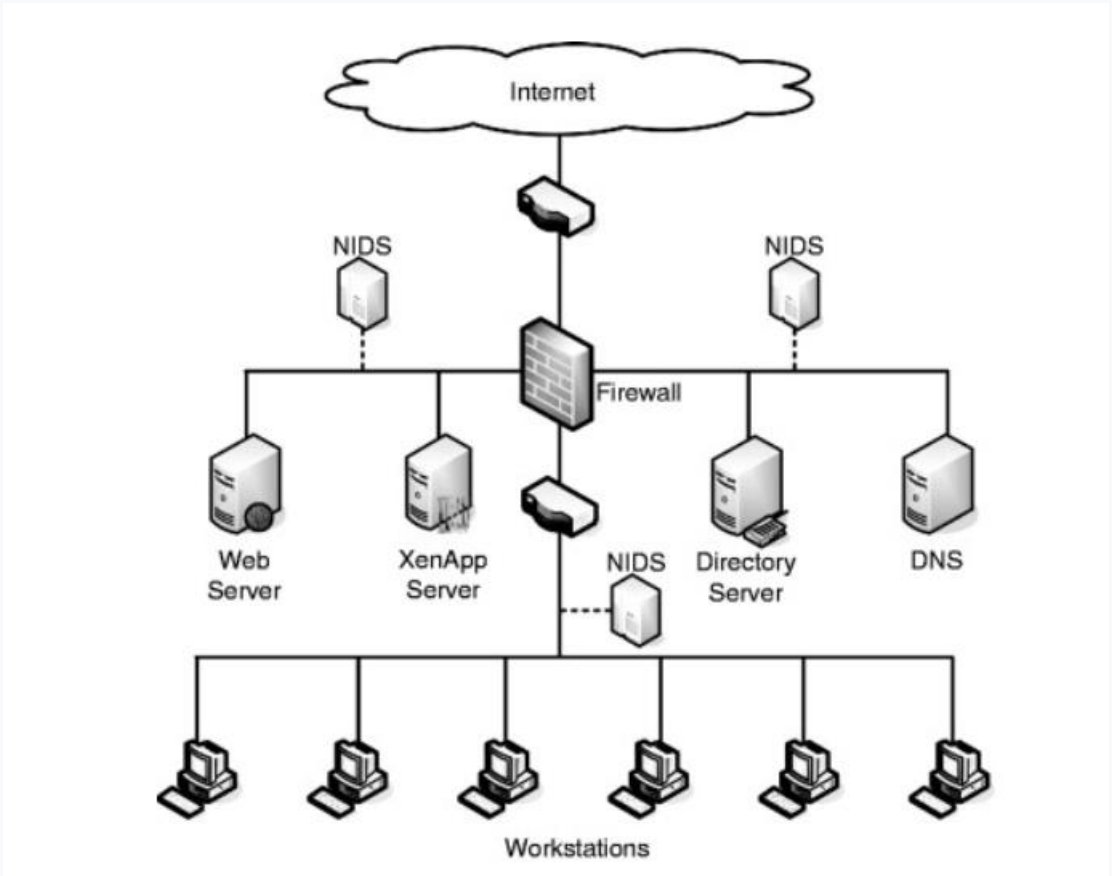
Εικόνα 2: Παράδειγμα λειτουργίας HIDS [3]

2.2.1.2 Σύστημα ανίχνευσης εισβολών δικτυακού συστήματος

Τα συστήματα ανίχνευσης εισβολών δικτυακού συστήματος (Network Based IDS – NIDS) [1], λειτουργούν συλλέγοντας πληροφορίες από τη συνολική δραστηριότητα του δικτύου και όχι από μεμονωμένα συστήματα όπως το HIDS. Το NIDS εξετάζει την κίνηση πακέτο προς πακέτο μέσα σε πραγματικό χρόνο, ή κοντά σε πραγματικό χρόνο, για να προσπαθήσει να εντοπίσει μοτίβα εισβολής. Το NIDS μπορεί να εξετάσει τη δραστηριότητα πρωτοκόλλου σε δύο επίπεδα, στο επίπεδο δικτύου, στο επίπεδο μεταφοράς και/ή εφαρμογής. Συνήθως περιλαμβάνονται στην περιμετρική υποδομή ασφαλείας ενός οργανισμού είτε ενσωματωμένα είτε σχετίζονται με το τείχος προστασίας. Τα συστήματα αυτά επικεντρώνονται στην παρακολούθηση για απόπειρες εξωτερικής εισβολής αναλύοντας τόσο τα πρότυπα κυκλοφορίας όσο και το περιεχόμενο επισκεψιμότητας για κακόβουλη δραστηριότητα.

Ακριβέστερα τα NIDS απαρτίζονται από αισθητήρες (sensors) που είναι τοποθετημένοι σε συγκεκριμένα σημεία του δικτύου. Οι προαναφερόμενοι αναλύουν την δικτυακή κίνηση καθώς αποτελούν συστήματα με ισχυρές δυνατότητες επεξεργαστικής ισχύος και δικτύωσης. Επιπρόσθετα έχουν τη δυνατότητα να αποκρύψουν την παρουσία τους (Stealth Mode). Αυτό έχει ως αποτέλεσμα ο επιτιθέμενος να μην γνωρίζει την ύπαρξη ή τη θέση τους ανά πάσα χρονική στιγμή.

Γενικά στα NIDS υπάρχει η κάρτα δικτύου, όπου λαμβάνει μόνο τα δικτυακά πακέτα που προορίζονται για την δική της φυσική διεύθυνση. Με αυτόν τον τρόπο αφουγκράζεται την συνολική δικτυακή δραστηριότητα.

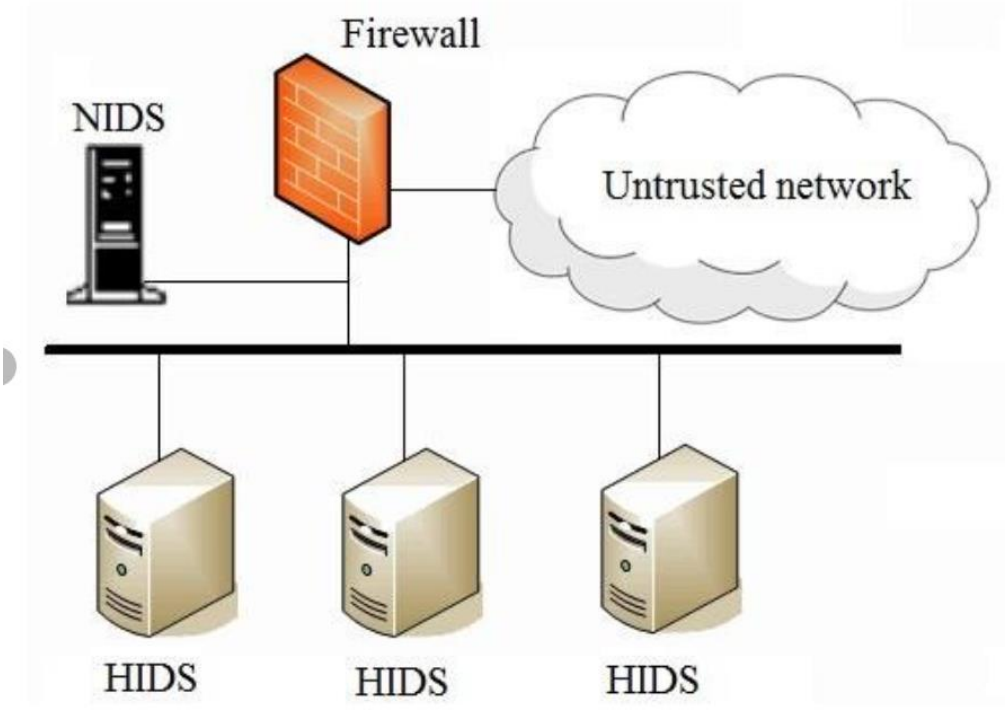


Εικόνα 3:Παράδειγμα λειτουργίας NIDS [4]

2.2.1.3 Συνδυαστική λύση μεμονωμένου και δικτυακού συστήματος ανίχνευσης εισβολών

Ο συνδυασμός των δύο προαναφερθέντων συστημάτων HIDS και NIDS [1] είναι ο πιο αποτελεσματικός μηχανισμός για την ορθή ανίχνευση των εισβολών σε ένα σύστημα. Η συνδυαστική αυτή λύση παρότι έχει αυξημένο φόρτο εργασίας για την εγκατάσταση και τη διαχείριση της καθιστά εφικτό τον εντοπισμό εισβολών σε όλα τα επίπεδα δικτύου από της εισόδου έως και κάθε μεμονωμένο υπολογιστικό σύστημα . Σε αυτή την προσέγγιση, οι ανιχνευτές ανωμαλιών σε τοπικούς κόμβους αναζητούν στοιχεία ασυνήθιστης δραστηριότητας. Μόνο με αυτά τα στοιχεία το τοπικό σύστημα κινδυνεύει με ψευδώς θετικό σήμα εάν αντιδράσει στην πιθανή επίθεση, αλλά κινδυνεύει με ψευδώς αρνητικό σήμα εάν αγνοεί την επίθεση ή περιμένει περαιτέρω στοιχεία. Σε ένα συνεταιριστικό σύστημα, ο τοπικός κόμβος χρησιμοποιεί ένα πρωτόκολλο peer-to-peer "gossip", όπου ενημερώνει άλλα μηχανήματα για την υποψία του με τη μορφή πιθανότητας ότι το δίκτυο δέχεται επίθεση. Εάν ένα μηχάνημα λάβει αρκετά από αυτά τα μηνύματα τότε μπορεί να ανταποκριθεί τοπικά για να αμυνθεί και επίσης να στείλει μια ειδοποίηση σε ένα κεντρικό σύστημα.

Επιπροσθέτως αυξάνεται η ακρίβεια και κατ’ επέκταση η αξιοπιστία όσον αφορά την αναγνώριση εισβολών αφού ο συνδυασμός των δύο επιφέρει αποτελεσματική ένωση πληροφοριών για την κατάσταση του συστήματος.



Εικόνα 4:Παράδειγμα συνδυαστικής λειτουργίας HIDS-NIDS [5]

2.2.2 Διευθυντής

Ο διευθυντής έχει τη δυνατότητα του περιορισμού/εξάλειψης των πληροφοριών που δέχεται από τους αντιπροσώπους εάν θεωρήσει πως είναι περιττές ή επαναλαμβάνονται. Με την βοήθεια μιας μηχανής ανάλυσης καθορίζει εάν το σύστημα βρίσκεται υπό εισβολή ή αν κάποια επίθεση είναι σε εξέλιξη. Πιο συγκεκριμένα, η μηχανή περιλαμβάνει ένα η περισσότερα πρότυπα ανίχνευσης εισβολών, που καθορίζουν βάσει συγκεκριμένων κανόνων/μεθόδων τεχνικής νοημοσύνης αν υφίσταται κάποια επίθεση.

Παράλληλα ο διευθυντής έχει την δυνατότητα να δώσει οδηγίες στους αντιπροσώπους προκειμένου εκείνοι να συλλέγουν περαιτέρω πληροφορίες της δικτυακής κίνησης.

Ο ρόλος του διευθυντή είναι αρκετά κρίσιμος για την αποτελεσματικότητα της ανίχνευσης για αυτό και το συγκεκριμένο πρόγραμμα εκτελείται σε εξωτερικό σύστημα, ξεχωριστό από τα υπόλοιπα δομικά στοιχεία. Αυτό έχει ως αποτέλεσμα, οι επιτιθέμενοι να έχουν περιορισμένη γνώση του τρόπου με τον οποίο μπορούν να ξεφύγουν από το σύστημα ανίχνευσης εισβολών.

2.2.3 Αγγελιοφόρος

Ο αγγελιοφόρος λαμβάνει τα αποτελέσματα της μηχανής ανάλυσης του διευθυντή και ενεργεί αναλόγως. Πιο συγκεκριμένα σε κάποιες περιπτώσεις αποστέλλει απλώς μια ειδοποίηση στον υπεύθυνο ασφαλείας ενώ άλλοτε σε περιπτώσεις έκτακτης ανάγκης πραγματοποιεί ο ίδιος ενέργειες, ώστε να προβεί εγκαίρως στον τερματισμό της επίθεσης.

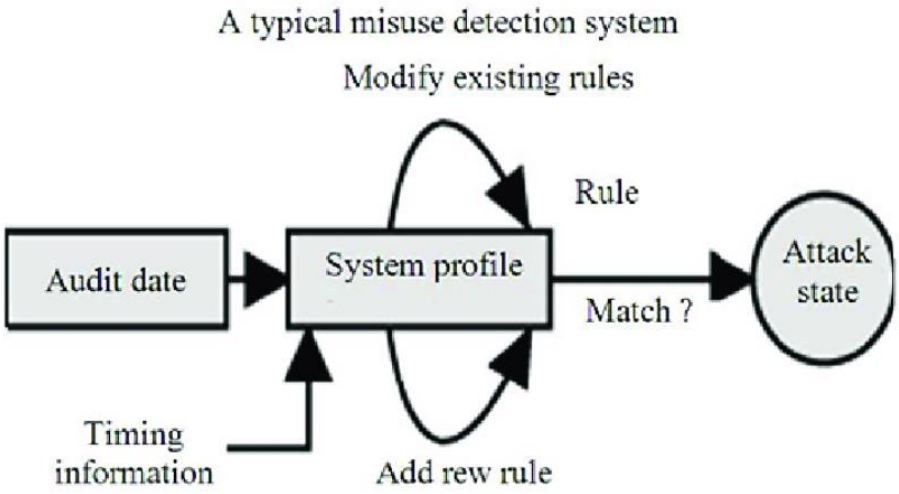
2.3 Μοντέλα εισβολών

Ο διευθυντής του συστήματος αξιοποιεί μοντέλα εισβολών προκειμένου να ελέγχει τα δεδομένα που λαμβάνει από τους αντιπροσώπους. Στην συνέχεια εκείνος τα ταξινομεί ανάλογα σε «καλά» και «κακά». Στα πρώτα ανήκουν εκείνα που θεωρούνται φυσιολογικά, ενώ στα δεύτερα αυτά που σηματοδοτούν μία πιθανή εισβολή. Οι κατηγορίες των μοντέλων ανίχνευσης εισβολών είναι τρεις και είναι κατά σειρά: μοντέλα κακής συμπεριφοράς (Misuse model), μοντέλα ανίχνευσης διαταραχών (anomaly model) καθώς και τα μοντέλα ανίχνευσης διαταραχών πρωτοκόλλων (protocol anomaly detection). Τα μοντέλα αυτά, μπορεί να είναι είτε στατικά είτε προσαρμοστικά. Πιο συγκεκριμένα μπορούν να αλλάζουν συμπεριφορά ανάλογα με τις ενέργειες του συστήματος ή να στηρίζονται σε ένα σύνολο δεδομένων που δεν τροποποιείται αντίστοιχα.

2.3.1 Μοντέλο κακής συμπεριφοράς

Το μοντέλο κακής συμπεριφοράς [6] είναι ένα από το πιο γνωστό και ευρέως χρησιμοποιούμενα μοντέλα ανίχνευσης εισβολών. Η ανίχνευση της κακής συμπεριφοράς, απαιτεί πλήρη γνώση του συστήματος αλλά και των ευπαθειών αυτού, που οι εισβολείς πρόκειται να εκμεταλλευτούν. Τα παραπάνω συνθέτουν του λεγόμενους κανόνες του συστήματος (rule set). Συγκεκριμένα, η λειτουργία του μοντέλου βασίζεται στην αντιστοίχιση της συμπεριφοράς του συστήματος με καθορισμένα πρότυπα εισβολών τις λεγόμενες υπογραφές-signatures. Σε περίπτωση που υπάρχει ταύτιση των δύο παραπάνω, τότε πιθανώς μια εισβολή βρίσκεται σε εξέλιξη.

Το συγκεκριμένο μοντέλο, είναι αξιόπιστο και έχει χαμηλό ποσοστό ψευδών σημάτων. Παρόλα αυτά, ένα αρνητικό του αποτελεί η αδυναμία αναγνώρισης μορφών εισβολών που δεν υπάρχουν στην λίστα υπογραφών των γνωστών επιθέσεων. Εξαιτίας αυτού, τα συστήματα που χρησιμοποιούν ως μοντέλο ανίχνευσης το μοντέλο κακής συμπεριφοράς χρειάζεται να ανανεώνουν συχνά το σύνολο των υπογραφών τους.



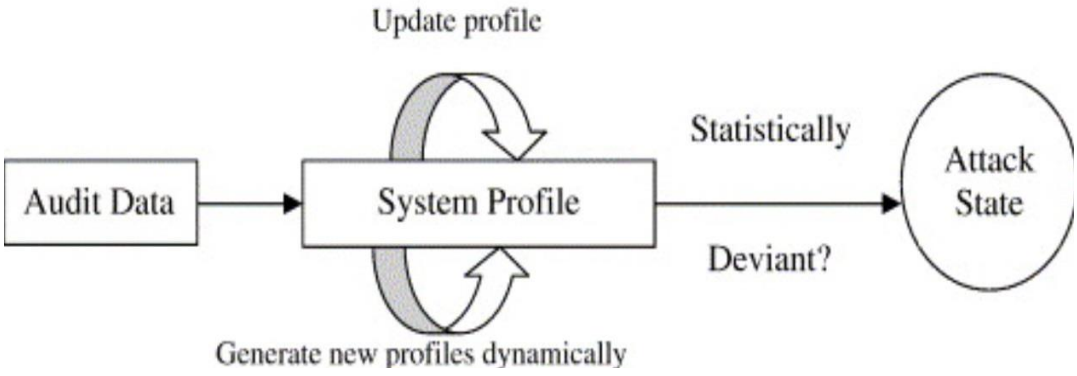
Εικόνα 5:Τυπική μορφή μοντέλου κακής συμπεριφοράς [7]

2.3.2 Μοντέλα ανίχνευσης διαταραχών

Στα μοντέλα ανίχνευσης διαταραχών [6] η ένδειξη πιθανής απειλής στο σύστημα αποτελεί η εμφάνιση απροσδόκητης συμπεριφοράς αυτού. Αναλυτικότερα πρώτο βήμα για την ανάπτυξη του συγκεκριμένου μοντέλου είναι η δημιουργία ενός συνόλου δεδομένων και στατιστικών στοιχείων που δείχνουν ποιες ενέργειες καθιστούν την συμπεριφορά του συστήματος φυσιολογική. Στη συνέχεια με βάση τα παραπάνω στοιχεία, αν μια ενέργεια στο σύστημα δεν εμπεριέχεται στις «φυσιολογικές», τότε ενημερώνεται ο διαχειριστής ασφαλείας για ενδεχόμενη διαταραχή.

Η μοντελοποίηση των στατιστικών στοιχείων που προκύπτει από την συμπεριφορά του συστήματος είναι το πιο δύσκολο κομμάτι, αφού το ίδιο το σύστημα παρουσιάζει πολλές διακυμάνσεις στην λειτουργία του.

Τα αναφερόμενα μοντέλα, δεν είναι τόσο αξιόπιστα όσο της κακής συμπεριφοράς. Παρόλα αυτά το κύριο πλεονέκτημα τους είναι πως αναγνωρίζουν άγνωστες μορφές εισβολών. Στις παρακάτω υπό-ενότητες αναλύονται κάποια τέτοιου είδους μοντέλα.



Εικόνα 6:Τυπική μορφή μοντέλου ανίχνευσης διαταραχών [8]

2.3.2.1 Μοντέλο τιμών κατωφλίου

Στο συγκεκριμένο μοντέλο καταμετράται και ελέγχεται το πλήθος κάποιων χαρακτηριστικών τόσο του χρήστη όσο και του συστήματος σε σχέση με ένα επιτρεπτό ανώτατο όριο. Παραδείγματα τέτοιων χαρακτηριστικών είναι ο αριθμός των αρχείων που έχει πρόσβαση ο χρήστης, το πλήθος των αποτυχημένων προσπαθειών εισόδου σε ένα σύστημα, ακόμα και το ποσοστό της χρήσης CPU. Το ανώτατο επιτρεπτό όριο μπορεί να έχει μια σταθερή τιμή ή και να εναλλάσσεται ανάλογα με τις ενέργειες που πραγματοποιούνται στο σύστημα και είναι «φυσιολογικές». Πιο συγκεκριμένα το μοντέλο λειτουργεί ως εξής: Κάποια ενέργεια στο σύστημα αναμένεται να συμβεί κατά ελάχιστο m φορές και κατά μέγιστο n. Αν κάποια συμβεί εκτός ορίων m και n τότε η συμπεριφορά θεωρείται διαταραγμένη.

Ένα από τα πιο χαρακτηριστικά παραδείγματα της χρήσης του μοντέλου τιμών κατωφλίου, είναι και η απαγόρευση της εισόδου ενός χρήστη στο ΛΣ MS-Windows NT 4.0, αφού ο ίδιος πραγματοποίησε υπεράριθμες αποτυχημένες προσπάθειες εισόδου[2].

2.3.2.2 Μοντέλο στατιστικών ροπών

Στο μοντέλο στατιστικών ροπών χρησιμοποιούνται στατιστικά μέτρα, όπως η μέση τιμή και η διακύμανση ενός γνωστού συνόλου δεδομένων. Αυτά τα στατιστικά ονομάζονται στατιστικές ροπές. Αν αυτά τα χαρακτηριστικά βρίσκονται εκτός κάποιων ορίων που έχουν τεθεί, τότε η αντίστοιχη ενέργεια καλείται διαταραγμένη. Επιπλέον λόγω της πιθανότητας ύπαρξης καθυστερήσεων στην κατατομή της περιγραφής του υπό εξέτασης συστήματος το συγκεκριμένο μοντέλο λαμβάνει υπόψιν τις αλλαγές αυτές. Το προαναφερόμενο είτε σταθμίζει τα δεδομένα είτε αλλάζει τους στατιστικούς κανόνες .

Το μοντέλο των στατιστικών ροπών παρότι είναι σύνθετο στη σχεδίαση του, παρουσιάζει μεγαλύτερη αξιοπιστία από αυτό του κατωφλίου. Πιο συγκεκριμένα, προκειμένου να υλοποιηθεί το μοντέλο χρειάζεται πρώτα να μοντελοποιηθούν τόσο η συμπεριφορά του χρήστη όσο και οι

διεργασίες του συστήματος σε μία ήδη γνωστή στατιστική κατανομή, όπως η Gauss. Ωστόσο, η συγκεκριμένη εργασία είναι δύσκολη λόγω των απρόβλεπτων ενεργειών των χρηστών. Στην περίπτωση όπου το σύνολο των διεργασιών των χρηστών και του λειτουργικού συστήματος δεν μπορεί να αντιστοιχηθεί, τότε γίνεται χρήση άλλων ενεργειών, όπως η ανάλυση συστοιχιών [3].

2.3.2.3 Μαρκοβιανό μοντέλο

Το Μαρκοβιανό μοντέλο [9], εξετάζει ένα σύστημα σε μία συγκεκριμένη χρονική στιγμή. Όσα γεγονότα (events) έχουν προηγηθεί, συνθέτουν την κατάσταση του συστήματος. Όσον αφορά τα συστήματα ανίχνευσης εισβολών η υλοποίηση καινούριας ενέργειας, οδηγεί το σύστημα σε νέα κατάσταση .Αυτό έχει σαν αποτέλεσμα την ανάπτυξη ενός πλήθους πιθανοτήτων μετάβασης από την μία κατάσταση στις επόμενες, ο λεγόμενος πίνακας Markov.

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix}$$

Εικόνα 7:Πίνακας πιθανοτήτων Markov

Όταν στο σύστημα συμβεί κάποιο γεγονός που έχει μικρή πιθανότητα, τότε καλείται διαταραχή. Το Μαρκοβιανό μοντέλο προτείνει για τον εντοπισμό των διαταραχών την χρήση κάποιας κατάστασης (state) ή προϊστορίας (parse history). Η αποτελεσματικότητα του εξαρτάται από την ορθότητα των δεδομένων που αξιοποιούνται για την αρχικοποίηση του μοντέλου, τα λεγόμενα δεδομένα εκμάθησης.

2.3.3 Μοντέλα ανίχνευσης διαταραχών πρωτοκόλλου

Τα μοντέλα ανίχνευσης διαταραχών πρωτοκόλλου ελέγχουν την δικτυακή δραστηριότητα και πιο συγκεκριμένα την σωστή χρήση των πρωτοκόλλων επικοινωνίας και κυρίως αυτών που ανήκουν στα TCP/IP. Τα προαναφερόμενα, είναι σύνολα κανόνων που ορίζουν τον τρόπο επικοινωνίας δύο υπολογιστικών συστημάτων. Οι ορισμοί υλοποίησης των πρωτοκόλλων ονομάζονται RFC (Request For Comments) . Τα προαναφερόμενα είναι έγγραφα που περιγράφουν την ακολουθία των ενεργειών, που κάθε πρωτόκολλο πρέπει να εκτελεί κατά την εφαρμογή του.

Οι επιθέσεις που πραγματοποιούνται σε τέτοια συστήματα στηρίζονται στο γεγονός πως δεν γίνεται φυσιολογική χρήση των πρωτοκόλλων και αποβλέπουν στο ότι οι ενέργειες που πραγματοποιούν δεν έχουν ληφθεί υπόψιν από τα RFC ή ακόμα πιθανώς να στηρίζονται σε ελλείψεις της αρχικής υλοποίησης των πρωτοκόλλων.

Συνεπώς διαπιστώνεται πως αυτού του είδους τα μοντέλα, μελετούν την δραστηριότητα που σχετίζεται με τα πρωτόκολλα επικοινωνίας και εξετάζουν αν αυτή συμφωνεί με συγκεκριμένους κανόνες φυσιολογικής και νόμιμης δραστηριότητας.

Η υλοποίηση των μοντέλων ανίχνευσης διαταραχών πρωτοκόλλου είναι ευκολότερη συγκριτικά με αυτή της ανίχνευσης διαταραχών, αφού γίνεται χρήση προκαθορισμένων κανόνων από τα RFC και όχι συνόλων εκπαίδευσης.

Τέλος το συγκεκριμένο μοντέλο σε σχέση με αυτό της κακής συμπεριφοράς, στηρίζεται στην υπόθεση, πως αν τηρούνται όλες οι προδιαγραφές των αντίστοιχων πρωτοκόλλων, η πολιτική ασφαλείας δεν δύναται να παραβιαστεί.

2.4 Οργάνωση συστημάτων ανίχνευσης εισβολών

Ένα σύστημα ανίχνευσης εισβολών οργανώνεται με βάση τους τρόπους παρακολούθησης των συστημάτων, καθώς και της επιλογή των μοντέλων εισβολών .

2.4.1 Παρακολούθηση της κυκλοφορίας στο δίκτυο: NSM

Το σύστημα Network Security Monitor [10] είναι ένα σύστημα ανίχνευσης εισβολών στο οποίο ο διευθυντής αξιοποιεί τόσο το μοντέλο κακής συμπεριφοράς όσο και το μοντέλο ανίχνευσης διαταραχών. Αρχικά το συγκεκριμένο σύστημα διαμορφώνει μια κατατομή για την αναμενόμενη χρήση του δικτύου. Στη συνέχεια συγκρίνει την κατατομή αυτή με την τρέχουσα χρήση του. Παράλληλα επιτρέπει και τον καθορισμό κανόνων (υπογραφών), ώστε να ανιχνεύονται συγκεκριμένες ακολουθίες της κίνησης του δικτύου, οι οποίες αναφέρονται σε πιθανές επιθέσεις.

Ταυτόχρονα, το NSM παρακολουθεί την πηγή της δικτυακής κίνησης, τον προορισμό και την παρεχόμενη υπηρεσία και ορίζει μια μοναδική ταυτότητα σύνδεσης για κάθε σύνδεση που πραγματοποιείται (connection ID). Ουσιαστικά, το NSM αξιοποιεί τον αριθμό των πακέτων που ανταλλάσσονται σε κάθε σύνδεση σε μια συγκεκριμένη χρονική περίοδο αλλά και το σύνολο των δεδομένων που περιλαμβάνονται στα πακέτα. Παράλληλα υπολογίζει και τον αναμενόμενο αριθμό των δεδομένων για την κάθε σύνδεση και τα συγκρίνει με αυτά της τρέχουσας . Αν ξεπερνούν το αναμενόμενο όριο, τότε το γεγονός αυτό ερμηνεύεται ως διαταραχή.

Οι υπεύθυνοι ανάπτυξης του NSM παρατήρησαν πως παράγονταν μεγάλος όγκος δεδομένων κατά την διάρκεια της ανάλυσης της δικτυακής κίνησης, με αποτέλεσμα το σύστημα να θεωρείται χρονικά δαπανηρό. Λόγω του γεγονότος αυτού, ομαδοποίησαν το σύνολο της δικτυακής κίνησης και δημιούργησαν συγκεκριμένους κανόνες (υπογραφές) που ήταν η βάση για την εξέλιξη του συστήματος σε ένα συνδυαστικό μοντέλο ανίχνευσης διαταραχών και κακής συμπεριφοράς.

2.4.2 Συνδυασμένη προσέγγιση:DIDS

Το σύστημα Distributed Instruction Detection System – DIDS [11] αποτελεί υβριδική λύση, αφού συνδυάζει τόσο μεμονωμένα, όσο και δικτυακά συστήματα ανίχνευσης εισβολών. Το DIDS συνδυάζει τις λειτουργίες του NSM με την δυνατότητα παρακολούθησης για ενδεχόμενες εισβολές σε μεμονωμένα συστήματα. Παράλληλα διαφοροποιείται στο σύνολο ταυτοτήτων δικτύου που αποδίδονται σε κάθε χρήστη, αφού αυτές είναι περισσότερες από μία. Ο λόγος που συνέβη το παραπάνω γεγονός ήταν η αδυναμία των αντιπροσώπων του συστήματος να αναγνωρίζουν τις περιπτώσεις όπου οι εισβολείς μετακινούνταν μεταξύ των συστημάτων . Κατά την διαδικασία της λειτουργίας του συγκεκριμένου συστήματος, τα δεδομένα εκπαίδευσης συλλέγονται από τους αντιπροσώπους με τα παρακάτω κατά σειρά βήματα:

- Αρχικά, συλλέγονται οι υπό εξέταση πληροφορίες τόσο από τους αντιπροσώπους του δικτύου όσο και από αυτούς των μεμονωμένων συστημάτων.
- Στη συνέχεια, εντοπίζονται όλοι οι χρήστες του δικτυακού συστήματος. Σε κάθε έναν από αυτούς αντιστοιχίζεται ένα υποκείμενο. Σε αυτό το υποκείμενο καταχωρούνται η ταυτότητα του χρήστη αλλά και οι ενέργειες που σχετίζονται με αυτόν.
- Ακόμη, κάποιες πληροφορίες που εξάγονται από τις ενέργειες του χρήστη, όπως το ποσοστό χρήστης της μνήμης, ο χρόνος χρήσης του επεξεργαστή αλλά και πληροφορίες ομοιότητας γεγονότων εξετάζονται. Χαρακτηριστικό παράδειγμα αυτών των πληροφοριών, είναι το ενδεχόμενο ο χρήστης να συνδεθεί στο σύστημα σε περίοδο που δεν έχει ξανασυνδεθεί χρονικά στο παρελθόν, γεγονός που θα θεωρηθεί ύποπτο.
- Παράλληλα πραγματοποιείται επόπτευση των απειλών στο δίκτυο. Είναι αναγκαίο να αναφερθεί πως απειλή ορίζεται ως η κακή συμπεριφορά που πρόκειται να παραβιάσει την πολιτική ασφαλείας του συστήματος χωρίς όμως να καταφέρει να την τροποποιήσει. Τέλος η απειλή αντίστοιχα καλείται ύποπτη αν δεν παραβιάζει την πολιτική ασφαλείας αλλά φαίνεται πως ενδέχεται να πραγματώσει μία επίθεση.
- Βαθμολογείται η κατάσταση ασφάλειας του δικτύου με βάση τις απειλές προς το σύστημα του προηγούμενου επιπέδου.

Τέλος κρίνεται απαραίτητο να σημειωθεί πως κάθε κανόνας του DIDS προσδιορίζεται από μια αξία. Αυτή χρησιμοποιείται για τον υπολογισμό της βαθμολογίας ενός συστήματος. Πιο συγκεκριμένα ο υπεύθυνος ασφαλείας δίνει αναφορά στο σύστημα ανάλυσης και σε περίπτωση λάθος ειδοποιήσεων η αξία αυτή ελαττώνεται.

2.4.3 Αυτόνομοι πράκτορες

Οι M. Crosbie και Spafford εξέτασαν πολλά συστήματα ανίχνευσης εισβολών και τα συνέκριναν μεταξύ τους με γνώμονα την ανοχή που παρουσίαζαν σε σφάλματα. Μετά από εκτενή έρευνα κατέληξαν στο συμπέρασμα, πως τα τυπικά συστήματα ανίχνευσης εισβολών δεν είναι τόσο αποτελεσματικά αφού στην περίπτωση που ο διευθυντής αποτύχει, τότε το IDS δεν θα λειτουργήσει και το σύστημα καθίσταται ευπρόσβλητο. Οι ίδιοι πρότειναν την δημιουργία ενός συστήματος, που περιλαμβάνει ξεχωριστές οντότητες ανεξάρτητες μεταξύ τους που όμως ανταλλάσσουν τις πληροφορίες που λαμβάνουν. Πιο συγκεκριμένα η αρχιτεκτονική του συστήματος περιλάμβανε αντιπροσώπους, όπου ο καθένας από αυτούς είχε εσωτερικό μοντέλο διευθυντή. Το προαναφερόμενο είχε τη δυνατότητα να αναλύει τις πληροφορίες που λαμβάνει ο εκάστοτε αντιπρόσωπος. Οι συνδυασμοί αυτοί ήταν οι λεγόμενοι αυτόνομοι πράκτορες.

Τα πλεονεκτήματα των αυτόνομων πρακτόρων ποικίλλουν με ένα από αυτά να αποτελεί το γεγονός πως αν κάποιος από τους αντιπροσώπους σταματήσει να λειτουργεί δεν επηρεάζεται ο συνολικός μηχανισμός άμυνας, αφού κάθε αντιπρόσωπος είναι ανεξάρτητος. Επιπλέον αν κάποιος εισβολέας «ρίξει» έναν αντιπρόσωπο δεν γνωρίζει πληροφορίες για τους υπόλοιπους του συστήματος ή για αυτούς που ελέγχουν το δίκτυο. Ακόμα αφού υπάρχουν πολλοί και ανεξάρτητοι αντιπρόσωποι ο καθένας μπορεί να εξειδικευθεί σε κάτι συγκεκριμένο, όπως ο έλεγχος ενός πόρου. Με αυτόν τον τρόπο κάθε αντιπρόσωπος παραμένει μικρός και απλός και ικανοποιεί την βασική αρχή οικονομίας των μηχανισμών (economy of mechanism).

Ωστόσο, η αρχιτεκτονική που πρότειναν οι M. Crosbie και Spafford έχει υψηλό υπολογιστικό κόστος (overhead). Αυτό συμβαίνει, γιατί μειώνονται όπως αναφέρεται και παραπάνω οι αρμοδιότητες του κάθε αντιπροσώπου .Επομένως χρειάζονται και περισσότεροι σε αριθμό για την σωστή και ολοκληρωμένη παρακολούθηση του δικτύου.

2.5 Απόκριση στις εισβολές

Μετά την διαδικασία ανίχνευσης των εισβολών σε ένα σύστημα είναι αναγκαίο να αναλυθούν και οι τρόποι με τους οποίους μπορεί αυτό να προστατευθεί. Ο τομέας της απόκρισης στην εισβολή είναι εκείνος που ασχολείται με το παραπάνω ζήτημα. Στόχος του είναι η αντιμετώπιση της αποπειραθείσας εισβολής με τέτοιο τρόπο, ώστε να ελαχιστοποιείται η ζημιά στο σύστημα.

2.5.1 Συστήματα Πρόληψης Εισβολών

Τα συστήματα πρόληψης εισβολών (Intrusion Prevention System – IPS) είναι το επόμενο βήμα στην εξέλιξη των ΣΑΕ. Τα προαναφερόμενα στοχεύουν στην αντιμετώπιση των επιθέσεων πριν εκείνες ολοκληρωθούν. Πιο συγκεκριμένα κατά την ανίχνευση μία εισβολής επιθυμητός στόχος είναι η άμεση αυτόματη διακοπή της χωρίς την παρέμβαση του ανθρώπινου παράγοντα. Με αυτόν τον τρόπο ελαχιστοποιείται η χρονική διάρκεια εξέλιξης της επίθεσης.

2.5.2 Ενεργές αποκρίσεις

Οι ενεργές αποκρίσεις είναι αυτοματοποιημένες ενέργειες που πραγματοποιούνται από τα ΣΑΕ . Αυτές στοχεύουν στην έγκαιρη αντιμετώπιση συγκεκριμένου είδους επιθέσεων. Αντίθετα με το IPS το σύστημα υφίσταται ήδη συγκεκριμένη εισβολή. Στη συνέχεια παρουσιάζονται οι ενέργειες στις οποίες μπορεί να προβεί το ΣΑΕ:

- ***Η συλλογή επιπρόσθετων πληροφοριών***: Η λειτουργία αυτή απαιτεί την συγκέντρωση περαιτέρω πληροφοριών για μία πιθανή εισβολή. Αυτό έχει σαν αποτέλεσμα την άνοδο της ακρίβειας όσον αφορά τον τύπο και το είδος της επίθεσης. Ανάλογα με τις πληροφορίες που συλλέγονται το σύστημα ανίχνευσης μπορεί να προβεί σε άλλες ενέργειες και να λάβει αποφάσεις.
- ***Η παρεμπόδιση του επιτιθέμενου***: Αυτή η λειτουργία στοχεύει στον άμεσο τερματισμό της επίθεσης ή στον περιορισμό της εξάπλωσής της στο σύστημα. Πιο συγκεκριμένα επαναπροσδιορίζονται οι κανόνες ασφαλείας του τοίχου προστασίας (firewall) ή των δρομολογητών που περιέχει το σύστημα. Με αυτόν τον τρόπο είναι δυνατόν να αποκλειστεί η IP διεύθυνση του επιτιθέμενου.
- ***Η αντεπίθεση στον επιτιθέμενο***: Η ενέργεια αυτή περιλαμβάνει δύο μορφές. Η πρώτη υπάγεται στο πλαίσιο υπαρχόντων νομικών μηχανισμών, οι οποίοι απαιτούν την σύνδεση με αποδεικτικά στοιχεία (chain of evidence). Με αυτόν τον τρόπο οι δικαστικές αρχές μπορούν να καταλάβουν πως πρόκειται για πραγματική επίθεση. Η επόμενη λύση σχετίζεται με την δημιουργία μιας τεχνικής επίθεσης, ώστε ο επιτιθέμενος να τερματίσει άμεσα την επίθεση ή να αποθαρρυνθεί για πιθανές μελλοντικές. Ωστόσο, αυτή η λύση δεν προτείνεται, αφού μπορεί να προκαλέσει αντίθετα αποτελέσματα με ποινικές διώξεις, πρόκληση βλάβης σε υπολογιστικά συστήματα κοκ.

2.5.3 Παθητικές αποκρίσεις

Ο στόχος των παθητικών αποκρίσεων είναι να ειδοποιηθεί ο υπεύθυνος ασφαλείας του συστήματος για την ύπαρξη εισβολών σε αυτό. Οι ειδοποιήσεις που αποστέλλονται μπορούν να έχουν διάφορους βαθμούς λεπτομέρειας. Ακόμα μπορούν να εμφανίζονται σε διάφορα σημεία του συστήματος από συγκεκριμένο χώρο, σε συσκευές τήλε-ειδοποίησης μέχρι τα αναδυόμενα παράθυρα. Επιπλέον, υπάρχουν συστήματα που τις ειδοποιήσεις τις αποστέλλουν σε ένα κεντρικό σύστημα που διαχειρίζεται το δίκτυο με τη χρήση του πρωτοκόλλου διαχείρισης δικτύων (SNMP).

Η αποθήκευση των ειδοποιήσεων αυτών καθώς και των πληροφοριών που προκύπτουν από μηχανισμούς ασφαλείας καθιστούν πιο σαφή την κατάσταση που βρίσκεται το δίκτυο, αφού συσχετίζονται αποτελέσματα από διαφορετικές πηγές.

Κεφάλαιο 3: Μηχανική Μάθηση και Τεχνητά Νευρωνικά Δίκτυα

Στο παρόν κεφάλαιο πραγματοποιείται εισαγωγή στον τομέα της μηχανικής μάθησης κι των κατηγοριών της καθώς και στα τεχνητά νευρωνικά δίκτυα, εξετάζοντας τον ορισμό του τεχνητού νευρώνα αλλά και πως αυτός συνθέτει ένα ολοκληρωμένο τεχνητό νευρωνικό δίκτυο . Ακόμα περιγράφονται οι κατηγορίες στις οποίες διακρίνεται. Επιπλέον παρουσιάζονται οι πιο διαδεδομένοι αλγόριθμοι μηχανικής μάθησης που χρησιμοποιήθηκαν προκειμένου να αναπτυχθεί το σύστημα ανίχνευσης εισβολών στην παρούσα διπλωματική.

3.1 Μηχανική Μάθηση

Η μηχανική μάθηση αποτελεί προσέγγιση για την επίτευξη της τεχνητής νοημοσύνης, αφού παρέχει την εύκολη και γρήγορη εμφύτευση νοημοσύνης σε μηχανές μέσω χρήσης ετικετών. Εξαιτίας του παραπάνω γεγονότος, η μηχανική μάθηση αποτελεί αναπόσπαστο κομμάτι σχεδόν κάθε τομέα στην σημερινή εποχή. Πιο συγκεκριμένα μέσω αυτής πραγματοποιείται η συλλογή δεδομένων από χρήστες με σκοπό την εκπαίδευση μοντέλων για την καλύτερη εξυπηρέτησή τους .

Τα βαθιά νευρωνικά δίκτυα (Deep Neural Networks), είναι μια κατηγορία αλγορίθμων της μηχανικής μάθησης η οποία, εξαιτίας της ακριβείας της, είναι πολύ δημοφιλής σε πολλούς τομείς .Ωστόσο, σε πολλές περιπτώσεις είναι ευπαθής απέναντι σε κακόβουλες ενέργειες. Τα ΤΝΔ εκπαιδεύονται, ώστε να μπορούν να λύνουν τα προβλήματα που τους ανατίθενται ή να είναι ικανά να επιτελούν ορισμένες διεργασίες από μόνα τους λ.χ. να αναγνωρίζουν εισβολές στο δίκτυο. Προτού πραγματοποιηθεί εκτενή αναφορά στα ΤΝΔ και στον τρόπο λειτουργίας τους, είναι χρήσιμο να αναφερθούν οι κατηγορίες που διακρίνεται η Μηχανική Μάθηση [12].

3.2 Κατηγορίες μηχανικής μάθησης

Οι αλγόριθμοι μηχανικής μάθησης κατηγοριοποιούνται με βάση τον τρόπο με τον οποίο λαμβάνουν την μάθηση ή με τον τρόπο μέσω του οποίου δίνεται η ανάδραση στην εκμάθηση για το ανεπτυγμένο σύστημα. Οι κατηγορίες της μηχανικής μάθησης είναι οι εξής κατά σειρά: επιβλεπόμενη, μη επιβλεπόμενη, ημι-επιβλεπόμενη και ενισχυτική.

3.2.1 Επιβλεπόμενη μηχανική μάθηση

Με την επιβλεπόμενη μηχανική μάθηση [13] (supervised machine learning), στόχος είναι η δημιουργία ενός μοντέλου, το οποίο είναι ικανό να προβλέψει ιδιότητες που δεν είναι παρατηρούμενες σε άγνωστα αντικείμενα, με τη χρήση ως σώματος εκπαίδευσης παραδειγμάτων όπου οι ιδιότητες–χαρακτηριστικά είναι γνωστές. Πιο συγκεκριμένα με την χρήση ενός προκαθορισμένου και ήδη κατηγοριοποιημένου συνόλου εκπαίδευσης τα υπό εξέταση αντικείμενα κατηγοριοποιούνται σε μία από τις υπάρχουσες κλάσεις.

Η επιβλεπόμενη μηχανική μάθηση περιλαμβάνει δύο βασικές καταστάσεις αυτή της ταξινόμησης (classification) και αυτή της παλινδρόμησης (regression), έννοιες που θα αναλυθούν παρακάτω.

- ***Ταξινόμηση:*** Η ταξινόμηση είναι η διαδικασία που εφαρμόζεται προκειμένου να γίνει πρόβλεψη μιας κλάσης ή ετικέτας. Πιο συγκεκριμένα οι νέες μεταβλητές εισόδου του συστήματος αντιστοιχίζονται σε μία κλάση που μπορεί και να ανήκουν . Αυτό γίνεται με βάση ένα προκαθορισμένο κατηγοριοποιημένο σύνολο δεδομένων (labeled data) που έχει δημιουργηθεί από τα δεδομένα εκπαίδευσης (training data) . Τα παραπάνω δεδομένα χρησιμοποιούνται για την εκπαίδευση ενός ταξινομητή, ώστε ο αλγόριθμος να παρουσιάζει μεγάλη απόδοση και σε δεδομένα που δεν έχουν ταξινομηθεί.
- ***Παλινδρόμηση:*** Η διαδικασία της παλινδρόμησης χρησιμοποιείται με σκοπό την πρόβλεψη συνεχόμενης τιμής. Πιο συγκεκριμένα έχει ως σκοπό την πιο κοντινή πρόβλεψη στην πραγματική τιμή της εξόδου αλλά και την αξιολόγηση αυτής με τον υπολογισμό της τιμής του σφάλματος. Όσο πιο μικρό είναι το σφάλμα τόσο υψηλότερη είναι και η ακρίβεια του μοντέλου παλινδρόμησης. Οι τύποι παλινδρόμησης είναι οι εξής:

    1. Γραμμική παλινδρόμηση (Linear Regression),
    2. Πολυωνυμική παλινδρόμηση (Polynomial Regression),
    3. Παλινδρόμηση διανυσμάτων υποστήριξης (Support Vector Regression),
    4. Παλινδρόμηση δέντρων απόφασης (Decision Tree Regression),
    5. Παλινδρόμηση τυχαίων δασών (Random Forest Regression).

3.2.2 Μη επιβλεπόμενη μηχανική μάθηση

Στην μη επιβλεπόμενη μάθηση [13] (unsupervised machine learning) ο αλγόριθμος ενεργεί χωρίς καθοδήγηση. Αυτό συμβαίνει, καθώς χρησιμοποιούνται πληροφορίες που δεν είναι ταξινομημένες. Σκοπός αυτής της κατηγορίας είναι η κατηγοριοποίηση ασαφών δεδομένων με βάση κάποιες ομοιότητες ή μοτίβα που παρουσιάζουν. Άρα η μηχανή περιορίζεται στην εύρεση κάποιων κρυφών δομών στα δεδομένα που διαθέτει.

Οι τεχνικές που εφαρμόζονται από τους αλγορίθμους μηχανικής μάθησης είναι :

- ***Ομαδοποίηση(clustering):*** Με την ομαδοποίηση διερευνώνται τα δεδομένα, ώστε να διαχωριστούν σε ομάδες με βάση κάποια μοτίβα που εντοπίζονται, χωρίς όμως καμία προηγούμενη γνώση πάνω στα χαρακτηριστικά κάθε ομάδας. Επομένως, η ομαδοποίηση γίνεται με βάση τις ομοιότητες αλλά και τις διαφορές που παρουσιάζουν τα δεδομένα, γεγονός που χρησιμοποιείται στην ανίχνευση ανωμαλιών.
- ***Μείωση διαστάσεων (Dimensionality reduction):*** Είναι γνωστό πως τα εισερχόμενα δεδομένα περιλαμβάνουν θόρυβο. Εξαιτίας αυτού, οι αλγόριθμοι μηχανικής μάθησης μειώνουν τις διαστάσεις των δεδομένων, προκειμένου να εξαλειφθεί και ο θόρυβος. Οι πιο γνωστοί αλγόριθμοι είναι:
  1. Κ-μέσων συσταδοποίησης (k-means clustering)
  2. t-SNE (t-Distributed Stochastic Neighbor Embedding)
  3. PCA (Principal Component Analysis)
  4. Κανόνες συσχετίσεων (Association rules)

3.2.3 Ημι -επιβλεπόμενη μηχανική μάθηση

Στην Ημι-επιβλεπόμενη μάθηση (semi-supervised machine learning) [13] ο αλγόριθμος χρησιμοποιεί ένα περιορισμένο σύνολο με επισημασμένα δεδομένα. Έτσι δημιουργείται ένα μερικώς εκπαιδευμένο μοντέλο, όπου καλείται να κατηγοριοποιήσει και τα μη επισημασμένα δεδομένα. Εξαιτίας αυτού του γεγονότος, τα αποτελέσματα της ταξινόμησης θεωρούνται ψευδό-επισημασμένα. Τέλος αφού συνδυαστούν τα παραπάνω δεδομένα αναπτύσσεται ένας ξεχωριστός αλγόριθμος, που συνδυάζει στοιχεία τόσο της επιβλεπόμενης όσο και της μη επιβλεπόμενης μάθησης.

3.2.4 Ενισχυμένη μηχανική μάθηση

Η ενισχυμένη μάθηση (reinforcement learning) χρησιμοποιείται για την ανάπτυξη ενός αυτοσυντηρούμενου συστήματος, που προσπαθεί και αποτυγχάνει και βελτιώνεται με βάση το συνδυασμό των δεδομένων και των αλληλεπιδράσεων με τα εισερχόμενα δεδομένα. Η ενισχυμένη μάθηση εκμεταλλεύεται την χρήση της τεχνικής που ονομάζεται εξερεύνηση/εκμετάλλευση. Η λειτουργία είναι απλή, αφού η δράση λαμβάνει χώρα, στη συνέχεια παρατηρούνται συνέπειες και η επόμενη ενέργεια είναι αυτή που εξετάζει τα αποτελέσματα της πρώτης δράσης. Βασικό στοιχείο

των αλγορίθμων της ενισχυμένης μάθησης είναι τα σήματα ανταμοιβής .Αυτά εμφανίζονται κατά την εκτέλεση συγκεκριμένων εργασιών. Οι πιο συνήθεις αλγόριθμοι ενίσχυσης είναι:

1. Q-Learning, Temporal Difference (TD)
2. Monte-Carlo Tree Search (MCTS)
3. Asynchronous Actor-Critic Agents (A3C)

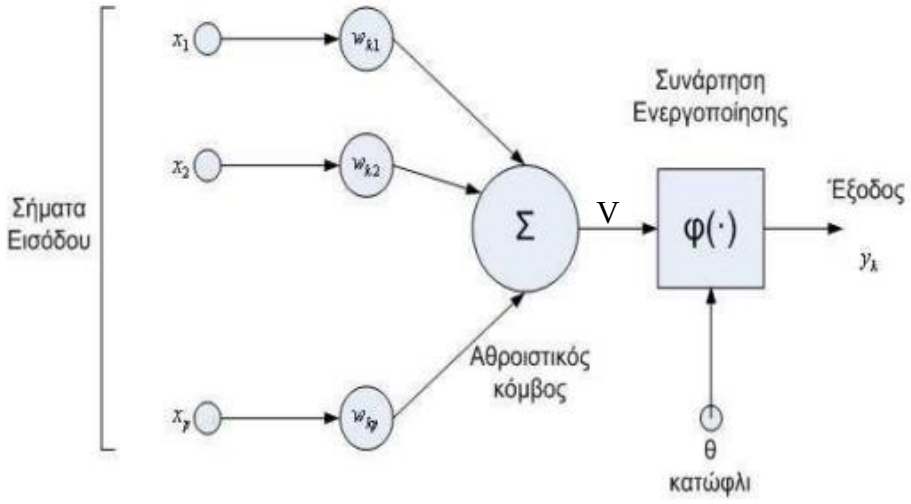
3.3 Ο Τεχνητός Νευρώνας

Στη σημερινή εποχή ο τεχνητός νευρώνας έχει σχεδιαστεί προκειμένου να μιμείται τον βιολογικό νευρώνα . Πιο συγκεκριμένα από την βιολογία γνωρίζουμε, πως η δομική μονάδα του εγκεφάλου είναι ο νευρώνας. Αυτός αποτελείται από το σώμα, το οποίο αποτελεί και τον πυρήνα του, τους δενδρίτες μέσω των οποίων παραλαμβάνει σήματα από γειτονικούς νευρώνες (σημεία εισόδου) καθώς και τον άξονα, που είναι η έξοδος του νευρώνα αλλά και το μέσο, όπου συνδέεται με άλλους νευρώνες. Σε κάθε δενδρίτη υπάρχει η σύναψη. Αυτή είναι ένα απειροελάχιστο κενό όπου μέσω των χημικών διαδικασιών επιταχύνει ή επιβραδύνει τη ροή των ηλεκτρικών φορτίων προς το σώμα του νευρώνα. Οι επιστήμονες ήθελαν να δημιουργήσουν τέτοιου είδους νευρώνες, που σκέφτονται σαν άνθρωποι, αλλά λύνουν και προβλήματα που μέχρι τότε ήταν άλυτα. Για αυτό το σκοπό δημιούργησαν τους τεχνητούς νευρώνες.

Ο τεχνητός νευρώνας αποτελείται από ένα σύνολο δεδομένων εισόδου (input), που εφαρμόζεται στην είσοδο ενός νευρώνα. Παράλληλα κάθε ένα σύνολο από αυτά αντιπροσωπεύει και τα δεδομένα εξόδου από κάποιον άλλον νευρώνα. Κάθε είσοδος είναι πολλαπλασιασμένη με ένα βάρος (weight) ανάλογα με τη συναπτική δύναμη που έχει. Στην συνέχεια όλες οι είσοδοι πολλαπλασιασμένες με τα αντίστοιχα βάρη, αθροίζονται και έτσι καθορίζουν τον βαθμό ενεργοποίησης κάθε νευρώνα.

Γενικότερα από τα παραπάνω προκύπτει το εξής: οι είσοδοι των νευρώνων συμβολίζονται με x (x1,x2,…xn), τα βάρη αυτών με w (w1,w2,…,wn), αλλά και το γινόμενο όλων των νευρώνων με τα τελευταία με το κεφαλαίο γράμμα ∑. Το αθροιστικό τμήμα των εισόδων με τα βάρη τους, συμβολίζεται με το γράμμα V . Τελικά με μία απλή μαθηματική εξίσωση προκύπτει το εξής:

$$V = x_1 * w_1 + x_2 * w_2 + ...x_n * w_n$$

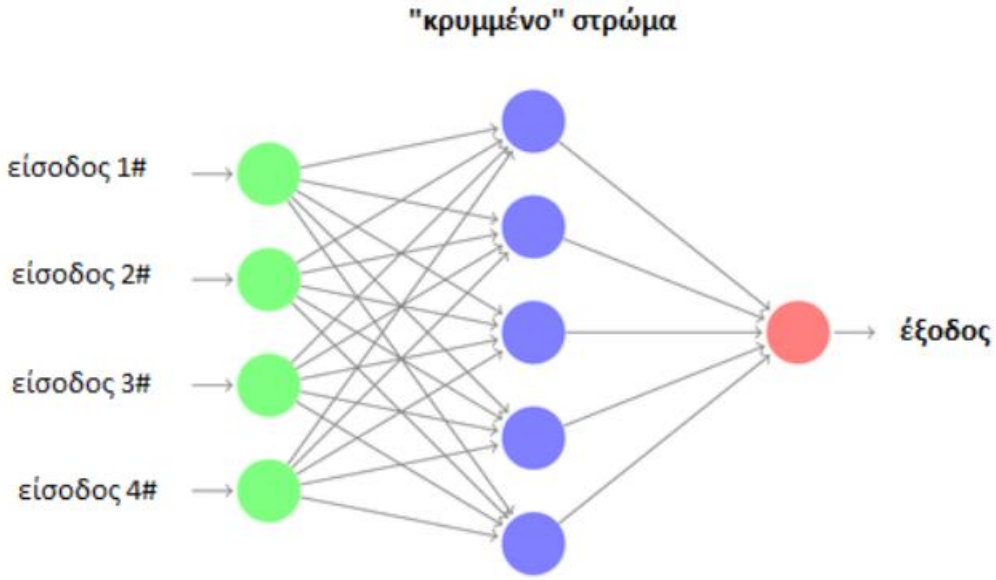


Εικόνα 8:Μορφή τεχνητού νευρώνα [14]

3.4 Τεχνητό Νευρωνικό Δίκτυο

Οι τεχνητοί νευρώνες αποτελούν την βάση για την δημιουργία ενός κεντρικού νευρικού συστήματος του λεγόμενου τεχνητού νευρωνικού δικτύου. Αναλυτικότερα οι τεχνητοί νευρώνες είναι οργανωμένοι σε επίπεδα ή αλλιώς κρυφά στρώματα (hidden layers) και κάθε ένα από αυτά αποτελεί είσοδο για άλλον νευρώνα.

Το πλήθος των επιπέδων και οι νευρώνες σε καθένα από αυτά δεν έχουν όριο στο πλήθος τους. Ωστόσο, αυξάνοντας τα επίπεδα και τους νευρώνες αυξάνονται και οι συνάψεις .Αυτό έχει ως αποτέλεσμα το δίκτυο να είναι δαπανηρό, τόσο στο θέμα μνήμης όσο και στο θέμα της επεξεργαστικής ικανότητας που απαιτείται.



Εικόνα 9:Μορφολογία ΤΝΔ [15]

Το βασικότερο στοιχείο των νευρωνικών δικτύων είναι ο αλγόριθμος εκπαίδευσης τους, αφού είναι η διαδικασία μέσω της οποίας εισάγεται η γνώση στο δίκτυο. Οι δυο βασικές λειτουργίες των ΤΝΔ είναι αυτή της μάθησης και της ανάκλασης. Με τον όρο «μάθηση», ορίζεται η διαδικασία μέσω της οποίας τροποποιούνται τα βάρη των εισόδων, ώστε να παραχθεί συγκεκριμένη επιθυμητή έξοδος με τελικό στόχο την αύξηση της απόδοσης των νευρώνων. Παράλληλα με τον όρο «ανάκλαση», ορίζεται η διαδικασία κατά την οποία από δοθέντα διανύσματα εισόδου και συναπτικών βαρών υπολογίζεται αντίστοιχο διάνυσμα εξόδου.

Το τεχνητό νευρωνικό δίκτυο «κατακτά» την γνώση με την χρήση αλγορίθμων εκπαίδευσης. Αυτοί μπορεί να είναι αλγόριθμοι οπισθοδρόμησης, ομαδοποίησης και Δένδρων Απόφασης (Decision Tree). Οι παραπάνω έχουν ως στόχο να μειωθεί το σφάλμα μεταξύ της επιθυμητής αλλά και της τιμής που παράγει το δίκτυο. Τα ΤΝΔ χωρίζονται σε δύο κατηγορίες μάθησης την επιβλεπόμενη μάθηση (supervised learning) και μη επιβλεπόμενη μάθηση (Unsupervised Learning). Η διαδικασία της μάθησης που ακολουθεί ένα ΤΝΔ είναι η ακόλουθη με τα εξής απλά τρία βήματα. Αρχικά το τελευταίο διεγείρεται από το περιβάλλον του. Στη συνέχεια, υλοποιεί μεταβολές στις παραμέτρους του και αλληλοεπιδρά με το νέο περιβάλλον του, μετά τις προηγούμενες αλλαγές.

Στην συνέχεια περιγράφονται οι δυο κατηγορίες μάθησης που αναφέρθηκαν προηγουμένως αλλά και ο τρόπος λειτουργίας τους:

- ***Επιβλεπόμενη Μάθηση:*** Ο εκπαιδευτής προωθεί στο δίκτυο τις τιμές των εισόδων αλλά και των επιθυμητών εξόδων. Αρχικά οι τιμές των βαρών είναι τυχαίες, ενώ με την διαδικασία της εκπαίδευσης αυτές τροποποιούνται, ώστε να ελαττωθεί το τελικό σφάλμα που προκύπτει από την τρέχουσα έξοδο και την πραγματική. Με αυτόν τον τρόπο το σύστημα ωθείται στην μέγιστη απόδοση του, αλλά με μεγάλο υπολογιστικό κόστος.
- ***Μη επιβλεπόμενη Μάθηση:*** Στην μη επιβλεπόμενη μάθηση προσφέρεται η είσοδος αλλά όχι η επιθυμητή έξοδος. Το δίκτυο δεν πραγματοποιεί καμία σύγκριση για την πορεία του σφάλματος, καθώς δεν ακολουθεί κάποια εξωτερική παράμετρο για την τροποποίηση των βαρών αλλά μια συγκεκριμένη διαδικασία που οδηγεί στην εκπαίδευση του δικτύου. Ωστόσο, με την πραγματοποίηση ενός εσωτερικού ελέγχου το ΤΝΔ προσπαθεί να εντοπίσει κάποια μοτίβα ή πρότυπα που ακολουθεί η είσοδος προσαρμόζοντας ανάλογα τα βάρη, ώστε και η έξοδος να προκύψει σε παρόμοια μορφή. Με χρήση αυτής της τεχνικής το εκπαιδευόμενο δίκτυο ελέγχει τον εαυτό του και διορθώνει στον πιο αποδοτικό βαθμό τα σφάλματα που μπορεί να υπάρξουν στα δεδομένα. Ο μηχανισμός αυτός ονομάζεται μηχανισμός ανάδρασης (feedback). Επομένως, το δίκτυο είναι αυτό-εκπαιδευόμενο και μεταβάλλει μόνο του τις τιμές των βαρών του.

3.5 Τεχνητά νευρωνικά δίκτυα και μηχανική μάθηση στην ανίχνευση εισβολών

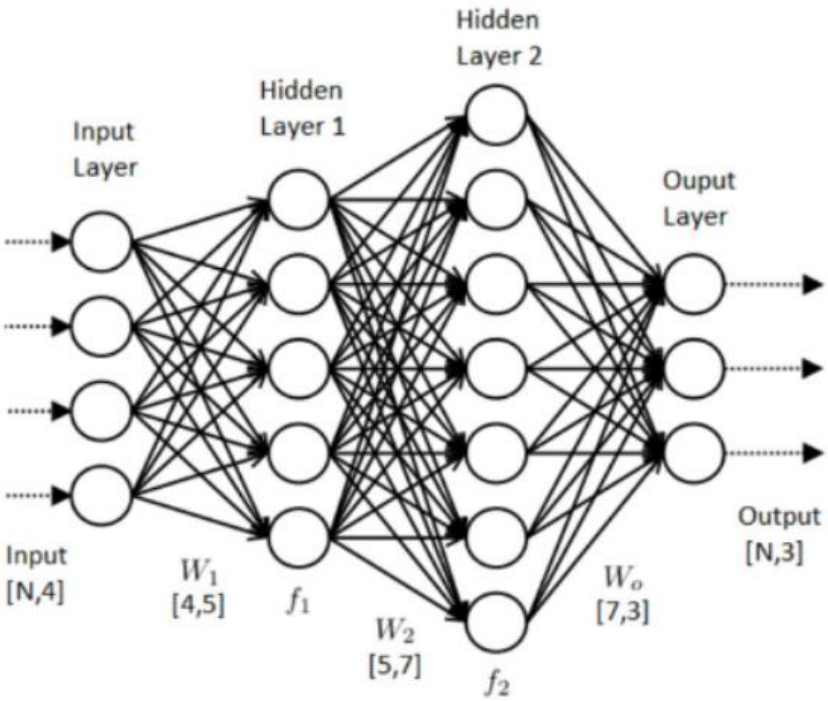
Είναι ευρέως γνωστό πως στη σημερινή εποχή η εξέλιξη των ΣΑΕ είναι μεγάλη. Ωστόσο, κοινή αδυναμία όλων αυτών παραμένει η δυσκολία στην ανίχνευση άγνωστων μορφών επιθέσεων . Η λύση στο πρόβλημα αποτελεί η χρήση των ΤΝΔ, αφού είναι αρκετά ικανά να προβλέψουν άγνωστες μορφές επιθέσεων αλλά και να ταξινομήσουν γνωστές κακόβουλες ενέργειες σε αντίστοιχες κατηγορίες.

Η πιο κοινή κατηγορία των ΤΝΔ είναι τα ΤΝΔ πολλαπλών επιπέδων, τα λεγόμενα Perceptron. Αρχικά χρησιμοποιήθηκαν για την ανίχνευση άγνωστων διαταραχών σε ένα σύστημα αλλά αργότερα και για την ταξινόμηση σε ήδη γνωστές κατηγορίες επιθέσεων. Το μοντέλο αυτό χρησιμοποιήθηκε για την υλοποίηση του ΣΑΠΕ στην παρούσα διπλωματική.

Πέρα από το μοντέλο του Perceptron, έγινε χρήση και άλλων βασικών αλγορίθμων Μηχανικής Μάθησης στη διπλωματική εργασία προκειμένου να υλοποιηθεί το ΣΑΠΕ. Οι αλγόριθμοι, όπως και ένα σύντομο θεωρητικό υπόβαθρό τους παρουσιάζονται στις επόμενες υπό-ενότητες.

3.5.1 Κατηγοριοποίηση με χρήση τεχνητών νευρωνικών δικτύων με πολλαπλά επίπεδα Perceptron

Τα ΤΝΔ πολλαπλών επιπέδων Perceptron [16] αποτελούνται από ένα επίπεδο εισόδου (input layer), το οποίο συντίθεται από πλήθος νευρώνων, ένα επίπεδο εξόδου (output layer) και ένα ή και περισσότερα κρυφά επίπεδα (hidden layer).



Εικόνα 10:Παράδειγμα νευρωνικού δικτύου [17]

Στην παραπάνω εικόνα απεικονίζεται ένα ΤΝΔ, το οποίο αποτελείται από ένα στρώμα εισόδου, ένα στρώμα εξόδου και δύο κρυφά επίπεδα. Ακόμα οι νευρώνες του ενός επιπέδου, επικοινωνούν με αυτούς του επόμενου επιπέδου. Επομένως το δίκτυο είναι πλήρως διασυνδεδεμένο και δεν υπάρχει περιορισμός στον αριθμό των κρυφών επιπέδων αλλά και στα σήματα εισόδου.

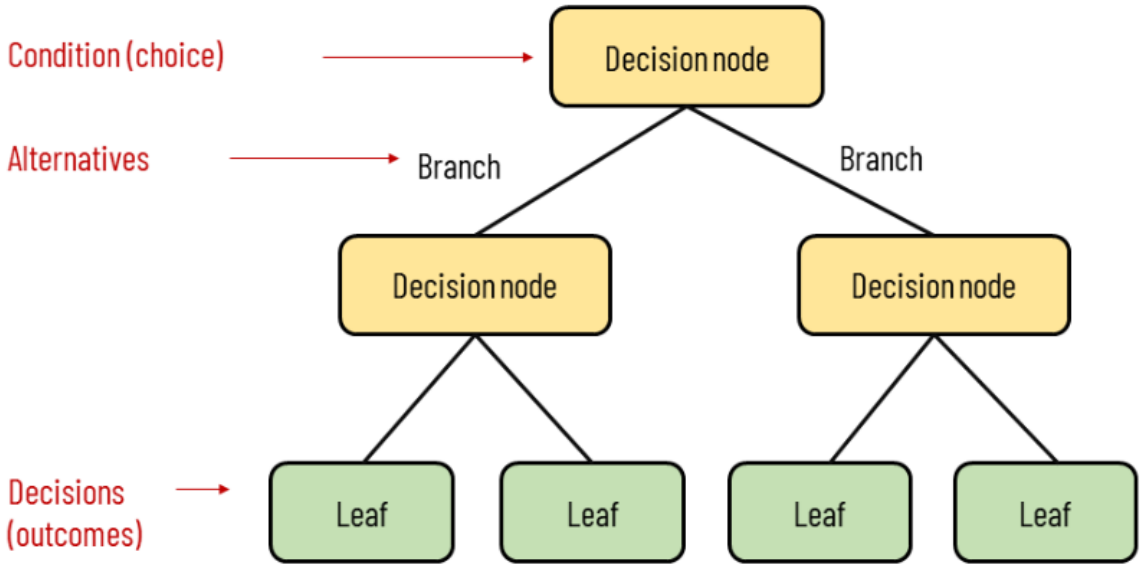
Επομένως, η λειτουργία του ΤΝΔ με πολλαπλά επίπεδα είναι η εξής: Οι νευρώνες που βρίσκονται στο επίπεδο εισόδου λαμβάνουν την πληροφορία και την μεταφέρουν, χωρίς να την επεξεργαστούν, στους νευρώνες του πρώτου κρυφού επιπέδου. Στη συνέχεια οι επόμενοι νευρώνες υπολογίζουν αθροίζοντας, τα γινόμενα των σημάτων, που εξέρχονται από τα προηγούμενα επίπεδα επί τα αντίστοιχα βάρη τους. Έπειτα γίνεται χρήση μιας συνάρτησης ενεργοποίησης, που λαμβάνει ως παράμετρο το προηγούμενο άθροισμα και αφαιρεί από αυτό την πόλωση του νευρώνα. Με αυτήν την διαδικασία εξάγεται τελικά το σήμα εξόδου.

3.5.2 Κατηγοριοποίηση με τον αλγόριθμο Decision Tree

Το δέντρο αποφάσεων [18] (Decision Tree) είναι ένας τύπος εποπτευόμενης μηχανικής εκμάθησης που χρησιμοποιείται για την κατηγοριοποίηση ή την πραγματοποίηση προβλέψεων με βάση τον τρόπο με τον οποίο απαντήθηκε ένα προηγούμενο σύνολο ερωτήσεων. Το μοντέλο αυτό είναι μια μορφή εποπτευόμενης μάθησης, αφού εκπαιδεύεται και δοκιμάζεται σε ένα σύνολο δεδομένων που περιέχει την επιθυμητή κατηγοριοποίηση.

Ένα δέντρο απόφασης μοιάζει με δέντρο. Η βάση του δέντρου είναι ο ριζικός κόμβος. Από τον ριζικό κόμβο ακολουθεί μια σειρά από κόμβους απόφασης που απεικονίζουν τις αποφάσεις που πρέπει να ληφθούν. Από τους κόμβους απόφασης είναι οι κόμβοι φύλλων που αντιπροσωπεύουν τις συνέπειες αυτών των αποφάσεων. Κάθε κόμβος απόφασης αντιπροσωπεύει μια ερώτηση ή ένα σημείο διαχωρισμού και οι κόμβοι φύλλων που προέρχονται από έναν κόμβο απόφασης αντιπροσωπεύουν τις πιθανές απαντήσεις. Οι κόμβοι φύλλων φυτρώνουν από κόμβους απόφασης παρόμοια με το πώς φυτρώνει ένα φύλλο σε ένα κλαδί δέντρου. Αυτός είναι ο λόγος που κάθε υπό-ενότητα ενός δέντρου αποφάσεων ονομάζεται «κλάδος».

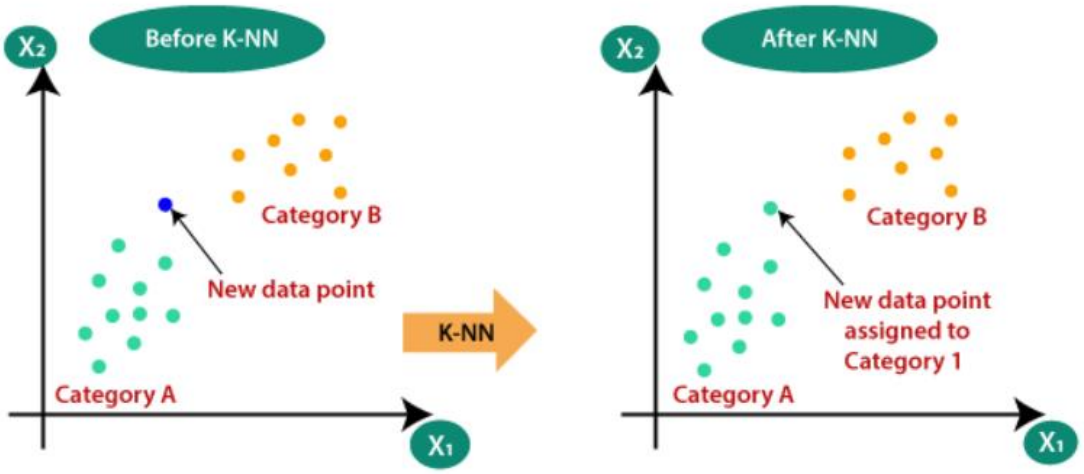
Ο στόχος της χρήσης ενός δέντρου αποφάσεων στο ΣΑΕ είναι η δημιουργία ενός μοντέλου εκπαίδευσης που χρησιμοποιείται για την πρόβλεψη της κλάσης ή της τιμής της μεταβλητής στόχου κατά την εκμάθηση απλών κανόνων απόφασης που συνάγονται από προηγούμενα δεδομένα (δεδομένα εκπαίδευσης). Στα δένδρα αποφάσεων για την πρόβλεψη μιας ετικέτας τάξης για μια εγγραφή αρχίζοντας από τη ρίζα του δέντρου συγκρίνονται οι τιμές του χαρακτηριστικού ρίζας με το χαρακτηριστικό της εκάστοτε εγγραφής.



Εικόνα 11: Μορφή Decision Tree [19]

3.5.3 Κατηγοριοποίηση με τον αλγόριθμο K-nearest neighbor

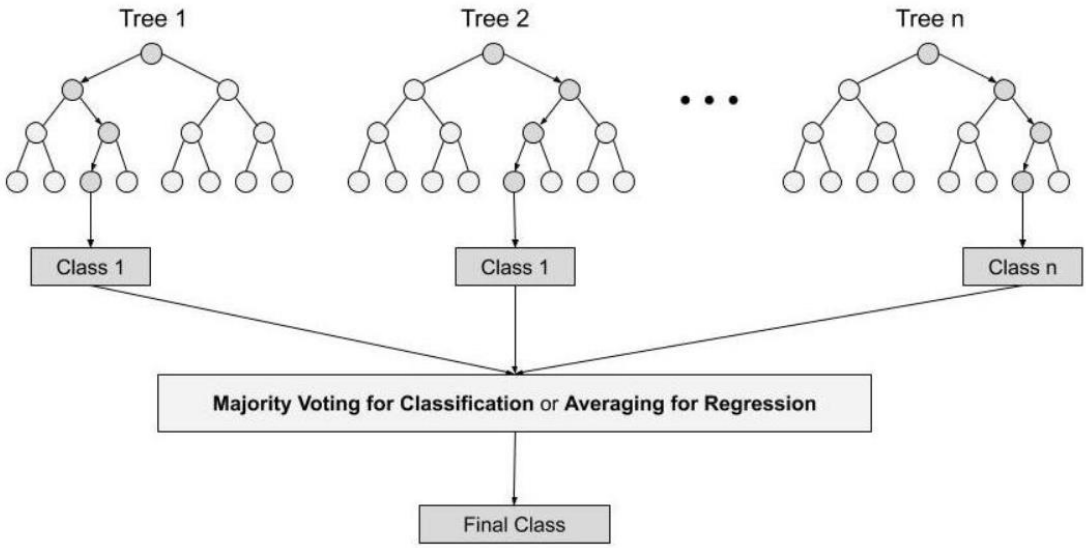
Ο ταξινομητής των k πλησιέστερων γειτόνων (K-Nearest Neighbor) [20] είναι ένας από τους απλούστερους αλγόριθμους μηχανικής εκμάθησης, που βασίζεται στην τεχνική εποπτευόμενης μάθησης. Υποθέτει την ομοιότητα μεταξύ της νέας περίπτωσης/δεδομένων και των διαθέσιμων περιπτώσεων και τοποθετεί τη νέα περίπτωση στην κατηγορία που είναι πιο όμοια με τις διαθέσιμες κατηγορίες. Αυτό σημαίνει ότι όταν εμφανίζονται νέα δεδομένα τότε μπορούν εύκολα να ταξινομηθούν σε μια κατηγορία χρησιμοποιώντας τον αλγόριθμο K-NN. Ο προαναφερόμενος, δύναται να χρησιμοποιηθεί για παλινδρόμηση καθώς και για ταξινόμηση, αλλά κυρίως χρησιμοποιείται για προβλήματα ταξινόμησης. Είναι ένας μη παραμετρικός αλγόριθμος, καθώς δεν κάνει καμία υπόθεση για τα υποκείμενα δεδομένα .Τέλος ο αλγόριθμος KNN στη φάση εκπαίδευσης απλώς αποθηκεύει το σύνολο δεδομένων και όταν λαμβάνει νέα δεδομένα, τότε τα ταξινομεί σε μια κατηγορία που μοιάζει πολύ με αυτό.



Εικόνα 12:Λειτουργία k-nn algorithm [21]

3.5.4 Κατηγοριοποίηση με τον αλγόριθμο Random Forest

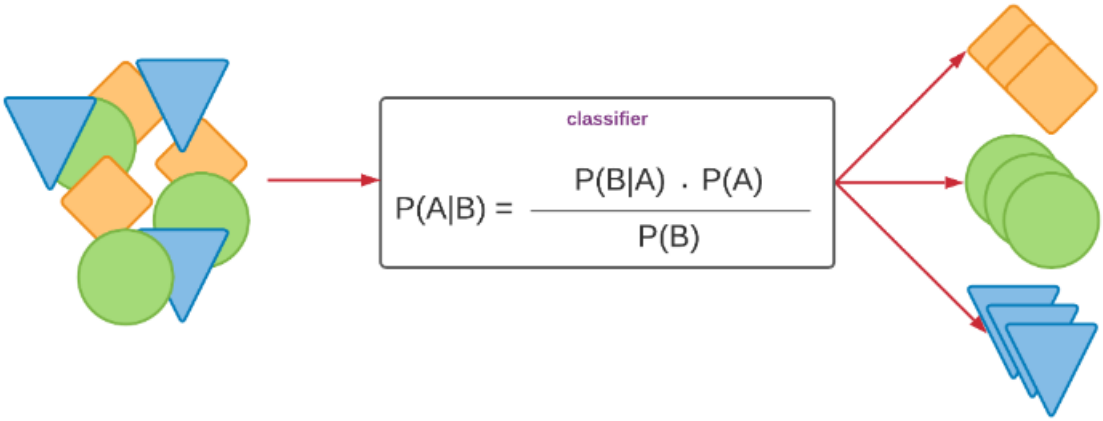
Το τυχαίο δάσος (Random Forest) [22] είναι ένας εποπτευόμενος αλγόριθμος μηχανικής μάθησης που χρησιμοποιείται ευρέως τόσο σε προβλήματα ταξινόμησης όσο και παλινδρόμησης. Δημιουργεί δένδρα απόφασης από τυχαίο υποσύνολο των δεδομένων, που χρησιμοποιούνται για εκπαίδευση. Ο αλγόριθμος προσθέτει τις αποφάσεις όλων των δένδρων και καθορίζεται η κλάση που θα κατηγοριοποιηθεί το αντικείμενο. Στην εικόνα που ακολουθεί απεικονίζεται η μορφή λειτουργίας του αλγορίθμου Random Forest.



Εικόνα 13:Μορφή λειτουργίας Random Forest [23]

3.5.5 Κατηγοριοποίηση με τον αλγόριθμο Naïve Bayes

Ο αφελής ταξινομητής Bayes (Naïve Bayes) [24] είναι ένας εποπτευόμενος αλγόριθμος μάθησης, ο οποίος βασίζεται στο θεώρημα Bayes και χρησιμοποιείται για την επίλυση προβλημάτων ταξινόμησης. Γίνεται χρήση του κυρίως στην ταξινόμηση κειμένου που περιλαμβάνει ένα σύνολο δεδομένων εκπαίδευσης υψηλών διαστάσεων. Ο Naïve Bayes Classifier είναι ένας από τους απλούς και πιο αποτελεσματικούς αλγόριθμους ταξινόμησης που βοηθά στη δημιουργία μοντέλων γρήγορης μηχανικής εκμάθησης για γρήγορες προβλέψεις. Είναι ένας πιθανοτικός ταξινομητής, που προβλέπει με βάση την πιθανότητα ενός αντικειμένου.



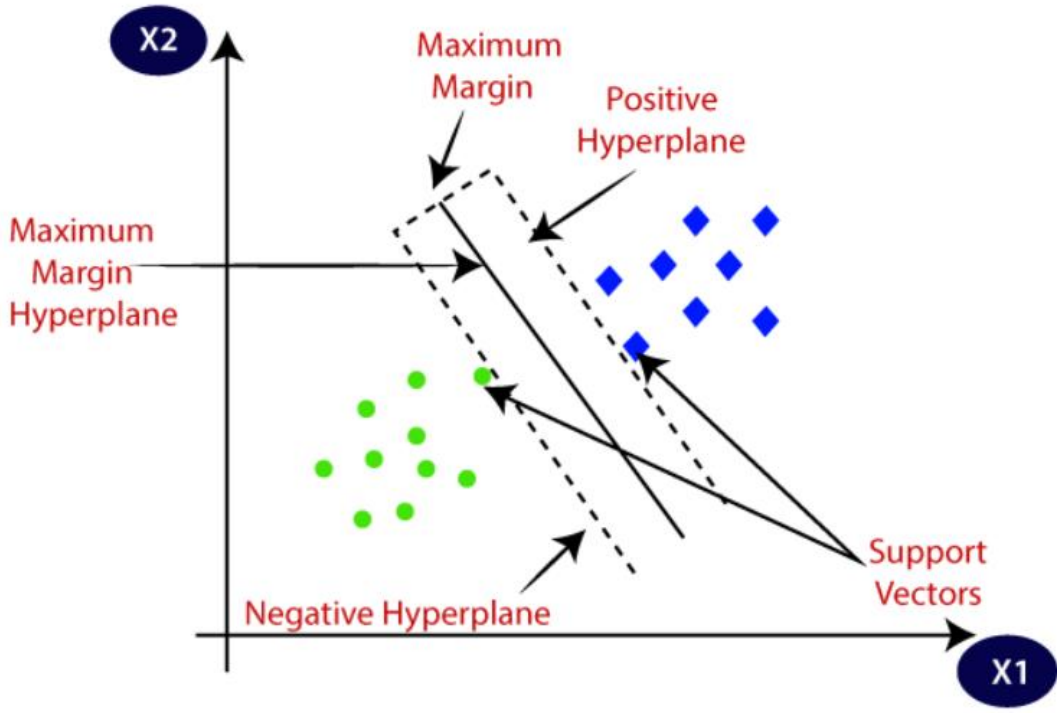
Εικόνα 14:Naïve Bayes classifier [25]

3.5.6 Κατηγοριοποίηση με τον αλγόριθμο SVM

Η μηχανή διανύσματος υποστήριξης (Support Vector Machine ή SVM) [26] είναι ένας από τους πιο δημοφιλείς αλγόριθμους εποπτευόμενης μάθησης, ο οποίος χρησιμοποιείται για προβλήματα ταξινόμησης και παλινδρόμησης. Ωστόσο, κατά κύριο λόγο, χρησιμοποιείται για προβλήματα ταξινόμησης στη μηχανική μάθηση.

Ο στόχος του αλγόριθμου SVM είναι να δημιουργήσει την καλύτερη γραμμή ή όριο απόφασης που μπορεί να διαχωρίσει το χώρο n-διαστάσεων σε κλάσεις, ώστε να πραγματοποιείται εύκολα η ταξινόμηση ενός νέου σημείου δεδομένων στη σωστή κατηγορία στο μέλλον. Το όριο καλύτερης απόφασης ονομάζεται υπερεπίπεδο.

Ο SVM επιλέγει τα ακραία σημεία/διανύσματα που βοηθούν στη δημιουργία του υπερεπίπεδου. Αυτές οι ακραίες περιπτώσεις ονομάζονται διανύσματα υποστήριξης και ως εκ τούτου ο αλγόριθμος ονομάζεται υποστηρικτική διανυσματική μηχανή. Στην παρακάτω εικόνα απεικονίζονται δύο διαφορετικές κατηγορίες ταξινόμησης χρησιμοποιώντας ένα όριο απόφασης ή ένα υπερεπίπεδο.



Εικόνα 15:SVM Classifier [27]

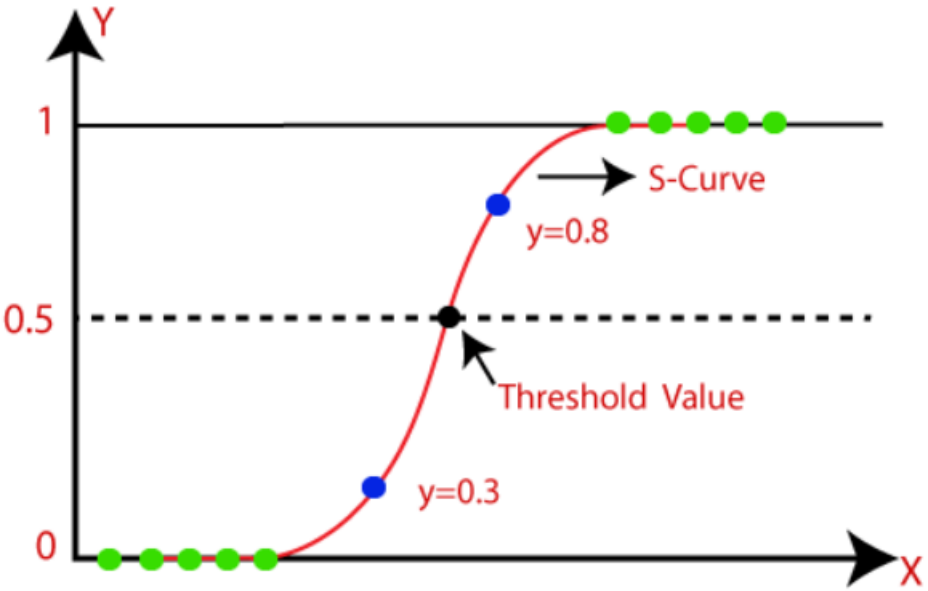
3.5.7 Κατηγοριοποίηση με τον αλγόριθμο Logistic Regression

Η λογιστική παλινδρόμηση (Logistic Regression) [28] είναι ένας από τους πιο δημοφιλείς αλγόριθμους μηχανικής μάθησης, ο οποίος εμπίπτει στην τεχνική της εποπτευόμενης μάθησης. Χρησιμοποιείται για την πρόβλεψη της κατηγορικής εξαρτημένης μεταβλητής αξιοποιώντας ένα δεδομένο σύνολο ανεξάρτητων μεταβλητών. Επομένως, το αποτέλεσμα πρέπει να είναι μια διακριτή τιμή. Μπορεί να είναι είτε Ναι είτε Όχι, 0 ή 1, Σωστό ή Λάθος . Ωστόσο, αντί να εξάγει την ακριβή τιμή 0 και 1, δίνει τις πιθανοτικές τιμές που βρίσκονται μεταξύ 0 και 1.

Η λογιστική παλινδρόμηση είναι παρόμοια με τη γραμμική παλινδρόμηση εκτός από τον τρόπο χρήσης τους. Η γραμμική παλινδρόμηση χρησιμοποιείται προκειμένου να επιλύσει προβλήματα παλινδρόμησης, ενώ η λογιστική παλινδρόμηση για προβλήματα ταξινόμησης.

Επιπλέον αντί να προσαρμοστεί μια γραμμή παλινδρόμησης, τοποθετείται μια λογιστική συνάρτηση σχήματος "S", η οποία προβλέπει δύο μέγιστες τιμές (0 ή 1). Η καμπύλη αυτή υποδεικνύει την πιθανότητα να συμβεί κάτι.

Διαπιστώνεται, πως ο Logistic Regression είναι ένας σημαντικός αλγόριθμος μηχανικής μάθησης, αφού παρέχει πιθανότητες και ταξινομεί νέα δεδομένα χρησιμοποιώντας συνεχή και διακριτά σύνολα δεδομένων.

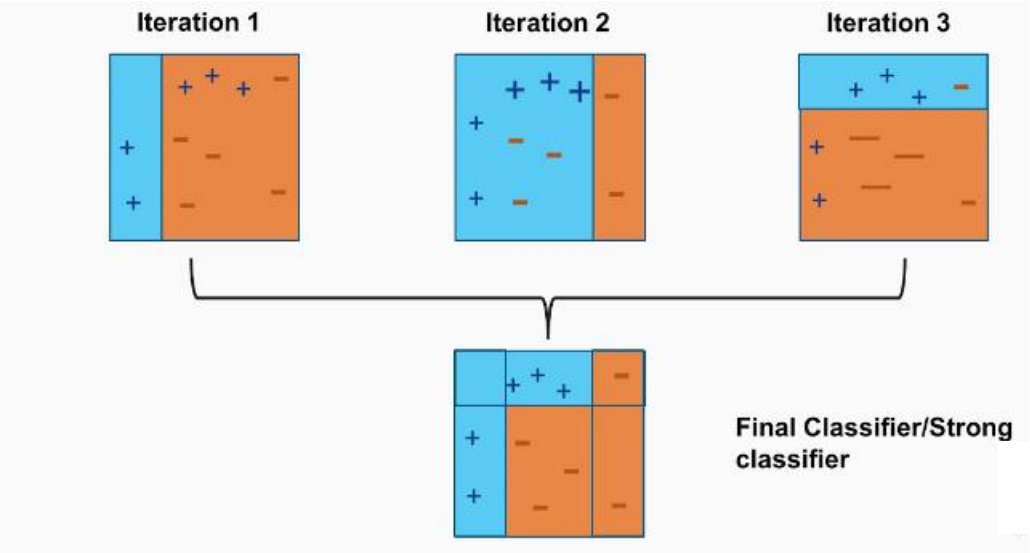


Εικόνα 16:Logistic Regression [29]

3.5.8 Κατηγοριοποίηση με τον αλγόριθμο Adaboost

Η προσαρμοστική ταξινόμηση (Adaboost) [30], συντομογραφία του Adaptive Boosting, είναι μια τεχνική Boosting που χρησιμοποιείται ως μέθοδος συνόλου στη μηχανική μάθηση. Ονομάζεται προσαρμοστική ενίσχυση, καθώς τα βάρη αντιστοιχίζονται εκ νέου, με τα υψηλότερα βάρη να εκχωρούνται σε εσφαλμένες ταξινομήσεις.

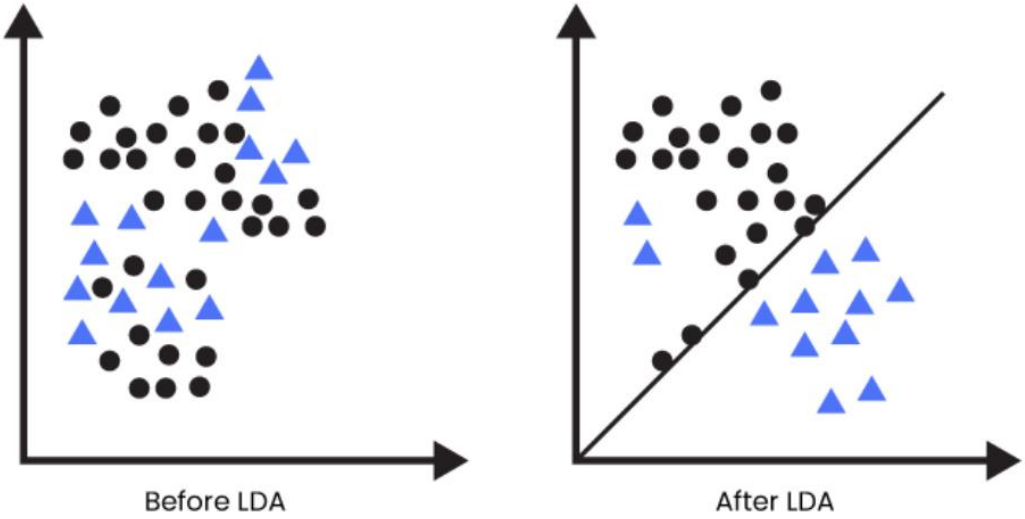
Ο αλγόριθμος δημιουργεί ένα μοντέλο και δίνει ίσα βάρη σε όλα τα σημεία δεδομένων. Στη συνέχεια αποδίδει υψηλότερα βάρη σε σημεία που ταξινομούνται λανθασμένα. Συνεπώς, σε όλα τα σημεία που έχουν μεγαλύτερα βάρη δίνεται μεγαλύτερη σημασία στο επόμενο μοντέλο. Η διαδικασία αυτή θα συνεχίσει μέχρι να ληφθεί χαμηλό σφάλμα.



Εικόνα 17: Διαδικασία εφαρμογής Adaboost [31]

3.5.9 Κατηγοριοποίηση με τον αλγόριθμο LDA

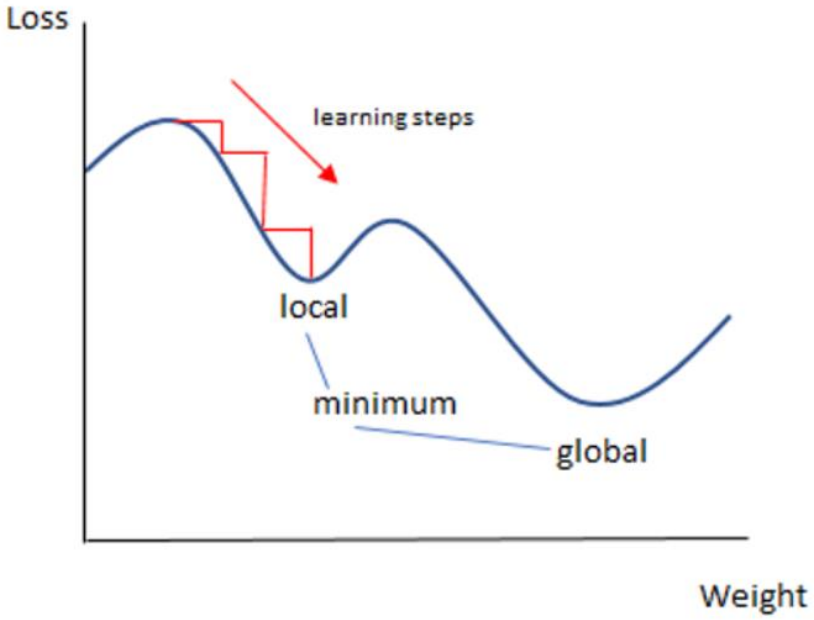
Η ανάλυση γραμμικής διάκρισης (LDA) [32] χρησιμοποιείται για την ταξινόμηση μοτίβων μεταξύ δύο κατηγοριών. Ωστόσο, μπορεί να επεκταθεί για να ταξινομήσει πολλαπλά μοτίβα. Ο LDA υποθέτει, ότι όλες οι κλάσεις είναι γραμμικά διαχωρίσιμες και σύμφωνα με αυτήν τη συνάρτηση πολλαπλής γραμμικής διάκρισης που αντιπροσωπεύει, δημιουργεί πολλά υπερ.-επίπεδα στον χώρο χαρακτηριστικών. Εάν υπάρχουν δύο κλάσεις, τότε ο LDA σχεδιάζει ένα υπερεπίπεδο και προβάλλει τα δεδομένα σε αυτό, με τέτοιο τρόπο ώστε να μεγιστοποιείται ο διαχωρισμός των δύο κατηγοριών. Αυτό το υπερεπίπεδο δημιουργείται σύμφωνα με τα δύο κριτήρια που εξετάζονται ταυτόχρονα δηλαδή, την μεγιστοποίηση της απόστασης μεταξύ των μέσων των δύο τάξεων και την ελαχιστοποίηση της διακύμανσης μεταξύ κάθε κατηγορίας.



Εικόνα 18: LDA algorithm [33]

3.5.10 Κατηγοριοποίηση με τον αλγόριθμο SGD

Η στοχαστική κλίση καθόδου (Stochastic Gradient Descent (SGD)) [34] είναι ένας απλός αλλά αποτελεσματικός αλγόριθμος βελτιστοποίησης, που χρησιμοποιείται για την εύρεση των τιμών των παραμέτρων/συντελεστών των συναρτήσεων, που ελαχιστοποιούν μια συνάρτηση κόστους. Ειδικότερα χρησιμοποιείται για τη διακριτική εκμάθηση γραμμικών ταξινομητών κάτω από κυρτές συναρτήσεις απώλειας όπως η SVM και η λογιστική παλινδρόμηση. Εφαρμόζεται με επιτυχία σε μεγάλης κλίμακας σύνολα δεδομένων, επειδή η ενημέρωση των συντελεστών πραγματοποιείται για κάθε περίπτωση εκπαίδευσης και όχι στο τέλος όλων των περιπτώσεων.



Εικόνα 19: SGD classifier [35]

Κεφάλαιο 4: Ανάλυση Συστημάτων Ανίχνευσης Εισβολών με χρήση Μηχανικής Μάθησης στο Διαδίκτυο των Πραγμάτων

Τα τελευταία χρόνια παρατηρείται η εξάπλωση του Διαδικτύου των Πραγμάτων (IoT) και ο αντίκτυπός του σε διάφορους τομείς από τη γεωργία, την υγειονομική περίθαλψη, τις μεταφορές έως και την αυτοκινητοβιομηχανία. Με στόχο να φέρει κάθε φυσικό αντικείμενο σε ψηφιακούς κόσμους, το IoT συνέδεσε δισεκατομμύρια συσκευές, στις οποίες είναι ενσωματωμένοι αισθητήρες, ενεργοποιητές και άλλες τεχνολογίες, στο Διαδίκτυο και δημιούργησε δισεκατομμύρια byte δεδομένων. Η δραστική εξέλιξη των IoT είχε ως αποτέλεσμα την ενίσχυση της απόδοσης πολλών υπηρεσιών σε διάφορους τομείς. Συνοπτικά το Διαδίκτυο των Πραγμάτων αναγνωρίζεται ως βασικό στοιχείο της ψηφιακής επανάστασης στην αναμόρφωση της κοινωνίας μας.

Ωστόσο, οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο και το απόρρητο των δεδομένων είναι οι κύριες ανησυχίες για την πλήρη απελευθέρωση των IoT. Το παραπάνω περιλαμβάνει πολλές έξυπνες συσκευές (π.χ. αισθητήρες, ενεργοποιητές) που έχουν περιορισμένους υπολογιστικούς πόρους και ετερογενές υλικό. Αρκετές εντατικές επιθέσεις καταγράφονται στον κυβερνοχώρο με στόχο συσκευές IoT οδηγώντας σε ανεπιθύμητα αποτελέσματα, όπως καταστροφή του υλικού της συσκευής και διαταραχή του συστήματος IoT. Για τον μετριασμό των επιθέσεων, στην συγκεκριμένη ενότητα, παρουσιάζονται ΣΑΠΕ με τη χρήση μηχανικής μάθησης.

Είναι σαφές ότι τα συστήματα ΣΑΠΕ είναι αφιερωμένα στην προστασία των δικτύων IoT και διαφέρουν από τα υπόλοιπα, που επικεντρώνονται στα συμβατικά δίκτυα υπολογιστών. Η προστασία τους είναι αρκετά απαιτητική, αφού μεταξύ των στοιχείων τους υπάρχουν πολλαπλές διασυνδέσεις και αλληλεπιδράσεις. Επομένως, απαιτείται η δημιουργία ενός ΣΑΠΕ, το οποίο παρακολουθεί και ελέγχει την δικτυακή κίνηση, καθώς και τα συστήματα καταγραφής των υπό-συστημάτων και συνδέσεων. Συγκεκριμένα το προαναφερόμενο απαιτείται να προσαρμόσει την λειτουργικότητά του , ανάλογα με τις δυνατότητες των βιομηχανικών συσκευών και των συσκευών IoT .

Σε αυτή την ενότητα, μελετήθηκαν 28 διαφορετικές περιπτώσεις ΣΑΠΕ . Πιο συγκεκριμένα, ο Πίνακας 1 τις συγκρίνει παρουσιάζοντας τα πιο σημαντικά χαρακτηριστικά τους. Η σύγκριση των ΣΑΠΕ, που εξετάστηκαν, βασίζεται κυρίως στην τεχνική ανίχνευσης των εισβολών και στην απόδοση αυτών. Ειδικότερα η υπό-ενότητα που ακολουθεί αφορά anomaly-based συστήματα .

Πίνακας 1: Συνοπτική Παρουσίαση των 28 συστημάτων IDPS

Literature work	Target System	Detection Technique	Protocols	Attacks	Performance	Dataset	Software
Chunhe Song et al. [36]	Smart grid	Anomaly based	Δεν παρέχεται	Δεν παρέχεται	1.ACC=0.8921 2.Precision=0.8242 3.Recall=0.9868 4.F1-score=0.8982	NSL-KDD	Δεν παρέχεται
Tala Talaei Khoei et al. [37]	Smart grid	Anomaly-based	Δεν παρέχεται	1.namely-reflection 2.exploitation-based 3.DDos attacks	A)reflection-based attacks 1.TPR =0.96 2.FNR =0.041 3.FPR=0.089 4.ACC=0.934 B)exploitation-based 1.TPR =0.96 2.FNR =0.01 3.FPR=0.007 4.ACC=0.973	CICDDoS 2019	Δεν παρέχεται
Tala Selim Ustun et al. [38]	Smart grid	Anomaly-based	IEC 62351	Cyberattacks based on goose messages	A)AdaBoost 1.ACC= 0.9487 2.DR=0.8507 3.FAR=0.0194 B)DT 1.ACC= 0.9448 2.DR=0.9231 3.FAR=0.0408 C)RF 1.ACC= 0.9519 2.DR=0.8657 3.FAR=0 D)k-NN 1.ACC= 0.9448 2.DR=0.9231 3.FAR=0.0408 E)SVM 1.ACC= 0.9512 2.DR=0.8718 3.FAR=0.0338	GOOSE dataset	IEC 61850 emulators
Chih Che Sun et al. [39]	Smart meters	Anomaly-based	IEEE 182.15.4	Δεν παρέχεται	A)SVM(RBF) 1.ACC=0.9871 2. Training time=0.52 A)NN(MLP) 1.ACC=0.9822 2. Training time=1.33	AMI testbed	NS-3
Jiayu Shi et al [40]	Smart grid	Anomaly-based	Δεν παρέχεται	FDI attacks	Detection accuracy=0.98	IEEE 118 Bus System	Δεν παρέχεται
Muhammad Ashfaq Khan et al. [41]	IoT network	Hybrid	Δεν παρέχεται	Δεν παρέχεται	1.DR=0.8 2. Precision=0.9633 3. Recall=0.9712 4.F1 score=0.976 5.FAR=2.5	CSE-CIC-IDS2018	Java
Jie Gua et al. [42]	Network security	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	A)UNSW-NB15 1.ACC=0.9375 2. DR=0.9473 3.FAR=7.33	1.UNSW-NB15 2.CICIDS2017 3.NSL-KDD	1.Clam Antivirus software 2.Ashula shellcode

					B)CICIDS2017 1.ACC=0.9892 2. DR=0.9946 3.FAR=3.00 C)NSL-KDD 1.ACC=0.9935 2. DR=0.9924 3.FAR=0.56 D)Kyoto 2006+ dataset 1.ACC=0.9858 2. DR=0.9973 3.FAR=2.62	4.Kyoto 2006+dataset	detection software
Giuseppina Adresini et al. [43]	Network security	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	A)KDDCUP99 1.ACC=0.8285 2.Recall(Attack)=0.854 3.Recall(Normal)=0.70 4.f1-score=0.8875 A)AAGM17 1.ACC=0.6759 2.Recall(Attack)=0.377 3.Recall(Normal)=0.75 4.f1-score=0.3176 A)CICIDS2017 1.ACC=0.5863 2.Recall(Attack)=0.389 3.Recall(Normal)=0.63 4.f1-score=0.2733	1.KDDCUP99 2.AAGM17 3. CICIDS17	Δεν παρέχεται
Giovanni Apruzzese et al [44]	Network Security	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	Δεν παρέχεται	1.CTU13 2.NB15 3.IDS18 4.DDOS19 5. UF-BotIoT 6.UF-NB15 7.UF-IDS18 8.UF-ToNIoT	NetFlow
Yanfang Fu et al. [45]	Network security	Anomaly-based	Δεν παρέχεται	1.Dos 2.Probe 3.R2L 4.U2R	1.ACC=0.9073 2.Precision=0.8638 3.Recall=0.9317 4.F1-score=0.8965	NSL-KDD	Δεν παρέχεται
Ski Tanzir Mehedi et al. [46]	IoT	Anomaly-based	Δεν παρέχεται	1.DoS 2.DDoS 3.data injection 4.MITM 5.Backdoor 6.PCA 7.Scanning 8.XSS 9.ransomware	1.ACC= 0.87 2.Precision=0.88 3.Recall=0.86 4.f1-score=0.86 5.ROC AUC=0.83	Combined Dataset	Δεν παρέχεται
Raisa Abedin Disha et al. [47]	Network security	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	A)UNSW-NB15 1.ACC=0.9301 2.Recall=0.9476 3.f1-score=0.9372 B)TON_IoT 1.ACC=0.999 2.Recall=0.9987 3.f1-score=0.9985	1.UNSW-NB15 2. Network TON_IoT datasets	Δεν παρέχεται
Panagiotis Radoglou - Grammatikis et al [48]	IoMT	Anomaly-based	IEC 60870-5-104	IEC 60870-5-104 cyberattacks	1.ACC=Δεν παρέχεται 2. TPR=Δεν παρέχεται 3. FPR =Δεν παρέχεται 4. F1-score=Δεν παρέχεται	IEC 60870-5-104 dataset	Δεν παρέχεται

Panagiotis Sarigiannidis et al. [49]	IoMT	Anomaly-based	1.HTTP 2.Modbus/TCP	14 Modbus/TCP-related cyberattacks	1.ACC=Δεν παρέχεται 2. TPR=Δεν παρέχεται 3. FPR =Δεν παρέχεται 4. F1-score=Δεν παρέχεται	Healthcare dataset	Δεν παρέχεται
Muhammad Azmi Umer et al. [26]	ICS	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	1.ACC=Δεν παρέχεται 2. TPR=Δεν παρέχεται 3. FPR =Δεν παρέχεται 4. F1-score=Δεν παρέχεται 5.ROC=Δεν παρέχεται 6.AUC=Δεν παρέχεται	Diff datasets	Δεν παρέχεται
Linxi Zhang et al. [50]	Vehicle Network	Combination of signature and anomaly based	CAN	CAN attacks	A)Honda Accord 2006 1.ACC=0.9991 2.TPR=0.999 3.FPR=0.00066 4.Time per msg=0.549ms B)Honda Civic 2018 1.ACC=0.9981 2.TPR=0.9975 3.FPR=0.00071 4.Time per msg=0.551ms C)Ford Fusion 2013 1.ACC=0.9981 2.TPR=0.9975 3.FPR=0.00071 4.Time per msg=0.546ms D)Chevrolet Volt 2013 1.ACC=0.9985 2.TPR=0.9981 3.FPR=0.00084 4.Time per msg=0.553ms	1.Honda Accord 2006 2.Honda Civic 2018 3.Ford Fusion 2013 4.Chevrolet Volt 2013	Δεν παρέχεται
Jaybed Al Faysal et al. [51]	IoT	Anomaly-based	Δεν παρέχεται	Botnet Attacks	1.ACC=0.999426 2. F1 score=0.999426 3. Kappa index=0.99936 4.MCC=0.999364 5 SE=0.999426 6.SP=0.999942 7. threat score=0.99892 8. balanced accuracy score=0.999683	N-BaIoT	Δεν παρέχεται
Ilias Siniosoglou et al. [52]	Smart grid	Anomaly-based	1.TCP 2.DNP3 3.FTP	1.14 Modbus/TCP-related cyberattacks. 2.five DNP3 cyberattacks	A)SG-lab 1.ACC=0.964 2.TPR=0.73 3.FPR=0.019 4.F1-score=0.73 B)Substation 1.ACC=0.965 2.TPR=0.759 3.FPR=0.018 4.F1-score=0.759 C)Hydropower plant 1.ACC=0.966 2.TPR=0.767 3.FPR=0.017 4.F1-score=0.767 D)Power plant	1.SG lab 2.Substation 3.Hydropower plant 4.Power plant	Δεν παρέχεται

					1.ACC=0.964 2.TPR=0.734 3.FPR=0.018 4.F1-score=0.734		
Andre Kummerow et al. [53]	Dynamic control centers	Anomaly-based	IEEE C37.118	Δεν παρέχεται	1.F1-score=Δεν παρέχεται	Traffic dataset	Δεν παρέχεται
Daojing He et al. [54]	CHs	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	1.ACC=Δεν παρέχεται 2.FPR=Δεν παρέχεται 3.FNR=Δεν παρέχεται	Real CHS dataset	Δεν παρέχεται
Z.Khalafi et al. [55]	PMU Network	Anomaly-based	Δεν παρέχεται	Integrity attacks	Δεν παρέχεται	Three scenarios are considered for evaluating PMUIDS on IEEE 14-bus system A)No attack B)One attack C)Three Attacks	Δεν παρέχεται
Vivek Kumar Singh et al. [56]	Smart grid	Combination of Anomaly-based, signature-based (Hybrid)	Δεν παρέχεται	1.IT -based attacks 2. SCADA -based attacks	1.ACC=1	CPS testbed	1.Snort 2. Zeek IDS tools
Adeel Abbas et al. [57]	IoT	Anomaly-based	Δεν παρέχεται	All types of attacks	A)Binary class 1.ACC=0.8892 B)Multi- class 1.ACC=0.8896	CICIDS2017	Δεν παρέχεται
Adedayo Aribisala et al. [58]	Smart grid	Anomaly-based	Δεν παρέχεται	1.DoS 2.Probe 3.U2R 4.R2L	A)TANH Activation 1.ACC=0.9897 2.Loss=0.053 B)ReLU 1.ACC=0.9959 2.Loss =0.011	NSL-KDD	Δεν παρέχεται
Azka Wani et al. [59]	IoT	Anomaly-based	Δεν παρέχεται	IoT network attacks	1.ACC=0.9905 2.FPR=0.0536 3.FNR=0.0039 4.TPR=0.9961 5.TNR=0.9464 6.Precision=0.9932 7.F1-score=0.9947	CSE-CIC-IDS2018	1.Python 2.Wireshark

Bo Cao et al. [60]	IDS	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	A)UNSW-NB15 1.ACC=0.8625 2.Precison=0.8692 3.Recall=0.862 4.F1-score=0.8659 B)NSL-KDD 1.ACC=0.9969 2.Precision=0.9965 3.Recall=0.996 4.F1-score=0.997 C)CIC-IDS2017 1.ACC=0.9965 2.Precision=0.9963 3.Recall=0.9965 4.F1-score=0.9964	1.UNSW-NB15 2.NSL-KDD 3.CIC-IDS2017	1.Python
Tuan A Tang et al. [61]	Network security	Anomaly-based	Δεν παρέχεται	Δεν παρέχεται	1.ACC=0.89 2.Precision=0.91 3.Recall=0.9 4.F1-score=0.9	NSL-KDD	1.Python 2.Openflow (Cbench tool)
Xuan-Ha Nguyen et al. [62]	IoT	Anomaly-based	Δεν παρέχεται	1.Botnet 2.DoSSlowhttptest 3.DosGoldenEye 4.DosSlowloris 5.DosHulk 6.FTP-Patator 7.SSH-Patator 8.Heartbleed 9.DDoS 10.Portscan	A)Botnet 1.TPR=0.9846 B)DoSSlowhttptest 1.TPR=0.9948 C)DosGoldenEye 1.TPR=0.9998 D)DosSlowloris 1.TPR=0.9952 E)DosHulk 1.TPR=0.9845 F)FTP-Patator 1.TPR=0.9992 G)SSH-Patator 1.TPR=0.9992 H)Heartbleed 1.TPR=0.9998 I)DDoS 1.TPR=1 J)Portscan 1.TPR=0.9994	CIC-IDS2017	1.Docker

4.1 Anomaly-based Σύστημα Ανίχνευσης και Πρόληψης Εισβολών

Στην συγκεκριμένη υπό-ενότητα περιγράφεται συνοπτικά το περιεχόμενο των άρθρων που παρουσιάστηκαν παραπάνω και πιο συγκεκριμένα το είδος των συστημάτων ανίχνευσης που αναλύονται σε αυτά, καθώς και οι αποδόσεις τους.

Στο άρθρο [36] παρουσιάζεται μία μέθοδο ανίχνευσης εισβολών, για τα έξυπνα δίκτυα, που συνδυάζει την μέθοδο βαθιάς μάθησης δικτύων μακράς και βραχύχρονης μνήμης (Long Short-term Memory-LSTM) και μηχανικής μάθησης Extreme Boosting (XGBoost). Η παραπάνω, παρόλο που είναι ένα δημοφιλές μοντέλο πρόβλεψης, βασισμένο στην εκμάθηση ενός συνόλου δένδρων, είναι ευαίσθητη στον καθορισμό των παραμέτρων της. Εξαιτίας αυτού, γίνεται η βελτιστοποίηση της με την Bayesian μέθοδο, η οποία αυξάνει την αποτελεσματικότητα της εκπαίδευσης για την ανίχνευση πιθανών επιθέσεων. Παρόλα αυτά η προαναφερόμενη δύναται να υποπέσει σε τοπικό βέλτιστο, για αυτό και χρησιμοποιείται η έννοια γενετικών αλγορίθμων (Genetic Algorithm-GA) για να το αποφύγει. Στο τελευταίο κομμάτι του άρθρου, παρουσιάζονται εκτενή πειραματικά αποτελέσματα, που αποδεικνύουν πως η προτεινόμενη μέθοδος αποδίδει καλύτερα σε σχέση με άλλες όσον αφορά την ανίχνευση εισβολών, καθώς η ακρίβεια της είναι περίπου 90%.

Ο Tala Talaei Khoei και οι υπόλοιποι συντάκτες του άρθρου [37] παρουσιάζουν τεχνικές εκμάθησης συνόλου για την ανίχνευση των εισβολών στα έξυπνα δίκτυα καθώς και τη σύγκριση τους με παραδοσιακές μεθόδους μηχανικής μάθησης. Αυτές οι τεχνικές είναι η τεχνική bagging-based, όπου μειώνει την διακύμανση του συνόλου δεδομένων, η boosting-based, όπου ενσωματώνει ένα σύνολο μοντέλων που είναι ασθενή αποσκοπώντας στη δημιουργία ενός μοντέλου με υψηλή ακρίβεια και η stacking-based, όπου συνδυάζει μοντέλα μηχανικής μάθησης και εντοπίζει το καλύτερο. Στη συνέχεια παραθέτονται από τους συντάκτες οι παραδοσιακές τεχνικές μηχανικής μάθησης για την ανίχνευση επιθέσεων, όπως η K nearest neighbor, Decision Trees και Naive Bayes. Παράλληλα, επισημαίνεται πως το σύνολο δεδομένων για την αξιολόγηση των παραπάνω τεχνικών και αλγορίθμων ήταν το CICDDoS 2019, που περιέχει πολλαπλές DDos επιθέσεις. Ακόμα πριν γίνει εξέταση των δεδομένων προείχε η προ-επεξεργασία τους, ώστε να επιφέρουν όσο το δυνατόν αποδοτικότερα αποτελέσματα, ενώ χρησιμοποιήθηκαν δυο μέθοδοι επιλογής χαρακτηριστικών, ο συντελεστής Pearson και ο αλγόριθμος βασισμένος σε δένδρα. Για την αξιολόγηση της αποτελεσματικότητας των μοντέλων ταξινόμησης έγινε χρήση μετρικών, όπως η ευαισθησία (True positive rate-TPR), η αδυναμία το σύστημα να συλλάβει σωστά μια επίθεση (False Negative Rate-FNR), ο λανθασμένος συναγερμός (False positive rate-FPR) και ακρίβεια (accuracy). Καταλήγοντας τα πειραματικά αποτελέσματα έδειξαν πως η τεχνική stacking-based είναι η πιο αποδοτική με ακρίβεια 95%.

Στο άρθρο [38] οι συντάκτες πραγματεύονται την ανίχνευση εισβολών σε έξυπνα δίκτυα, με βάση τη μηχανική μάθηση, μέσω της χρήσης μηνυμάτων GOOSE του προτύπου IEC 61850. Τα μηνύματα GOOSE ενεργοποιούνται από συμβάντα του συστήματος και μεταδίδονται, ώστε να ληφθούν οι κατάλληλες αποφάσεις, εφόσον αυτό κριθεί αναγκαίο. Διαθέτουν δύο παραμέτρους με τη βοήθεια των οποίων διαπιστώνεται αν το σύστημα βρίσκεται υπό εισβολή. Αυτές είναι οι stNum, όπου εκφράζει την ποσότητα αποστολής ενός μηνύματος και sqNum, όπου αποθηκεύει την αύξηση του χρόνου κάθε φορά που το μήνυμα επαναλαμβάνεται. Παρόλα αυτά τα μηνύματα GOOSE δεν διαθέτουν τα ίδια μηχανισμό κυβερνοασφάλειας και έτσι είναι ορατά σε όλο το δίκτυο.

Στο σημείο αυτό ο αρθρογράφος τονίζει την αναγκαιότητα δημιουργίας του συστήματος αυτού με βάση αλγορίθμους μηχανικής μάθησης. Οι αλγόριθμοι που εξετάστηκαν ήταν τα Decision Trees, Random Forest, SVM, k-NN και Adaboost και οι δοκιμές έγιναν σε ρεαλιστικό σύνολο δεδομένων σε έξυπνα δίκτυα . Η αξιολόγηση των αλγορίθμων βασίστηκε σε παραμέτρους όπως η ακρίβεια, το ποσοστό σφάλματος και ο χρόνος εκπαίδευσης και το συμπέρασμα ήταν πως ο καλύτερος αλγόριθμος ήταν τα Decision Trees, αφού συνδύαζαν μεγαλύτερη ακρίβεια σε λιγότερο χρόνο εκπαίδευσης.

Οι συντάκτες του άρθρου [39] προτείνουν μια μέθοδο ανίχνευσης εισβολών για έξυπνους μετρητές δύο σταδίων, όπου συνδυάζει το μοντέλου μάθησης SVM και την τεχνική Propagation Graph. Η αρχιτεκτονική του προτεινόμενου συστήματος αποτελείται από τρία μέρη. Στο πρώτο στάδιο, το μοντέλο SVM, ανιχνεύει ανώμαλες συμπεριφορές και συμβάλλει στην αποφυγή υπερβολικής χρήσης του αλγορίθμου ανίχνευσης δευτέρου σταδίου. Έπειτα υπολογίζεται η ομοιότητα των γεγονότων του συστήματος, που στάλθηκαν για περαιτέρω επιθεώρηση, με κάποια ήδη καταγεγραμμένα . Προκειμένου να κριθούν ως εισβολές, προτείνονται πιθανές διαδρομές επιθέσεων και καταγράφονται πληροφορίες με μη φυσιολογική συμπεριφορά .Αν κάποιο γεγονός του συστήματος ταιριάξει με τα παραπάνω, τότε θεωρείται εισβολή. Για την δοκιμή του προτεινόμενου συστήματος αναπτύχθηκε πλατφόρμα δοκιμών Advanced Metering Infrastructure (AMI) με επιθέσεις στον κυβερνοχώρο. Παράλληλα έγινε χρήση αλγορίθμων μηχανικής μάθησης όπως SVM με συναρτήσεις Kernel και NN αλγόριθμοι. Για την αξιολόγηση του μοντέλου οι συγγραφείς υπολόγισαν μετρικές όπως η ακρίβεια και ο χρόνος εκπαίδευσης. Τελικά κατέληξαν στο συμπέρασμα πως ο SVM εμφανίζει καλύτερη απόδοση με μεγάλη ακρίβεια και μικρό χρόνο εκπαίδευσης.

Στο άρθρο [40] οι αρθρογράφοι πραγματεύονται τη δημιουργία ΣΑΕ βάσει κατανεμημένων δεδομένων, ώστε να αποκαλυφθεί η κρυφή έγχυση ψευδών δεδομένων στα έξυπνα δίκτυα. Στον προτεινόμενο μηχανισμό κάθε περιοχή έχει το δικό της ανιχνευτή που βασίζεται στη μηχανική μάθηση και επικοινωνεί με άλλες γειτονικές. Η κατάσταση που εξάγεται από κάθε περιοχή χρησιμοποιείται για τον εντοπισμό επιθέσεων, που αφορούν ψευδή έγχυση δεδομένων (False data injection-FDI). Μέσω της μεθόδου αυτής το πρόβλημα αναλύεται σε ανεξάρτητα προβλήματα δυαδικής ταξινόμησης. Για τον έλεγχο της αποδοτικότητας του προτεινόμενου συστήματος έγινε χρήση του IEEE Bus test system. Εξετάστηκαν η μέθοδος του αρθρογράφου, το μοντέλο μάθησης SVM και το νευρωνικό δίκτυο ANN. Τα αποτελέσματα έδειξαν πως η μέθοδος που αναγράφεται στο άρθρο μπορεί επιτυχώς να εντοπίζει τέτοιους είδους επιθέσεις έχοντας παράλληλα καλύτερες δυνατότητες από τις προαναφερόμενες με κυριότερες να είναι η υψηλή ακρίβεια, αλλά και ο εντοπισμός της περιοχής που δέχεται επίθεση, ενώ εκείνη ανιχνεύεται.

Ο Muhammad Ashfaq Khan στο άρθρο [63] παρουσιάζει την ανάπτυξη ΣΑΕ βασισμένο σε νευρωνικά δίκτυα. Το σύστημα αυτό είναι συνδυασμός μηχανικής και βαθιάς μάθησης με ανανεωμένες μεθόδους της τελευταίας, όπως τα συνελικτικά νευρωνικά δίκτυα (Convolutional Neural Network-CNN) αλλά και κλασικών της πρώτης, όπως τα επαναλαμβανόμενα νευρωνικά δίκτυα (Recurrent Neural Network-RNN). Στην συνέχεια παραθέτει την αρχιτεκτονική του προτεινόμενου συστήματος. Τα συνελικτικά νευρωνικά δίκτυα, αποτελούνται από τον εξαγωγέα χαρακτηριστικών και τον ταξινομητή. Ο πρώτος απαρτίζεται από δύο επιμέρους στρώματα τα συνελικτικά και τα συγκεντρωτικά. Ότι χαρακτηριστικό εξάγεται από αυτόν οδηγείται στον ταξινομητή. Τα στρώματα CNN ακολουθούνται από επαναλαμβανόμενα στρώματα, ώστε να

αποτυπωθούν τόσο τα χρονικά όσο και τα χωρικά χαρακτηριστικά . Παράλληλα το δίκτυο οργανώνεται και πραγματοποιείται προ-επεξεργασία των δεδομένων με κατάλληλες μετατροπές απαραίτητες για την ορθή λειτουργία του συστήματος. Έπειτα τα δεδομένα εισάγονται σε ένα πλήρως συνδεδεμένο στρώμα πριν οδηγηθούν σε επίπεδο Softmax, υπεύθυνο για την ταξινόμησή τους. Για τη δοκιμή της προτεινόμενης μεθόδου έγινε χρήση βάσης με πραγματικά δεδομένα, η CSE-CIC-IDS2018, που περιέχει επτά ειδών επιθέσεις. Οι αρθρογράφοι εξέτασαν τα αποτελέσματα μετρικών διάφορων αλγορίθμων. Ωστόσο, τα αποτελέσματα έδειξαν πως το προτεινόμενο σύστημα έχει την υψηλότερη ακρίβεια, το μικρότερο ποσοστό λαθών αλλά και το μεγαλύτερο βαθμό ανίχνευσης .

Στο άρθρο [42] οι συγγραφείς προτείνουν την ανάπτυξη ΣΑΕ, που είναι βασισμένο σε τεχνικές μηχανικής μάθησης και πιο συγκεκριμένα σε SVM με ενσωμάτωση χαρακτηριστικών της τεχνικής Naive Bayes. Πιο συγκεκριμένα η τελευταία τροποποιεί τα αρχικά δεδομένα σε νέα υψηλότερης ποιότητας και εξασφαλίζει μεγαλύτερη ακρίβεια και μικρότερο ποσοστό σφαλμάτων. Στη συνέχεια η μέθοδος SVM χρησιμοποιεί τα νέα δεδομένα προκειμένου να δημιουργήσει έναν ισχυρό μηχανισμό ανίχνευσης επιθέσεων. Με τον συνδυασμό των μεθόδων αυτών είναι πιο διακριτός ο διαχωρισμός των δεδομένων σε εισβολές και μη. Για την εκτίμηση της αποτελεσματικότητας του προτεινόμενου συστήματος πραγματοποιήθηκαν πειράματα σε τέσσερις βάσεις δεδομένων και εξετάστηκαν πολλοί αλγόριθμοι. Τελικά οι αρθρογράφοι κατέληξαν στο συμπέρασμα, πώς η προτεινόμενη μέθοδος είναι πιο αποδοτική όσον αφορά την ακρίβεια, τον βαθμό ανίχνευσης των εισβολών, την ταχύτητα εκπαίδευσης αυτού αλλά και το ποσοστό των σφαλμάτων, καθώς και στις τέσσερις βάσεις δεδομένων η ακρίβεια ξεπερνούσε το 93% , ενώ σε κάποιες περιπτώσεις άγγιζε και το 99%.

Το άρθρο [43] αφορά την ανάπτυξη μιας νέας μεθόδου DML, την λεγόμενη RENOIR, για την ανίχνευση εισβολών στο δίκτυο λόγω της ανισορροπίας των δεδομένων κίνησής του. Πιο συγκεκριμένα το προτεινόμενο σύστημα επεξεργάζεται την ροή των δεδομένων στο δίκτυο και σύμφωνα με τις πληροφορίες που λαμβάνει για τα πακέτα ανιχνεύει ανώμαλες συμπεριφορές. Αξιοποιεί λοιπόν μία μέθοδο εκμάθησης βαθιάς μετρικής και συνδυάζει αυτό-κωδικοποιητές και δίκτυα Triplet, που βοηθούν στην κατανομή των όμοιων και μη αντικειμένων του δικτύου. Το προτεινόμενο σύστημα αποτελείται από δύο στάδια, το στάδιο της εκπαίδευσης και αυτό των δοκιμών. Στο πρώτο στάδιο αναλύονται τα χαρακτηριστικά των δεδομένων για την εκπαίδευση δύο αυτό-κωδικοποιητών. Αυτοί με τη σειρά τους εισέρχονται στο δίκτυο Triplet. Στο στάδιο της δοκιμής το RENOIR χρησιμοποιεί τους αυτό-κωδικοποιητές, ώστε να κατανέμει την ροή σε ανώμαλες και μη συμπεριφορές. Για την εκτίμηση του συστήματος έγινε μελέτη τριών βάσεων δεδομένων σε διαφορετικούς χρόνους και σενάρια και εξετάστηκαν ποικίλες μετρικές όπως η ακρίβεια και το F1-score. Το προτεινόμενο σύστημα τέθηκε υπό σύγκριση με άλλους αλγορίθμους αλλά και με συνδυασμούς συστημάτων που εκπαιδεύτηκαν από το RENOIR .Τελικά, οι αρθρογράφοι παρουσίασαν ενθαρρυντικά αποτελέσματα από το προτεινόμενο σύστημα σε σχέση με τα υπόλοιπα στην ανίχνευση εισβολών.

Ο Giovanni Apruzzese και οι υπόλοιποι συγγραφείς του άρθρου [44] επισημαίνουν την δυσκολία ενσωμάτωσης της επιβλεπόμενης μηχανικής μάθησης στα ΣΑΕ. Οι ίδιοι προτείνουν την εφαρμογή της διαδικασίας του cross-evaluation με την εκμετάλλευση ήδη υπαρχόντων δεδομένων από διαφορετικά δίκτυα. Με τη διασταυρούμενη επικύρωση πραγματοποιείται η αξιολόγηση μοντέλων μηχανικής μάθησης σε ήδη διαθέσιμα δεδομένα. Στο πλαίσιο αυτό, αναπτύχθηκε το

μοντέλο XeNIDS, που μετριάζει τους κινδύνους από τα δεδομένα προερχόμενα από διαφορετικά δίκτυα . Το XeNIDS είναι ευέλικτο και κατάλληλο για ανίχνευση. Την αρχιτεκτονική του XeNIDS, συνθέτουν τέσσερα στάδια. Το πρώτο είναι το λεγόμενο Standarize, όπου η εξεταζόμενη βάση δεδομένων υφίσταται προ-επεξεργασία και μορφοποίηση. Στη συνέχεια ακολουθεί το isolate, όπου διαχωρίζει τα δεδομένα σε κακόβουλα και μη. Ακόμα έπεται το contextualize, όπου διαμορφώνει τις κατηγορίες των δεδομένων που προκύπτουν . Τέλος πραγματοποιείται το cross-evaluation στις κατηγορίες και παράγονται αποτελέσματα. Καταλήγοντας έγιναν πειράματα σε έξι γνωστές βάσεις δεδομένων, όπου έδειξαν πως το XeNIDS είναι αποδοτικό και μειώνει το κίνδυνο του over-fitting.

Το άρθρο [45] πραγματεύεται την ανάπτυξη ενός Deep Learning Network Intrusion (DLNID) μοντέλου με τον αλγόριθμο ADASYN, για την αντιμετώπιση της άνισης κατανομής των δεδομένων. Ο ADASYN είναι αλγόριθμος υπέρ-δειγματοληψίας με βάση τα δεδομένα της μειονοτικής τάξης και είναι κατάλληλος για την διαχείριση κίνησης του δικτύου με ανισορροπία δεδομένων . Η αρχιτεκτονική του προτεινόμενου συστήματος αποτελείται από επτά στάδια. Το πρώτο είναι το στρώμα εισόδου που δέχεται δεδομένα από την βάση. Στο στρώμα του κωδικοποιητή το μοντέλο χρησιμοποιεί τον βελτιωμένο αυτό-κωδικοποιητή για την μείωση των διαστάσεων των δεδομένων. Στο πολλαπλό συνελικτικό στρώμα πραγματοποιούνται ενέργειες, ώστε να εξαχθούν τα χαρακτηριστικά των παραπάνω δεδομένων. Στο επίπεδο προσοχής γίνεται χρήση του μηχανισμού CBAM, για να αναδιανεμηθούν τα βάρη κάθε καναλιού και να αντιστοιχιστούν τα σημαντικά κανάλια με τα υψηλότερα βάρη. Στο επίπεδο Bi-LSTM το μοντέλο εξάγει πληροφορίες για τα χαρακτηριστικά κάθε διάστασης. Στο πλήρως συνδεδεμένο και στο επίπεδο εξόδου εκπαιδευμένα χαρακτηριστικά εισάγονται στον ταξινομητή και εξάγονται τα αποτελέσματα της ταξινόμησης . Πριν την εξέταση των δεδομένων, αυτά υφίστανται προ-επεξεργασία μέσω του one-hot-encoding, του data augmentation και του normalization . Για την εκτίμηση του μοντέλου πραγματοποιήθηκε σύγκριση με αντίστοιχα μοντέλα και αποδείχθηκε, πως η απόδοση του σε μετρικές όπως ακρίβεια, precision, recall και F1-score στην βάση δεδομένων NSL-KDD ήταν υψηλότερη.

Ο Skin Tanzir Mehedi και οι λοιποί συντάκτες του άρθρου [46] πραγματεύονται την ανάπτυξη αξιόπιστου συστήματος ResNet, για ανίχνευση εισβολών σε δίκτυα IoT βασισμένο στη μάθηση βαθιάς μεταφοράς. Το προτεινόμενο σύστημα πραγματοποιεί ακριβή ταξινόμηση μεταξύ φυσιολογικών και μη συμπεριφορών στο δίκτυο για επτά διαφορετικές IoT συσκευές με μικρή βάση δεδομένων και πολυπλοκότητα. Η αρχιτεκτονική του συστήματος απαρτίζεται από διάφορα στρώματα. Τα πρώτα τέσσερα στρώματα αποτελούνται από φίλτρα Kernel. Καθένα από αυτά είναι ένα μονοδιάστατο συνελικτικό στρώμα ακολουθούμενο από μία συνάρτηση ενεργοποίησης, το λεγόμενο feature smoothing layer. Στη συνέχεια ακολουθεί το στρώμα FEL, όπου εξάγει σημαντικές πληροφορίες για το προηγούμενο στρώμα βελτιώνοντας το πλήρως συνδεδεμένο επίπεδο. Κάθε μπλοκ της αρχιτεκτονικής χρησιμοποιεί πληροφορίες από το προηγούμενο, προκειμένου να αυξηθεί η απόδοση του. Για την εκτίμηση του προτεινόμενου συστήματος, τα δεδομένα υπέστηκαν επεξεργασία μέσω της διαδικασίας της προ-επεξεργασίας δεδομένων (data-preprocessing) και transform step. Στη συνέχεια τα δεδομένα διαιρέθηκαν σε test set και train set και πραγματοποιήθηκαν όλες οι κατάλληλες μορφοποιήσεις. Τέλος έγινε σύγκριση με άλλους αλγορίθμους βαθιάς μάθησης και μάθησης μεταφοράς και εξήχθη το συμπέρασμα πως το προτεινόμενο σύστημα είναι αποδοτικότερο όσον αφορά την ακρίβεια, το recall, το precision και το F1-score.

Στο άρθρο [47] εκπαιδεύτηκαν και εκτιμήθηκαν διάφορα μοντέλα μηχανικής μάθησης σε δύο μεγάλες βάσεις δεδομένων (UNSW-NB15 και Network Ton_IoT dataset) για την ανίχνευση των εισβολών στον κυβερνοχώρο. Οι συντάκτες προτείνουν την ανάπτυξη ενός μοντέλου ονόματι Gini impurity–based weighted Random Forest προκειμένου να μειωθούν οι διαστάσεις των δεδομένων. Το συγκεκριμένο μοντέλο διαχειρίζεται τα δεδομένα ανάλογα με την σημασία τους. Το ποσοστό της σημασίας προκύπτει από την προσαρμογή των βαρών στον αλγόριθμο Random Forest για τα ανισόρροπα κατανεμημένα σε τάξεις δεδομένα και από το κριτήρια διαχωρισμού δένδρων Gini. Για την εκτίμηση του μοντέλου έγινε σύγκριση με άλλες τεχνικές μηχανικής μάθησης προσαρμοσμένες για ανισόρροπα δεδομένα. Οι μετρικές που χρησιμοποιήθηκαν ήταν οι ακρίβεια, precision, recall και F1-score.Σε όλα τα πειράματα που προέβησαν, αποδείχθηκε πως τα decision trees με την τεχνική που αναφέρθηκε παραπάνω ήταν πιο αποδοτικά σε σχέση με τις υπόλοιπες τεχνικές.

Στο άρθρο [48] οι συντάκτες αναφέρουν πως η ανάγκη της ψηφιοποίησης του υγειονομικού συστήματος συνεπάγει και πιθανή αύξηση εισβολών στο δίκτυο. Επομένως, πραγματεύονται την υιοθέτηση ενός ΣΑΕ εισβολών στο IEC 60870-5-104, πρωτόκολλο απαραίτητο για τέτοιου είδους συστήματα. Το παραπάνω συνδυάζει τόσο μηχανική μάθηση όσο και τεχνολογίες δικτύωσης (Software Defined Networking-SDN). Η αρχιτεκτονική του συστήματος απαρτίζεται κυρίως από τρία μέρη. Το data plane ή αλλιώς το επίπεδο δεδομένων, το οποίο συγκεντρώνει πόρους όπως φυσικές και εικονικές συσκευές που είναι συνδεδεμένες στο SDN. Ακολουθεί το Control plane ή επίπεδο ελέγχου, το οποίο διαχειρίζεται τις συσκευές αυτές. Τέλος το application plane ή επίπεδο εφαρμογής , το οποίο περιλαμβάνει μία ή περισσότερες εφαρμογές που καθοδηγούν τις παραπάνω συσκευές, προκειμένου να μεταβάλλουν την συμπεριφορά τους ανάλογα με τις ανάγκες του δικτύου. Το προτεινόμενο σύστημα βασίζεται στο επίπεδο εφαρμογών που αποτελείται από τέσσερα στάδια το NTCM,NFEM,DE και NRM. Το πρώτο, διαχειρίζεται και λαμβάνει την κίνηση στο δίκτυο, το δεύτερο δέχεται την κίνηση αυτή και εξάγει στατιστικά για τα χαρακτηριστικά δικτύου, το τρίτο είναι υπεύθυνο για την ανίχνευση εισβολών ενώ το τελευταίο αποστέλλει ειδοποίηση-μήνυμα στον διαχειριστή. Μετά το στάδιο της ανίχνευσης ακολουθεί το στάδιο του μετριασμού (NRM) που πρέπει να αποφασίσει αν η συσκευή που σχετίζεται με την κυβερνοεπίθεση στο πρωτόκολλο χρειάζεται να απομονωθεί η όχι. Ακολουθεί στην συνέχεια η εκτίμηση του προτεινόμενου συστήματος, το οποίο αξιολογήθηκε με μετρικές όπως accuracy, precision,recall,f1-score . Ακόμα εξετάστηκε η ικανότητα ανίχνευσης και πρόληψης εισβολών και αποδείχθηκε πως το προτεινόμενο σύστημα είναι αποτελεσματικότερο συγκρινόμενο με άλλα .

Στο άρθρο [49] παρουσιάζεται ένα ΣΑΠΕ, που είναι βασισμένο σε πρωτόκολλα HTTP και TCP με την δυνατότητα επανεκπαίδευσης. Η διαδικασία πραγματοποιείται με μία βάση δεδομένων και επαναλαμβάνεται με την συνεχόμενη επανεκπαίδευση της, η οποία στηρίζεται σε δεδομένα που προέκυψαν από την αρχική ανίχνευση. Η αρχιτεκτονική του προτεινόμενου συστήματος είναι βασισμένη σε τρία μέρη, το Network Flow Monitor and Extraction Module, το Intrusion Detection Engine και το Notification and Response Module. Το πρώτο καταγράφει την κίνηση του δικτύου, εξάγοντας τα πακέτα TCP/IP. Το δεύτερο είναι υπεύθυνο για την ανίχνευση επιθέσεων σε HTTP και TCP πρωτόκολλα. Το τελευταίο πληροφορεί τον ειδικό για πιθανές απειλές έχοντας την δυνατότητα λήψης αποφάσεων και μέτρων. Ακόμα η αρχιτεκτονική του συστήματος περιλαμβάνει και την μεθοδολογία του Active Learning (AL) τεσσάρων βημάτων . Στο πρώτο τα δεδομένα χωρίς ετικέτα αξιολογούνται από την Δειγματοληψία Δεδομένων Αβεβαιότητας. Μετά τροφοδοτούνται στους

ταξινομητές που προβλέπουν τις ετικέτες τους. Τελικά τα νέα δεδομένα χρησιμοποιούνται για επανεκπαίδευση. Γενικά οι αρθρογράφοι αναφέρουν πως το AL προτιμάται, καθώς επιλέγει τα πιο σημαντικά δεδομένα δημιουργώντας μια καλή βάση δεδομένων και κάτ.΄ επέκταση καλύτερα αποτελέσματα. Για την εκτίμηση του προτεινόμενου συστήματος χρησιμοποιήθηκαν μετρικές ,όπως accuracy, TPR, FPR και F1-score και πραγματοποιήθηκε σύγκριση με άλλους αλγορίθμους μηχανικής μάθησης. Αποδείχθηκε πως στο προτεινόμενο σύστημα η πορεία της ακρίβειας κατά την επανεκπαίδευση ήταν ανοδική.

Ο Muhamad Azmi Umer και οι λοιποί στο άρθρο [41] πραγματεύονται τέσσερις μεθόδους μηχανικής μάθησης για ανίχνευση επιθέσεων σε βιομηχανικά συστήματα ελέγχου (Industrial Control System-ICS), την supervised, unsupervised, semi-supervised και reinforcement learning. Στην supervised προσέγγιση απαιτούνται δεδομένα που έχουν εκπαιδευτεί σε φυσιολογικές και μη συμπεριφορές. Στην unsupervised δεν απαιτούνται επισημασμένα δεδομένα αφού βασίζεται στην φυσιολογική συμπεριφορά των δεδομένων . Στην semi-supervised προσέγγιση γίνεται χρήση τόσο των labeled όσο και των un-labeled δεδομένων. Ειδικότερα σε πρώτο στάδιο γίνεται χρήση των επισημασμένων δεδομένων και στην συνέχεια ορίζονται ετικέτες και στα υπόλοιπα με βάση το μοντέλο του προηγούμενου σταδίου . Με αυτόν τον τρόπο χρησιμοποιούνται όλου του είδους τα δεδομένα. Επιπρόσθετα στην ενισχυτική μάθηση υπάρχουν τρία συστατικά, ο πράκτορας, το περιβάλλον και η ανταμοιβή. Πιο συγκεκριμένα ένας πράκτορας εκτελεί ενέργειες στο περιβάλλον και λαμβάνει ανταμοιβή, θετική ή αρνητική. Σε όλες τις παραπάνω μεθόδους οι συντάκτες ανέλυσαν αλγορίθμους και προσεγγίσεις τόσο στη μηχανική όσο και στη βαθιά μάθηση, ανέπτυξαν τα υπέρ και τα κατά αυτών, καθώς και κάποιες από τις προκλήσεις τους. Κατέληξαν στο συμπέρασμα πώς οι παραπάνω προσεγγίσεις είναι αρκετά ελπιδοφόρες όσον αφορά την ανίχνευση των εισβολών τόσο σε επίπεδο δικτύου όσο και σε φυσικό επίπεδο στα ICS, αν και μπορούν να υπάρξουν βελτιώσεις.

Στο άρθρο [50] προτείνεται ένα υβριδικό μοντέλο ΣΑΕ για την ασφάλεια του CAN Bus αλλά και την προστασία των οχημάτων από κακόβουλες εισβολές .Το προτεινόμενο σύστημα συνδυάζει δύο προσεγγίσεις, την rule-based και machine learning-based προσέγγιση. Η πρώτη βασίζεται στα χαρακτηριστικά ενός φυσιολογικού μηνύματος CAN, έχει αρκετά υψηλό κόστος και χαμηλό ποσοστό ανίχνευσης ενώ η δεύτερη παρέχει υψηλή ακρίβεια . Το προτεινόμενο ΣΑΕ τοποθετείται κεντρικά, ενώ πριν την διαδικασία της ανίχνευσης πραγματοποιείται offline εκπαίδευση με δεδομένα εισόδου τα μηνύματα CAN. Όταν εφαρμόζεται το ΣΑΕ το μήνυμα εισάγεται πρώτα στο στάδιο του rule-based. Κάθε μήνυμα που δεν ανιχνεύεται ως κακόβουλη ενέργεια εισέρχεται και στο δεύτερο στάδιο, αλλιώς αν δεν συμβαδίζει με τους κανόνες θεωρείται εισβολή. Με αυτήν την σειρά των γεγονότων επιτυγχάνεται γρήγορη ανίχνευση και μείωση φόρτου χωρίς παράλληλα να μειώνεται η ακρίβεια του συστήματος. Παράλληλα στο στάδιο του machine-learning γίνεται χρήση του βαθύ νευρωνικού δικτύου (Deep Neural Network-DNN) με πέντε κρυφά στρώματα για τέσσερα οχήματα. Στο σύστημα εφαρμόσθηκαν διάφορες επιθέσεις, διορθώθηκε η ανισορροπία δεδομένων (class imbalance) και εξετάστηκαν μετρικές όπως accuracy, TPR και FPR. Αποδείχθηκε πως το ΣΑΕ είχε υψηλή ακρίβεια. Ακόμα εξετάστηκαν ο χρόνος απόδοσης του συστήματος, τα αποτελέσματα της εφαρμογής του σε διαφορετικές βάσεις δεδομένων αλλά και σε ποικίλο αριθμό από εισβολές. Δόθηκε έμφαση στην απώλεια του μοντέλου αλλά και στην υπερ-προσαρμογή (overfitting) και οι συντάκτες κατέληξαν πως το προτεινόμενο υβριδικό μοντέλο είναι αρκετά αποτελεσματικό.

Στο άρθρο [51] οι συντάκτες επισημαίνουν την ανάγκη της προστασίας των συστημάτων με IoT συσκευές από πιθανές εισβολές. Το προτεινόμενο σύστημα ανίχνευσης εισβολών είναι ο συνδυασμός των αλγορίθμων μηχανικής μάθησης XGB και RF . Ο Random Forest χρησιμοποιείται για την επιλογή των χαρακτηριστικών στην N-BaIoT dataset και ο XGB για την ανίχνευση εισβολών. Η αρχιτεκτονική του συστήματος απαρτίζεται από κάποια στάδια. Αρχικά πραγματοποιείται δειγματοληψία με δεδομένα που παρουσιάζουν τόσο φυσιολογική όσο και μη συμπεριφορά. Στη συνέχεια λόγω της ανισορροπίας των δεδομένων ακολουθεί η προ-επεξεργασία τους καθώς και η επιλογή των πιο σημαντικών χαρακτηριστικών με εφαρμογή του αλγορίθμου RF . Τέλος έπεται η εφαρμογή των ταξινομητών (classifiers), όπου μετά την επιλογή των χαρακτηριστικών από τον RF, ο XGBoost συνδυάζει αδύναμους classifiers, ώστε να δημιουργήσει έναν ισχυρό. Χρησιμοποιεί feedback από προηγούμενα DT προσπαθώντας να μειώσει το σφάλμα που προκύπτει . Για την εκτίμηση του προτεινόμενου συστήματος γίνεται χρήση αρκετών μετρικών αλλά και έξι confusion matrices, όπου έδειξαν ότι το προτεινόμενο σύστημα έχει υψηλή ακρίβεια της τάξεως του 99% και είναι πιο αποδοτικό σε σχέση με τα υπόλοιπα.

Στο άρθρο [52] οι συντάκτες αναφέρουν πως η ανάπτυξη των έξυπνων δικτύων (Smart Grid) συνεπάγει την ύπαρξη εισβολέων στο δίκτυο, γεγονός που επέφερε την ανάπτυξη των ΣΑΕ. Το προτεινόμενο σύστημα, το λεγόμενο MENSA, υιοθετεί την GAN αρχιτεκτονική για να ανιχνεύει ανωμαλίες και να ταξινομεί τις TCP και DNP3 επιθέσεις. Η αρχιτεκτονική MENSA απαρτίζεται από τα παρακάτω στοιχεία. Πρώτο στοιχείο αποτελεί το στρώμα εισόδου (input layer), που δέχεται τα δεδομένα του DNN και πιο συγκεκριμένα ένα διάνυσμα θορύβου. Μετά ακολουθεί ο αποκωδικοποιητής γεννήτριας (Generator Decoder), όπου είναι εκπαιδευμένος να παράγει φυσιολογικά δεδομένα. Έπεται ο κωδικοποιητής διάκρισης (Discriminator Encoder), όπου διακρίνει τα πραγματικά από τα παραγόμενα δείγματα δεδομένων. Όσον αφορά την αρχιτεκτονική MENSA για την ταξινόμηση αποτελεσμάτων αυτή αποτελείται από τα ίδια τρία μέρη με μόνη διαφορά ότι έχει σχεδιαστεί για να διαχειρίζεται δεδομένα πολλαπλών κλάσεων με λιγότερα χαρακτηριστικά. Το MENSA αξιολογείται σε τέσσερα πραγματικά SG περιβάλλοντα και συγκρίνεται με άλλες τεχνολογίες σε μετρικές όπως accuracy, TPR, FPR, F1-score και precision . Αποδείχθηκε πως την καλύτερη απόδοση την κατείχε το προτεινόμενο σύστημα με υψηλή απόδοση, υψηλό TPR και χαμηλό FPR.

Ο Andree Kummerow και οι υπόλοιποι συγγραφείς του άρθρου [53] πραγματεύονται την ανάπτυξη συστήματος ανίχνευσης ανωμαλιών δεδομένων εισβολής δικτύου και φάσης για την προστασία των δυναμικών κέντρων ελέγχου από επιθέσεις κυβερνοχώρου. Το εν λόγω σύστημα περιλαμβάνει την χρήση ειδικών κανόνων, μιας κλάσης ταξινομητή και επαναλαμβανόμενα νευρωνικά δίκτυα για την παρακολούθηση των πακέτων δικτύου. Επομένως έγινε χρήση πολλών αλγορίθμων ανίχνευσης που βασίζονται τόσο στη μηχανική μάθηση για την ανάλυση της διαδικτυακής κίνησης όσο και σε ειδικούς κανόνες που αφορούν την ανάλυση IP address, Src port ,Dst port καθώς και time ή quality flags. Με αυτόν τον τρόπο ελέγχεται η μεταφορά δεδομένων SCADA και PMU μεταξύ του δυναμικού κέντρου ελέγχου και του επιπέδου υποσταθμού. Η αρχιτεκτονική του προτεινόμενου συστήματος απαρτίζεται από ένα υβριδικό NIDS και μια εφαρμογή ανίχνευσης και διόρθωσης ανωμαλιών δεδομένων φάσης. Κάθε μία από τις παραπάνω εφαρμογές εστιάζει σε διαφορετικό κομμάτι πληροφοριών των IMU και MMS πακέτων . Το NIDS χρησιμοποιεί ειδικούς κανόνες ενώ η δεύτερη ένα επαναλαμβανόμενο αυτόματο κωδικοποιητή και μοντέλο πρόβλεψης βασισμένο σε νευρωνικά δίκτυα που ανιχνεύει και αντικαθιστά

χειριζόμενα δεδομένα φάσης. Για την αξιολόγηση του συστήματος χρησιμοποιήθηκε προσομοιωμένη μηχανή σε πραγματικό χρόνο με κίνηση δικτύου υπό διαφορετικές καταστάσεις συστήματος. Ενσωματώθηκε ένας αντίπαλος όπου πραγματοποιούσε επιθέσεις MITM και τα αποτελέσματα έδειξαν την υψηλή αποτελεσματικότητα του προτεινόμενου συστήματος με μετρικές όπως το F1-Score κάτω από διαφορετικά σενάρια.

Στο άρθρο [54] οι συγγραφείς αναφέρουν πως η εξ αποστάσεως υγειονομική περίθαλψη απορροφάται με υψηλούς ρυθμούς στο χώρο της ιατρικής. Ωστόσο, υπάρχουν ζητήματα ασφαλείας στα συστήματα αυτά που επηρεάζουν την αξιοπιστία τους και το απόρρητο των ασθενών. Αρχικά οι συντάκτες πραγματοποιούν μια επισκόπηση στα CHS και στις απειλές που δέχονται ενώ στην συνέχεια παραθέτουν ΣΑΕ που έχουν υλοποιηθεί για την αντιμετώπιση τους χωρίς όμως ιδιαίτερα αποτελέσματα. Έπειτα παρουσιάζουν το προτεινόμενο σύστημα, το λεγόμενο SAE, δηλαδή στοιβαγμένος αυτό-κωδικοποιητής, όπου όχι μόνο μειώνει τις διαστάσεις των χαρακτηριστικών των δεδομένων, αλλά και το υπολογιστικό κόστος. Με το SAE εξάγονται υψηλής ποιότητας χαρακτηριστικά ικανά να κρίνουν πιθανές επιθέσεις. Η αρχιτεκτονική του συστήματος, απαρτίζεται από τρία μέρη. Το πρώτο είναι η προ-επεξεργασία δεδομένων (data preprocessing), όπου είναι υπεύθυνο για την ενιαία μετατροπή των αρχικών δεδομένων . Το δεύτερο είναι η εξαγωγή χαρακτηριστικών (feature extraction), που αποτελείται από το pre-training και το fine-tuning, όπου θέτει καλή αρχική τιμή στο SAE και προσαρμόζει τα βάρη στους νευρώνες αντίστοιχα. Το τρίτο είναι το Intrusion Behavior Detection, όπου χρησιμοποιεί τον αλγόριθμο XGBoost, για να κατανοήσει αν πρόκειται για ενδεχόμενη επίθεση ή όχι. Για την αξιοπιστία του συστήματος χρησιμοποιήθηκε ένα πραγματικό CHS με αληθινές DOS επιθέσεις ενώ με μετρικές όπως accuracy, FPR και FNR αποδείχθηκε πως η αποτελεσματικότητα του προτεινόμενου συστήματος ήταν ιδιαίτερα μεγάλη.

Στο άρθρο [55] οι συγγραφείς πραγματεύονται την ανάγκη ακριβούς εκτίμησης της ηλεκτρικής κατάστασης του δικτύου ηλεκτρικής ενέργειας, αφού με την ύπαρξη των κυβερνοεπιθέσεων ενδέχεται να γίνει ανακριβής με αποτέλεσμα να οδηγήσει σε λανθασμένες αποφάσεις. Προκειμένου να γίνεται ανίχνευση των επιθέσεων παρουσιάζεται ένα σύστημα βασισμένο στην ομαδοποίηση, το λεγόμενο PMUIDS. Στο προαναφερόμενο αρχικά τοποθετείται με βέλτιστο τρόπο η συσκευή του PMU, ώστε όλο το δίκτυο να είναι πλήρως παρατηρήσιμο. Στη συνέχεια αφαιρούνται οι μετρήσεις ενός PMU υπολογίζεται το διάνυσμα κατάστασης και μετά γίνεται η ταξινόμηση των δεδομένων. Με αυτόν τον τρόπο η αφαιρετική ομαδοποίηση λαμβάνει τον αριθμό συστάδων και η ασαφής ομαδοποίηση C-means εκχωρεί τα διανύσματα αυτά σε σωστό σύμπλεγμα. Έπειτα παρατίθεται η σύγκριση του προτεινόμενου συστήματος με άλλα όσον αφορά την ανίχνευση των κρυφών επιθέσεων σύμφωνα με συγκεκριμένες ιδιότητες. Έτσι αποδείχθηκε η ικανότητα ανίχνευσης επιθέσεων του PMUIDS με δύο θεωρήματα όπου δείχνουν πως δεν μπορούν να πραγματοποιηθούν επιθέσεις σε αυτό αλλά και την ικανότητα του να εντοπίζει ψευδή δεδομένα στις μετρήσεις. Για την εκτίμηση του προτεινόμενου συστήματος υλοποιήθηκαν τρία σενάρια. Στο πρώτο δεν συνέβησαν επιθέσεις, στο δεύτερο πραγματοποιήθηκε μία, ενώ στο τρίτο σενάριο τρεις. Σε όλες τις περιπτώσεις φάνηκε η αποτελεσματικότητα του συστήματος, καθώς το PMUIDS ήταν ικανό να ανιχνεύσει, να κρίνει και να αποφασίσει για την φύση της επίθεσης.

Ο Vivek Kumar Singh και οι υπόλοιποι συντάκτες του άρθρου [56] ισχυρίστηκαν πως η ανάπτυξη ενός ολοκληρωμένου και αποτελεσματικού ΣΑΕ για την προστασία ενός ηλεκτρικού δικτύου είναι δύσκολη, καθώς απαιτεί πλήρη γνώση του δικτύου και της αρχιτεκτονικής του. Στο

συγκεκριμένο άρθρο παρουσιάστηκε ένα network-based, model-based και State of the art ML IDS, για την ανίχνευση επιθέσεων με την βοήθεια του μοντέλου kill-chain. Μέσω του προαναφερόμενου οι διαχειριστές του συστήματος δύναται να κατανοήσουν τα βήματα που χρειάζεται να ακολουθήσουν οι εισβολείς για να εκπληρώσουν τους σκοπούς τους. Στην αρχή του άρθρου οι συντάκτες παραθέτουν τις κατηγορίες ενός συστήματος ανίχνευσης εισβολών, καθώς και τις προκλήσεις που αντιμετωπίζουν. Όσον αφορά την αρχιτεκτονική του προτεινόμενου συστήματος απαρτίζεται από τα επόμενα μέρη. Το πρώτο είναι το signature-based IDS, όπου ελέγχεται και αναλύεται η κίνηση δικτύου SCADA και εφαρμόζονται κανόνες ώστε να ανιχνεύονται απειλές που αντιστοιχούν σε ήδη επιβεβαιωμένες. Το δεύτερο είναι το model-based, όπου βασίζεται στο μοντέλο CPS για τον εντοπισμό μη φυσιολογικών συμπεριφορών και εξάγει στο επόμενο στρώμα alert messages, σε περίπτωση ανίχνευσης ανώμαλης συμπεριφοράς. Στο τρίτο στρώμα, εφαρμόζονται τεχνικές μηχανικής μάθησης προκειμένου να εντοπιστούν κρυφές επιθέσεις. Ακόμα, το σύστημα διαχείρισης συναγερμών (Alert Management System), δέχεται μηνύματα και από τα παραπάνω τρία στρώματα. Η αξιολόγηση του προτεινόμενου συστήματος, έγινε με πείραμα σε CPS βάση δεδομένων, όπου αποδείχθηκε πως ο συνδυασμός των μοντέλων για την ανάπτυξη του ΣΑΕ παρείχε υψηλή ακρίβεια.

Το άρθρο [57] σχετίζεται με τον τομέα του IoT, που έχει γνωρίσει τεράστια εξέλιξη, αφού βοηθά τον κόσμο να πραγματοποιεί τις υποχρεώσεις του αυτοματοποιημένα. Ωστόσο με την δραστική αυτή πρόοδο, έχει αυξηθεί και ο κίνδυνος των δικτυακών επιθέσεων σε τέτοιου είδους συστήματα. Εξαιτίας αυτού, εξετάστηκαν και εφαρμόστηκαν πολλαπλά συστήματα ανίχνευσης εισβολών. Στο συγκεκριμένο άρθρο οι συγγραφείς προτείνουν την ανάπτυξη συστήματος, που είναι βασισμένο στην μάθηση και πιο συγκεκριμένα σε αλγορίθμους όπως το Logistic Regression, Naive Bayes και Decision Trees. Παρουσιάζονται διεξοδικά τα χαρακτηριστικά των παραπάνω αλγορίθμων όπως και η βάση δεδομένων (CICIDS2017) πάνω στην οποία θα εφαρμοστούν. Παράλληλα αναφέρεται η ανάγκη προ-επεξεργασίας της βάσης δεδομένων, αφού μπορεί να περιέχει «άχρηστα δεδομένα», μηδενικές γραμμές και άλλα περιττά χαρακτηριστικά. Στη συνέχεια, εφαρμοστήκαν αλγόριθμοι μηχανικής μάθησης και εξήχθη το συμπέρασμα, πως το προτεινόμενο σύστημα έχει υψηλή ακρίβεια και υπόσχεται την ανίχνευση όλων των ειδών επιθέσεων.

Στη σημερινή εποχή, ο τομέας των Smart Grid και SDN Networks προσελκύον πολλών ειδών δικτυακές απειλές. Στο άρθρο [58] οι συγγραφείς προτείνουν την ανάπτυξη ενός συστήματος , που είναι βασισμένο στην αυτό-μάθηση του ΤΝΔ με στόχο τον εντοπισμό και την ταξινόμηση επιθέσεων στον κυβερνοχώρο. Η παραπάνω προσέγγιση προσφέρει μια λεπτομερή ανάλυση για την απόδοση των διαδοχικών ταξινομητών σε νευρωνικά στρώματα όπως tanh και ReLU. Προκειμένου να αναπτυχθεί αποτελεσματικά το μοντέλο η βάση δεδομένων NSL-KDD υπέστη προ-επεξεργασία. Πιο συγκεκριμένα, πραγματοποιήθηκαν η κανονικοποίηση των δεδομένων καθώς και η επιλογή συγκεκριμένων χαρακτηριστικών. Στη συνέχεια αναπτύχθηκε το SEQ-FNN model, το οποίο αποτελούνταν από 4 στρώματα MLP, ANN, Tensorflow, και Keras Dense I/O επίπεδα. Το SEQ-FFNN είναι μοντέλο αυτό-μάθησης που παρέχει ακρίβεια 98,95% για τα ενεργοποιημένα στρώματα Tanh και 99,59% για ενεργοποιημένα επίπεδα ReLU. Τα αποτελέσματα που καταγράφηκαν επιβεβαιώνουν την κυριαρχία του ReLU κατά την ταξινόμηση. Τέλος το SEQ-FFNN εντόπισε με ακρίβεια DOS, R2L και U2R επιθέσεις καθώς και πραγματοποίησε ορθή ταξινόμηση του NSL-KDD συνόλου δεδομένων σε κλάσεις με φυσιολογική ή όχι συμπεριφορά.

Στο άρθρο [59] οι αρθρογράφοι προτείνουν την ανάπτυξη ενός ΣΑΕ βασισμένο σε SDN, το οποίο χρησιμοποιεί τεχνικές βαθιάς μάθησης για να εκπληρώσει το στόχο του. Πιο συγκεκριμένα ανέπτυξαν το λεγόμενο IDSIoT-SDL σύστημα, το οποίο απαρτίζεται από τρία μέρη που σχετίζονται με την καταγραφή και την ανάλυση κυκλοφορίας, την εξαγωγή χαρακτηριστικών αλλά και την ανίχνευση ανωμαλιών. Ειδικότερα αποτελείται από τον activity monitor, υπεύθυνος για την καταγραφή και την ανάλυση της κίνησης, αφού καταγράφει την κίνηση με το εργαλείο του Wireshark και συλλέγει δεδομένα για την επιλογή των μετέπειτα χαρακτηριστικών. Επιπρόσθετο στοιχείο του προτεινόμενου συστήματος είναι ο activity analyzer, που ανιχνεύει την ύποπτη συμπεριφορά. Κύρια αρμοδιότητα του είναι η εξαγωγή των χαρακτηριστικών μέσω του αλγορίθμου LSTM. Αναπόσπαστο κομμάτι του συστήματος αποτελεί ο ταξινομητής, ο οποίος κατηγοριοποιεί την κίνηση σε ύποπτη ή μη. Σε αυτό το σημείο συμβαίνει η εκπαίδευση του ταξινομητή και η ανίχνευση εισβολών. Η βάση δεδομένων που χρησιμοποιήθηκε για την αξιολόγηση του μοντέλου ήταν η CSE-CIC-IDS2018, που περιέχει στοιχεία κι πακέτα από πραγματική δικτυακή κίνηση σε IoT συσκευές. Εξετάστηκαν αρκετές μετρικές όπως ακρίβεια, precision, recall, F1-score, FPR, FNR και αποδείχθηκε πως το προτεινόμενο σύστημα ήταν αρκετά αποτελεσματικό σε σχέση με άλλα.

Στο άρθρο [60] ένα μοντέλο ανίχνευσης εισβολών, που συγχωνεύει τόσο CNN όσο και τη νέα γενιά των RNN τα Gated Recurrent Unit (GRU), προτείνεται από τους συγγραφείς, για την αντιμετώπιση προβλημάτων, που αφορούν την χαμηλή ακρίβεια των ήδη υπαρχόντων IDS . Πιο συγκεκριμένα το μοντέλο αποτελείται από τρία στάδια τα οποία περιγράφονται κατά σειρά. Αρχικά, είναι το στάδιο της προ-επεξεργασίας, όπου τα πρωταρχικά δεδομένα μετατρέπονται σε νούμερα, δηλαδή κανονικοποιούνται. Στη συνέχεια το σύνολο των δεδομένων εξισορροπείται με τον αλγόριθμο ADRDB, όπου μετά από αυτόν εξάγονται χαρακτηριστικά από τον αλγόριθμο RF σε συνδυασμό με την ανάλυση συσχέτισης Pearson και μετατρέπονται σε κλίμακα grey-scale. Σε δεύτερο στάδιο, όπου είναι και το στάδιο της εκπαίδευσης αποδίδονται στα προ-επεξεργασμένα δεδομένα διαφορετικά βάρη από το CBAM, ενώ μετέπειτα εξάγονται τα χωρικά χαρακτηριστικά από το CNN. Περαιτέρω πληροφορίες συλλέγονται από το συνδυασμό στρωμάτων Average pooling -Max pooling. Έπειτα τα χρονικά χαρακτηριστικά εξάγονται από πολλαπλές μονάδες GRU. Τέλος η ταξινόμηση εκτελείται από τη συνάρτηση Softmax. Στο τρίτο στάδιο, αυτό της δοκιμής, το τεστ δοκιμής εισάγεται στο εκπαιδευμένο μοντέλο για ταξινόμηση. Για την αξιολόγηση του μοντέλου έγινε χρήση τριών βάσεων δεδομένων της UNSW-NB15, της NSL-KDD και CIC-IDS2017, ενώ παράλληλα εξετάστηκαν μετρικές όπως accuracy, precision, recall , f1-score και αποδείχθηκε η υψηλή αποτελεσματικότητα του προτεινόμενου μοντέλου.

Το SDN είναι βασικό εργαλείο για την ευελιξία της αρχιτεκτονικής του Διαδικτύου. Ωστόσο, επιφέρει προβλήματα ασφαλείας εξαιτίας της ευελιξίας που παρέχει. Στο άρθρο [61] οι αρθρογράφοι προτείνουν ΣΑΕ που συνδυάζει RNN και GRU, προκειμένου να γίνει εφικτή η ανίχνευση ανωμαλιών στα δίκτυα SDN. Το σύστημα ανίχνευσης υλοποιείται σαν εφαρμογή στον ελεγκτή του SDN και απαρτίζεται από τρία μέρη. Αρχικά πρώτο στοιχείο αποτελεί ο Flow Collector, όπου συλλέγει δεδομένα που σχετίζονται με τα πρωτόκολλα, την πηγή καθώς και την Ip του προορισμού .Στη συνέχεια αυτά αποστέλλονται στον Anomaly Detector. Ο προαναφερόμενος έχει ως πυρήνα του το GRU-RNN και φορτώνει ένα εκπαιδευμένο μοντέλο, που λαμβάνει τα στατιστικά από τον Flow Collector και αποφασίζει αν πρόκειται για εισβολή ή όχι. Τέλος στοιχείο του συστήματος είναι ο Anomaly Mitigator, όπου αποφασίζει για την πορεία της ροής. Για την

αξιολόγηση του μοντέλου χρησιμοποιήθηκε το NSL-KDD dataset όπως και μετρικές accuracy, precision, recall, f1-score. Τελικά αποδείχθηκε πως το προτεινόμενο σύστημα είναι αρκετά αποδοτικό.

Η εξέλιξη των IoT δημιουργεί τεράστιες προκλήσεις όσον αφορά την ασφάλεια των συσκευών του δικτύου, αλλά και την προστασία της ιδιωτικότητας των ανθρώπων. Στο άρθρο [62] οι συγγραφείς προτείνουν την ανάπτυξη του συστήματος Realguard, σύστημα ανίχνευσης εισβολής δικτύου, που βασίζεται σε DNN και λειτουργεί άμεσα σε τοπικές πύλες για την προστασία των IoT συσκευών. Η αρχιτεκτονική του Realguard απαρτίζεται από τέσσερα στοιχεία. Το πρώτο είναι το Packet Observation Component (POC), που καταγράφει την κίνηση του δικτύου και εξάγει πληροφορίες για τα δεδομένα. Στην συνέχεια ακολουθεί το Feature Extraction Component (FEC), που υπολογίζει τα στατιστικά του δικτύου με βάση την συλλογή των δεδομένων από το πρώτο βήμα. Ακόμα το Attack Detection Component (ADE) είναι υπεύθυνο για τον εντοπισμό ανωμαλιών στην κίνηση δικτύου σε δεδομένα δικτύου σε πραγματικό χρόνο. Για την επίτευξη αυτού του στόχου προτείνεται μοντέλο DNN που όχι μόνο ανιχνεύει εάν συνέβη μια επίθεση ή όχι, αλλά και προσδιορίζει τον τύπο της επίθεσης. Τέλος ακολουθεί το Action Manager Component (AMC) , όπου λαμβάνονται αποφάσεις για τις ενέργειες που χρειάζεται να γίνουν εάν ανιχνευθεί επίθεση από το ADE. Για την αξιολόγηση του μοντέλου έγινε χρήση της βάσης δεδομένων CIC-IDS 2017 και μετρικών όπως το TPR τόσο σε δυαδική όσο και σε πολλαπλή ταξινόμηση. Τελικά αποδείχθηκε πως το σύστημα είναι αρκετά αποτελεσματικό σε σχέση με άλλα και έχει την δυνατότητα ανίχνευσης δέκα γνωστών επιθέσεων.

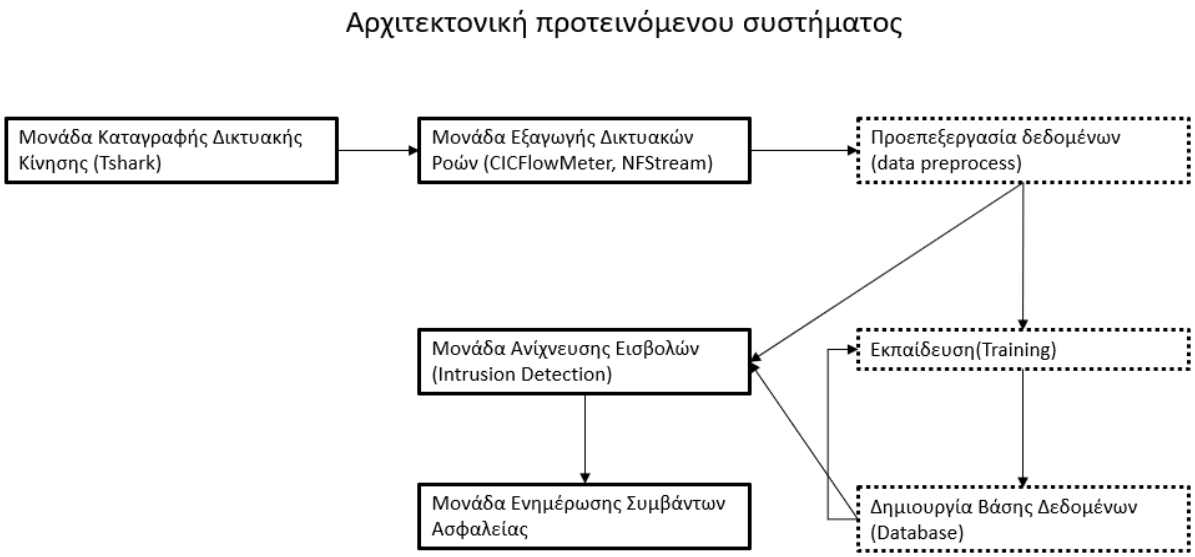
Συνοψίζοντας, στην παρούσα ενότητα παρουσιάστηκαν 28 συστήματα ανίχνευσης και πρόληψης εισβολών στο Διαδίκτυο των Πραγμάτων. Ειδικότερα, στην πλειοψηφία τους ο τύπος των IDPS ήταν Anomaly-based, εκτός από ελάχιστες περιπτώσεις, όπου συνδύαζαν τόσο anomaly-based όσο και signature based προσέγγιση. Για την αξιολόγηση των συστημάτων έγινε χρήση αλγορίθμων μηχανικής και βαθιάς μάθησης με κυριότερους από αυτούς τους LSTM, XGBoost, SVM, k-NN, CNN, Naïve Bayes, Random Forest, Decision Trees, DNN και Adaboost. Παράλληλα για την εκτίμηση της απόδοσης των προτεινόμενων μοντέλων χρησιμοποιήθηκαν δημόσιες βάσεις δεδομένων και εξετάστηκαν ποικίλες μετρικές, όπως ακρίβεια, precision, recall, F1-score, TPR, FPR, TNR,FNR και χρόνος ανίχνευσης εισβολών. Τέλος όλα τα προαναφερόμενα συστήματα επέφεραν βελτίωση στον τομέα της ανίχνευσης εισβολών, αφού καθένα από αυτά είχε διαφορετική αρχιτεκτονική, άρα και άλλες δυνατότητες.

Κεφάλαιο 5: Αρχιτεκτονική προτεινόμενου Συστήματος Ανίχνευσης Εισβολών για το Διαδίκτυο των Πραγμάτων

Στο συγκεκριμένο κεφάλαιο θα αναλυθεί η αρχιτεκτονική του ΣΑΕ που αναπτύχθηκε για την υλοποίηση της παρούσας διπλωματικής. Αναλυτικότερα θα παρουσιαστούν στις παρακάτω υπό-ενότητες όλα τα μέρη που απαρτίζεται το ΣΑΕ καθώς και οι αντίστοιχες λειτουργίες τους.

5.1 Συνολική περιγραφή του προτεινόμενου ΣΑΕ

Το Σχήμα 1 απεικονίζει την αρχιτεκτονική του προτεινόμενου ΣΑΕ. Το παραπάνω απαρτίζεται από τέσσερις ενότητες και συγκεκριμένα α)Μονάδα Καταγραφής Δικτυακής Κίνησης, β)Μονάδα Εξαγωγής Δικτυακών Ροών, γ)Μονάδα Ανίχνευσης Εισβολών και δ) Μονάδα Ενημέρωσης Συμβάντων Ασφαλείας. Καθένα από αυτά περιγράφεται αναλυτικά στις παρακάτω υπό-ενότητες. Η Μονάδα Καταγραφής Δικτυακής Κίνησης και η Μονάδα Εξαγωγής Δικτυακών Ροών είναι υπεύθυνες για την καταγραφή της κίνησης αλλά και την τροφοδοσία του συστήματος με τα απαραίτητα δεδομένα για τον εντοπισμό των κυβερνοεπιθέσεων. Η Μονάδα Ανίχνευσης Εισβολών είναι υπεύθυνη για την ανίχνευση των επιθέσεων που πραγματοποιούνται στο σύστημα, ενώ η Μονάδα Ενημέρωσης Συμβάντων Ασφαλείας δημιουργεί συμβάντα ασφαλείας, προκειμένου να μετριαστεί έγκαιρα η υπάρχουσα εισβολή.



Σχήμα 1: Αρχιτεκτονική Συστήματος Ανίχνευσης Εισβολών

5.2 Μονάδα Καταγραφής Δικτυακής Κίνησης

Η ανάλυση του δικτύου (network analysis) ορίζεται ως η διαδικασία μέσω της οποίας καταγράφονται και αναλύονται δικτυακά πακέτα που διακινούνται μέσα σε ένα δίκτυο υπολογιστικών συστημάτων. Στην παρούσα διπλωματική γίνεται χρήση του T-shark , ενός αναλυτή πρωτοκόλλου δικτύου.

Το T-shark επιτρέπει την ζωντανή σύλληψη πακέτων δικτύου αλλά και την ανάγνωση ή ανάλυση των πακέτων δεδομένων από προηγούμενα αποθηκευμένα αρχεία.

Όπως είναι γνωστό, η δικτυακή κίνηση ή κίνηση δεδομένων είναι ο όγκος των δεδομένων που μεταφέρονται μέσω του δικτύου σε κάποια δεδομένη χρονική στιγμή. Τα δεδομένα δικτύου στα δίκτυα υπολογιστών έχουν τη μορφή δικτύου πακέτα δεδομένων. Η ανάλυση αυτών των πακέτων δικτύου παρέχει ασφάλεια δικτύου, καθώς βοηθά στην παρακολούθηση της κυκλοφορίας . Επομένως, εάν παρατηρηθεί ασυνήθιστη ποσότητα κίνησης δεδομένων σε ένα δίκτυο που είναι ένα πιθανό σημάδι μιας επίθεσης, τότε το Tshark βοηθά στον έγκαιρο εντοπισμό της .

Συνοπτικά, το Tshark χρησιμοποιείται ως αναλυτής δικτύου που αναπτύχθηκε από την Wireshark. Η δομή εργασίας του είναι αρκετά παρόμοια με το Tcpdump, αλλά έχει ισχυρούς αποκωδικοποιητές και φίλτρα. Είνα ικανό να συλλαμβάνει τις πληροφορίες των πακέτων δεδομένων από διαφορετικά επίπεδα δικτύου και να τα εμφανίζει σε διαφορετικές μορφές. Το Tshark χρησιμοποιείται για την ανάλυση του πραγματικής ώρας κυκλοφορίας του δικτύου και μπορεί να διαβάσει .pcap αρχεία για να αναλύσει τις πληροφορίες και να εμβαθύνει στις λεπτομέρειες των συνδέσεων, βοηθώντας τους επαγγελματίες ασφαλείας να αναγνωρίσουν το δικτυακό πρόβλημα.

5.3 Μονάδα Εξαγωγής Δικτυακών Ροών

Η παρακολούθηση της κυκλοφορίας και των υπηρεσιών κατέχει πάντα στρατηγικό ρόλο στην κατανόηση και διαχείριση δικτύων υπολογιστών. Αρκετές μεθοδολογίες και εργαλεία έχουν κατασκευαστεί για να βοηθούν καθημερινά ρουτίνες διαχείρισης, απόκτηση κριτικής γνώσης και βοήθεια στη διατήρηση του δικτύου. Εξαιτίας του παραπάνω γεγονότος, στην συγκεκριμένη μονάδα εξαγωγής δικτυακών ροών έγινε χρήση αναλυτών κυκλοφορίας δικτύου και ειδικότερα του CICFlowMeter και του NFStream.

Το CICFlowMeter [64] είναι μια γεννήτρια ροής κυκλοφορίας δικτύου που διανέμεται από την CIC για τη δημιουργία 84 χαρακτηριστικών κυκλοφορίας δικτύου. Διαβάζει το αρχείο pcap και δημιουργεί μια γραφική αναφορά των δυνατοτήτων που εξήχθησαν. Παράλληλα, παρέχει ένα αρχείο csv της αναφοράς. Είναι μια εφαρμογή ανοιχτού κώδικα γραμμένη σε Java και μπορεί να ληφθεί από το Github, ενώ λειτουργεί τόσο εντός όσο και εκτός σύνδεσης. Οι πηγαίοι κώδικές του μπορούν να ενσωματωθούν σε ένα έργο, καθώς προσφέρει μεγαλύτερη ευελιξία όσον αφορά την επιλογή των χαρακτηριστικών που πρέπει να υπολογιστούν, την προσθήκη νέων, καθώς και τον καλύτερο έλεγχο της διάρκειας του χρονικού ορίου ροής.

Το NFStream [65] είναι ένα πλαίσιο ανοιχτού κώδικα που επιτρέπει υψηλή απόδοση στην ανάλυση της ροής κυκλοφορίας δικτύου. Εκτός από τον υπολογισμό στατιστικών στοιχείων ροής, το NFStream μπορεί επίσης να καθορίσει τους τύπους εφαρμογών που δημιουργούν τις ροές.

Σχεδιάστηκε για να λειτουργεί τόσο σε λειτουργίες ζωντανής όσο και εκτός σύνδεσης και βασίζεται στο libpcap, την de facto τυπική βιβλιοθήκη που χρησιμοποιείται για καταγραφή πακέτων . Ακόμα μπορεί να αναγνωρίσει σωστά πακέτα που προέρχονται από διαφορετικές ροές αντανακλώντας τα πραγματικά χαρακτηριστικά της κυκλοφορίας παρέχοντας ακριβέστερη αντίληψη ροής. Επιπλέον μπορεί να χρησιμοποιηθεί ως βιβλιοθήκη επιτρέποντας την απλή ενσωμάτωση με άλλα εργαλεία και υπηρεσίες που λειτουργούν σε λειτουργικά δίκτυα.

Συνοψίζοντας τόσο το CICFlowMeter όσο και το NFStream χρησιμοποιούνται αποτελεσματικά από την συγκεκριμένη μονάδα της αρχιτεκτονικής του προτεινόμενου συστήματος ανίχνευσης εισβολών, προκειμένου να εξαχθούν τα απαραίτητα χαρακτηριστικά των δικτυακών ροών και να μελετηθεί η κίνηση του δικτύου για ύπαρξη πιθανών εισβολών.

5.4 Μονάδα Ανίχνευσης Εισβολών

Η μονάδα ανίχνευσης εισβολών αποτελεί τον πυρήνα του προτεινόμενου ΣΑΠΕ. Πρώτα λαμβάνει τις συλληφθείσες ροές από την βάση δεδομένων CIC IoT Dataset 2022 και έπειτα εφαρμόζει μοντέλα και τεχνικές, προκειμένου να ανιχνευθούν ανωμαλίες.

Έπειτα από την σύνθεση της βάσης ,στην εκπόνηση της εργασίας, δόθηκε έμφαση στην διαδικασία χαρακτηρισμού των δεδομένων, αφού η ορθή επισήμανσή τους, διαδραματίζει καθοριστικό ρόλο στην ακρίβεια της ανίχνευσης των εισβολών. Επομένως τα δεδομένα χωρίστηκαν σε τρεις κατηγορίες, σε αυτά που ήταν φυσιολογικά (Normal) , σε αυτά που ήταν επιθέσεις Flood αλλά και σε RTSP Brute-Force.

Τα φυσιολογικά δεδομένα (Normal) αναφέρονται σε φυσιολογική ανταλλαγή πακέτων μέσα στο δίκτυο. Αντίθετα στις επιθέσεις πλημμύρας (Flood), που είναι επίσης γνωστές ως επιθέσεις άρνησης υπηρεσίας (DoS), οι εισβολείς στέλνουν πολύ μεγάλο όγκο κίνησης σε ένα σύστημα, ώστε να μην μπορεί να εξετάσει και να επιτρέψει την επιτρεπόμενη κυκλοφορία δικτύου. Όσον αφορά την επίθεση ωμής βίας (brute force) είναι μια μέθοδος hacking που χρησιμοποιεί δοκιμή και σφάλμα για να σπάσει κωδικούς πρόσβασης, διαπιστευτήρια σύνδεσης και κλειδιά κρυπτογράφησης. Είναι μια απλή αλλά αξιόπιστη τακτική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε μεμονωμένους λογαριασμούς-συστήματα και δίκτυα οργανισμών.

Στις ακόλουθες υπό-ενότητες περιγράφονται η διαδικασία της προ-επεξεργασίας των δεδομένων πριν γίνει η εκπαίδευση του συστήματος αλλά και η αρχιτεκτονική των νευρωνικών δικτύων που εφαρμόστηκαν με καλύτερο να αποδεικνύεται το ΤΝΔ με το μεγαλύτερο πλήθος κρυφών στρωμάτων.

5.4.1 Προ-επεξεργασία δεδομένων

Η προ-επεξεργασία των δεδομένων αναφέρεται στον χειρισμό ή και την απόρριψη δεδομένων, πριν χρησιμοποιηθούν, προκειμένου να διασφαλιστεί υψηλή απόδοση του ΣΑΕ. Πιο συγκεκριμένα, δεδομένα που δεν έχουν υποστεί την απαραίτητη επεξεργασία μπορεί να παράγουν παραπλανητικά αποτελέσματα.

Η αναπαράσταση και η ποιότητα των δεδομένων είναι πρώτα και κύρια πριν από την εκτέλεση οποιασδήποτε ανάλυσης, αφού είναι η πιο σημαντική φάση ενός έργου μηχανικής μάθησης. Εάν υπάρξουν άσχετες και περιττές πληροφορίες ή θορυβώδη και αναξιόπιστα δεδομένα, τότε η ανακάλυψη γνώσης κατά τη φάση της εκπαίδευσης είναι πιο δύσκολη. Τα βήματα προετοιμασίας και φιλτραρίσματος δεδομένων μπορεί να απαιτήσουν σημαντικό χρόνο επεξεργασίας. Παραδείγματα προ-επεξεργασίας δεδομένων περιλαμβάνουν τον καθαρισμό, την επιλογή στιγμιότυπου, την κανονικοποίηση, μετασχηματισμό, εξαγωγή και επιλογή χαρακτηριστικών. Το προϊόν της προ-επεξεργασίας δεδομένων είναι το τελικό σετ εκπαίδευσης.

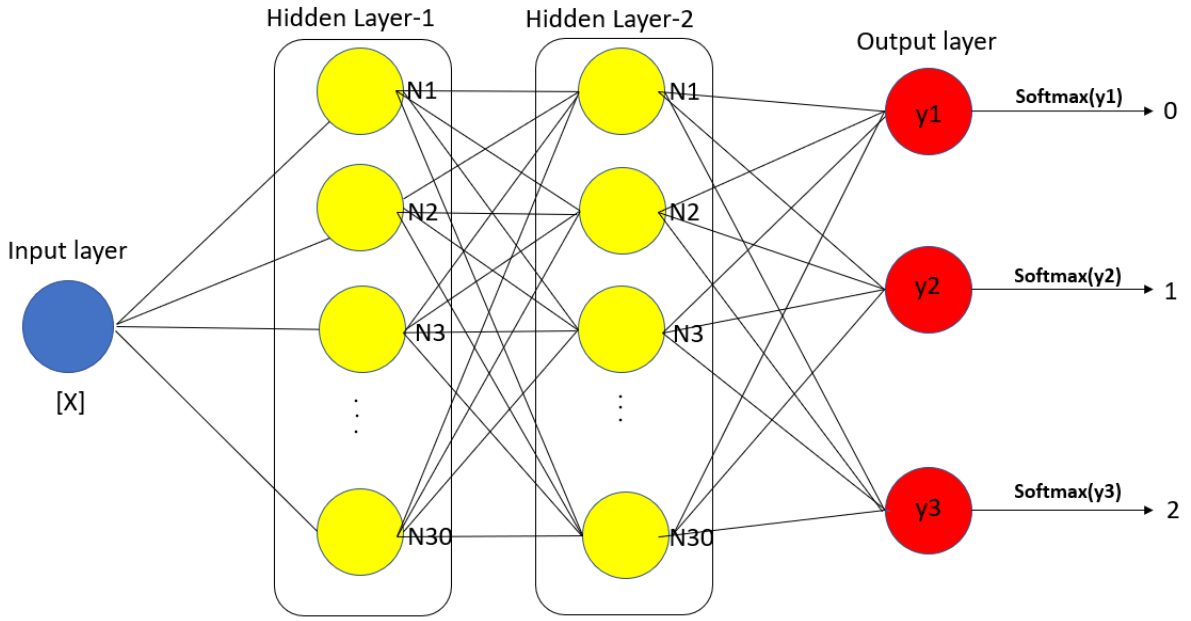
Στην παρούσα διπλωματική, πραγματοποιήθηκε επιλογή των χαρακτηριστικών από τις δικτυακές ροές, ενώ ταυτόχρονα διαγράφηκαν περιττές στήλες και συμπληρώθηκαν κενές γραμμές με τις τρεις κατηγορίες χαρακτηρισμού των δεδομένων. Στη συνέχεια έγινε χρήση δυο δημοφιλών τεχνικών, για την κλιμάκωση των δεδομένων πριν από την μοντελοποίηση, η κανονικοποίηση και η τυποποίηση. Ειδικότερα η κανονικοποίηση κλιμακώνει κάθε μεταβλητή εισόδου ξεχωριστά στο εύρος 0-1, ενώ η τυποποίηση κλιμακώνει κάθε μεταβλητή εισόδου ξεχωριστά αφαιρώντας τον μέσο όρο (που ονομάζεται κεντράρισμα) και διαιρώντας με την τυπική απόκλιση. Σκοπός της παραπάνω τεχνικής είναι η μετατόπιση της κατανομής, ώστε να έχει μέσο όρο μηδέν και τυπική απόκλιση ίση με ένα. Οι τεχνικές αυτές ονομάζονται MinMaxScaler και StandardScaler Transforms αντίστοιχα [66].

Μετά την ολοκλήρωση της προ-επεξεργασίας των δεδομένων ακολούθησε η εκπαίδευση (training) με την χρήση της εντολής train_test_split, όπου χωρίστηκε η βάση δεδομένων σε δύο σύνολα , το σύνολο εκπαίδευσης και το σύνολο δοκιμών με ποσοστά 70% και 30% αντίστοιχα.

Συνοψίζοντας στην μονάδα ανίχνευσης εισβολών του συστήματος πραγματοποιείται η προ-επεξεργασία των δεδομένων, η εκπαίδευσή τους και τελικά η εφαρμογή μοντέλων μηχανικής μάθησης για την εύρεση της ακρίβειας ανίχνευσης. Στην υπό-ενότητα που ακολουθεί παρουσιάζονται τα ΤΝΔ που εφαρμόστηκαν προκειμένου να ανιχνευθούν πιθανές εισβολές και ήταν τα πιο αποτελεσματικά σε σχέση με άλλες τεχνικές, με καλύτερο το ΤΝΔ με το μεγαλύτερο πλήθος κρυφών στρωμάτων.

5.4.2 Τεχνητό νευρωνικό δίκτυο με δύο κρυφά στρώματα

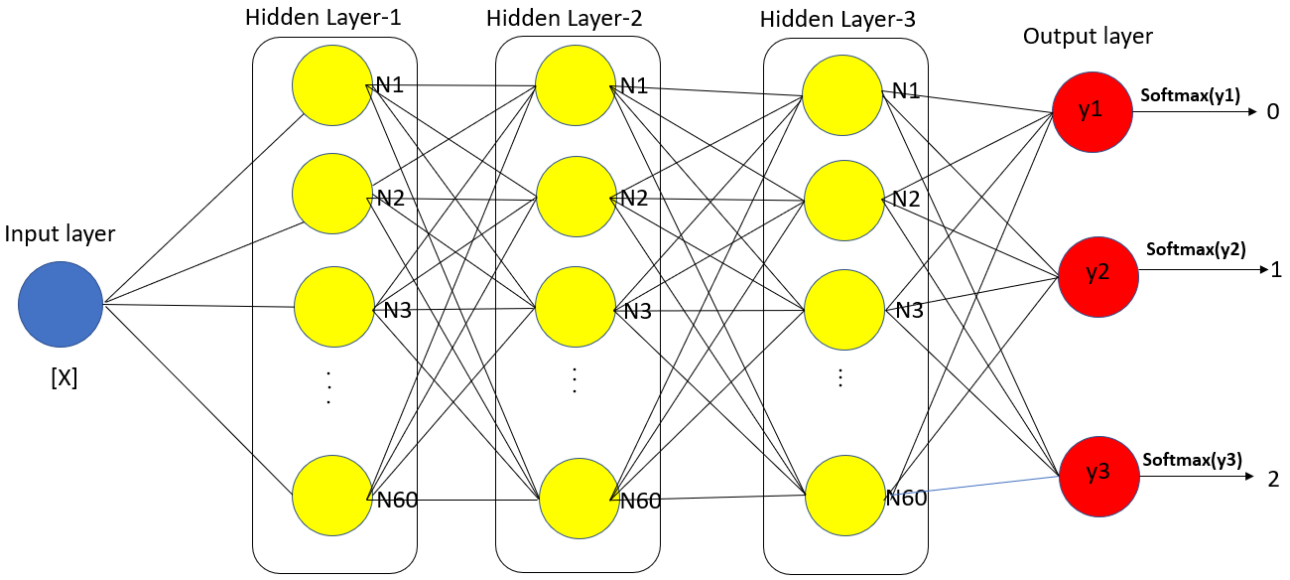
Η πρώτη περίπτωση ΤΝΔ που εφαρμόστηκε στην παρούσα διπλωματική ήταν το ΤΝΔ με δύο κρυφά στρώματα (hidden layers), ένα στρώμα εισόδου και τρία στρώματα εξόδου. Κάθε κρυφό στρώμα, περιείχε 30 κόμβους (nodes), ενώ σε κάθε έξοδο εφαρμόζεται συνάρτηση ενεργοποίησης SoftMax, υπεύθυνη για την ταξινόμηση των δεδομένων στις κατηγορίες 0,1,2 και πιο συγκεκριμένα σε Normal, Flood και RTSP Brute-Force επιθέσεις αντίστοιχα.



Σχήμα 2: ΤΝΔ με δύο κρυφά στρώματα

5.4.3 Τεχνητό νευρωνικό δίκτυο με τρία κρυφά στρώματα

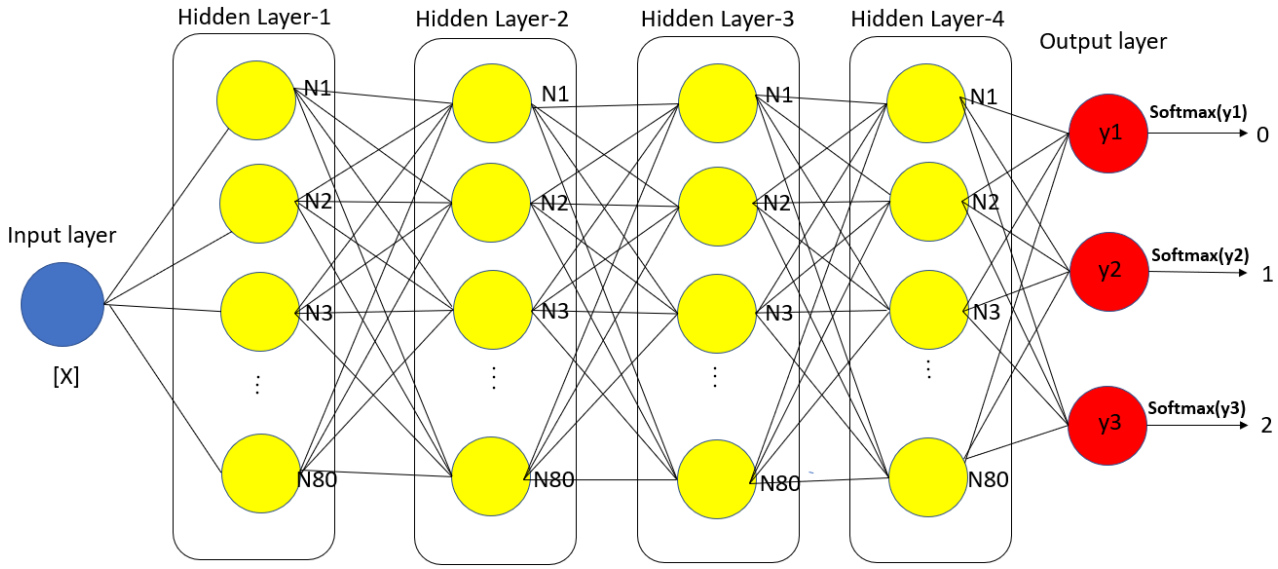
Έπειτα από την χρήση του ΤΝΔ με δύο κρυφά στρώματα, εφαρμόζεται ΤΝΔ με τρία κρυφά στρώματα. Το παραπάνω είχε παρόμοια αρχιτεκτονική με μόνη διαφορά τον αριθμό των κρυφών στρωμάτων, αλλά και των κόμβων αυτών.



*Σχήμα 3:*ΤΝΔ με τρία κρυφά στρώματα

5.4.4 Τεχνητό νευρωνικό δίκτυο με τέσσερα κρυφά στρώματα

Τελευταία περίπτωση των ΤΝΔ αποτελεί το ΤΝΔ με τέσσερα κρυφά στρώματα, όπου κάθε στρώμα περιέχει 80 κόμβους (nodes). Το συγκεκριμένο ΤΝΔ, παρουσίασε την μεγαλύτερη απόδοση σε σχέση με τα υπόλοιπα ΤΝΔ, αλλά και όλους τους αλγορίθμους-τεχνικές που εφαρμόστηκαν στην Μονάδα Ανίχνευσης Εισβολών.



Σχήμα 4: ΤΝΔ με τέσσερα κρυφά στρώματα

5.5 Μονάδα Ενημέρωσης Συμβάντων Ασφαλείας

Η Μονάδα Ενημέρωσης Συμβάντων Ασφαλείας αναλαμβάνει να ενημερώσει τον χρήστη σχετικά με διάφορα γεγονότα ασφαλείας. Ακόμα παρέχει στατιστικά γραφήματα, που βοηθούν τον χρήστη να κατανοήσει καλύτερα την κατάσταση ασφαλείας της υποδομής. Μέσω της έγκαιρης ενημέρωσης μπορούν οι χρήστες του συστήματος να αποφασίσουν για την πορεία των δικτυακών ροών που θεωρήθηκαν εισβολές.

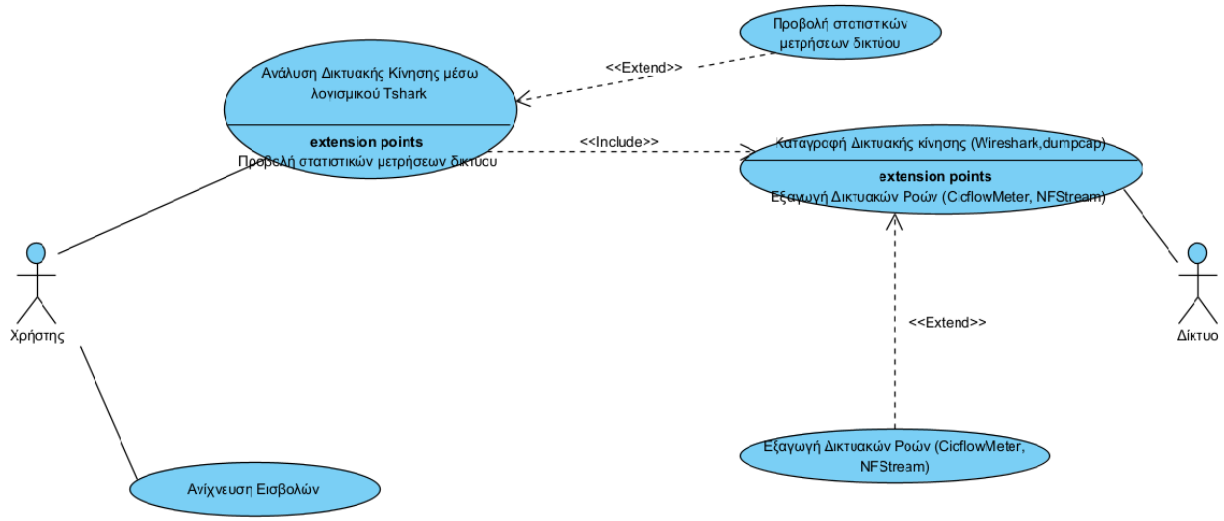
5.6 Περιγραφή Απαιτήσεων και Υλοποίηση Εφαρμογής

Στην ενότητα αυτή παρουσιάζονται το σκεπτικό με βάση το οποίο δημιουργήθηκε το προτεινόμενο σύστημα με την κατασκευή διαγραμμάτων, όπως περιπτώσεων χρήσης και δραστηριότητας . Ακόμα αναλύονται τα προγραμματιστικά εργαλεία με την βοήθεια των οποίων υλοποιήθηκε η εφαρμογή στην παρούσα διπλωματική.

5.6.1 Διάγραμμα Περιπτώσεων Χρήσης

Το διάγραμμα περιπτώσεων χρήσης περιγράφει τις λειτουργικές απαιτήσεις του συστήματος. Μία περίπτωση χρήσης είναι ένα σύνολο σεναρίων, που αποσκοπεί στην εκπλήρωση κάποιου στόχου του εκάστοτε χρήστη. Οι χρήστες ονομάζονται ερμηνευτές ή δρώντες και δεν είναι απαραίτητα άνθρωποι. Τέλος μία περίπτωση χρήσης μπορεί να περιλαμβάνει (include) ή να επεκτείνει μία άλλη (extend).

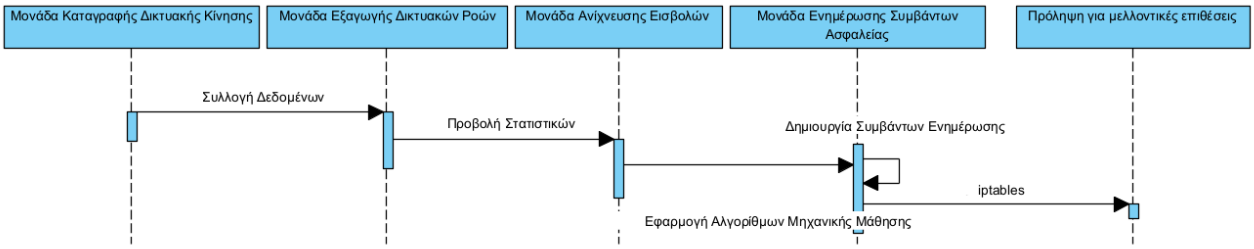
Το προτεινόμενο σύστημα αποτελείται από δύο οντότητες, τον χρήστη αλλά και το δίκτυο, ενώ οι περιπτώσεις χρήσεις που απεικονίζουν τις λειτουργίες που μπορεί να πραγματοποιήσει ο χρήστης, είναι η καταγραφή/ ανάλυση της δικτυακής κίνησης, αλλά και η ανίχνευση των εισβολών. Στο παρακάτω σχήμα απεικονίζεται ένα ενδεικτικό διάγραμμα περιπτώσεων χρήσης για το προτεινόμενο σύστημα.



Σχήμα 5:Διάγραμμα Περιπτώσεων Χρήσης προτεινόμενου συστήματος

5.6.2 Διάγραμμα Δραστηριοτήτων

Τα διαγράμματα δραστηριοτήτων αναπαριστούν την ροή εργασιών ενός συστήματος και απεικονίζουν την ακολουθία των δραστηριοτήτων που εκτελούνται παράλληλα ή σύμφωνα με τις συνθήκες που ικανοποιούνται. Στο παρακάτω σχήμα απεικονίζεται το διάγραμμα δραστηριότητας του ΣΑΠΕ της παρούσας διπλωματικής.



Σχήμα 6: Διάγραμμα Δραστηριοτήτων Συστήματος Ανίχνευσης και Πρόληψης Εισβολών

Στο παραπάνω σχήμα απεικονίζεται η ακολουθία των δραστηριοτήτων προκειμένου να επιτευχθεί ορθή ανίχνευση των εισβολών στο σύστημα, όπως αναφέρεται και σε προηγούμενες υπό-ενότητες. Ωστόσο, σε τελικό στάδιο μετά την Μονάδα Ενημέρωσης Συμβάντων Ασφαλείας υπάρχει η δραστηριότητα, που αφορά την πρόληψη για πιθανές μελλοντικές επιθέσεις.

Όσον αφορά την Πρόληψη, με βάση τα συμβάντα ασφαλείας που εξάγονται, εφαρμόζονται και αντίστοιχοι κανόνες συστήματος ασφαλείας, που υποδεικνύονται από το iptables. Το iptables είναι ένα τείχος προστασίας γραμμής εντολών Linux που επιτρέπει στους διαχειριστές συστήματος να διαχειρίζονται την εισερχόμενη και την εξερχόμενη κίνηση μέσω ενός συνόλου κανόνων/πίνακα με δυνατότητα διαμόρφωσης. Το Iptables χρησιμοποιεί ένα σύνολο πινάκων που έχουν αλυσίδες, που περιέχουν σύνολο ενσωματωμένων ή καθορισμένων κανόνων από το χρήστη. Με αυτόν τον τρόπο πραγματοποιείται η πρόληψη για πιθανές εισβολές.

5.6.3 Προγραμματιστικά εργαλεία

Η υλοποίηση του ΣΑΠΕ στο διαδίκτυο των πραγμάτων με τεχνικές βαθιάς μάθησης, βασίστηκε σε προγραμματιστικά εργαλεία και τεχνικές. Πιο συγκεκριμένα έγινε χρήση της γλώσσας Προγραμματισμού Python, αλλά και βασικών βιβλιοθηκών της όπως pandas, NumPy και Scikit-learn. Ακόμα έγινε χρήση λογισμικών ανάλυσης-καταγραφής-εξαγωγής δικτυακών ροών και ειδικότερα του CICFlowMeter και του NFStream.

Με την βοήθεια της Python και των βιβλιοθηκών της, υλοποιήθηκαν σχεδόν όλα τα στάδια της αρχιτεκτονικής του προτεινόμενου συστήματος, αφού πραγματοποιήθηκε η προ-επεξεργασία των δεδομένων, η εκπαίδευση τους, η εφαρμογή αλγορίθμων Μηχανικής Μάθησης αλλά και η αξιολόγηση των αποτελεσμάτων τους.

Όσον αφορά το CICFlowMeter είναι γεννήτρια ροής κυκλοφορίας δικτύου αρκετά αναλυτική, αφού εξάγει 84 χαρακτηριστικά κυκλοφορίας δικτύου. Διαβάζει το αρχείο pcap και δημιουργεί μια γραφική αναφορά των δυνατοτήτων που εξήχθησαν, ενώ λειτουργεί τόσο εντός όσο και εκτός σύνδεσης.

Αντίστοιχα το NFStream είναι ένα πλαίσιο ανοιχτού κώδικα που επιτρέπει υψηλή απόδοση στην ανάλυση της ροής κυκλοφορίας δικτύου. Εκτός από τον υπολογισμό στατιστικών στοιχείων ροής το NFStream μπορεί να καθορίσει τους τύπους εφαρμογών που δημιουργούν τις ροές. Σχεδιάστηκε για να λειτουργεί τόσο σε λειτουργίες ζωντανής όσο και εκτός σύνδεσης και έχει πληθώρα πλεονεκτημάτων, που αναλύθηκαν στην υπό -ενότητα 5.3.

Κεφάλαιο 6: Αποτελέσματα αξιολόγησης

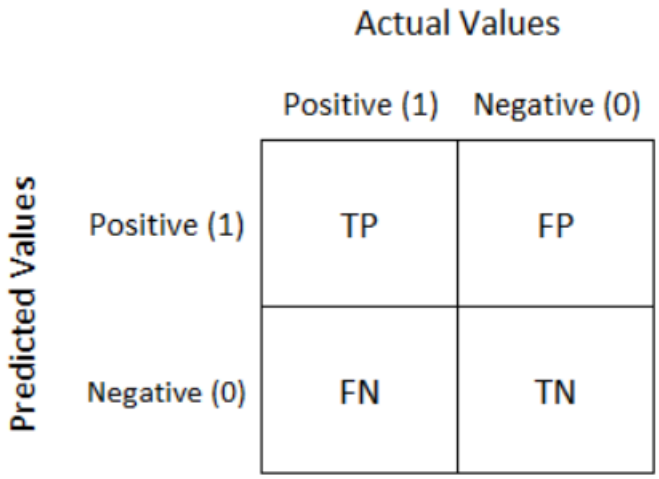
Στο παρόν κεφάλαιο γίνεται ανάλυση των μετρικών αξιολόγησης των αλγορίθμων μηχανικής μάθησης, περιγραφή του συνόλου δεδομένων και έπειτα παρουσιάζονται τα πειραματικά αποτελέσματα της ανίχνευσης εισβολών.

6.1 Μετρικές αξιολόγησης

Με το πέρας της δημιουργίας και της εκπαίδευσης του εκάστοτε μοντέλου μηχανικής μάθησης, κρίνεται απαραίτητη και η αξιολόγησή του, προκειμένου να εξαχθεί το ποσοστό των ορθών προβλέψεων.

Αρχικά γίνεται κατηγοριοποίηση των δεδομένων σε train και test set που έχουν την ίδια μορφή, αλλά δεν είναι ίδια, αφού παρατηρείται υπέρ-προσαρμογή ή αλλιώς overfitting. Πιο συγκεκριμένα, αν συμβεί overfitting, το μοντέλο αντί να εντοπίζει σχέσεις ανάμεσα στα δεδομένα απομνημονεύει αυτά που του δίνονται σαν είσοδος.

Τα δεδομένα που προκύπτουν μετά την εφαρμογή ενός μοντέλου μηχανικής μάθησης χρησιμοποιούνται για τον υπολογισμό μετρικών αξιολόγησης όπως η ακρίβεια, ορθότητα, F1-score και recall. Στην παρούσα διπλωματική πέρα από αυτές τις μετρικές έγινε χρήση και του πίνακα σύγχυσης (confusion matrix), που περιέχει συνοπτικά πολλές από αυτές.



Εικόνα 20:Confusion Matrix [67]

Στον παραπάνω πίνακα φαίνονται τέσσερις δυνατές εκβάσεις για δυαδική ταξινόμηση, που είναι απαραίτητες για τις εξισώσεις που αναλύονται παρακάτω:

- ***TP (True Positive):*** Περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως μη φυσιολογική κίνηση από τον κατηγοριοποιητή και είναι πράγματι έτσι.
- ***TN (True Negative):*** Περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως φυσιολογική κίνηση από τον κατηγοριοποιητή και είναι πράγματι έτσι .
- ***FP (False Positive):*** Περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως μη φυσιολογική κίνηση ,που στην πραγματικότητα είναι περιπτώσεις φυσιολογικής κίνησης.
- ***FN (False Negative):*** Περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως φυσιολογική κίνηση που στην πραγματικότητα είναι περιπτώσεις μη φυσιολογικής κίνησης .

Όπως αναφέρθηκε παραπάνω, οι εκβάσεις αυτές χρησιμοποιούνται για τον υπολογισμό των υπόλοιπων μετρικών [68] ως εξής:

6.6.1 Ακρίβεια

Ως ακρίβεια (accuracy) ορίζεται η αναλογία των προβλέψεων από τον ταξινομητή που ήταν ορθές. Πιο συγκεκριμένα σε ένα πρόβλημα ταξινόμησης δύο κατηγοριών ο τύπος της ακρίβειας είναι ο εξής:

$$\text{Ακρίβεια} = \frac{TP+TN}{TP+TN+FP+FN}$$

6.6.2 Ορθότητα

Ως ορθότητα (precision) ορίζεται μια πιθανότητα, που δείχνει αν η κατηγορία που έχει προβλέψει ο ταξινομητής για το νέο αντικείμενο ταυτίζεται με αυτή της πραγματικότητας.

$$\text{Ορθότητα p} = \frac{TP}{TP+FP} \text{ , Ορθότητα N} = \frac{TN}{TN+FN}$$

6.6.3 Ανάκληση

Ως ανάκληση (recall) ορίζεται μια δεσμευμένη πιθανότητα, που δείχνει αν ένα στιγμιότυπο ανήκει σε μία κλάση, έστω c, και έπειτα αυτή αναγνωριστεί σωστά από τον ταξινομητή:

$$\text{Ανάκληση p} = \frac{TP}{TP+FN} \text{ , Ανάκληση N} = \frac{TN}{TN+FP}$$

6.6.4 F1-score

Οι παραπάνω δύο μετρικές δεν είναι δυνατόν να εκτιμηθούν η καθεμία μόνη της, αφού δημιουργούν μια ολοκληρωμένη εικόνα για τον ταξινομητή. Μια μετρική που συνδυάζει τις άλλες δύο είναι και το μέτρο F, που δίνεται από τον παρακάτω τύπο:

$$\text{F1-score} = \frac{2x\ Ορθότητα\ cx\ Ανάκληση\ c}{Ορθότητα\ c + Ανάκληση\ c}$$

6.2 Περιγραφή συνόλου δεδομένων

Το σύνολο δεδομένων που χρησιμοποιήθηκε για την υλοποίηση του ΣΑΕ [69] είναι ανεπτυγμένο από το Πανεπιστήμιο του Brunswick στον Καναδά και ονομάζεται CIC IoT Dataset 2022.

Αυτό το έργο στοχεύει να δημιουργήσει ένα σύνολο δεδομένων τελευταίας τεχνολογίας για δημιουργία προφίλ, ανάλυση συμπεριφοράς και δοκιμές ευπάθειας διαφορετικών συσκευών IoT με διαφορετικά πρωτόκολλα όπως το IEEE 802.11, το Zigbee-based και το Z-Wave. Τα ακόλουθα επεξηγούν τους κύριους στόχους του έργου δεδομένων CIC-IoT:

1. Διαμόρφωση διαφόρων συσκευών IoT και ανάλυση της συμπεριφοράς που εμφανίζεται.
2. Διεξαγωγή χειροκίνητων και ημιαυτόματων πειραμάτων διαφόρων κατηγοριών.
3. Ανάλυση κίνησης δικτύου όταν οι συσκευές είναι σε αδράνεια για τρία λεπτά και όταν είναι ενεργοποιημένες για τα δύο πρώτα λεπτά.
4. Δημιουργία διαφορετικών σεναρίων και ανάλυση της συμπεριφοράς των συσκευών σε διαφορετικές καταστάσεις.
5. Διεξαγωγή και καταγραφή του δικτύου των συσκευών υπό ρεύμα και σημαντικών επιθέσεων σε περιβάλλον IoT.

Για την σύνθεση της βάσης δεδομένων συλλέχθηκαν δεδομένα από την καταγραφή της κίνησης δικτύου των συσκευών IoT, χρησιμοποιώντας Wireshark και dumpcap σε έξι διαφορετικούς τύπους πειραμάτων. Τα παραπάνω πειράματα κατηγοριοποιούνται ως εξής:

- ***Ισχύς*:** Σε αυτό το πείραμα ενεργοποιήθηκαν όλες οι συσκευές στο εργαστήριο ξεχωριστά και ξεκίνησε μεμονωμένα η καταγραφή της κυκλοφορίας δικτύου.
- ***Αδράνεια***: Σε αυτό το πείραμα καταγράφηκε ολόκληρη η κίνηση του δικτύου από αργά το βράδυ έως νωρίς το πρωί. Σε αυτή την περίοδο ολόκληρο το εργαστήριο εκκενώθηκε πλήρως και δεν υπήρξαν ανθρώπινες αλληλεπιδράσεις.
- ***Αλληλεπιδράσεις:*** Σε αυτό το πείραμα, όλες οι πιθανές λειτουργίες σε συσκευές IoT έχουν εξαχθεί και η αντίστοιχη δραστηριότητα δικτύου και τα μεταδιδόμενα πακέτα για κάθε λειτουργικότητα/δραστηριότητα έχουν καταγραφεί.
- ***Σενάρια:*** Σε αυτά τα πειράματα, πραγματοποιήθηκαν έξι διαφορετικοί τύποι πειραμάτων σεναρίων χρησιμοποιώντας έναν συνδυασμό συσκευών ως προσομοιώσεις της δραστηριότητας δικτύου μέσα σε ένα έξυπνο σπίτι.
- ***Ενεργό***: Εκτός από το χρόνο αδράνειας, καταγράφηκαν όλες οι επικοινωνίες δικτύου καθ' όλη τη διάρκεια της ημέρας. Σε όλους τους ερευνητές κατά τη διάρκεια αυτής της περιόδου

επετράπη να εισέλθουν στο εργαστήριο όποτε ήθελαν. Μπορούσαν να αλληλοεπιδρούν με συσκευές και να δημιουργούν κίνηση δικτύου είτε παθητικά είτε ενεργά.

- ***Επιθέσεις:*** Σε αυτό το πείραμα, πραγματοποιήθηκαν δύο διαφορετικές επιθέσεις, οι Flood και RTSP- Brute Force σε ορισμένες από τις συσκευές και καταγράφηκε η κυκλοφορία του δικτύου επίθεσης.

Από τα παραπάνω πειράματα δημιουργήθηκε και η τελική βάση δεδομένων που χρησιμοποιήθηκε για την υλοποίηση του ΣΑΕ.

6.3 Πειραματικά αποτελέσματα

Στην παρούσα υπό-ενότητα παρουσιάζονται τα πειραματικά αποτελέσματα της εφαρμογής των αλγορίθμων μηχανικής μάθησης. Ειδικότερα παρατίθενται δύο αναλυτικοί πίνακες με τα δεδομένα όλων των αλγορίθμων τόσο για το CICFlowMeter, όσο και για το NFStream και στην συνέχεια όλοι οι confusion matrixes με την ορθότητα των αποτελεσμάτων που εξήχθησαν από κάθε μέθοδο. Τέλος παρουσιάζονται διαγράμματα με τις αποδόσεις όλων των αλγορίθμων.

6.3.1 CICFlowMeter

Στον πίνακα που ακολουθεί παρουσιάζονται τα συγκεντρωτικά αποτελέσματα της εφαρμογής όλων των αλγορίθμων στη βάση δεδομένων που διαμορφώθηκε με το λογισμικό του CICFlowMeter.

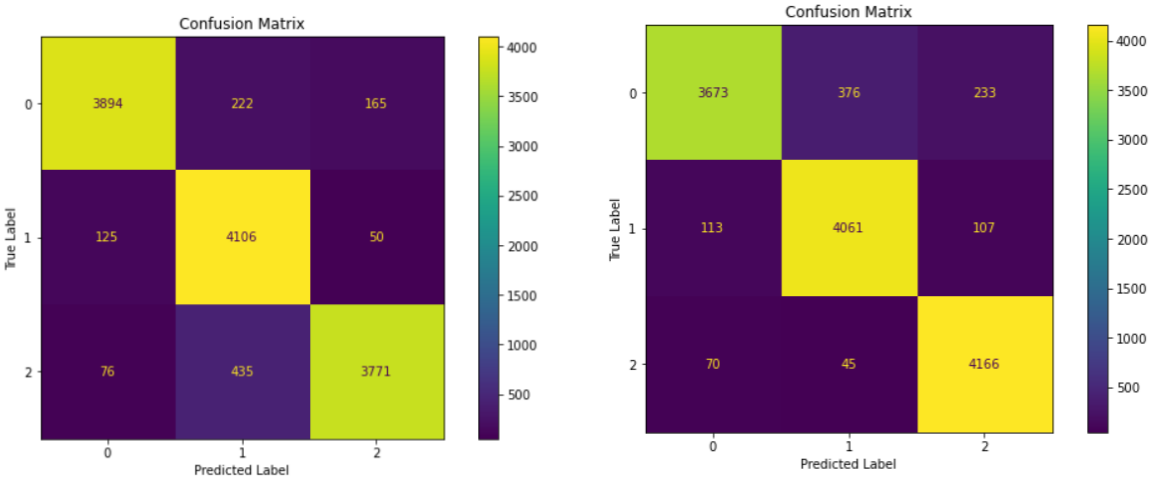
Πίνακας 2:Πειραματικά αποτελέσματα εφαρμογής αλγορίθμων- CICFlowMeter

Model	ACC	Precision	TPR	FPR	F1-Score
DNN-1	0.92	0.92	0.916	0.041	0.919
DNN-2	0.98	0.98	0.987	0.006	0.98
DNN-3 *[1]	0.998	0.998	0.997	0.001	0.997
Decision Tree *	0.997	0.997	0.997	0.001	0.997
k-NN	0.969	0.969	0.968	0.015	0.969
Random Forest *	0.994	0.994	0.994	0.002	0.994
Naïve Bayes *[2]	0.812	0.843	0.811	0.094	0.812
SVM-Linear	0.964	0.964	0.964	0.017	0.964
SVM-RBF	0.966	0.966	0.966	0.016	0.966
SVM-Sigmoid	0.82	0.82	0.819	0.09	0.82
Logistic Regression	0.937	0.938	0.929	0.035	0.938
AdaBoost	0.911	0.916	0.91	0.04	0.911
LDA	0.874	0.885	0.89	0.05	0.875
SGD	0.938	0.939	0.938	0.03	0.938

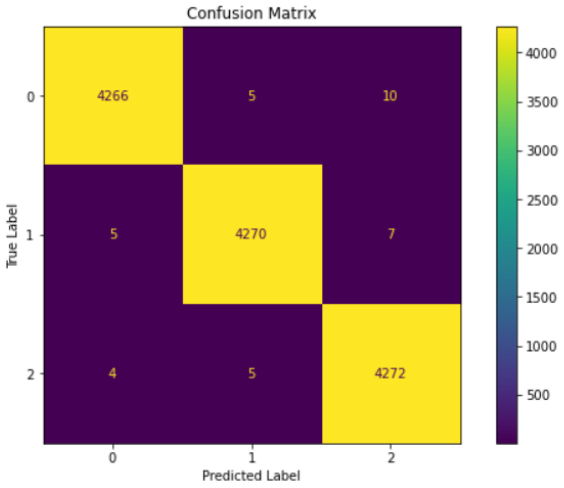
[1] Ο κόκκινος αστερίσκος, συμβολίζει τους αλγορίθμους με τα υψηλότερα ποσοστά ακρίβειας
[2] Ο μαύρος αστερίσκος συμβολίζει τον αλγόριθμο με τα χαμηλότερα ποσοστά ακρίβειας

Στη συνέχεια, όπως αναφέρθηκε, παραθέτονται οι confusion matrixes των αλγορίθμων που επιδεικνύουν την ορθότητα των αποτελεσμάτων, ξεκινώντας από τις τρεις περιπτώσεις των DNN.

Πίνακας 3: Confusion matrix DNN-1 / DNN-2



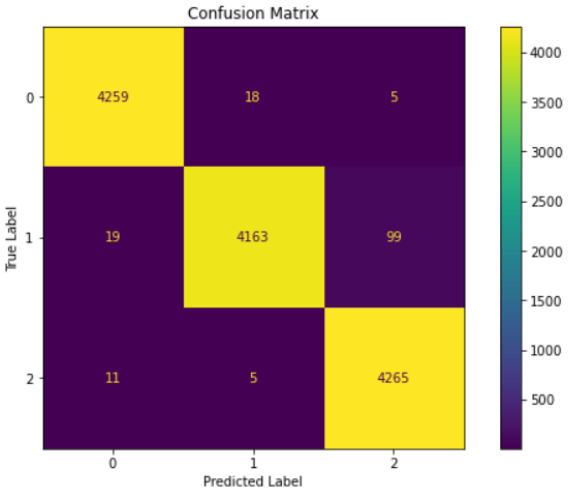
Πίνακας 4:Confusion matrix DNN-3



Από τους παραπάνω πίνακες, φαίνεται πως την καλύτερη ταξινόμηση σε 0 (Normal) , 1 (Flood) και 2 (RTSP-Brute Force), πραγματοποιεί το βαθύ νευρωνικό δίκτυο 3, αφού διαθέτει τα περισσότερα κρυφά στρώματα. Η διαγώνιος του Πίνακα 4 έχει πολύ μεγάλα νούμερα, ενώ τα υπόλοιπα «κουτάκια» μικρά. Επομένως, ο αλγόριθμος προβλέπει σε πολύ μεγάλο ποσοστό, ορθά .

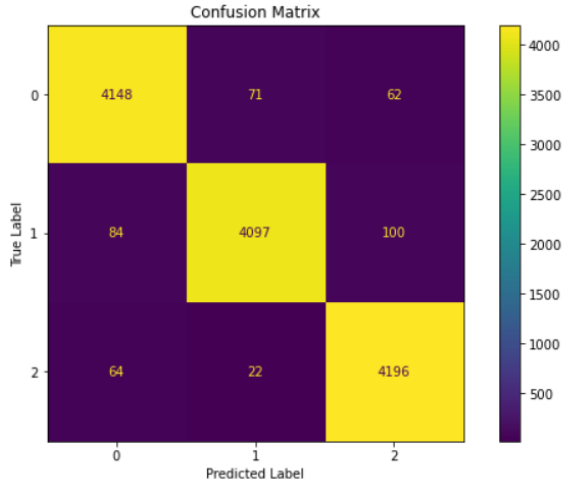
Έπειτα ακολουθούν οι confusion matrixes των αλγορίθμων Decision Tree, k-NN και Random Forest.

Πίνακας 5:Confusion matrix -Decision Tree



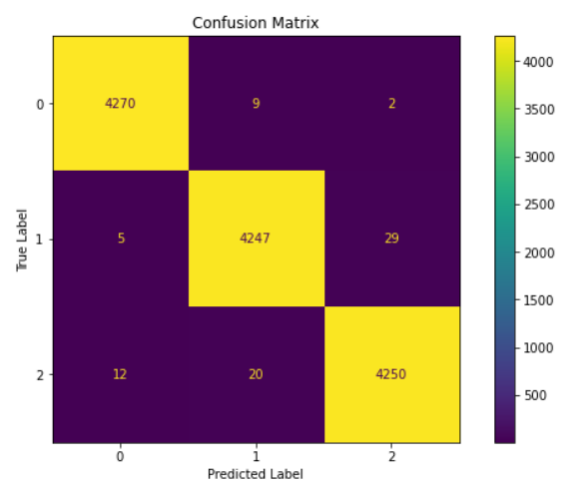
Η ταξινόμηση του αλγορίθμου Decision Tree, είναι μερικώς ικανοποιητική. Παρατηρείται μεγάλος αριθμός λανθασμένων ταξινομήσεων στην περίπτωση που οι επιθέσεις στο σύστημα ανήκαν στην κατηγορία Flood .Ο αλγόριθμος, 99 περιπτώσεις που ανήκαν στην κατηγορία Flood , τις ταξινόμησε στην κατηγορία του RTSP-Brute Force.

Πίνακας 6:Confusion matrix -k-NN



Ο αλγόριθμος k-NN είναι αρκετά αποδοτικός . Ωστόσο παρατηρείται μεγάλος αριθμός λανθασμένων ταξινομήσεων στην περίπτωση που οι επιθέσεις στο σύστημα ήταν επιθέσεις πλημμύρας. Ο αλγόριθμος τις ταξινόμησε στην κατηγορία των επιθέσεων RTSP-Brute Force.

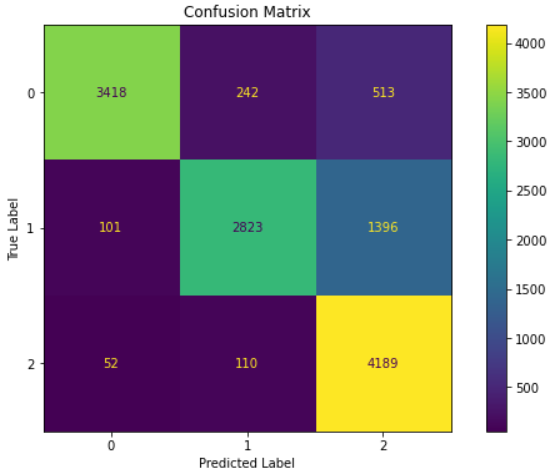
Πίνακας 7:Confusion matrix-Random Forest



Ο αλγόριθμος Random Forest παρουσιάζει σχεδόν άριστα αποτελέσματα στην ταξινόμηση των δεδομένων . Πιο συγκεκριμένα, από τον πίνακα σύγχυσης φαίνεται πως η ταξινόμηση στις τρεις κλάσεις 0, 1 και 2 είναι σχεδόν άριστη με ελάχιστα σφάλματα.

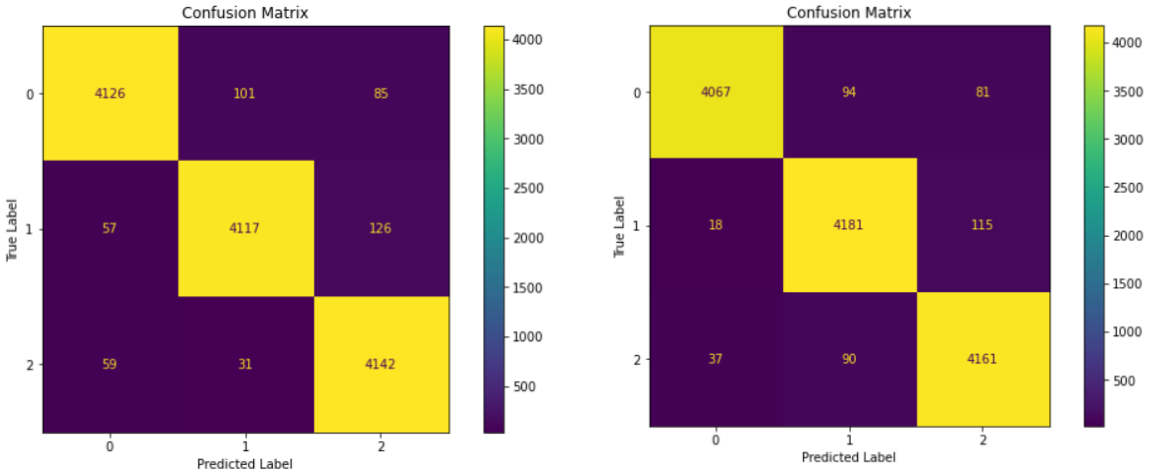
Παρακάτω δίδονται οι confusion matrixes του αλγορίθμου Naïve Bayes αλλά και των τριών περιπτώσεων SVM.

Πίνακας 8:Confusion matrix -Naïve Bayes

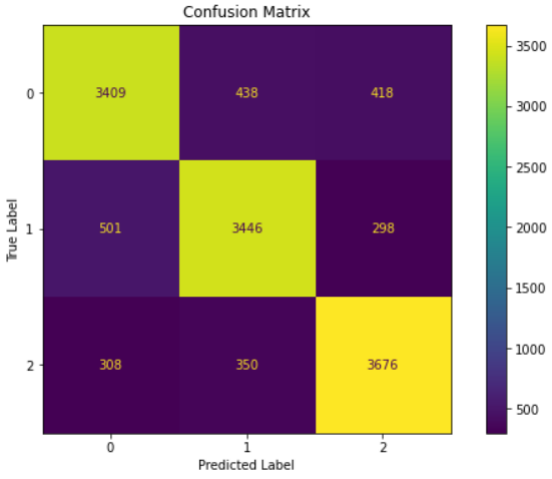


Η ταξινόμηση που πραγματοποιεί ο Naïve Bayes στις κλάσεις 0, 1 και 2 είναι λανθασμένη σε μεγάλο ποσοστό ειδικά στις κατηγορίες 0 και 1. Εξαιτίας αυτού, ο αλγόριθμος παρουσιάζει και την μικρότερη ακρίβεια.

Πίνακας 9:Confusion matrix SVM-Linear – SVM-RBF



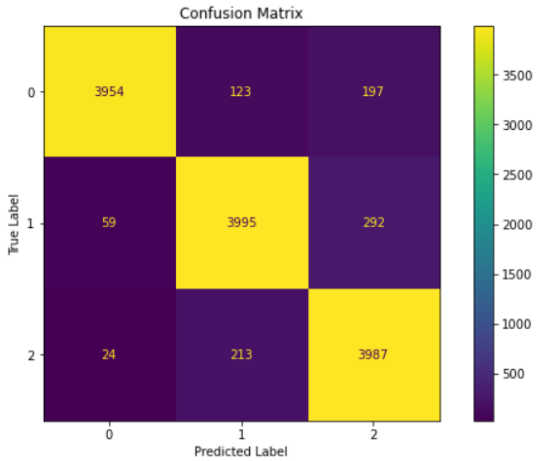
Πίνακας 10:SVM Sigmoid



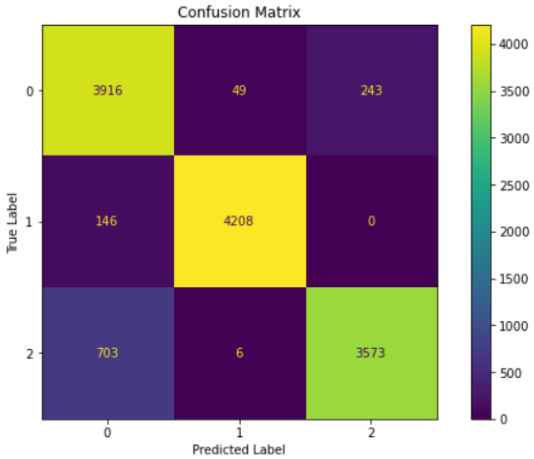
Από τους παραπάνω confusion matrixes, πιο αποτελεσματικός ήταν ο SVM με kernel RBF, αφού πραγματοποιεί τις λιγότερες λανθασμένες ταξινομήσεις σε σχέση με τις άλλες περιπτώσεις.

Τέλος ακολουθούν οι confusion matrixes των αλγορίθμων Logistic Regression, AdaBoost, LDA και SGD.

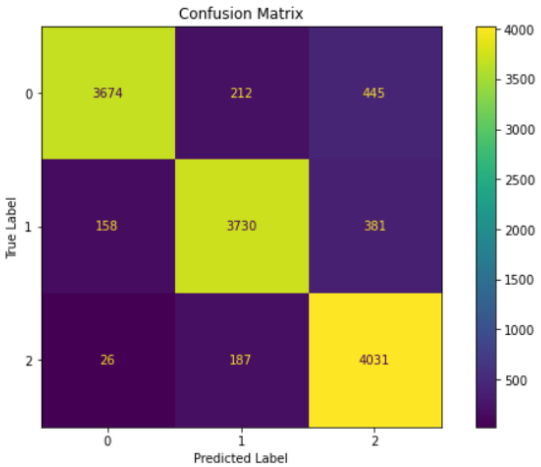
Πίνακας 11:Confusion matrix-Logistic Regression



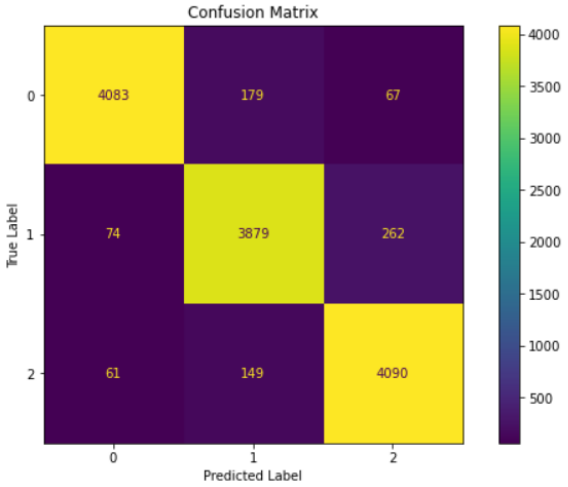
Πίνακας 12:Confusion matrix -AdaBoost



Πίνακας 13:Confusion matrix -LDA

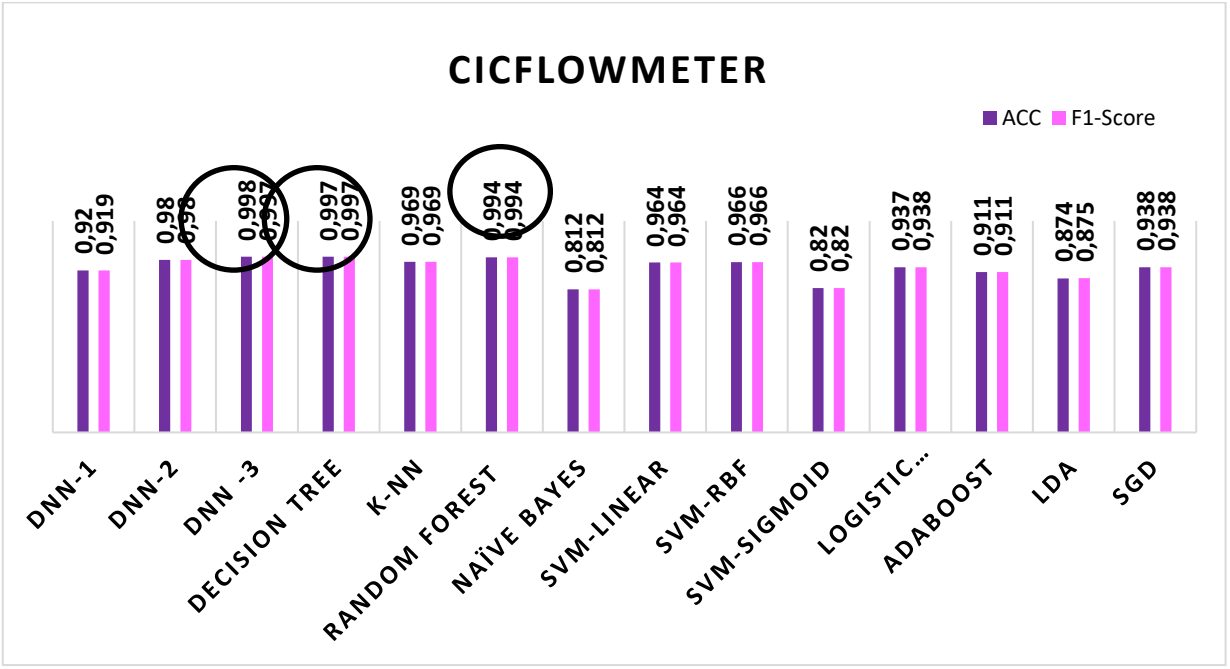


Πίνακας 14:Confusion matrix-SGD



Από τα παραπάνω φαίνεται πως ο αλγόριθμος LDA είναι ο λιγότερο αποδοτικός στην ταξινόμηση σε σχέση με τους υπόλοιπους, αφού παρουσιάζει μεγάλο ποσοστό λανθασμένων ταξινομήσεων και στις τρεις κατηγορίες ταξινόμησης.

Συμπερασματικά, από τον Πίνακα 2 και όλους τους confusion matrixes που παρουσιάστηκαν, οι καλύτεροι αλγόριθμοι όσον αφορά την ακρίβεια, το F1-score και ποσοστό ορθών και λανθασμένων προβλέψεων ήταν ο DNN με τέσσερα κρυφά στρώματα, με ποσοστό ακρίβειας και F1-score 99,8%, ο Decision Tree με 99,7% και ο Random Forest με 99,4%. Αντίθετα τα μικρότερα ποσοστά παρουσίασε ο αλγόριθμος Naïve Bayes, αφού η ακρίβεια του άγγιζε το 81.2%. Ακολούθως, παρατίθεται συγκεντρωτικό διάγραμμα αποδόσεων των παραπάνω αλγορίθμων μηχανικής μάθησης, όπου φαίνονται κυκλωμένοι οι αλγόριθμοι με τις μεγαλύτερες αποδόσεις.



Σχήμα 7:Συγκεντρωτικό διάγραμμα αποδόσεων αλγορίθμων μηχανικής μάθησης με CICFlowMeter

6.3.2 NFStream

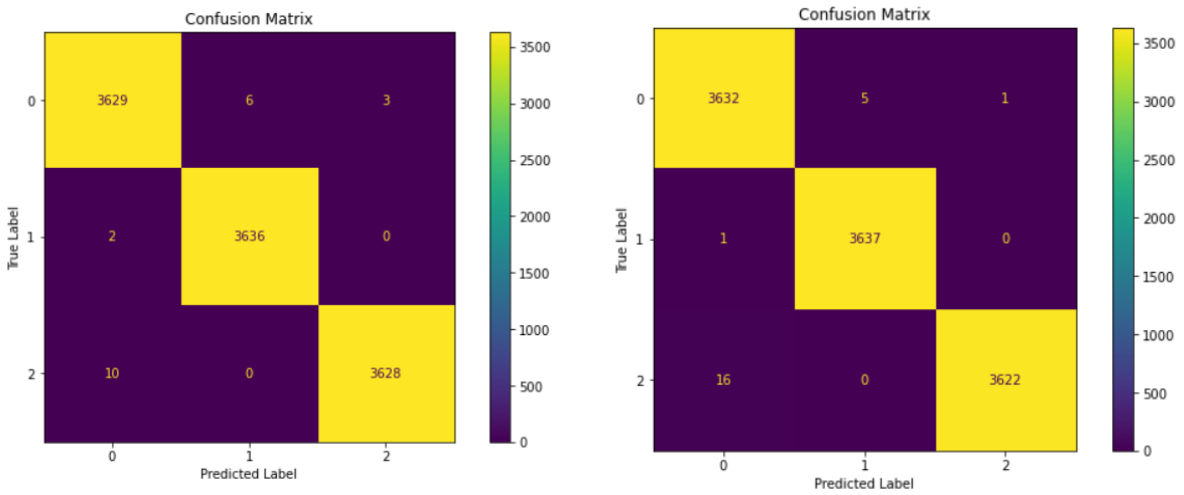
Στον πίνακα που ακολουθεί παρουσιάζονται τα συγκεντρωτικά αποτελέσματα της εφαρμογής όλων των αλγορίθμων στη βάση δεδομένων που διαμορφώθηκε με το λογισμικό του NFStream.

Πίνακας 15:Συγκεντρωτικός πίνακας αποτελεσμάτων αλγορίθμων -NFStream

Model	ACC	Precision	TPR	FPR	F1-Score
DNN-1	0.998	0.998	0.998	0.0008	0.998
DNN-2 *	0.998	0.998	0.997	0.01	0.998
DNN-3 *[3]	0.999	0.999	0.999	0.001	0.999
Decision Tree	0.972	0.974	0.972	0.013	0.972
k-NN *	0.997	0.997	0.997	0.012	0.997
Random Forest *	0.998	0.998	0.998	0.01	0.998
Naïve Bayes	0.935	0.936	0.934	0.032	0.935
SVM-Linear	0.932	0.932	0.931	0.034	0.932
SVM-RBF	0.983	0.983	0.983	0.008	0.983
SVM-Sigmoid *[4]	0.8	0.8	0.798	0.1	0.8
Logistic Regression	0.897	0.897	0.897	0.05	0.897
AdaBoost	0.891	0.898	0.889	0.05	0.897
LDA	0.867	0.867	0.866	0.06	0.867
SGD	0.872	0.872	0.871	0.064	0.872

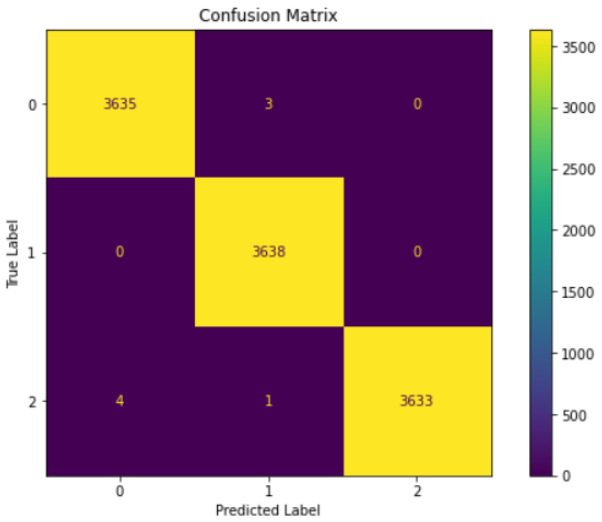
Στη συνέχεια παρουσιάζονται οι confusion matrixes όλων των μεθόδων που χρησιμοποιήθηκαν για την υλοποίηση του ΣΑΕ , ξεκινώντας από τις τρεις περιπτώσεις των DNN.

Πίνακας 16:Confusion matrix DNN1 / DNN2



[3] Ο κόκκινος αστερίσκος, συμβολίζει τους αλγορίθμους με τα υψηλότερα ποσοστά ακρίβειας
[4] Ο μαύρος αστερίσκος συμβολίζει τον αλγόριθμο με τα χαμηλότερα ποσοστά ακρίβειας

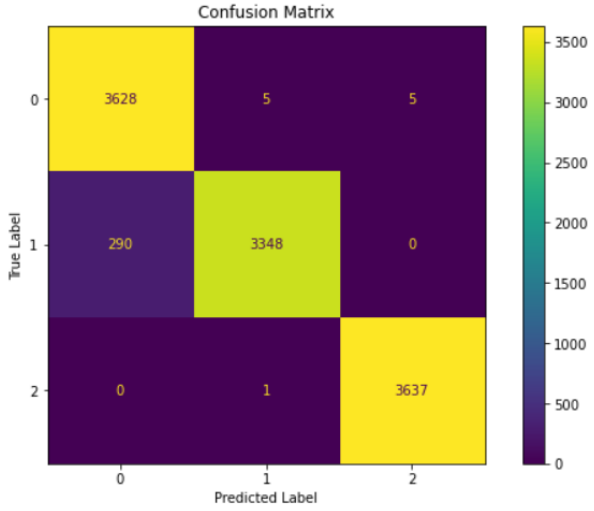
Πίνακας 17:Confusion matrix DNN-3



Από τους παραπάνω πίνακες , είναι φανερό πως και οι τρεις περιπτώσεις DNN είναι αρκετά αποτελεσματικές. Ωστόσο, την καλύτερη ταξινόμηση πραγματοποιεί το μοντέλο DNN-3, αφού έχει το μικρότερο ποσοστό λανθασμένων ταξινομήσεων και την μεγαλύτερη ακρίβεια.

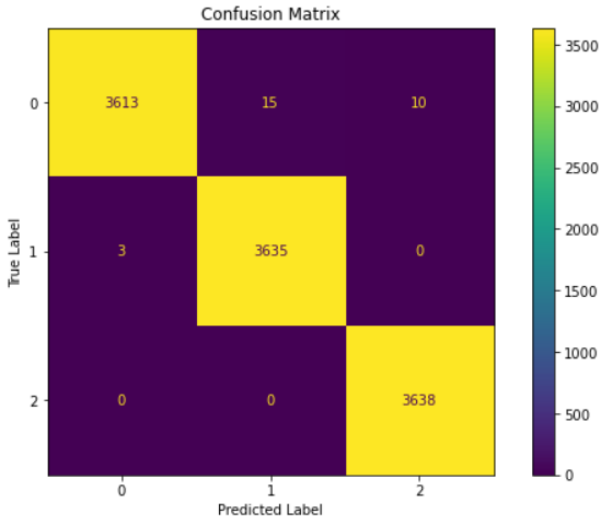
Έπειτα ακολουθούν οι confusion matrixes των αλγορίθμων Decision Tree, k-NN και Random Forest.

Πίνακας 18:Confusion matrix Decision Tree



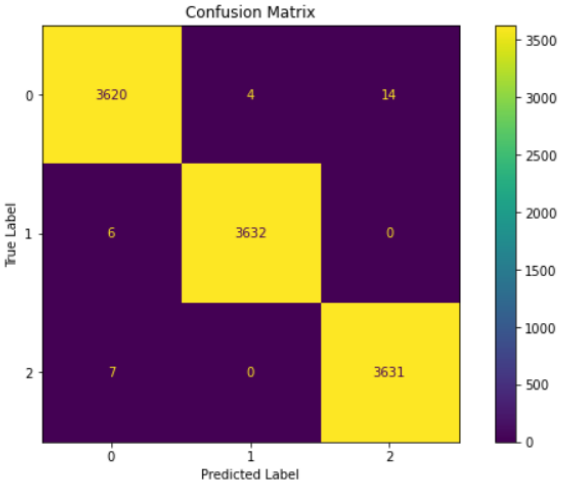
Ο αλγόριθμος Decision Tree, παρουσιάζει υψηλή αποδοτικότητα ταξινόμησης δεδομένων σε κλάσεις, με ένα μικρό πρόβλημα στην ταξινόμηση αυτών που ανήκουν στην κλάση 1. Σε αυτήν την περίπτωση ο αλγόριθμος τα ταξινομεί στην κλάση 0.

Πίνακας 19:Confusion matrix k-NN



Ο αλγόριθμος k-NN, παρουσιάζει υψηλή αποδοτικότητα ταξινόμησης δεδομένων σε κλάσεις, με πολύ μικρό ποσοστό λανθασμένων ταξινομήσεων

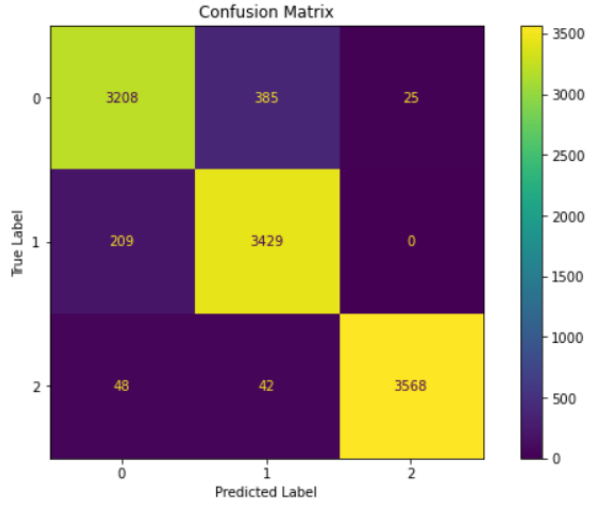
Πίνακας 20:Confusion matrix Random Forest



Ο αλγόριθμος Random Forest, ανήκει στους αλγορίθμους, όπου παρουσιάζει μεγάλη αποδοτικότητα ταξινόμησης , αφού ο αριθμός των σφαλμάτων είναι σχεδόν αμελητέος.

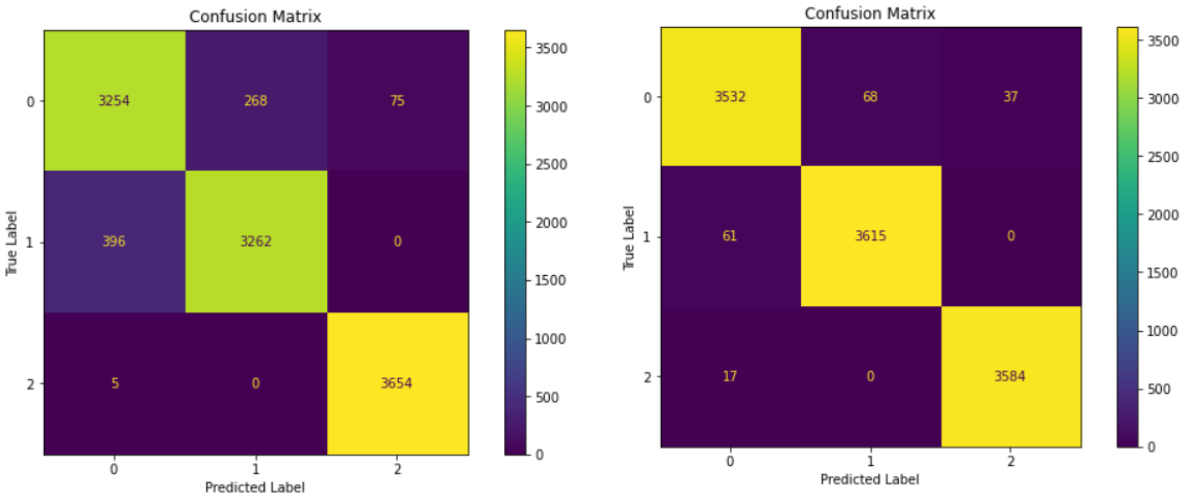
Ακολουθούν οι confusion matrixes των αλγορίθμων Naïve Byes και των τριών περιπτώσεων SVM.

Πίνακας 21:Confusion matrix Naive Bayes

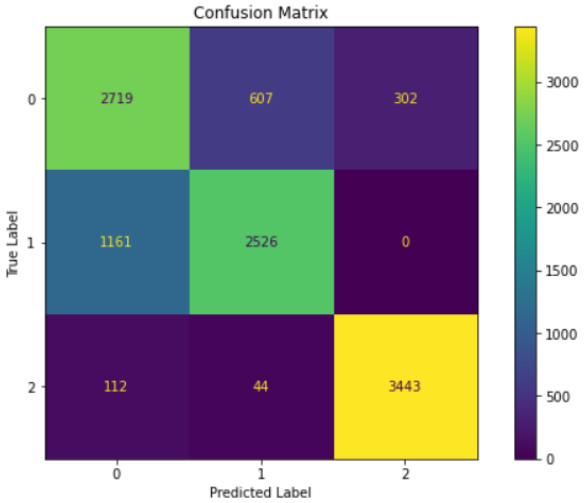


Ο αλγόριθμος Naïve Bayes παρουσιάζει καλή αποδοτικότητα ταξινόμησης . Ωστόσο, ειδικά στις κατηγορίες 0 και 1 ο αριθμός λανθασμένων ταξινομήσεων δεν θεωρείται αμελητέος.

Πίνακας 22:Confusion matrix SVM-Linear/ RBF



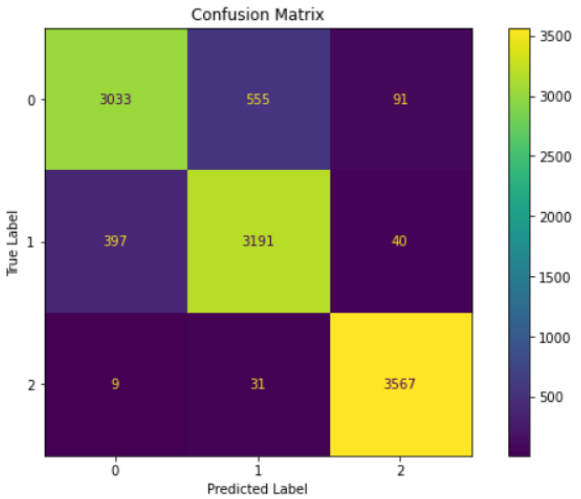
Πίνακας 23:Confusion matrix SVM-Sigmoid



Από τους παραπάνω πίνακες διαπιστώνουμε πως καλύτερη απόδοση έχει ο SVM με kernel RBF, αφού ταξινομεί σχεδόν ολόσωστα τα δεδομένα. Αντίθετα ο SVM με kernel Sigmoid , παρουσιάζει μεγάλο αριθμό σφαλμάτων ταξινόμησης .

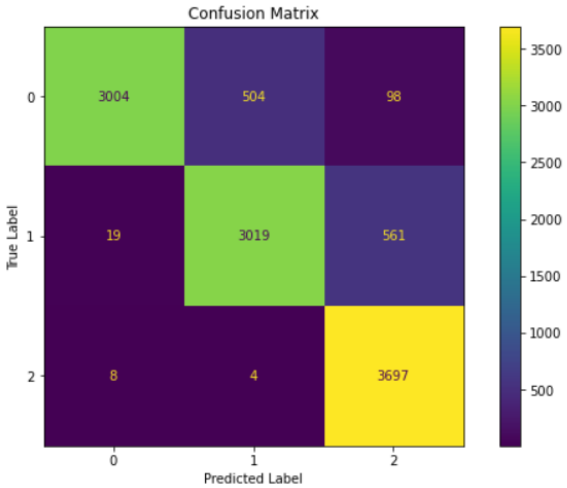
Έπειτα , ακολουθούν οι confusion matrixes των αλγορίθμων Logistic Regression, AdaBoost, LDA και SGD.

Πίνακας 24:Confusion matrix Logistic Regression



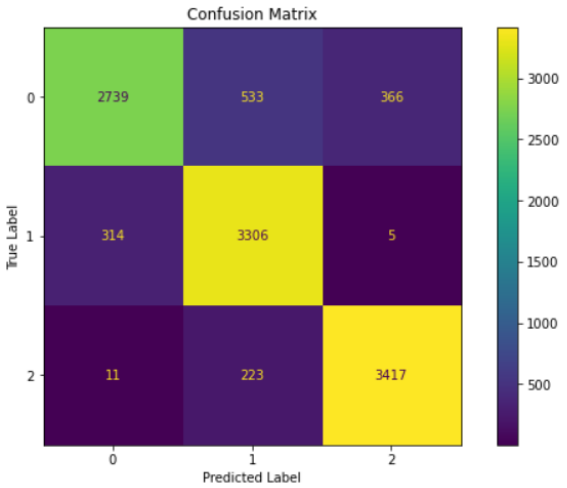
Ο αλγόριθμος Logistic Regression παρουσιάζει ποσοστό σφαλμάτων ειδικά στην 0 και 1 κατηγορία, γεγονός που τον καθιστά όχι και τόσο αποδοτικό σε σχέση με τους υπολοίπους.

Πίνακας 25:Confusion matrix AdaBoost

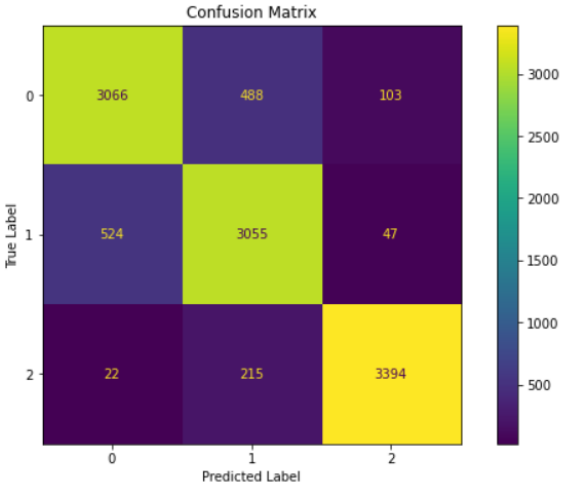


Ο αλγόριθμος AdaBoost παρουσιάζει ποσοστό λανθασμένων ταξινομήσεων ειδικά στην 0 και 1 κλάση με αποτέλεσμα να μην είναι τόσο ακριβής στις προβλέψεις του.

Πίνακας 26:Confusion matrix LDA

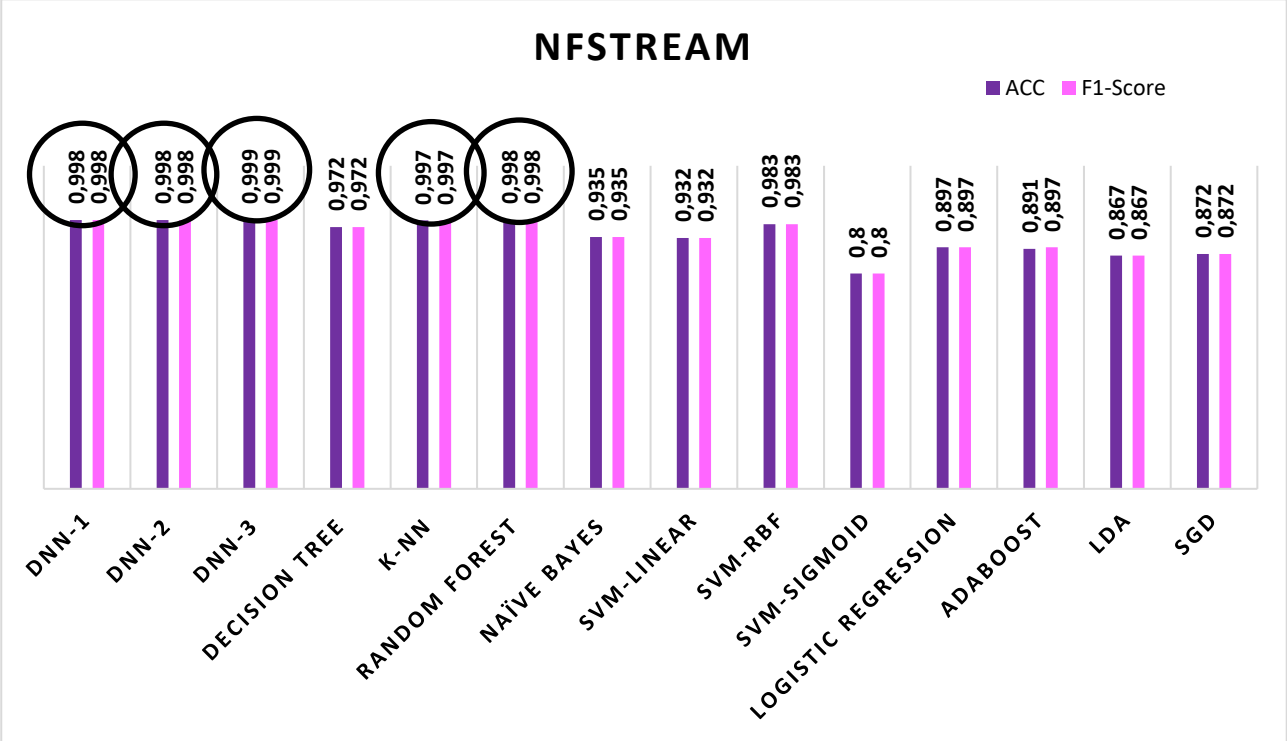


Ο αλγόριθμος LDA παρουσιάζει υψηλό αριθμό λανθασμένων ταξινομήσεων και στις 3 κλάσεις με αποτέλεσμα η ταξινόμηση να μην είναι σωστή σε όλες τις περιπτώσεις.



Ο αλγόριθμος SGD παρουσιάζει υψηλό αριθμό λανθασμένων ταξινομήσεων όπως και οι 3 προηγούμενοι αλγόριθμοι.

Συμπερασματικά, από τον Πίνακα 15 και όλους τους confusion matrixes που παρουσιάστηκαν, οι καλύτεροι αλγόριθμοι όσον αφορά την ακρίβεια, το F1-score και ποσοστό ορθών και λανθασμένων προβλέψεων ήταν όλες οι περιπτώσεις DNN με καλύτερη την τελευταία, αφού παρουσιάζει ακρίβεια και F1-score σε ποσοστό 99,9%. Ακόμα υψηλά ποσοστά ακρίβειας και F1-score παρουσίασαν οι αλγόριθμοι k-NN και Random Forest με ποσοστά 99,7% και 99,8% αντίστοιχα. Αντίθετα τα μικρότερα ποσοστά παρουσίασε ο αλγόριθμος SVM με kernel Sigmoid, αφού η ακρίβεια του άγγιζε το 80%. Ακολούθως, παρατίθεται συγκεντρωτικό διάγραμμα αποδόσεων των παραπάνω αλγορίθμων μηχανικής μάθησης, όπου φαίνονται κυκλωμένοι οι αλγόριθμοι με τις μεγαλύτερες αποδόσεις.



Σχήμα 8: Συγκεντρωτικό διάγραμμα αποδόσεων αλγορίθμων μηχανικής μάθησης με NFStream

Κεφάλαιο 7: Συμπεράσματα και μελλοντικές επεκτάσεις

7.1 Συμπεράσματα της μελέτης

Η αξιοποίηση των κλάδων της πληροφορικής και των δικτύων αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας. Ωστόσο, η αυτοματοποίηση ολοένα και περισσότερων διαδικασιών απαιτεί μέγιστη προσοχή και αξιοπιστία, αφού ο όγκος ανταλλαγής δεδομένων είναι μεγάλος, γεγονός που καθιστά τα υπολογιστικά συστήματα πόλο έλξης σε επιθέσεις κατά της ασφάλειάς τους. Εξαιτίας αυτού, στην πάροδο του χρόνου αναπτύχθηκαν και υλοποιήθηκαν ΣΑΠΕ, που βοήθησαν στην διατήρηση της ασφάλειας τέτοιων συστημάτων. Ο κλάδος που φάνηκε πως διαδραμάτισε σημαντικό ρόλο στην εξέλιξη τους ήταν αυτός της μηχανικής μάθησης και των αλγορίθμων της.

Στα πλαίσια της παρούσας διπλωματικής εργασίας αναπτύχθηκε ένα ΣΑΠΕ στο διαδίκτυο των πραγμάτων με τεχνικές βαθιάς μάθησης. Τα δεδομένα που καταγράφηκαν και συνέθεσαν την βάση δεδομένων για την υλοποίηση του συστήματος, υπέστησαν επεξεργασία με την χρήση του λογισμικού CICFlowMeter, αλλά και του NFStream, προγραμμάτων ανάλυσης δικτυακής ροής. Στην συνέχεια επισημάνθηκαν τα δεδομένα σε επιθέσεις και μη, ενώ ταυτόχρονα υπέστησαν επεξεργασία μέσω της Python προκειμένου να αφαιρεθούν οι περιττές πληροφορίες και να κανονικοποιηθούν σε κλίμακα από 0 έως 1.

Οι αλγόριθμοι μηχανικής μάθησης που χρησιμοποιήθηκαν για την υλοποίηση του προτεινόμενου συστήματος τόσο με την βοήθεια του CICFlowMeter όσο και με του NFStream ήταν κατά σειρά οι Adaboost, decision tree, k-nearest neighbor, LDA, Logistic Regression, MLP, Naïve Bayes, Random Forest, SGD και SVM.

Όσον αφορά το CICFlowMeter, καλύτερα αποτελέσματα παρουσίασαν οι αλγόριθμοι DNN με τέσσερα κρυφά στρώματα, τα Decision Trees και ο Random Forest. Πιο συγκεκριμένα ο DNN, παρουσίασε ακρίβεια 99,8% και F1-score 99%. Τα δένδρα αποφάσεων, είχαν ακρίβεια 99,7% ενώ παράλληλα το F1-score άγγιξε το 99%. Τέλος ο αλγόριθμος Random Forest παρουσίασε ακρίβεια και F1-score στα 99,4%. Από τους confusion matrixes, φαίνεται πως τα νούμερα στην διαγώνιο του πίνακα είναι αρκετά μεγάλα. Εξαιτίας αυτού, το ποσοστό των σωστών προβλέψεων είναι πολύ μεγάλο, ενώ οι λανθασμένες ταξινομήσεις ελάχιστες. Αντίθετα, λιγότερο υποσχόμενα αποτελέσματα παρουσίασε ο αλγόριθμος Naïve Bayes με ακρίβεια 81.2%. Από τον πίνακα σύγχυσης, φαίνεται πως ο παραπάνω αλγόριθμος πραγματοποιεί μεγάλο ποσοστό λανθασμένων ταξινομήσεων στην περίπτωση όπου τα δεδομένα ανήκαν στις κλάσεις 0 και 1, δηλαδή σε δεδομένα Normal και Flood αντίστοιχα. Στην πρώτη περίπτωση, προβλέπει ως επίθεση τύπου RTSP -Brute Force, 513 δικτυακές ροές που ανήκαν στην πραγματικότητα στην κατηγορία 0. Παράλληλα, κατηγοριοποιεί 1396 δικτυακές ροές στην κλάση 2, ενώ ανήκαν στην κατηγορία επιθέσεων τύπου Flood. Γενικά όλοι οι αλγόριθμοι που εφαρμόστηκαν είχαν υποσχόμενα αποτελέσματα, ωστόσο οι παραπάνω τρεις ξεχώρισαν.

Παράλληλα η ίδια βάση δεδομένων που χρησιμοποιήθηκε για την υλοποίηση του συστήματος με την βοήθεια του CICFlowMeter, αξιοποιήθηκε και από το NFStream. Καλύτερα αποτελέσματα παρουσίασαν ο DNN , ο k-NN και ο Random Forest. Ειδικότερα, ο DNN παρουσίασε ακρίβεια και F1-score 99,9%, ο k-NN 99,7%, ενώ ο Random Forest 99,8%. Ωστόσο, υπήρξαν και αλγόριθμοι που δεν ήταν ιδιαίτερα αποτελεσματικοί με έναν από αυτούς να αποτελεί ο αλγόριθμος SVM με kernel sigmoid. Ο παραπάνω παρουσίασε ακρίβεια 80% με μεγάλο ποσοστό λανθασμένων ταξινομήσεων ειδικά στις περιπτώσεις 0 και 1. Από τον πίνακα σύγχυσης φαίνεται πως ο αλγόριθμος πραγματοποίησε ταξινομήσεις δεδομένων στην κατηγορία 0, ενώ αυτά ανήκαν στην κατηγορία 1 και 2 αντίστοιχα. Τόσο στο NFStream όσο και στο CICFlowMeter οι παράγοντες του TPR και FPR ήταν υψηλοί και χαμηλοί αντίστοιχα.

Τα αποτελέσματα των παραπάνω αλγορίθμων συνθέτουν ένα σύστημα ΣΑΠΕ, ικανό να ανιχνεύσει έγκαιρα και ορθά πιθανές εισβολές και να διατηρήσει την ακεραιότητα του εκάστοτε υπολογιστικού συστήματος.

7.2 Μελλοντικές επεκτάσεις

Πιθανή επέκταση της υλοποίησης του συστήματος στην παρούσα διπλωματική, θα μπορούσε να αποτελέσει η βελτίωση της ακρίβειας και του βαθμού ανίχνευσης εισβολών με την χρήση διαφορετικών αλγορίθμων μηχανικής μάθησης. Ακόμα, θα ήταν εφικτό να αλλάξει η αρχιτεκτονική των ΤΝΔ με την κατάλληλη αύξηση των κρυφών στρωμάτων, προκειμένου να επιτευχθεί μεγαλύτερη απόδοση.

Παράρτημα Α

Πίνακας 27: Συγκεντρωτικός πίνακας με τα χαρακτηριστικά του CICFlowMeter

Features	**Meaning**
Flow ID	Το ID της εκάστοτε δικτυακής ροής
Src IP	Περιέχει την διεύθυνση IP του σταθμού εργασίας από τον οποίον προήλθε
Src Port	Είναι ο αριθμός TCP ή UDP που χρησιμοποιείται από ένα πρόγραμμα για την αποστολή δεδομένων σε άλλο πρόγραμμα στη μία άκρη
Dst IP	Περιέχει τη διεύθυνση IP του σταθμού εργασίας στον οποίο απευθύνεται.
Dst Port	Είναι ο αριθμός TCP ή UDP που χρησιμοποιείται από ένα πρόγραμμα στη μία πλευρά της επικοινωνίας για τη λήψη δεδομένων από ένα άλλο πρόγραμμα στην άλλη άκρη.
Protocol	Είναι ένα σύνολο καθιερωμένων κανόνων που υπαγορεύουν τον τρόπο διαμόρφωσης, μετάδοσης και λήψης δεδομένων έτσι ώστε οι συσκευές δικτύου υπολογιστών να μπορούν να επικοινωνούν, ανεξάρτητα από τις διαφορές στις υποκείμενες υποδομές, σχέδια ή πρότυπα.
Timestamp	Τρέχουσα ώρα ενός συμβάντος που καταγράφει ένας υπολογιστής
Flow Duration	Διάρκεια δικτυακής ροής σε ms
Total Fwd Packet	Σύνολο πακέτων προς την κατεύθυνση προς τα εμπρός
Total Bwd Packets	Σύνολο πακέτων προς την κατεύθυνση προς τα πίσω
total Length of Fwd Packet	Συνολικό μέγεθος πακέτου προς τα εμπρός
total Length of Bwd Packet	Συνολικό μέγεθος πακέτου προς τα πίσω
Fwd Packet Length Min	Ελάχιστο μέγεθος πακέτου προς τα εμπρός
Fwd Packet Length Max	Μέγιστο μέγεθος πακέτου προς τα εμπρός
Fwd Packet Length Mean	Μέσο μέγεθος πακέτου προς τα εμπρός
Fwd Packet Length Std	Τυπικό μέγεθος απόκλισης πακέτου προς τα εμπρός
Bwd Packet Length Min	Ελάχιστο μέγεθος πακέτου προς τα πίσω
Bwd Packet Length Max	Μέγιστο μέγεθος πακέτου προς τα πίσω
Bwd Packet Length Mean	Μέσο μέγεθος πακέτου προς τα πίσω
Bwd Packet Length Std	Τυπικό μέγεθος απόκλισης πακέτου προς τα πίσω
Flow Bytes/s	Αριθμός bytes ροής ανά δευτερόλεπτο
Flow Packets/s	Αριθμός πακέτων ροής ανά δευτερόλεπτο
Flow IAT Mean	Μέσος χρόνος μεταξύ δύο πακέτων που αποστέλλονται στη ροή
Flow IAT Std	Τυπικός χρόνος απόκλισης μεταξύ δύο πακέτων που αποστέλλονται στην ροή
Flow IAT Max	Μέγιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται στην ροή
Flow IAT Min	Ελάχιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται στην ροή
Fwd IAT Min	Ελάχιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα εμπρός
Fwd IAT Max	Μέγιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα εμπρός
Fwd IAT Mean	Μέσος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα εμπρός
Fwd IAT Std	Χρόνος τυπικής απόκλισης μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα εμπρός
Fwd IAT Total	Συνολικός χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα εμπρός
Bwd IAT Min	Ελάχιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα πίσω
Bwd IAT Max	Μέγιστος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα πίσω
Bwd IAT Mean	Μέσος χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα πίσω

Bwd IAT Std	Χρόνος τυπικής απόκλισης μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα πίσω
Bwd IAT Total	Συνολικός χρόνος μεταξύ δύο πακέτων που αποστέλλονται προς την κατεύθυνση προς τα πίσω
Fwd PSH Flags	Ο αριθμός των φορών που τέθηκε η σημαία PSH σε πακέτα που ταξιδεύουν προς την κατεύθυνση προς τα εμπρός (0 για το UDP)
Bwd PSH Flags	Ο αριθμός των φορών που τέθηκε η σημαία PSH σε πακέτα που ταξιδεύουν προς την κατεύθυνση προς τα πίσω (0 για το UDP)
Fwd URG Flags	Ο αριθμός των φορών που τέθηκε η σημαία URG σε πακέτα που ταξιδεύουν προς την κατεύθυνση προς τα εμπρός (0 για το UDP)
Bwd URG Flags	Ο αριθμός των φορών που τέθηκε η σημαία URG σε πακέτα που ταξιδεύουν προς την κατεύθυνση προς τα πίσω (0 για το UDP)
Fwd Header Length	Συνολικά BYTE που χρησιμοποιούνται για κεφαλίδες προς τα εμπρός
Bwd Header Length	Συνολικά BYTE που χρησιμοποιούνται για κεφαλίδες προς τα πίσω
FWD Packets/s	Αριθμός προωθημένων πακέτων ανά δευτερόλεπτο
Bwd Packets/s	Αριθμός προς τα πίσω πακέτων ανά δευτερόλεπτο
Packet Length Min	Ελάχιστο μήκος πακέτου
Packet Length Max	Μέγιστο μήκος πακέτου
Packet Length Mean	Μέσο μήκος πακέτου
Packet Length Std	Τυπικό μήκος απόκλισης ενός πακέτου
Packet Length Variance	Μήκος διακύμανσης πακέτου
FIN Flag Count	Αριθμός πακέτων με FYN
SYN Flag Count	Αριθμός πακέτων με SYN
RST Flag Count	Αριθμός πακέτων με RST
PSH Flag Count	Αριθμός πακέτων με PSH
ACK Flag Count	Αριθμός πακέτων με ACK
URG Flag Count	Αριθμός πακέτων με URG
CWR Flag Count	Αριθμός πακέτων με CWR
ECE Flag Count	Αριθμός πακέτων με ECE
Down/UP Ratio	Αναλογία λήψης και αποστολής
Average Packet Size	Μέσο μέγεθος πακέτου
Fwd Segment Size Avg	Μέσο μέγεθος που παρατηρείται προς τα εμπρός
Bwd Segment Size Avg	Μέσο μέγεθος που παρατηρείται προς τα πίσω
Fwd Bytes/Bulk Avg	Μέσος αριθμός byte διόγκωσης προς την κατεύθυνση προς τα εμπρός
Fwd Packets/Bulk Avg	Μέσος αριθμός πακέτων διόγκωσης προς την κατεύθυνση προς τα εμπρός
Fwd Bulk Rate Avg	Μέσος αριθμός ποσοστού προς την κατεύθυνση προς τα εμπρός
Bwd Bytes/Bulk Avg	Μέσος αριθμός byte διόγκωσης προς την κατεύθυνση προς τα πίσω
Bwd Packets/Bulk Avg	Μέσος αριθμός πακέτων διόγκωσης προς την κατεύθυνση προς τα πίσω
Bwd Bulk Rate Avg	Μέσος αριθμός ποσοστού προς την κατεύθυνση προς τα πίσω
Subflow Fwd Packets	Ο μέσος αριθμός πακέτων σε μια δευτερεύουσα ροή προς την κατεύθυνση προς τα εμπρός
Subflow Fwd Bytes	Ο μέσος αριθμός bytes σε μια δευτερεύουσα ροή προς την κατεύθυνση προς τα εμπρός
Subflow Bwd Packets	Ο μέσος αριθμός πακέτων σε μια δευτερεύουσα ροή προς την κατεύθυνση προς τα πίσω
Subflow Bwd Bytes	Ο μέσος αριθμός bytes σε μια δευτερεύουσα ροή προς την κατεύθυνση προς τα πίσω

Fwd Init Win bytes	Ο συνολικός αριθμός των byte που στάλθηκαν στο αρχικό παράθυρο προς την κατεύθυνση προς τα εμπρός
Bwd Init Win bytes	Ο συνολικός αριθμός των byte που στάλθηκαν στο αρχικό παράθυρο προς την κατεύθυνση προς τα πίσω
Fwd Act Data Pkts	Πλήθος πακέτων με τουλάχιστον 1 byte ωφέλιμου φορτίου δεδομένων TCP προς την κατεύθυνση προς τα εμπρός
Fwd Seg Size Min	Ελάχιστο μέγεθος τμήματος που παρατηρείται προς τα εμπρός
Active Min	Ελάχιστος χρόνος ενεργοποίησης μιας ροής πριν από την αδράνεια
Active Mean	Μέσος όρος όπου, μια ροή ήταν ενεργή πριν γίνει αδρανής
Active Max	Μέγιστος χρόνος ενεργοποίησης μιας ροής πριν από την αδράνεια
Active Std	Χρόνος τυπικής απόκλισης μιας ροής ενέργειας πριν γίνει αδρανής
Idle Min	Ελάχιστος χρόνος αδράνειας μιας ροής πριν γίνει ενεργή
Idle Mean	Μέσος όρος όπου , μια ροή ήταν αδρανής πριν γίνει ενεργή
Idle Max	Μέγιστος χρόνος αδράνειας μιας ροής πριν γίνει ενεργή
Idle Std	Χρόνος τυπικής απόκλισης μια ροή ήταν αδρανής πριν γίνει ενεργή

*Πίνακας 28:*Συγκεντρωτικός πίνακας χαρακτηριστικών NFStream

Features	**Meaning**
Id	Αναγνωριστικό ροής
Expiration id	Αναγνωριστικό τύπου λήξης ροής (π.χ. 0 για ανενεργό, 1 για ενεργό)
Src_ip	Αναπαράσταση συμβολοσειράς διεύθυνσης IP πηγής ροής
Src_mac	Αναπαράσταση συμβολοσειράς διεύθυνσης MAC πηγής ροής
Src_oui	Πηγή αναπαράστασης ροής συμβολοσειρών με μοναδικό αναγνωριστικό
Src_port	Θύρα πηγής στρώματος μεταφοράς ροής
Dst_ip	Αναπαράσταση συμβολοσειράς διεύθυνσης IP πηγής προορισμού
Dst_mac	Αναπαράσταση συμβολοσειράς διεύθυνσης MAC πηγής προορισμού
Dst_oui	Προορισμός αναπαράστασης ροή συμβολοσειρών με μοναδικό αναγνωριστικό
Dst_port	Θύρα προορισμού στρώματος μεταφοράς ροής
Protocol	Αναγνωριστικό πρωτοκόλλου επιπέδου μεταφοράς ροής
ip_version	Έκδοση ροής ip
vlan_id	Αναγνωριστικό εικονικού LAN ροής
First_seen_ms(src2dst, dst2src)	Χρονική σήμανση σε χιλιοστά του δευτερολέπτου στο πρώτο πακέτο ροής
Last_seen_ms(src2dst, dst2src)	Χρονική σήμανση σε χιλιοστά του δευτερολέπτου στο τελευταίο πακέτο ροής
Duration_ms(src2dst, dst2src)	Χρονική διάρκεια ροής σε ms
packets(src2dst, dst2src)	Συσσωρευτής πακέτων ροής
bytes(src2dst, dst2src)	Συσσωρευτής bytes ροής
Tunnel_id	Αναγνωριστικό σήραγγας
Application_name	Όνομα εφαρμογής Ndpi
Application_category_name	Όνομα κατηγορίας εφαρμογής Ndpi
Application_is_guessed	Υποδεικνύει εάν η ανίχνευση βασίζεται σε καθαρή ανατομή ή σε εικασία με βάση την θύρα.
Requested_server_name	Ζητούμενο όνομα διακομιστή (SSL/TLS, DNS, HTTP)
Client_fingerprint	Δακτυλικό αποτύπωμα πελάτη (δακτυλικό αποτύπωμα DHCP για DHCP, JA3 για SSL/TLS, και HASSH για SSH)
Server_fingerprint	Δακτυλικό αποτύπωμα διακομιστή (JA3 για SSL/TLS και HASSH για SSH)
User_agent	Εξαγόμενος παράγοντας χρήστη για HTTP ή Αναγνωριστικό παράγοντα χρήστη για QUIC
Content_type	Εξαγόμενος τύπος περιεχομένου HTTP
udps.packet_with_40_ip_size	Αμφίδρομα πακέτα με ακριβές μέγεθος IP ίσο με 40 μετρητή ανά ροή.

Βιβλιογραφία-Αναφορές

[1] «Intrusion Detection,» p. 37.

[2] A. Hunt, «Intrusion Detection System and Practises,» σε *Firewalls*.

[3] J. Firch, «SIEM VS IDS: What's The Difference?,» 2022.

[4] E. Conrad, «Introduction To Intrusion and Detection Systems,» 2017.

[5] K. B. G. Mohammed Jamal Almansor, «Intrusion Detection Systems: Principles And Perspectives,» 2018.

[6] S. M. Jaydip Sen, «Machine Learning Applications in Misuse and Anomaly Detection,» σε *Security and Privacy From a Legal, Ethical, and Technical Perspective*, 2020.

[7] O. P. Binod Kumar Pattanayak, «Security in vehicular ad hoc network based on intrusion detection system,» 2014.

[8] E. T. Mihret, «Intrusion Detection System - IDS - Journal - by Sci-Tech with Estif,» 2021.

[9] L. S. Qingbo Yin, «Intrusion detection based on hidden Markov model,» 2003.

[10] C. Sanders, «Chapter 1 - The Practice of Applied Network Security Monitoring,» 2014.

[11] N. Einwechter, «An Introduction To Distributed Intrusion Detection Systems,» 2001\.

[12] P. M. Eda Kavlakoglu, «AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?,» 2020.

[13] Π. Κ. Ν. Β. Φ. Κ. Η. Σ. Ι. Βλαχάβας, «Τεχνητή Νοημοσύνη - Β΄Έκδοση».

[14] Π. Κ. Ν. Β. Φ. Κ. Η. Σ. Ι. Βλαχάβας, «Τεχνητά Νευωνικά Δίκτυα,» σε *Τεχνητή Νοημοσύνη -Β Έκδοση*.

[15] Α. Χρηστος, «Τεχνητά νευρωνικά δίκτυα: το μέλλον της υπολογιστικής επιστήμης [part 1],» *Techmaniac*, 2016.

[16] C. Bento, «Multilayer Perceptron Explained with a Real-Life Example and Python Code: Sentiment Analysis,» 2021.

[17] P. V. C. S. A. J. G. T. S. R. Vinicius Jonathan Silva Araujo, «Using Resistin, Glucose, Age and BMI and Pruning Fuzzy Neural Network for the Construction of Expert Systems in the Prediction of Breast Cancer,» 2019.

[18] C. Bento, «Decision Tree Classifier explained in real-life: picking a vacation destination,» 2021.

[19] K. Kiran, «Decision Tree Model for Classification -Terminologies , Steps , Advantages.,» 2022.

[20] O. Harisson, «Machine Learning Basics with the K-Nearest Neighbors Algorithm,» 2018.

[21] S. Parameswaran, «KNN Classifier from scratch,» 2022.

[22] T. Yiu, «Understanding Random Forest,» 2019.

[23] Pratishtha, «Random Forest Classification,» 2020.

[24] «GeeksforGeeks,» 2022. [Ηλεκτρονικό].

[25] B. Alam, «Implementing Naive Bayes Classification using Python,» 2022.

[26] R. Gandhi, «Support Vector Machine — Introduction to Machine Learning Algorithms,» 2018.

[27] A. Navlani, «Support Vector Machines with Scikit-learn Tutorial,» 2019.

[28] A. Raj, «Perfect Recipe for Classification Using Logistic Regression,» 2020.

[29] «Logistic Regression in Machine Learning,» JavaTpoint. [Ηλεκτρονικό].

[30] A. Saini, «AdaBoost Algorithm – A Complete Guide for Beginners,» 2021.

[31] A. Desarda, «Understanding AdaBoost,» *Data Science,* 2019.

[32] M. Lopes, «Is LDA a dimensionality reduction technique or a classifier algorithm?,» 2017.

[33] N. Tyagi, «Introduction to Linear Discriminant Analysis in Supervised Learning,» *Analytic Steps,* 2019.

[34] «Scikit Learn - Stochastic Gradient Descent».

[35] M. Fuchs, «Introduction to SGD Classifier,» 2019.

[36] Y. S. ,. G. H. ,. J. J. R. Chunhe Song, «Intrusion detection based on hybrid classifiers for smart grid,» 2022.

[37] N. K. C. H. A. Tala Talaei Khoei, «Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid,» 2021.

[38] S. M. S. H. ,. A. U. ,. A. O. ,. M. M. R. ,. M. Taha Selim Ustun, «Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC61850 GOOSE Messages,» 2021.

[39] D. J. S. H. C.-C. L. Chih-Che Sun, «Intrusion Detection for Cybersecurity of Smart Meters,» 2020.

[40] S. L. B. C. L. Y. Jiayu Shi, «Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids,» 2020.

[41] K. N. J. T. J. P. M. Muhammad Azmi Umer, «Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations,» 2022.

[42] S. L. Jie Gua, «An effective intrusion detection approach using SVM with naıve Bayes feature embedding».*2020.*

[43] A. A. ,. D. M. Giuseppina Andresini, «Autoencoder-based deep metric learning for network intrusion detection,» 2021.

[44] L. P. M. C. Giovanni Apruzzese, «The Cross-evaluation of Machine Learning-based Network Intrusion Detection Systems,» 2022.

[45] Y. D. Z. C. ,. Q. L. W. X. Yanfang Fu, « A Deep Learning Model for Network Intrusion Detection with Imbalanced Data,» 2022.

[46] A. A. Z. R. K. A. M. R. I. Sk. Tanzir Mehedi, «Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach,» 2022.

[47] S. W. Raisa Abedin Disha, «Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique,» 2022.

[48] K. R. P. S. ,. A. ,. L. A. S. S. G. W. Panagiotis Radoglou-Grammatikis, «Modelling, Detecting and Mitigating Threats Against Industrial Healthcare Systems: A combined SDN and Reinforcement Learning Approach,» 2021.

[49] P. S. G. E. L. G. F. A. S. Panagiotis Radoglou-Grammatikis, «A Self-Learning Approach for Detecting Intrusions in Healthcare Systems,» 2021.

[50] D. M. LINXI ZHANG, «A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks,» 2022.

[51] S. T. M. ,. J. S. T. ,. K. M. M. ,. M. M. A. ,. M. A. A. ,. A. S. a. S. S. M. Jabed Al Faysal, «XGB-RF: A Hybrid Machine Learning Approach for IoT Intrusion Detection,» 2022.

[52] P. R.-G. G. E. P. F. P. S. Ilias Siniosoglou, «A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments,» 2021.

[53] K. S. P. G. S. N. ,. B. André Kummerow, «Combined Network Intrusion and Phasor Data Anomaly Detection for Secure Dynamic Control Centers,» 2022.

[54] Q. Q. Y. G. J. Z. S. C. J. L. a. N. G. Daojing He, «Intrusion Detection Based on Stacked Autoencoder for Connected Healthcare Systems,» 2019.

[55] Z. s. D. M. K. A. S. A. V. N. D. T. Khalafi, «Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks,» 2022.

[56] M. G. Vivek Kumar Singh, «Cyber Kill-Chain basedHybrid Intrusion Detection System for Smart Grid,» 2022.

[57] M. A. K. S. L. ,. M. A. ,. A. A. S. ,. J. A. Adeel Abbas, «A New Ensemble-Based Intrusion Detection System for Internet ofThings,» 2021.

[58] M. S. K. G. H. ADEDAYO ARIBISALA, «FEED-FORWARD INTRUSION DETECTION AND CLASSIFICATION ON A SMART GRID NETWORK,» 2022.

[59] R. S. R. K. Azka Wani, «SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL),» 2020.

[60] C. L. ,. Y. S. ,. Y. Q. ,. C. C. Bo Cao, «Network Intrusion Detection Model Based on CNN and GRU,» 2022.

[61] S. A. R. Z. D. M. L. M. M. G. Tuan A Tang, «Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks,» 2018.

[62] X.-D. N. ,. H.-H. H. ,. K.-H. L. Xuan-Ha Nguyen, «Realguard: A Lightweight Network Intrusion Detection System for IoT Gatewaysω,» 2022.

[63] M. A. Khan, «HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System,» 2021.

[64] A. H. Lashkari, «Github,» [Ηλεκτρονικό]. Available: https://github.com/ahlashkari/CICFlowMeter/blob/master/ReadMe.txt.

[65] A. P. Zied Aouini, «NFStream: A flexible network data analysis framework,» 2022.

[66] J. Browniee, «Machine Learning Mastery,» 2020.

[67] S. Narkhede, «Understanding Confusion Matrix,» *Towards Data Science,* 2018.

[68] S. K. Agrawai, «Metrics to Evaluate your Classification Model to take the right decisions,» *Analytics Vidhya,* 2021.

[69] UNB, «UNIVERSITY OF NEW BRUNSWICK,» [Ηλεκτρονικό]. Available: https://www.unb.ca/cic/datasets/iotdataset-2022.html.

Συντομογραφίες - Αρκτικόλεξα - Ακρωνύμια

πχ	παραδείγματος χάρη
κ.λπ.	και λοιπά
κ.ο.κ	και ούτω καθεξής
λ.χ.	λόγου χάρη
ΤΝΔ	Τεχνητό Νευρωνικό Δίκτυο
ML	Machine Learning
NN	Neural Network
SVM	Support Vector Machine
AMI	Advanced Metering Infrastructure
FDI	False Data Injection
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
DIDS	Distributed Intrusion Detection System
DLNIDS	Deep Learning NIDS
RF	Random Forest
SDN	Software Defined Networking
PCAP	Packet Capture
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Diagram Protocol
HTTP	Hypertext Transfer Protocol Secure
AL	Active Learning
ICS	Industrial Control System
MITM	Man In The Middle
SCADA	Supervision Control And Data Acquisition
GRU	Gated Recurrent Unit
ΣΑΕ	Σύστημα Ανίχνευσης Εισβολών
ΣΑΠΕ	Σύστημα Ανίχνευσης και Πρόληψης Εισβολών

Απόδοση Ξενόγλωσσων Όρων

Βάση Δεδομένων	Database
Σύνολο Εκπαίδευσης	Training Set
Σύνολο Δοκιμών	Test Set
Επισημασμένα Δεδομένα	Labeled Data
Μη επισημασμένα Δεδομένα	Un-Labeled Data